echo

To customize the default behavior of echo packets, use the **echo** command in MPLS OAM configuration mode. To set the echo packet's behavior to its default value, use the **no** form of this command.

echo {**revision** {**3** | **4**} | **vendor-extension**}

no echo {**revision** {**3** | **4**} | **vendor-extension**}

Syntax Description

revision	Specifies the revision number of the echo packet's default values. Valid values are: • **3**—draft-ietf-mpls-lsp-ping-03 (Revision 2) • **4**—RFC 4379 compliant (default)
vendor-extension	Sends Cisco-specific extension of type, length, values (TLVs) with echo packets.

Command Default

Cisco-specific extension TLVs are sent with the echo packet. Revision 4 is the router's default.

Command Modes

MPLS OAM configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
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.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Before you can enter the **echo** command, you must first enter the **mpls oam** command to enter MPLS OAM configuration mode.

Specify the **revision** keyword only if one of the following conditions exists:

- You want to change the revision number from the default of revision **4** to revision **3**.
- You previously entered the **mpls oam** command and changed the revision number to **3** and now you want to change the revision back to **4**.

To prevent failures reported by the replying router due to TLV version issues, you can use the **echo revision** command to configure all routers in the core for the same version of the Internet Engineering Task Force (IEFT) label switched paths (LSP) ping draft. For example, if the network is running draft RFC 4379 implementations, but one router is capable of only Version 3 (Cisco Revision 3), configure all

routers in the network to operate in Revision 3 mode. Revision 3 mode is used only with Multiprotocol Label Switching (MPLS) LSP ping or traceroute. Revision 3 mode does not support MPLS multipath LSP traceroute.

The **vendor-extension** keyword is enabled by default in the router. If your network includes routers that are not Cisco routers, you may want to disable Cisco extended TLVs. To disable Cisco extended TLVs, specify the **no echo vendor-extension** command in MPLS OAM configuration mode. To enable Cisco extended TLVs again, respecify the **echo** command with the **vendor-extension** keyword.

Examples

The following example uses Revision 3 of the echo packets and sends the vendor's extension TLV with the echo packet:

```
mpls oam
 echo revision 3
 echo vendor-extension
 exit
```

Related Commands

Command	Description
mpls oam	Enters MPLS OAM configuration mode for customizing the default behavior of echo packets.

encapsulation (Any Transport over MPLS)

To configure the ATM adaptation layer (AAL) encapsulation for an Any Transport over MPLS (AToM), use the **encapsulation** command in the appropriate configuration mode. To remove the ATM encapsulation, use the **no** form of this command.

encapsulation *layer-type*

no encapsulation *layer-type*

Syntax Description

layer-type	The adaptation layer type, which is one of the following: • **aal5**—ATM adaptation layer 5 • **aal0**—ATM adaptation layer 0

Command Default

The default encapsulation is AAL5.

Command Modes

L2transport VC configuration—for ATM PVCs
VC class configuration—for 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 ATM encapsulations 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(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.

Usage Guidelines

In L2transport VC configuration mode, the **pvc** command and the **encapsulation** command work together. Use the commands for AToM differently than for all other applications. Table 1 shows the differences in how the commands are used.

Table 1 AToM-Specific Variations of the pvc and encapsulation Commands

Other Applications	AToM
`Router(config-if)# pvc 1/100` `Router(config-if-atm-vc)# encapsulation aal5snap`	`Router(config-if)# pvc 1/100 l2transport` `Router(config-if-atm-l2trans-pvc)# encapsulation aal5`

The following list highlights the differences:

- **pvc** command: For most applications, you create a permanent virtual circuit (PVC) by using the **pvc** *vpi/vci* command. For AToM, you must add the **l2transport** keyword to the **pvc** command. The **l2transport** keyword enables the PVC to transport Layer 2 packets.
- **encapsulation** command: The **encapsulation** command for AToM has only two keyword values: **aal5** or **aal0**. You cannot specify an encapsulation type, such as aal5snap. In contrast, the **encapsulation aal5** command you use for most other applications requires you to specify the encapsulation type, such as **aal5snap**.
- You cannot create switched virtual circuits or VC bundles to transport Layer 2 packets.

When you use the **aal5** keyword, incoming cells (except Operation, Administration, and Maintenance [OAM] cells) on that PVC are treated as AAL5 encapsulated packets. The router reassembles the packet from the incoming cells. The router does not check the contents of the packet, so it does not need to know the encapsulation type (such as aal5snap and aal5mux). After imposing the Multiprotocol Label Switching (MPLS) label stack, the router sends the reassembled packet over the MPLS core network.

When you use the **aal0** keyword, the router strips the header error control (HEC) byte from the cell header and adds the MPLS label stack. The router sends the cell over the MPLS core network.

Examples

The following example shows how to configure a PVC to transport ATM cell relay packets for AToM:

```
Router> enable
Router# configure terminal
Router(config)# interface atm1/0
Router(config-if)# pvc 1/100 l2transport
Router(config-if-atm-l2trans-pvc)# encapsulation aal0
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

The following example shows how to configure ATM AAL5 over MPLS in VC class configuration mode. The VC class is applied to a PVC.

```
Router> enable
Router# configure terminal
Router(config)# vc-class atm aal5class
Router(config-vc-class)# encapsulation aal5
Router(config)# interface atm1/0
Router(config-if)# pvc 1/200 l2transport
Router(config-if-atm-l2trans-pvc)# class-vc aal5class
Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls
```

Related Commands

Command	Description
pvc	Creates or assigns a name to an ATM PVC.

encapsulation (Layer 2 local switching)

To configure the ATM adaptation layer (AAL) for a Layer 2 local switching ATM permanent virtual circuit (PVC), use the **encapsulation** command in ATM PVC L2transport configuration mode. To remove an encapsulation from a PVC, use the **no** form of this command.

encapsulation *layer-type*

no encapsulation *layer-type*

Syntax Description

layer-type	Adaptation layer type. The values are: • **aal5** • **aal0** • **aal5snap** • **aal5mux** • **aal5nlpid** (not available on Cisco 12000 series)

Command Default

If you do not create a PVC, one is created for you. The default encapsulation types for autoprovisioned PVCs are as follows:

- For ATM-to-ATM local switching, the default encapsulation type for the PVC is AAL0.
- For ATM-to-Ethernet or ATM-to-Frame Relay local switching, the default encapsulation type for the PVC is AAL5SNAP.

Command Modes

ATM PVC L2transport configuration

Command History

Release	Modification
12.0(27)S	This command was introduced for Layer 2 local switching.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
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.

Usage Guidelines

The **pvc** command and the **encapsulation** command work together. The use of these commands with Layer 2 local switching is slightly different from the use of these commands with other applications. The following list highlights the differences:

- For Layer 2 local switching, you must add the **l2transport** keyword to the **pvc** command. The **l2transport** keyword enables the PVC to transport Layer 2 packets.
- The Layer 2 local switching **encapsulation** command works only with the **pvc** command. You cannot create switched virtual circuits or VC bundles to transport Layer 2 packets. You can use only PVCs to transport Layer 2 packets.

Table 2 shows the encapsulation types supported for each transport type:

Table 2 Supported Encapsulation Types

Interworking Type	Encapsulation Type
ATM to ATM	AAL0, AAL5
ATM to Ethernet with IP interworking	AAL5SNAP, AAL5MUX
ATM to Ethernet with Ethernet interworking	AAL5SNAP
ATM to Frame-Relay	AAL5SNAP, AAL5NLPID

Examples

The following example shows how to configure a PVC to transport AAL0 packets for Layer 2 local switching:

```
pvc 1/100 l2transport
 encapsulation aal0
```

Related Commands

Command	Description
pvc	Creates or assigns a name to an ATM PVC.

encapsulation dot1q

To enable IEEE 802.1Q encapsulation of traffic on a specified subinterface in a virtual LAN (VLAN), use the **encapsulation dot1q** command in interface range configuration mode or subinterface configuration mode. To disable IEEE 802.1Q encapsulation, use the **no** form of this command.

Interface Range Configuration Mode

encapsulation dot1q *vlan-id* [**native**]

no encapsulation dot1q

Subinterface Configuration Mode

encapsulation dot1q *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id*-*vlan-id*[**,***vlan-id*-*vlan-id*]}

no encapsulation dot1q *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id*-*vlan-id*[**,***vlan-id*-*vlan-id*]}

Syntax Description

vlan-id	Virtual LAN identifier. The allowed range is from 1 to 4094. For the IEEE 802.1Q-in-Q VLAN Tag Termination feature, the first instance of this argument defines the outer VLAN ID, and the second and subsequent instances define the inner VLAN ID.
native	(Optional) Sets the VLAN ID value of the port to the value specified by the *vlan-id* argument. **Note** This keyword is not supported by the IEEE 802.1Q-in-Q VLAN Tag Termination feature.
second-dot1q	Supports the IEEE 802.1Q-in-Q VLAN Tag Termination feature by allowing an inner VLAN ID to be configured.
any	Sets the inner VLAN ID value to a number that is not configured on any other subinterface. **Note** The **any** keyword in the **second-dot1q** command is not supported on a subinterface configured for IP over Q-in-Q (IPoQ-in-Q) because IP routing is not supported on ambiguous subinterfaces.
-	Hyphen must be entered to separate inner and outer VLAN ID values that are used to define a range of VLAN IDs.
,	(Optional) Comma must be entered to separate each VLAN ID range from the next range.

Defaults

IEEE 802.1Q encapsulation is disabled.

Command Modes

Interface range configuration
Subinterface configuration

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.1(3)T	The **native** keyword was added.
12.2(2)DD	Configuration of this command in interface range mode was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.3(7)T	The **second-dot1q** keyword was added to support the IEEE 802.1Q-in-Q VLAN Tag Termination feature.
12.3(7)XI1	This command was integrated into Cisco IOS Release 12.3(7)XI and implemented on the Cisco 10000 series routers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

Interface Range Configuration Mode

IEEE 802.1Q encapsulation is configurable on Fast Ethernet interfaces. IEEE 802.1Q is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies.

Use the **encapsulation dot1q** command in interface range configuration mode to apply a VLAN ID to each subinterface within the range specified by the **interface range** command. The VLAN ID specified by the *vlan-id* argument is applied to the first subinterface in the range. Each subsequent interface is assigned a VLAN ID, which is the specified *vlan-id* plus the subinterface number minus the first subinterface number (VLAN ID + subinterface number – first subinterface number).

Note The Cisco 10000 series router does not support the **interface range** command nor the interface range configuration mode.

Do not configure encapsulation on the native VLAN of an IEEE 802.1Q trunk without using the **native** keyword. (Always use the **native** keyword when *vlan-id* is the ID of the IEEE 802.1Q native VLAN.)

Subinterface Configuration Mode

Use the **second-dot1q** keyword to configure the IEEE 802.1Q-in-Q VLAN Tag Termination feature. 802.1Q in 802.1Q (Q-in-Q) VLAN tag termination adds another layer of 802.1Q tag (called “metro tag” or “PE-VLAN”) to the 802.1Q tagged packets that enter the network. Double tagging expands the VLAN space, allowing service providers to offer certain services such as Internet access on specific VLANs for some customers and other types of services on other VLANs for other customers.

After a subinterface is defined, use the **encapsulation dot1q** command to add outer and inner VLAN ID tags to allow one VLAN to support multiple VLANs. You can assign a specific inner VLAN ID to the subinterface; that subinterface is unambiguous. Or you can assign a range or ranges of inner VLAN IDs to the subinterface; that subinterface is ambiguous.

Examples

The following example shows how to create the subinterfaces within the range 0.11 and 0.60 and apply VLAN ID 101 to the Fast Ethernet0/0.11 subinterface, VLAN ID 102 to Fast Ethernet0/0.12 (*vlan-id* = 101 + 12 – 11 = 102), and so on up to VLAN ID 150 to Fast Ethernet0/0.60 (*vlan-id* = 101 + 60 – 11 = 150):

```
Router(config)# interface range fastethernet0/0.11 - fastethernet0/0.60
Router(config-int-range)# encapsulation dot1q 101
```

The following example shows how to terminate a Q-in-Q frame on an unambiguous subinterface with an outer VLAN ID of 100 and an inner VLAN ID of 200:

```
Router(config)# interface gigabitethernet1/0/0.1
Router(config-subif)# encapsulation dot1q 100 second-dot1q 200
```

The following example shows how to terminate a Q-in-Q frame on an ambiguous subinterface with an outer VLAN ID of 100 and an inner VLAN ID in the range from 100 to 199 or from 201 to 600:

```
Router(config)# interface gigabitethernet1/0/0.1
Router(config-subif)# encapsulation dot1q 100 second-dot1q 100-199,201-600
```

Related Commands

Command	Description
encapsulation isl	Enables the ISL, which is a Cisco proprietary protocol for interconnecting multiple switches and maintaining VLAN information as traffic goes between switches.
encapsulation sde	Enables IEEE 802.10 encapsulation of traffic on a specified subinterface in VLANs.
interface range	Specifies multiple subinterfaces on which subsequent commands are executed at the same time.
show vlans dot1q	Displays information about 802.1Q VLAN subinterfaces.

encapsulation (pseudowire)

To specify an encapsulation type for tunneling Layer 2 traffic over a pseudowire, use the **encapsulation** command in pseudowire class configuration mode.

encapsulation {**mpls** | **udp**}

Syntax Description

mpls	Specifies that Multiprotocol Label Switching (MPLS) is used as the data encapsulation method.
udp	Specifies that User Datagram Protocol (UDP) is used as the data encapsulation method.

Command Default

Encapsulation type for tunneling Layer 2 traffic is not configured.

Command Modes

Pseudowire class configuration (config-pw-class)

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(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
15.1(2)S	This command was modified. The **udp** keyword was added.

Usage Guidelines

To change the data encapsulation method for tunneling Layer 2 traffic over a pseudowire, use the **no pseudowire-class** command in global configuration mode to delete the pseudowire. Then use the **pseudowire-class** command to reestablish the pseudowire. Then change the encapsulation method using the **encapsulation mpls** command.

You cannot use the **no encapsulation mpls** command to remove a pseudowire. Nor can you change the **encapsulation mpls** command's setting using the **encapsulation l2tpv3** command. Those methods result in the following error message:

```
Encapsulation changes are not allowed on an existing pw-class.
```

You must configure the **ip local interface** command on the same pseudowire class to define the local IP address. Any existing TTL and TOS setting values configured by the **ip ttl** and **ip tos** (L2TP) commands are allowed in the pseudowire class.

Examples

The following example shows how to configure MPLS as the data encapsulation method for the pseudowire class ether-pw:

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

The following example shows how to configure UDP as the data encapsulation method for the pseudowire class ether-pw:

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

Related Commands

Command	Description
encapsulation l2tpv3	Configures L2TPv3 as the data encapsulation method over IP networks.
ip ttl	Configures the TTL byte in the IP headers of Layer 2 tunneled packets.
ip tos (L2TP)	Configures the ToS byte in the header of Layer 2 tunneled packets.
pseudowire-class	Specifies the name of a pseudowire class and enters pseudowire class configuration mode.
xconnect	Binds an attachment circuit to an L2TPv3 pseudowire for xconnect service and enters xconnect configuration mode.

exclude-address

To exclude an address from an IP explicit path, use the **exclude-address** command in global configuration mode after entering explicit path configuration mode via the **ip-explicit path** command. To remove an address exclusion from an IP explicit path, use the **no index** command.

exclude-address *A.B.C.D*

no index *number*

Syntax Description

A.B.C.D	Excludes an address from subsequent partial path segments. You can enter the IP address of a link or the router ID of a node.
number	Removes the specified address exclusion from an IP explicit path.

Defaults

Addresses are not excluded from an IP explicit path unless explicitly excluded by the **exclude-address** command.

Command Modes

Global configuration mode

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(4)T2	This command was implemented on the Cisco 7500 series.
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(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path. If you enter the **exclude-address** command and specify the IP address of a link, the constraint-based Shortest Path First (SPF) routine does not consider that link when it sets up Multiprotocol Label Switching (MPLS) traffic engineering paths. If the excluded address is a flooded MPLS traffic engineering router ID, the constraint-based SPF routine does not consider that entire node. The person performing the configuration must know the router IDs of the routers because it will not be apparent whether the specified number is for a link or for a node.

Note MPLS traffic engineering will accept an IP explicit path that comprises either all excluded addresses configured by the **exclude-address** command or all included addresses configured by the **next-address** command, but not a combination of both.

Examples

The following example shows how to exclude IP addresses 10.0.0.125 and 10.0.0.135 from IP explicit path 500:

```
Router(config-ip-expl-path)# exclude-address 10.0.0.125
Explicit Path identifier 500:
       1: exclude-address 10.0.0.125
Router(config-ip-expl-path)# exclude-address 10.0.0.135
Explicit Path identifier 500:
       1: exclude-address 10.0.0.125
       2: exclude-address 10.0.0.135
Router(config-ip-expl-path)# end
```

To remove IP address 10.0.0.135 from the excluded addresses for explicit path 500, use the following commands:

```
Router(config)# ip explicit-path identifier 500
Router(cfg-ip-expl-path)# no index 1
Explicit Path identifier 500:
    2: exclude-address 10.0.0.135
Router(cfg-ip-expl-path)# end
```

Related Commands

Command	Description
ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies a specified path.

exit (LSP Attributes)

To exit from the label switched path (LSP) attribute list, use the **exit** command in LSP Attributes configuration mode.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

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 after you have configured LSP-related attributes for a traffic engineering (TE) tunnel to exit the LSP attribute list and the LSP Attributes configuration mode.

Examples

The following example shows how to set up an LSP attribute list and exit the LSP Attributes configuration mode when the list is complete:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# priority 7 7
Router(config-lsp-attr)# affinity 0 0
Router(config-lsp-attr)# exit
```

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.

exit-address-family

To exit from address family configuration mode, use the **exit-address-family** command in address family configuration mode.

exit-address-family

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Address family configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(22)S	Enhanced Interior Gateway Routing Protocol (EIGRP) support was added in 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(15)T	EIGRP support was added in Cisco IOS Release 12.2(15)T.
12.2(18)S	EIGRP support was added.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is used to exit address family configuration mode.

This command can be abbreviated to **exit**.

Examples

In the following example, the router is configured to exit address family configuration mode:

```
Router(config-router-af)# exit-address-family
```

Related Commands

Command	Description
address-family ipv4	Enters IPv4 address family configuration mode.
address-family ipv6	Enters IPv6 address family configuration mode.
address-family nsap	Enters CLNS address family configuration mode.
address-family vpnv4	Enters VPNv4 address family configuration mode.

exp

To configure Multiprotocol Label Switching (MPLS) experimental (EXP) levels for a Frame Relay permanent virtual circuit (PVC) bundle member, use the **exp** command in Frame Relay VC-bundle-member configuration mode. To remove the EXP level configuration from the PVC, use the **no** form of this command.

exp {*level* | **other**}

no exp

Syntax Description

level	The MPLS EXP level or levels for this Frame Relay PVC bundle member. The range is from 0 to 7. A PVC bundle member can be configured with a single level, multiple individual levels, a range of levels, multiple ranges of levels, or a combination of individual levels and level ranges. Levels can be specified in ascending or descending order (although a subsequent **show running-config** command will display them in ascending order). Examples are as follows: • 0 • 0,2,3 • 6-5 • 0-2,4-5 • 0,1,2-4,7
other	Specifies that this Frame Relay PVC bundle member will handle all of the remaining MPLS EXP levels that are not explicitly configured on any other bundle member PVCs.

Defaults

EXP levels are not configured.

Command Modes

Frame Relay VC-bundle-member configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(16)BX	This command was integrated into Cisco IOS Release 12.2(16)BX.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

Assignment of MPLS EXP levels to Frame Relay PVC bundle members lets you create differentiated services, because you can distribute the levels over the various PVC bundle members. You can map a single level or a range of levels to each discrete PVC in the bundle, which enables PVCs in the bundle to carry packets marked with different levels.

Use the **exp other** command to indicate that a PVC can carry traffic marked with EXP levels not specifically configured for other PVCs. Only one PVC in the bundle can be configured using the **exp other** command.

All EXP levels must be accounted for in the PVC bundle configuration, or the bundle will not come up. However, a PVC can be a bundle member but have no EXP level associated with it. As long as all valid EXP levels are handled by other PVCs in the bundle, the bundle can come up, but the PVC that has no EXP level configured will not participate in it.

The **exp** command is available only when MPLS is configured on the interface with the **mpls ip** command.

You can overwrite the EXP level configuration on a PVC by reentering the **exp** command with a new value.

The MPLS experimental bits are a bit-by-bit copy of the IP precedence bits. When Frame Relay PVC bundles are configured for IP precedence and MPLS is enabled, the **precedence** command is replaced by the **exp** command. When MPLS is disabled, the **exp** command is replaced by the **precedence** command.

Examples

The following example shows the configuration of four Frame Relay PVC bundle members in PVC bundle bundle1 configured with MPLS EXP level support:

```
interface serial 0.1 point-to-point
 encapsulation frame-relay
 ip address 10.1.1.1
 mpls ip
 frame-relay vc-bundle bundle1
 pvc 100 ny-control
 class control
 exp 7
 protect vc
 pvc 101 ny-premium
 class premium
 exp 6-5
 protect group
 no bump traffic
 bump explicit 7
 pvc 102 my-priority
 class priority
 exp 4-2
 protect group
 pvc 103 ny-basic
 class basic
 exp other
 protect group
```

Related Commands

Command	Description
bump	Configures the bumping rules for a specific PVC member of a bundle.
class	Associates a map class with a specified DLCI.

Command	Description
dscp (Frame Relay VC-bundle-member)	Configures the DSCP value or values for a Frame Relay PVC bundle member.
match	Specifies which bits of the IP header to use for mapping packet service levels to Frame Relay PVC bundle members.
mpls ip	Enables label switching of IPv4 packets on an interface.
precedence (Frame Relay VC-bundle-member)	Configures the precedence levels for a Frame Relay PVC bundle member.
protect	Configures a Frame Relay PVC bundle member with protected group or protected PVC status.

export map

To associate an export map with a VPN Routing and Forwarding (VRF) instance, use the **export map** command in IP VRF configuration mode.

export map *route-map*

no export map *route-map*

Syntax Description

route-map	Specifies the route map to be used as an export map.

Command Default

No export maps are associated with a VRF instance.

Command Modes

IP VRF configuration

Command History

Release	Modification
12.0(5)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

The **export map** command is used to associate a route map with the specified VRF. The export map is used to filter routes that are eligible for export out of a VRF, based on the route target extended community attributes of the route. Only one export route map can be configured for a VRF.

An export route map can be used when an application requires finer control over the routes that are exported out of a VRF than the control that is provided by import and export extended communities configured for the importing and exporting VRFs.

Examples

In the following example, an export is configured under the VRF and an access list and route map are configured to specify which prefixes are exported:

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 1:1
Router(config-vrf)# export map BLUE
Router(config-vrf)# route-target import 2:1
Router(config-vrf)# exit
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)# route-map BLUE permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# set extcommunity rt 2:1
Router(config-route-map)# end
```

Related Commands

Command	Description
import map	Configures an import route map for a VRF.
ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
ip vrf	Configures a VRF routing table.
route-target	Creates a route-target extended community for a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

extended-port

Note Effective with Cisco IOS Release 12.4(20)T, the **extended-port** command is not available in Cisco IOS software.

To associate the currently selected extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interface with a particular external interface on the remotely controlled ATM switch, use the **extended-port** command in interface configuration mode.

extended-port *ctrl-if* {**bpx** *bpx-port-number* | **descriptor** *vsi-descriptor* | **vsi** *vsi-port-number*}

Syntax Description

ctrl-if	Identifies the ATM interface used to control the remote ATM switch. You must configure Virtual Switch Interface (VSI) on this interface using the **label-control-protocol** interface configuration command.
bpx *bpx-port-number*	Specifies the associated Cisco BPX interface using the native BPX syntax. *slot.port* [.*virtual port*] You can use this form of the command only when the controlled switch is a Cisco BPX switch.
descriptor *vsi-descriptor*	Specifies the associated port by its VSI physical descriptor. The *vsi-descriptor* string must match the corresponding VSI physical descriptor.
vsi *vsi-port-number*	Specifies the associated port by its VSI port number. The *vsi-port-number* string must match the corresponding VSI physical port number.

Defaults

Extended MPLS ATM interfaces are not associated.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.4(20)T	This command was removed.

Usage Guidelines

The **extended-port** interface configuration command associates an XTagATM interface with a particular external interface on the remotely controlled ATM switch. The three alternate forms of the command permit the external interface on the controlled ATM switch to be specified in three different ways.

Examples

The following example shows how to associate an extended MPLS ATM interface and bind it to BPX port 2.3:

```
ATM(config)# interface XTagATM23
ATM(config-if)# extended-port atm0/0 bpx 2.3
```

The following example shows how to associate an extended MPLS ATM interface and bind it to port 2.4:

```
ATM(config)# interface XTagATM24
ATM(config-if)# extended-port atm0/0 descriptor 0.2.4.0
```

The following example shows how to associate an extended MPLS ATM interface and binds it to port 1622:

```
ATM(config)# interface XTagATM1622
ATM(config-if)# extended-port atm0/0 vsi 0x00010614
```

Related Commands

Command	Description
interface XTagATM	Enters interface configuration mode for an extended MPLS ATM (XTagATM) interface.
show controller vsi status	Displays a summary of each VSI-controlled interface.

flow-label enable

To enable the imposition and disposition of flow labels for a pseudowire for virtual private LAN services (VPLS), use the **flow-label enable** command in pseudowire-class configuration mode. To disable the imposition and disposition of flow labels, use the **no** form of this command.

flow-label enable

no flow-label enable

Syntax Description

This command has no arguments or keywords.

Command Default

Flow labels are not enabled.

Command Modes

pseudowire-class (config-pw-class)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.

Usage Guidelines

This command enables flow labels. MPLS adds flow labels to the label stack because they contain the flow information of a VC.

Examples

The following example configures a pseudowire and enables flow labels:

```
Router(config)# pseudowire-class try
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# flow-label enable
```

Related Commands

Command	Description
load-balance flow	Enables load balancing of traffic across multiple core interfaces using equal cost multipaths (ECMP) for virtual private LAN services (VPLS).

forward permit l2protocol

To define the VPLS pseudowire that is used to transport bridge protocol data unit (BPDU) information between two network provider edge (N-PE) routers, use the **forward permit l2protocol** command in Layer 2 VFI configuration mode. To remove the pseudowire, use the **no** form of this command.

forward permit l2protocol all

no forward permit l2protocol all

Syntax Description

all	Enables the transport of BPDU information between the two N-PE routers.

Command Default

The VPLS pseudowire between the two N-PE routers is not created.

Command Modes

Layer 2 VFI configuration (config-vfi)#

Command History

Release	Modification
12.2(33)SRC	This command was introduced as part of the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature.
12.2(50)SY	This command was integrated into Cisco IOS Release 12.2(50)SY.

Usage Guidelines

Only one pseudowire between the two N-PE routers is allowed.

Examples

The following example creates a VPLS pseudowire between the two N-PE routers:

```
l2 vfi lab2 manual
vpn id 20
forward permit l2protocol all
neigbor 10.10.10.10 encapsulation mpls
```

Related Commands

Command	Description
show vfi	Displays information related to the VFI.

import map

To configure an import route map for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **import map** command in VRF configuration submode.

import map *route-map*

Syntax Description

route-map	Specifies the route map to be used as an import route map for the VRF.

Defaults

A VRF has no import route map unless one is configured using the **import map** command.

Command Modes

VRF configuration submode

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.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)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(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

Use an import route map when an application requires finer control over the routes imported into a VRF than provided by the import and export extended communities configured for the importing and exporting VRF.

The **import map** command associates a route map with the specified VRF. You can use a route map to filter routes that are eligible for import into a VRF, based on the route target extended community attributes of the route. The route map might deny access to selected routes from a community that is on the import list.

The **import map** command does not replace the need for a route-target import in the VRF configuration. You use the **import map** command to further filter prefixes that match a route-target import statement in that VRF.

Examples

The following example shows how to configure an import route map for a VRF:

```
Router(config)# ip vrf vrf1
Router(config-vrf)# import map importmap1
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
route-target	Creates a route-target extended community for a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

index

To insert or modify a path entry at a specific index, use the **index** command in IP explicit path configuration mode. To remove the path entry at the specified index, use the **no** form of this command.

index *index command*

no index *index*

Syntax Description

index	Index number at which the path entry will be inserted or modified. Valid values are from 0 to 65534.
command	An IP explicit path configuration command that creates or modifies a path entry. (You can use only the **next-address** command.)

Defaults

This command is disabled.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 insert the next address at index 6:

```
Router(cfg-ip-expl-path)# index 6 next-address 10.3.29.3

Explicit Path identifier 6:
    6: next-address 10.3.29.3
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number. Commands might be renumbered as a result.
interface fastethernet	Enters the command mode for IP explicit paths and creates or modifies the specified path.
list	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

inter-as-hybrid

To specify a VRF as an Option AB VRF, use the **inter-as-hybrid** command. Routes imported to this VRF can be advertised to Option AB peers and VPNv4 iBGP peers. When routes are received from Option AB peers and imported into the VRF, the next-hop tableid of the route is set to the tableid of the VRF.

inter-as-hybrid [**csc**] [**next-hop** *ip-address*]

no inter-as-hybrid [**csc**] [**next-hop** *ip-address*]

Syntax Description

csc	(Optional) If the **csc** keyword is used, then a per-prefix label is allocated for imported routes. For routes received from Option AB peers that are imported into the VRF, the learned outlabel is installed in forwarding.
next-hop	(Optional) Specifies the next-hop IP address to be set on paths that are imported into the VRF and that are received from an Option AB peer. The next-hop context is also set to the VRF, which imports these paths. If the **next-hop** keyword is not used, the received next-hop is retained but the next-hop context (for paths received from Option AB peers) is still set to that of the VRF.
ip-address	Specifies the IP address of the Inter-AS AB neighbor.

Defaults

No VRF is specified as an Option AB VRF.

Command Modes

VRF address family configuration (config-vrf-af)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
15.0(1)M	This command was modified. It was integrated into the release.

Usage Guidelines

The following usage guidelines apply to the **csc** keyword:

- If the **csc** keyword is not used, a per-VRF label is allocated for imported routes.
- When routes are received from Option AB peers and are imported next into the VRF, the learned out label can only be installed in forwarding when the **csc** keyword is used.
- For routes received from Option AB peers that are imported into the VRF, the learned outlabel is installed in forwarding.

Examples

The following example specifies a VRF as an Option AB VRF:

```
Router(config-vrf-af)# inter-as-hybrid
```

Related Commands

Command	Description
address-family ipv4	Enters VRF address family configuration mode to specify an address family for a VRF.
bgp neighbor inter-as-hybrid	Configures the eBGP peer router (ASBR) as an Inter-AS Option AB peer.
rd	Creates routing and forwarding tables for a VPN.
route-target	Creates a route-target extended community for a VRF.
vrf definition	Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode.

interface auto-template

To create the template interface, use the **interface auto-template** command in global configuration mode. To delete this interface, use the **no** form of this command.

interface auto-template *interface-num*

no interface auto-template

Syntax Description

interface-num	Interface number. Valid values are from 1 to 25.

Command Default

No default behavior or values are required to create templates.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.0(27)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

The space before the *interface-num* argument is optional.

Use the **shutdown** command to disable mesh tunnel interface creation when creating a template.

Examples

The following example shows how to create template interface 1:

```
Router(config)# interface auto-template 1
```

Related Commands

Command	Description
clear mpls traffic-eng auto-tunnel mesh	Removes all the mesh tunnel interfaces and re-creates them.
mpls traffic-eng auto-tunnel mesh	Enables autotunnel mesh groups globally.
show mpls traffic-eng auto-tunnel mesh	Displays the cloned mesh tunnel interfaces of each autotemplate interface and the current range of mesh tunnel interface numbers.

interface tunnel-tp

To create a Multiprotocol Label Switching (MPLS) transport profile (TP) tunnel and configure its parameters, use the **interface tunnel-tp** command in global configuration mode. To remove the MPLS-TP tunnel, use the **no** form of the command.

interface tunnel-tp *number*

no interface tunnel-tp *number*

Syntax Description

number	The number of the MPLS-TP tunnel.

Command Default

No MPLS-TP tunnel parameters are configured.

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

Use this command on endpoint routers to specify the parameters of the MPLS-TP tunnel.

This command also enters interface configuration mode (config-if). From that mode, you can configure the following MPLS-TP parameters:

Command	Description
bfd *bfd-template*	The Bidirectional Forwarding Detection (BFD) template for the tunnel. • If the BFD template for an MPLS-TP tunnel is updated after the tunnel is brought up, a BFD session is brought up on both the working and, if configured, the protect LSPs. • If the BFD template for a tunnel is changed, the BFD sessions for the working and protect LSPs is brought down and then brought back up with the new BFD template. • If a BFD template is not configured on an MPLS-TP tunnel, the initial LSP state will be DOWN.

Command	Description
protect-lsp	Enters protect LSP interface configuration mode (config-if-protect). From this mode, you can configure the following parameters: • Incoming label (**in-label** *num*). • Lock (**lockout)** • Number of the protect LSP (**lsp-number**). By default, the protect LSP number is 1. • Outgoing label and link numbers (**out-label** *num* **out-link** *num*) A protect LSP is a backup for a working LSP. If the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time forwarding reverts back to the working LSP. You can lock out traffic on either the working LSP or the protect LSP but not both. When traffic is locked out of the working or protect LSP, no traffic is forwarded on that LSP. The lock out of the LSP is signaled from one endpoint to the other. When one end has locked out one LSP, the other end may only lock out the same LSP. It is strongly advised to lock out the LSP from both ends, so that both sides know (locally) that the LSP is locked out in the absence of further signaling, which may be the case if connectivity of the LSP is broken due to maintenance for an extended time. In the absence of connectivity, a single-ended lock out expires at the remote end in under 15 minutes (256 * 3.5 seconds).

Command	Description
protection trigger [**ais** | **ldi** | **lkr**]	(Optional) Specifies protection triggers for Alarm Indication Signal (AIS), Link Down Indication (LDI), Lock Report (LKR) messages. These triggers should be used in rare cases. They allow you to specify which of these fault notifications can trigger a protection switch. The default is to inherit the setting of the similar commands from the global settings of the protection trigger. This command allows a tunnel to override the global settings. The default for the global settings is that protection is triggered on receipt of LDI and LKR, but not AIS. (AIS is a nonfatal indication of potential issues, which turns into LDI when it is known to be fatal.) This command is useful when other devices send AIS or LDI in unexpected ways. For example, a device from another vendor sends AIS when there are link failures and never sends AIS with the LDI flag. In that case, you can configure the **protection trigger ais** command. If a device sends LDI when there is no actual failure, but there is a possible failure, and you want BFD to detect the actual failure and cause protection switching, you can configure the **no protection trigger ldi** command. To undo these configuration settings and resume inheriting the global settings, enter the **default protection trigger** [**ais** | **ldi** | **lkr**] command.
tp bandwidth *num*	(Optional) Transmit bandwidth, in kilobytes. Range: 1 to 10000000. Default: 0. With MPLS-TP, you cannot use the **bandwidth** command in interface configuration mode. You must use the **tp bandwidth** command.
tp destination *node-id* [**tunnel-tp** *num*] [**global-id** *num*]	Destination MPLS-TP node ID. **global-id** *num:* (Optional) The global ID used for the remote end of this MPLS-TP tunnel Range: 0 to 2147483647. Default: The global ID that is configured with the **mpls tp** command. **tunnel-tp** *num:* (Optional) The tunnel-TP number of the MPLS-TP tunnel destination. If the tunnel-TP number is not specified, the number assigned to the local tunnel is used.

Command	Description
tp source *node-id* [**global-id** *num*]	(Optional) Source MPLS-TP tunnel node ID. This is the ID of the endpoint router being configured. You can specify the source ID to override the router ID configured in the global MPLS-TP configuration. **global-id** *num:* (Optional) The global ID of the local endpoint for this tunnel. Range: 0 to 2147483647. Default: The global ID that is configured with the **mpls tp** command. The **tp source** command is optional and not typically used, because the global router ID and global ID can be used to identify the tunnel source at the endpoint. All tunnels on the router generally use the same (globally specified) source information.
tp tunnel-name *name*	(Optional) Specifies the name of the MPLS-TP tunnel. The TP tunnel name is displayed in **show mpls tp tunnel** command output. This command is useful for consistently identifying the tunnel at all endpoints and midpoints.
working-lsp	Enters working LSP interface configuration mode (config-if-working). From this mode, you can configure the following parameters: • Incoming label (**in-label** *num*). • Lock (**lockout).** • Number of the working LSP (**lsp-number**). By default, the working LSP number is 0. • Outgoing label and link numbers (**out-label** *num* **out-link** *num*) A working LSP is the primary LSP. If the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time forwarding reverts back to the working LSP. The lock out of the LSP is signaled from one endpoint to the other. When one end has locked out one LSP, the other end may only lock out the same LSP. It is strongly advised to lock out the LSP from both ends, so that both sides know (locally) that the LSP is locked out in the absence of further signaling, which may be the case if connectivity of the LSP is broken due to maintenance for an extended time. In the absence of connectivity, a single-ended lock out expires at the remote end in under 15 minutes (256 * 3.5 seconds).

Examples

The following example specifies the parameters for an MPLS-TP tunnel:

```
interface Tunnel-tp1
 description "MPLS-TP tunnel # 1"
 no ip address
 no keepalive
 tp bandwidth 10000
```

```
tp destination 10.1.1.1
bfd mpls-tp-bfd-2
working-lsp
 out-label 112 out-link 1
 in-label 211
protect-lsp
 out-label 115 out-link 2
 in-label 511
```

Related Commands

Command	Description
mpls tp	Specifies global values used across the MPLS TP implementation and applies to all tunnels and midpoint LSPs.
mpls tp link	Specifies the parameters for an MPLS TP link.
mpls tp lsp	Specifies the parameters for forwarding of a MPLS-TP LSP at the tunnel midpoint.

interface virtual-ethernet

To create a virtual Ethernet interface, use the **interface virtual-ethernet** command in privileged EXEC configuration mode. To remove the virtual Ethernet interface, use the **no** form of this command.

interface virtual-ethernet *num*

no interface virtual-ethernet *num*

Syntax Description

num	Specifies a unique number assigned to the virtual Ethernet interface. Valid values are 0 to 4094.

Command Default

Virtual Ethernet interfaces are not created.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.

Usage Guidelines

This command allows several ethernet virtual circuits (EVCs) to be bundled over a single pseudowire. The pseudowire terminating at this virtual Ethernet interface acts like a virtual ethernet trunk port. This allows Layer 2 protocols to be run over the pseudowire. Similar to a physical Ethernet interface, a virtual Ethernet interface allows configuration of Ethernet flow points.

Examples

The following example creates a virtual Ethernet interface:

```
Router(config)# interface virtual-ethernet 1
```

Related Commands

Command	Description
show interface virtual-ethernet	Displays the status of virtual Ethernet interfaces.

interface xtagatm

Note Effective with Cisco IOS Release 12.4(20)T, the **interface xtagatm** command is not available in Cisco IOS software.

To create an extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interface, use the **interface xtagatm** command in global configuration mode.

interface xtagatm *interface-number*

Syntax Description

interface-number	The interface number.

Defaults

XTagATM interfaces are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(4)T	This command was updated to reflect the MPLS IETF terminology.
12.4(20)T	This command was removed.

Usage Guidelines

XTagATM interfaces are virtual interfaces that are created on reference-like tunnel interfaces. An XTagATM interface is created the first time the **interface xtagatm** command is issued for a particular interface number. These interfaces are similar to ATM interfaces, except that the former only supports LC-ATM encapsulation.

Examples

The following example shows how to create an XTagATM interface with interface number 62:

```
Router(config)# interface xtagatm62
```

Related Commands

Command	Description
extended-port	Associates the currently selected extended XTagATM interface with a remotely controlled switch.

interval (MPLS-TP)

To configure the transmit and receive intervals between Bidirectional Forwarding Detection (BFD) packets and to specify the number of consecutive BFD control packets to miss before BFD declares that a peer is unavailable, use the **interval** command in BFD configuration mode. To disable interval values, use the **no** form of this command.

interval [**microseconds**] {**both** *time* | **min-tx** *time* **min-rx** *time*} [**multiplier** *multiplier-value*]

no interval

Syntax Description

microseconds	(Optional) Specifies, in microseconds, the rate at which BFD control packets are sent to and received from BFD peers. If the **microseconds** keyword is not specified, the interval defaults to milliseconds.
both *time*	Specifies the rate at which BFD control packets are sent to BFD peers and the rate at which BFD control packets are received from BFD peers.
min-tx *time*	Specifies the rate at which BFD control packets are sent to BFD peers.
min-rx *time*	Specifies, the rate at which BFD control packets are received from BFD peers.
multiplier *multiplier-value*	(Optional) Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. Range: 3 to 50. Default: 3.

Command Default

No session parameters are set.

Command Modes

BFD configuration (config-bfd)

Command History

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

Usage Guidelines

The **interval** command allows you to configure the session parameters for a BFD template.

Examples

The following example shows how to configure interval settings for the node1 BFD template:

```
Router(config)# bfd-template single-hop node1
Router(bfd-config)# interval min-tx 120 min-rx 100 multiplier 3
```

Related Commands

Command	Description
bfd-template	Creates a BFD template and enters BFD configuration mode.

interworking

To enable the L2VPN Interworking feature, use the **interworking** command in pseudowire class configuration mode. To disable the L2VPN Interworking feature, use the **no** form of this command.

interworking {**ethernet** | **ip** | **vlan**}

no interworking {**ethernet** | **ip** | **vlan**}

Syntax Description

ethernet	Causes Ethernet frames to be extracted from the attachment circuit and sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that do not contain Ethernet frames are dropped. In the case of VLAN, the VLAN tag is removed, which leaves a pure Ethernet frame.
ip	Causes IP packets to be extracted from the attachment circuit and sent over the pseudowire. Attachment circuit frames that do not contain IPv4 packets are dropped.
vlan	Causes Ethernet frames and the VLAN tag to be sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that do not contain Ethernet frames are dropped.

Defaults

L2VPN interworking is not enabled.

Command Modes

Pseudowire class configuration (config-pw)

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
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(52)SE	This command was modified. The **vlan** keyword was added as part of the L2VPN Interworking: VLAN Enable/Disable Option feature.
12.2(33)SRE	This command was modified. The **vlan** keyword was added as part of the L2VPN Interworking: VLAN Enable/Disable Option feature.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Table 3 shows which L2VPN Interworking features support Ethernet, IP, and VLAN types of interworking.

Table 3 L2VPN Interworking Feature Support

L2VPN Interworking Feature	Interworking Support
Frame Relay to PPP	IP
Frame Relay to ATM AAL5	IP
Ethernet/VLAN to ATM AAL5	IP and Ethernet
Ethernet/VLAN to Frame Relay	IP and Ethernet
Ethernet/VLAN to PPP	IP
Ethernet to VLAN	IP, Ethernet, and VLAN
L2VPN Interworking: VLAN Enable/Disable Option for AToM	Ethernet VLAN

Examples

The following example shows a pseudowire class configuration that enables the L2VPN Interworking feature:

```
pseudowire-class ip-interworking
 encapsulation mpls
 interworking ip
```

Related Commands

Command	Description
encapsulation l2tpv3	Specifies that L2TPv3 is used as the data encapsulation method for tunneling IP traffic over the pseudowire.
encapsulation mpls	Specifies that MPLS is used as the data encapsulation method for tunneling Layer 2 traffic over the pseudowire.

ip explicit-path

To enter the command mode for IP explicit paths and create or modify the specified path, use the **ip explicit-path** command in global configuration mode. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path. To disable this feature, use the **no** form of this command.

ip explicit-path {**name** *word* | **identifier** *number*} [**enable** | **disable**]

no explicit-path {**name** *word* | **identifier** *number*}

Syntax Description

name *word*	Name of the explicit path.
identifier *number*	Number of the explicit path. Valid values are from 1 to 65535.
enable	(Optional) Enables the path.
disable	(Optional) Prevents the path from being used for routing while it is being configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 enter the explicit path command mode for IP explicit paths and creates a path numbered 500:

```
Router(config)# ip explicit-path identifier 500
Router(config-ip-expl-path)#
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number. Commands might be renumbered as a result.
index	Inserts or modifies a path entry at a specific index.
ip route vrf	Displays all or part of the explicit paths.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

ip flow-cache mpls label-positions

To enable Multiprotocol Label Switching (MPLS)-Aware NetFlow, use the **ip flow-cache mpls label-positions** command in global configuration mode. To disable MPLS-aware NetFlow, use the **no** form of this command.

ip flow-cache mpls label-positions [*label-position-1* [*label-position-2* [*label-position-3*]]] [**exp-bgp-prefix-fields**] [**no-ip-fields**] [**mpls-length**]

no ip flow-cache mpls label-positions

Syntax Description

label-position-l	(Optional) Position of an MPLS label in the incoming label stack. Label positions are counted from the top of the stack, starting with 1.
exp-bgp-prefix-fields	(Optional) Generates a MPLS Provider Edge (PE) PE-to-PE traffic matrix. The following IP-related flow fields are included: • Input interface • BGP Nexthop • MPLS Experimental (EXP) bits The MPLS label values will be set to zero on the Cisco 10000 in the display output of the **show ip cache verbose flow aggregation exp-bgp-prefix** command.
no-ip-fields	(Optional) Controls the capture and reporting of MPLS flow fields. If the **no-ip-fields** keyword is not specified, the following IP-related flow fields are included: • Source IP address • Destination IP address • Transport layer protocol • Source application port number • Destination application port number • IP type of service (ToS) • TCP flag If the **no-ip-fields** keyword is specified, the IP-related fields are reported with a value of 0.
mpls-length	(Optional) Controls the reporting of packet length. If the **mpls-length** keyword is specified, the reported length represents the sum of the MPLS packet payload length and the MPLS label stack length. If the **mpls-length** keyword is not specified, only the length of the MPLS packet payload is reported.

Defaults

MPLS-Aware NetFlow is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.0(25)S	The **no-ip-fields** and **mpls-length** keywords were.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **exp-bgp-prefix-fields** keyword was added.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Use this command to configure the MPLS-aware NetFlow feature on a label switch router (LSR) and to specify labels of interest in the incoming label stack. Label positions are counted from the top of the stack, starting with 1. The position of the top label is 1, the position of the second label is 2, and so forth.

With MPLS-aware NetFlow enabled on the router, NetFlow collects data for incoming IP packets and for incoming MPLS packets on all interfaces where NetFlow is enabled in full or in sampled mode.

Caution When you enter the **ip flow-cache mpls label-positions** command on a Cisco 12000 series Internet router, NetFlow will stop collecting data for incoming IP packets on any Engine 4P line cards installed in the router on which NetFlow is enabled in full or in sampled mode. Engine 4P line cards in a Cisco 12000 series Internet router do not support NetFlow data collection of incoming IP packets and MPLS packets concurrently.

Tip MPLS-aware NetFlow is enabled in global configuration mode. NetFlow is enabled per interface.

Examples

The following example shows how to configure MPLS-aware NetFlow to capture the first (top), third, and fifth label:

```
Router(config)# ip flow-cache mpls label-positions 1 3 5
```

The following example shows how to configure MPLS-aware NetFlow to capture only MPLS flow information (no IP-related flow fields) and the length that represents the sum of the MPLS packet payload length and the MPLS label stack length:

```
Router(config)# ip flow-cache mpls label-positions no-ip-fields mpls-length
```

The following example shows how to configure MPLS PE-to-PE Traffic Statistics for Netflow:

```
Router(config)# ip flow-cache mpls label-positions 1 2 exp-bgp-prefix-fields
```

Related Commands

Command	Description
ip flow egress	Enables NetFlow egress accounting for traffic that the router is forwarding.
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters.

Command	Description
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip multicast mpls traffic-eng

To enable IP multicast traffic on a tailend router enabled with Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) functionality, use the **ip multicast mpls traffic-eng** command in privileged EXEC mode. To disable IP multicast for MPLS TE P2MP on tailend routers, use the **no** form of this command.

ip multicast mpls traffic-eng [**range** {*access-list-number* | *access-list-name*}]

no ip multicast mpls traffic-eng [**range**]

Syntax Description

range	(Optional) Enables multicast for a specific set of multicast streams.
access-list-number	The specific number of the access list. Valid values are 100–199.
access-list-name	The specific name of the access list.

Command Default

MPLS TE P2MP functionality is not enabled.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

You configure this command on the tailend routers in an MPLS TE P2MP topology.

Examples

The following example enables multicast routing on tailend routers configured with MPLS TE P2MP functionality:

```
Router(config)# ip multicast-routing
Router(config)# ip multicast mpls traffic-eng
```

Related Commands

Command	Description
show ip mroute	Displays IP multicast forwarding on MPLS TE P2MP tailend routers.

ip path-option

To specify an explicit or dynamic path option for a particular destination address in a destination list, use the **ip path-option** command in traffic engineering destination list configuration mode. To remove the path option, use the **no** form of this command.

ip *ip-address* **path-option** *id* {**dynamic** | **explicit** {**name** *name* | **identifier** *number*} [**verbatim**]}

no ip *ip-address* **path-option** *id*

Syntax Description

ip-address	The destination address of the path.
id	The preference for this path option for the same destination address. The valid values are 1–1000. Only one path option is supported for each destination address.
dynamic	Specifies that the traffic engineering paths be dynamically computed.
explicit	Specifies that the traffic engineering paths be explicitly configured.
name *name*	Specifies the name of the explicit path.
identifier *number*	Specifies the number of the explicit path.
verbatim	(Optional) Specifies that the path should be sent out without any checking.

Command Default

Path options are not configured.

Command Modes

Traffic engineering destination list (cfg-te-dest-list)

Command History

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

Usage Guidelines

- The **ip path-option** command is supported at a sublabel switched path (sub-LSP) level.
- Point-to-multipoint traffic engineering supports only one path option per destination.

Examples

The following example shows the configuration of a destination list with explicit path options:

```
Router(config)# mpls traffic-eng destination list identifier 1
Router(cfg-te-dest-list)# ip 10.10.10.10 path-option 1 explicit identifier 1
```

Related Commands

Command	Description
mpls traffic-eng destination list	Specifies a MPLS traffic engineering point-to-multipoint destination list.

ip route static inter-vrf

To allow static routes to point to Virtual Private Network (VPN) routing and forwarding (VRF) interfaces other than those to which the static route belongs, use the **ip route static inter-vrf** command in global configuration mode. To prevent static routes from pointing to VRF interfaces in VRFs to which they do not belong, use the **no** form of this command.

ip route static inter-vrf

no ip route static inter-vrf

Syntax Description

This command has no arguments or keywords.

Defaults

Static routes are allowed to point to VRF interfaces in any VRF.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
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(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 **ip route static inter-vrf** command is turned on by default. The **no ip route static inter-vrf** command causes the respective routing table (global or VRF) to reject the installation of static routes if the outgoing interface belongs to a different VRF than the static route being configured. This prevents security problems that can occur when static routes that point to a VRF interface in a different VRF are misconfigured. You are notified when a static route is rejected, then you can reconfigure it.

For example, a static route is defined on a provider edge (PE) router to forward Internet traffic to a customer on the interface pos1/0, as follows:

```
Router(config)# ip route 10.1.1.1 255.255.255.255 pos 1/0
```

The same route is mistakenly configured with the next hop as the VRF interface pos10/0:

```
Router(config)# ip route 10.1.1.1 255.255.255.255 pos 10/0
```

By default, Cisco IOS software accepts the command and starts forwarding the traffic to both pos1/0 (Internet) and pos10/0 (VPN) interfaces.

If the static route is already configured that points to a VRF other than the one to which the route belongs when you issue the **no ip route static inter-vrf** command, the offending route is uninstalled from the routing table and a message similar to the following is sent to the console:

```
01:00:06: %IPRT-3-STATICROUTESACROSSVRF: Un-installing static route x.x.x.x/32 from global
routing table with outgoing interface intx/x
```

If you enter the **no ip route static inter-vrf** command before a static route is configured that points to a VRF interface in a different VRF, the static route is not installed in the routing table and a message is sent to the console.

Configuring the **no ip route static inter-vrf** command prevents traffic from following an unwanted path. A VRF static route points to a global interface or any other VRF interface as shown in the following **ip route vrf** commands:

- Interface serial 1/0.0 is a global interface:

```
Router(config)# no ip route static inter-vrf

Router(config)# ip route vrf vpn1 10.10.1.1 255.255.255.255 serial 1/0.0
```

- Interface serial 1/0.1 is in vpn2:

```
Router(config)# no ip route static inter-vrf

Router(config)# ip route vrf vpn1 10.10.1.1 255.255.255.255 serial 1/0.1
```

With the **no ip route static inter-vrf** command configured, these static routes are not installed into the vpn1 routing table because the static routes point to an interface that is not in the same VRF.

If you require a VRF static route to point to a global interface, you can use the **global** keyword with the **ip route vrf** command:

```
Router(config)# ip route vrf vpn1 10.12.1.1 255.255.255.255 serial 1/0.0 10.0.0.1 global
```

The **global** keyword allows the VRF static route to point to a global interface even when the **no ip route static inter-vrf** command is configured.

Examples

The following example shows how to prevent static routes that point to VRF interfaces in a different VRF:

```
Router(config)# no ip route static inter-vrf
```

Related Commands

Command	Description
ip route vrf	Establishes static routes for a VRF.

ip route vrf

To establish static routes for a Virtual private Network (VPN) routing and forwarding (VRF) instance, use the **ip route vrf** command in global configuration mode. To disable static routes, use the **no** form of this command.

ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]

no ip route vrf *vrf-name prefix mask* [*next-hop-address*] [*interface interface-number*] [**global**] [*distance*] [**permanent**] [**tag** *tag*]

Syntax Description

vrf-name	Name of the VRF for the static route.
prefix	IP route prefix for the destination, in dotted decimal format.
mask	Prefix mask for the destination, in dotted decimal format.
next-hop-address	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
interface	(Optional) Type of network interface to use.
interface-number	(Optional) Number identifying the network interface to use.
global	(Optional) Specifies that the given next hop address is in the non-VRF routing table.
distance	(Optional) An administrative distance for this route.
permanent	(Optional) Specifies that this route will not be removed, even if the interface shuts down.
tag *tag*	(Optional) Label (tag) value that can be used for controlling redistribution of routes through route maps.

Defaults

No default behavior or values.

Command Modes

Global configuration

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.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)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(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

Use a static route when the Cisco IOS software cannot dynamically build a route to the destination.

If you specify an administrative distance when you set up a route, you are flagging a static route that can be overridden by dynamic information. For example, Interior Gateway Routing Protocol (IGRP)-derived routes have a default administrative distance of 100. To set a static route to be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes each have a default administrative distance of 1.

Static routes that point to an interface are advertised through the Routing Information Protocol (RIP), IGRP, and other dynamic routing protocols, regardless of whether the routes are redistributed into those routing protocols. That is, static routes configured by specifying an interface lose their static nature when installed into the routing table.

However, if you define a static route to an interface not defined in a network command, no dynamic routing protocols advertise the route unless a **redistribute static** command is specified for these protocols.

Supported Static Route Configurations

When configuring static routes in a Multiprotocol Label Switching (MPLS) or MPLS VPN environment, some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS Releases 12.xT, 12.xM, and 12.0S. The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS Release 12.2(25)S and later releases. Use the following guidelines when configuring static routes.

Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in MPLS environment:

ip route *destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

ip route *destination-prefix mask* **interface1 next-hop1**
ip route *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the next hop can be reached through two paths:

ip route *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the destination can be reached through two next hops:

ip route *destination-prefix mask* **next-hop1**
ip route *destination-prefix mask* **next-hop2**

Use the *interface* and *next-hop* arguments when specifying static routes.

Supported Static Routes in an MPLS VPN Environment

The following **ip route vrf** commands are supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask* **interface1 next-hop1**
  ip route vrf *vrf-name destination-prefix mask* **interface2 next-hop2**

The following **ip route vrf** commands are supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the Internet Gateway.

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address* **global**
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
  (This command is supported when the next hop and interface are in the core.)

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interfaces:

ip route *destination-prefix mask* **interface1 next-hop1**
ip route *destination-prefix mask* **interface2 next-hop2**

Unsupported Static Routes in an MPLS VPN Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

ip route vrf *destination-prefix mask next-hop-address* **global**

The following **ip route** commands are not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

ip route vrf *destination-prefix mask* **next-hop1 global**
ip route vrf *destination-prefix mask* **next-hop2 global**

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

ip route vrf *vrf-name destination-prefix mask* **next-hop1**
ip route vrf *vrf-name destination-prefix mask* **next-hop2**

Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf** command is supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table on the customer equipment (CE) side. For example, the following command is supported when the destination prefix is the CE router's loopback address, as in external BGP (EBGP) multihop cases.

ip route vrf *vrf-name destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static nonrecursive routes and a specific outbound interfaces:

ip route *destination-prefix mask* **interface1 nexthop1**
ip route *destination-prefix mask* **interface2 nexthop2**

Examples

The following command shows how to reroute packets addressed to network 10.23.0.0 in VRF vpn3 to router 10.31.6.6:

```
Router(config)# ip route vrf vpn3 10.23.0.0 255.255.0.0 10.31.6.6
```

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.

ip rsvp msg-pacing

To set up message pacing (that is, to control the transmission rate for Resource Reservation Protocol (RSVP) messages), use the **ip rsvp msg-pacing** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp msg-pacing [**period** *ms* [**burst** *msgs* [**maxsize** *qsize*]]]

no rsvp msg-pacing

Syntax Description

period *ms*	(Optional) Length of the interval, in milliseconds, during which a router can send the number of RSVP messages specified in the *burst* keyword. The value can be from 1 to 1000 milliseconds.
burst *msgs*	(Optional) Maximum number of RSVP messages that a router can send to an output interface during each interval specified in the *period* keyword. The value can be from 1 to 2000.
maxsize *qsize*	(Optional) Size of per-interface output queues in the sending router. Valid values are from 1 to 2000.

Command Default

RSVP messages are not paced.
If you enter the command without the optional arguments, the transmission rate for RSVP messages is limited to 200 messages per second per outgoing interface.
The default output queue size, specified in the **maxsize** keyword, is 500.

Command Modes

Global configuration

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.

Usage Guidelines

You can use this command to prevent a burst of RSVP traffic engineering signaling messages from overflowing the input queue of a receiving router, which would cause the router to drop some messages. Dropped messages substantially delay the completion of signaling for LSPs for which messages have been dropped.

Examples

In the following example, a router can send a maximum of 150 RSVP traffic engineering signaling messages in 1 second to a neighbor, and the size of the output queue is 750:

```
Router(config)# ip rsvp msg-pacing period 1 burst 150 maxsize 750
```

Related Commands

Command	Description
clear ip rsvp msg-pacing	Clears the RSVP message pacing output from the **show ip rsvp neighbor** command.

ip rsvp signalling hello (configuration)

To enable Hello globally on the router, use the **ip rsvp signalling hello** command in global configuration mode. To disable Hello globally on the router, use the **no** form of this command.

ip rsvp signalling hello

no ip rsvp signalling hello

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
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.

Usage Guidelines

To enable Hello globally on the router, you must enter this command. You also must enable Hello on the interface.

Examples

In the following example, Hello is enabled globally on the router:

```
Router(config)# ip rsvp signalling hello
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.

ip rsvp signalling hello (interface)

To enable Hello on an interface where you need Fast Reroute protection, use the **ip rsvp signalling hello** command in interface configuration mode. To disable Hello on an interface where you need Fast Reroute protection, use the **no** form of this command

ip rsvp signalling hello

no ip rsvp signalling hello

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
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.

Usage Guidelines

You must configure Hello globally on the router and on the specific interface.

Examples

In the following example, Hello is enabled on an interface:

```
Router(config-if)# ip rsvp signalling hello
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello dscp	Sets the DSCP value that is in the IP header of the Hello messages sent out from the interface.
ip rsvp signalling hello refresh misses	Specifies how many Hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.
ip rsvp signalling hello refresh interval	Configures the Hello request interval.

ip rsvp signalling hello bfd (configuration)

To enable the Bidirectional Forwarding Detection (BFD) protocol globally on the router for Multiprotocol Label Switching (MPLS) traffic engineering (TE) link and node protection, use the **ip rsvp signalling hello bfd** command in global configuration mode. To disable BFD globally on the router, use the **no** form of this command.

ip rsvp signalling hello bfd

no ip rsvp signalling hello bfd

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is not enabled globally on the router for MPLS TE link and node protection.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

To enable the BFD protocol on the router, you must enter this command. You also must enter the **ip rsvp signalling hello bfd** command on the interface.

Examples

The following example allows you to use the BFD protocol on the router for MPLS TE link and node protection:

```
Router(config)# ip rsvp signalling hello bfd
```

Related Commands

Command	Description
ip rsvp signalling hello bfd (interface)	Enables the BFD protocol on an interface where you need MPLS TE link and node protection.
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

ip rsvp signalling hello bfd (interface)

To enable the Bidirectional Forwarding Detection (BFD) protocol on an interface for Multiprotocol Label Switching (MPLS) traffic engineering (TE) link and node protection, use the **ip rsvp signalling hello bfd** command in interface configuration mode. To disable BFD on an interface for MPLS TE link and node protection, use the **no** form of this command.

ip rsvp signalling hello bfd

no ip rsvp signalling hello bfd

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is not enabled on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(33)SRC	This command was introduced.

Usage Guidelines

You must enter the **ip rsvp signalling hello bfd** command on the router and on the specific interface.

Examples

In the following example, the BFD protocol is enabled on an interface:

```
Router(config-if)# ip rsvp signalling hello bfd
```

Related Commands

Command	Description
ip rsvp signalling hello bfd (configuration)	Enables the BFD protocol on the router for MPLS TE link and node protection.
show ip rsvp hello bfd nbr	Displays information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr detail	Displays detailed information about all MPLS TE clients that use the BFD protocol.
show ip rsvp hello bfd nbr summary	Displays summarized information about all MPLS TE clients that use the BFD protocol.

ip rsvp signalling hello dscp

To set the differentiated services code point (DSCP) value that is in the IP header of a Resource Reservation Protocol (RSVP) traffic engineering (TE) hello message sent from an interface, use the **ip rsvp signalling hello dscp** command in interface configuration mode. To set the DSCP value to its default, use the **no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **dscp** *num*

no ip rsvp signalling hello [**fast-reroute**] **dscp**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
num	DSCP value. Valid values are from 0 to 63.

Command Default

The default DSCP value is 48.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute** keyword was added.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
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.

Usage Guidelines

If a link is congested, it is recommended that you set the DSCP to a value higher than 0 to reduce the likelihood that hello messages will be dropped.

You configure the DSCP per interface, not per flow.

The DSCP applies to the RSVP hellos created on a specific interface. You can configure each interface independently for DSCP.

If you issue the **ip rsvp signalling hello dscp** command without the optional **fast-reroute** keyword, the command applies to Fast Reroute hellos. This command is provided for backward compatibility; however, we recommend that you use the **ip rsvp signalling hello fast-reroute dscp** command.

Examples

In the following example, hello messages sent from this interface have a DSCP value of 30 and Fast Reroute capability is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute dscp 30
```

In the following example, hello messages sent from this interface have a DSCP value of 30 and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello dscp 30
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables hellos on an interface where you need Fast Reroute protection.
ip rsvp signalling hello refresh interval	Sets the hello refresh interval in hello messages.
ip rsvp signalling hello reroute refresh misses	Sets the missed refresh limit in hello messages.

ip rsvp signalling hello refresh interval

To configure the Resource Reservation Protocol (RSVP) traffic engineering (TE) hello refresh interval, use the **ip rsvp signalling hello refresh interval** command in interface configuration mode. To set the refresh interval to its default value, use the **no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **refresh interval** *interval-value*

no ip rsvp signalling hello [**fast-reroute**] **refresh interval**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
interval-value	Frequency, in milliseconds (msec), at which a node sends hello messages to a neighbor. Valid values are from 10 to 30000 msec. **Note** Values below the default of 200 msec are not recommended, because they can cause RSVP Hellos to falsely detect a neighbor down event and unecessarily trigger Fast ReRoute.

Command Default

The default frequency at which a node sends hello messages to a neighbor is 200 msec.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute** keyword was added.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You can configure the hello request interval on a per-interface basis. A node periodically generates a hello message containing a Hello Request object for each neighbor whose status is being tracked. The frequency of those hello messages is determined by the hello interval.

If you issue the **ip rsvp signalling hello refresh interval** command without the optional **fast-reroute** keyword, the command applies to Fast Reroute hellos. This command is provided for backward compatibility; however, we recommend that you use the **ip rsvp signalling hello fast-reroute refresh interval** command.

Examples

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh interval 5000
```

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello refresh interval 5000
```

Related Commands

Command	Description
ip rsvp signalling hello dscp	Sets the DSCP value in hello messages.
ip rsvp signalling hello graceful-restart fresh interval	Sets the refresh interval in graceful restart hello messages.
ip rsvp signalling hello reroute refresh misses	Sets the missed refresh limit in hello messages.

ip rsvp signalling hello refresh misses

To specify how many Resource Reservation Protocol (RSVP) traffic engineering (TE) hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down, use the **ip rsvp signalling hello refresh misses** command in interface configuration mode. To return the missed refresh limit to its default value, use the **no** form of this command.

ip rsvp signalling hello [**fast-reroute**] **refresh misses** *msg-count*

no ip rsvp signalling hello [**fast-reroute**] **refresh misses**

Syntax Description

fast-reroute	(Optional) Initiates Fast Reroute capability.
msg-count	Number of sequential hello acknowledgments that a node can miss before RSVP considers the state expired and tears it down. Valid values are from 4 to 10.

Command Default

The default *number of sequential hello acknowledgments* is 4.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The optional **fast-reroute** keyword was added.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
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.

Usage Guidelines

A hello comprises a hello message, a Hello Request object, and a Hello ACK object. Each request is answered by an acknowledgment. If a link is very congested or a router has a very heavy load, set this number to a value higher than the default value to ensure that hello does not falsely declare that a neighbor is down.

If you issue the **ip rsvp signalling hello refresh misses** command without the optional **fast-reroute** keyword, the command applies to Fast Reroute hellos and Fast Reroute capability is enabled by default. This command is provided for backward compatibility; however, we recommend that you use the **ip rsvp signalling hello fast-reroute refresh misses** command.

Examples

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down and Fast Reroute is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh misses 5
```

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down and Fast Reroute is enabled by default:

```
Router(config-if)# ip rsvp signalling hello refresh misses 5
```

Related Commands

Command	Description
ip rsvp signalling hello dscp	Sets the DSCP value in hello messages.
ip rsvp signalling hello refresh interval	Sets the refresh interval in hello messages.

ip rsvp signalling hello statistics

To enable Hello statistics on the router, use the **ip rsvp signalling hello statistics** command in global configuration mode. To disable Hello statistics on the router, use the **no** form of this command.

ip rsvp signalling hello statistics

no ip rsvp signalling hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
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.

Examples

In the following example, Hello statistics are enabled on the router.

```
Router(config)# ip rsvp signalling hello statistics
```

Related Commands

Command	Description
clear ip rsvp hello instance statistics	Clears Hello statistics for an instance.
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

ip vrf

To define a VPN routing and forwarding (VRF) instance and to enter VRF configuration mode, use the **ip vrf** command in global configuration mode. To remove a VRF instance, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)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 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)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.

Usage Guidelines

The **ip vrf** *vrf-name* command creates a VRF instance named *vrf-name*. To make the VRF functional, a route distinguisher (RD) must be created using the **rd** *route-distinguisher* command in VRF configuration mode. The **rd** *route-distinguisher* command creates the routing and forwarding tables and associates the RD with the VRF instance named *vrf-name*.

The **ip vrf default** command can be used to configure a VRF instance that is a NULL value until a default VRF name can be configured. This is typically before any VRF related AAA commands are configured.

Examples

The following example shows how to import a route map to a VRF instance named VPN1:

```
ip vrf vpn1
 rd 100:2
 route-target both 100:2
 route-target import 100:1
```

Related Commands

Command	Description
ip vrf forwarding (**interface configuration**)	Associates a VRF with an interface or subinterface.
rd	Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.

ip vrf forwarding (interface configuration)

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) instance with an interface or subinterface, use the **ip vrf forwarding** command in interface configuration mode. To disassociate a VRF, use the **no** form of this command.

ip vrf forwarding *vrf-name* [**downstream** *vrf-name2*]

no ip vrf forwarding *vrf-name* [**downstream** *vrf-name2*]

Syntax Description

vrf-name	Associates the interface with the specified VRF.
downstream	(Optional) Enables Half Duplex VRF (HDVRF) functionality on the interface and associates the interface with the downstream VRF.
vrf-name2	(Optional) Associates the interface with the specified downstream VRF.

Defaults

The default for an interface is the global routing table.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(6)	The **downstream** keyword was added to support MPLS VPN Half-Duplex VRFs.
12.3(11)T	This command was modified. Support was added for interfaces and subinterfaces that are configured with X.25 encapsulation.
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 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

Use this command to associate an interface with a VRF. Executing this command on an interface removes the IP address. The IP address should be reconfigured. The **downstream** keyword is available on supported platforms with virtual interfaces. The **downstream** keyword associates the interfaces with a downstream VRF, which enables half duplex VRF functionality on the interface. Some functions operate in the upstream VRFs, and others operate in the downstream VRFs. The following functions operate in the downstream VRFs:

- PPP peer routes are installed in the downstream VRFs.

- Authentication, authorization, and accounting (AAA) per-user routes are installed in the downstream VRFs.
- A Reverse Path Forwarding (RPF) check is performed in the downstream VRFs.

Forwarding Between X.25 Interfaces and Interfaces Configured for MPLS

This command enables IP forwarding between X.25 interfaces and interfaces configured for MPLS, which lets you connect customer premises equipment (CPE) devices to a provider edge (PE) router via an X.25 network by forwarding IP traffic between the CPE devices and the MPLS network. You must configure MPLS on the PE and provider routers in the network.

This command lets you perform an X.25 aggregation function on a PE router for several CPE devices with X.25 VCs into an MPLS network. The PE router performs the aggregation function of terminating X25 VCs and also performs the mapping function (in which VCs are mapped to the appropriate MPLS VRF domains).

Distributed CEF switching, CEF switching, and fast switching are not supported (only process switching is supported). Forwarding of IPv6 traffic is not supported.

Note Configuring IP VRF forwarding on an interface or subinterface that already has an IP address causes that IP address to be deleted from the running configuration. On an X.25 interface or subinterface, it does not cause any existing **x25 map ip** or **x25 pvc ip** statements to be deleted. Configuring an **x25 map ip** or **x25 pvc ip** statement with an IP address that matches an IP address configured on the same interface (or any subinterface of the same interface) might be rejected, even when the conflicting address is in another VRF instance.

For additional references, see CCITT 1988 Recommendation X.25 *(Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit)*, RFC 1356 *(Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode)*, and RFC 1461 *(SNMP MIB extension for Multiprotocol Interconnect over X.25)*.

Examples

The following example shows how to link a VRF to ATM interface 0/0:

```
Router(config)# interface atm0/0
Router(config-if)# ip vrf forwarding vpn1
```

The following example associates the VRF named U with the virtual-template 1 interface and specifies the downstream VRF named D:

```
Router> enable
Router# configure terminal
Router(config)# interface virtual-template 1
Router(config-if)# ip vrf forwarding U downstream D
Router(config-if)# ip unnumbered Loopback1
```

Related Commands

Command	Description
ip route vrf	Establishes static routes for a VRF.
ip vrf	Configures a VRF routing table.
show ip vrf	Displays the set of defined VRF instances and associated interfaces.

ip vrf receive

To insert the IP address of an interface as a connected route entry in a Virtual Private Network (VPN) routing and forwarding instance (VRF) routing table, use the **ip vrf receive** command in interface configuration mode. To remove the connected entry from the VRF routing table, use the **no** form of this command.

ip vrf receive *vrf-name*

no ip vrf receive *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF into which you want to add the IP address of the interface.

Command Default

No IP address of an interface is inserted as connected route entry in a VRF routing table.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	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 **ip vrf receive** command supports VRF route selection for the following features:

- MPLS VPN: VRF Selection Based on Source IP Address
- MPLS VPN: VRF Selection Using Policy-Based Routing

This command is used to install a primary or secondary IP address of an interface as a connected route entry in the VRF routing table. These entries appear as “receive” entries in the Cisco Express Forwarding table. MPLS VPNs require Cisco Express Forwarding switching to make IP destination prefix-based switching decisions. This command can be used to selectively install the interface IP address in the VRF that is specified with the *vrf-name* argument. Only the local interface IP address is added to the VRF routing table. This command is used on a per-VRF basis. In other words, you must enter this command for each VRF in which you need to insert the IP address of the interface. This command does not remove the interface IP address from the global routing table.

Note This command cannot be used with the **ip vrf forward** command for the same interface.

VRF Selection Based on Source IP Address Guidelines

The **ip vrf receive** command is automatically disabled when the **no ip vrf** *vrf-name* command is entered for the local interface. An error message is displayed when the **ip vrf receive** command is disabled in this manner. Interfaces where the VRF Selection Based on Source IP Address feature is enabled can forward packets that have an IP address that corresponds to an IP address entry in the VRF table. If the VRF table does not contain a matching IP address, the packet is dropped, by default, because there is no corresponding "receive" entry in the VRF entry.

VRF Selection Using Policy Based Routing Guidelines

You must enter the **ip policy route-map** command before the **ip vrf receive** command can be enabled. The **ip vrf receive** command is automatically disabled when either the **no ip policy route-map** *map-name* or the **no ip vrf** *vrf-name* command is entered for the local interface. An error message is displayed when the **ip vrf receive** command is disabled in this manner. With the VRF Selection Using Policy-Based Routing implementation of the VRF selection feature, a route map filters the VRF routes. If a match and set operation occurs in the route map but there is no receive entry in the local VRF table, the packet is dropped.

Examples

VRF Selection Based on Source IP Address

The following example shows how to configure Ethernet interface 0/2 (172.16.1.3) and insert its IP address in VRF1 and VRF2 with the **ip vrf receive** command. You must enter the **ip vrf select source** command on the interface or subinterface to enable VRF selection on the interface or subinterface. You must also enter the **vrf selection source** command in global configuration mode to populate the VRF selection table and to configure the VRF Selection Based on Source IP Address feature. (The **vrf selection source** command is not shown in this example.)

```
Router(config)# interface Ethernet0/2
Router(config-if)# ip address 172.16.1.3 255.255.255.255
Router(config-if)# ip vrf select source
Router(config-if)# ip vrf receive VRF1
Router(config-if)# ip vrf receive VRF2
Router(config-if)# end
```

VRF Selection Using Policy-Based Routing

The following example shows how to configure Ethernet interface 0/1 (192.168.1.2) and insert its IP address in VRF1 and VRF2 with the **ip vrf receive** command. You must configure an access list and a route map to allow the VRF Section Using Policy-Based Routing feature to select a VRF. (The access list and route map configuration are not shown in this example.)

```
Router(config)# interface Ethernet0/1
Router(config-if)# ip address 192.168.1.2 255.255.255.255
Router(config-if)# ip policy route-map PBR-VRF-SELECTION
Router(config-if)# ip vrf receive VRF1
Router(config-if)# ip vrf receive VRF2
Router(config-if)# end
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip vrf	Configures a VRF routing table.
ip vrf select source	Enables VRF selection on an interface.
set vrf	Enables VRF selection and filtering under a route map.
vrf selection source	Populates a single source IP address, or range of source IP addresses, to a VRF selection table.

ip vrf select source

To enable the VRF Selection feature on a particular interface or subinterface, use the **ip vrf select source** command in interface configuration mode. To disable the VRF Selection feature on a particular interface or subinterface, use the **no** form of this command.

ip vrf select source

no ip vrf select source

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(23)S	This command was integrated into Cisco IOS Release 12.0(23)S.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)SZ	This command was integrated into Cisco IOS Release 12.2(14)SZ to support the Cisco 7304 router.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S to support the Cisco 7304 router.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S to support the Cisco 7200 and 7500 series routers.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S to support the Cisco 7200 and 7500 series routers.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	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 **ip vrf select source** and **ip vrf forwarding** commands are mutually exclusive. If the VRF Selection feature is configured on an interface, you cannot configure VRFs (using the **ip vrf forwarding** command) on the same interface.

Examples

The following example shows how to enable the VRF Selection feature on an interface:

```
Router(config-if)# ip vrf select source
```

The following example shows the message you receive after you have deleted the VRF Selection feature on an interface:

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router (config)# interface pos4/0
Router (config-if)# no ip vrf select source
Router (config-if)#
INTERFACE_VRF_SELECT unset for POS4/0, slot: 4
Router (config-if)#
```

The following example shows the message you receive after you have enabled the VRF Selection feature on an interface:

```
Router (config-if)#
Router (config-if)# ip vrf select source
Router (config-if)#
INTERFACE_VRF_SELECT set for POS4/0, slot: 4
Router (config-if)#
```

Related Commands

Command	Description
ip vrf receive	Adds all the IP addresses that are associated with an interface into a VRF table.
vrf selection source	Populates a single source IP address, or range of source IP addresses, to a VRF Selection table.

ip vrf sitemap

To configure Site of Origin (SoO) filtering on an interface, use the **ip vrf sitemap** command in interface configuration mode. To disable SoO filtering on an interface, use the **no** form of this command.

ip vrf sitemap *route-map*

no ip vrf sitemap

Syntax Description

route-map	The name of the route map that is configured with the as-number and network of the VPN site.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
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.

Usage Guidelines

The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the re-advertisement of that prefix back to the source site can be prevented. The SoO extended community attribute uniquely identifies the site from which a PE router has learned a route.

Examples

The following example configures SoO filtering on an interface:

```
Router(config)# route-map Site-of-Origin permit 10
Router(config-route-map)# set extcommunity soo 100:1
Router(config-route-map)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip vrf forwarding RED
Router(config-if)# ip vrf sitemap Site-of-Origin
Router(config-if)# ip address 10.0.0.1 255.255.255.255
Router(config-if)# end
```

Related Commands

Command	Description
ip vrf forwarding	Associates a VRF with an interface or subinterface.

l2 pseudowire routing

To enter Layer 2 pseudowire routing configuration mode, use the **l2 pseudowire routing** command in global configuration mode. To exit Layer 2 pseudowire routing configuration mode, use the **no** form of this command.

l2 pseudowire routing

no l2 pseudowire routing

Syntax Description

This command has no arguments or keywords.

Command Default

Layer 2 pseudowire routing mode is not entered.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **l2 pseudowire routing** command enters Layer 2 pseudowire routing configuration mode (config-l2_pw_rtg) from 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 VPLS 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 enables Layer 2 pseudowire routing configuration mode:

```
Router>
Router# enable
Router(config)# configure terminal
Router(config)# l2 pseudowire routing
Router(config-l2_pw_rtg)# terminating-pe tie-breaker
Router(config-l2_pw_rtg)# end
```

Related Commands

Command	Description
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.

l2 vfi point-to-point

To establish a point-to-point Layer 2 virtual forwarding interface (VFI) between two separate networks, use the **l2 vfi point-to-point** command in global configuration mode. To disable the connection, use the **no** form of this command.

l2 vfi *name* **point-to-point**

no l2 vfi *name* **point-to-point**

Syntax Description

name	Name of the connection between the two networks.

Command Default

Point-to-point Layer 2 virtual forwarding interfaces are not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(31)S	This command was introduced.
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.
15.0(1)M	This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

If you disable L2VPN Pseudowire Switching with the **no l2 vfi point-to-point** command, the virtual circuits (VCs) are deleted.

Examples

The following example establishes a point-to-point Layer 2 VFI:

```
Router(config)# l2 vfi atomvfi point-to-point
```

Related Commands

Command	Description
neighbor (**L2VPN Pseudowire Switching**)	Establishes the two routers with which to form a connection.

list

To show all or part of the explicit path or paths, use the **list** command in IP explicit path configuration mode.

list [*starting-index-number*]

Syntax Description

starting-index-number	(Optional) Index number at which the explicit path(s) will start to be displayed. Valid values are from 1 to 65535.

Defaults

Explicit paths are not shown.

Command Modes

IP explicit path configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
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 list the explicit path:

```
Router(cfg-ip-expl-path)# list

Explicit Path name path1:
    1:next-address 10.0.0.1
    2:next-address 10.0.0.2
```

The following example shows how to list the explicit path starting at index number 2:

```
Router(cfg-ip-expl-path)# list 2

Explicit Path name path1:
    2:next-address 10.0.0.2
Router(cfg-ip-expl-path)#
```

Related Commands

Command	Description
append-after	Inserts the new path entry after the specified index number. Commands might be renumbered as a result.
index	Inserts or modifies a path entry at a specific index.
ip explicit-path	Enters the command mode for IP explicit paths, and creates or modifies the specified path.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

list (LSP Attributes)

To display the contents of a label switched path (LSP) attribute list, use the **list** command in LSP Attributes configuration mode.

list

Syntax Description

This command has no arguments or keywords.

Command Default

Contents of an LSP attribute list is not displayed.

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

This command displays the contents of the LSP attribute list. You can display each of the following configurable LSP attributes using the **list** command: affinity, auto-bw, bandwidth, lockdown, priority, protection, and record-route.

Examples

The following example shows how to display the contents of an LSP attribute list identified with the string priority:

```
!
Router(config)# mpls traffic-eng lsp attributes priority
Router(config-lps-attr)# priority 0 0
Router(config-lps-attr)# list

LIST priority
 priority 0 0

Router(config-lsp-attr)#
```

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.

lockdown (LSP Attributes)

To disable reoptimization of the label switched path (LSP), use the **lockdown** command in LSP Attributes configuration mode. To reenable reoptimization, use the **no** form of this command.

lockdown

no lockdown

Syntax Description

This command has no arguments or keywords.

Command Default

Reoptimization of the LSP is enabled.

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 disabling of reoptimization of an LSP triggered by a timer, or the issuance of the **mpls traffic-eng reoptimize** command, or a configuration change that requires the resignalling of an LSP.

To associate the LSP lockdown 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 configure disabling of reoptimization in an LSP attribute list:

```
Configure terminal
!
mpls traffic-eng lsp attributes 4
 bandwidth 1000
 priority 1 1
 lockdown
 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.

load-balance flow

To enable load-balancing of traffic across multiple core interfaces using equal cost multipaths (ECMP) for virtual private LAN services (VPLS), use the **load-balance flow** command in pseudowire-class configuration mode. To disable load-balancing of VPLS traffic, use the **no** form of this command.

load-balance flow

no load-balance flow

Syntax Description

This command has no arguments or keywords.

Command Default

Load-balancing is not enabled by default.

Command Modes

pseudowire-class (config-pw-class)

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
Cisco IOS XE Release 3.4S	This command was modified. Support was added for the Cisco ASR 1000 Series Router.

Usage Guidelines

This command enables ECMP load-balancing only for the pseudowire for which it was configured.

Examples

The following example configures a pseudowire and enables flow-based load-balancing:

```
Router(config)# pseudowire-class try
Router(config-pw-class)# encapsulation mpls
Router(config-pw-class)# load-balance flow
```

Related Commands

Command	Description
flow-label enable	Enables the imposition and disposition of flow labels.

local interface

To specify the pseudowire type when configuring pseudowires in a Mutliprotocol Label Switching Transport Protocol (MPLS-TP) network, use the **local interface** command in virtual forwarding interface (VFI) neighbor configuration mode. This command enters enters VFI neighbor interface configuration mode. To disble the pseudowire type, use the **no** form of this command.

local interface *pseudowire-type*

no local interface *pseudowire-type*

Syntax Description

pseudowire-type	Psuedowire type by its number in hexadecimal format: 01 Frame Relay DLCI (Martini Mode) 02 ATM AAL5 SDU VCC transport 03 ATM transparent cell transport 04 Ethernet Tagged Mode 05 Ethernet 06 HDLC 07 PPP 08 SONET/SDH Circuit Emulation Service Over MPLS 09 ATM n-to-one VCC cell transport 0A ATM n-to-one VPC cell transport 0B IP Layer2 Transport 0C ATM one-to-one VCC Cell Mode 0D ATM one-to-one VPC Cell Mode 0E ATM AAL5 PDU VCC transport 0F Frame-Relay Port mode 10 SONET/SDH Circuit Emulation over Packet 11 Structure-agnostic E1 over Packet 12 Structure-agnostic T1 (DS1) over Packet 13 Structure-agnostic E3 over Packet 14 Structure-agnostic T3 (DS3) over Packet 15 CESoPSN basic mode 16 TDMoIP AAL1 Mode 17 CESoPSN TDM with CAS

Command Default

No pseudowire type is defined.

Command Modes VFI neighbor configuration

Command History

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

Usage Guidelines The VC types 04 and 05 are supported.

Examples The following example sets the pseudowire VC type to Ethernet and enters VFI neighbor interface configuration mode:

```
Router(config-vfi-neighbor)# local interface 5
R1(config-vfi-neighbor-interface)# tlv mtu 1 4 1500
```

logging (MPLS-TP)

To enable the display of Multiprotocol Label Switching (MPLS) transport profile (TP) events, use the **logging** command in MPLS-TP configuration mode. To disable the display of MPLS-TP events, use the **no** form of this command.

logging {**config-change** | **events**}

no logging {**config-change** | **events**}

Syntax Description

config-change	Displays events related to any configuration change to an MPLS-TP tunnel, link, or midpoint label switched path (LSP).
events	Displays events related to any interface or LSP state changes.

Command Default

Logging is not enabled.

Command Modes

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

Command History

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

Usage Guidelines

The following events are captured in the logs:

MPLS-TP Tunnel Down or MPLS-TP Tunnel Up:

```
%MPLS-TP-3-UPDOWN: Tunnel-tp<Tunnel_Num>, changed state to (Up | Down | AdminDown)
%LINK-3-UPDOWN: Interface Tunnel-tp<Tunnel_Num>, changed state to (Up | Down)
%LINK-5-CHANGED: Interface Tunnel-tp<Tunnel_Num>, changed state to administratively down
```

LSP Down or LSP Up:

```
%LSP-3-UPDOWN: (Working | Protect) LSP <LSP_ID> is (Up | Down): <Failure
Condition>:<Failure Location>
```

Where:

- *LSP_ID* is the complete LSP ID
- *Failure Condition* is AIS, LDI, LKR, CC
- *Failure Location* is an IF ID in the form: [*Global_ID*] *Node_ID*::*IF_Num*

MPLS-TP Tunnel Switchover

```
%MPLS-TP-5-REDUNDANCY: Tunnel-tp<Tunnel_Num> Switched from (Working to Protect | Protect
to Working).
```

LSP Lockout or LSP Lockout Clear

```
%MPLS-TP-5-LOCKOUT: (Working | Protect) LSP <LSP_ID> (Entering | Exiting) Lock Down State
```

MPLS-TP Tunnel End-Point Created/Deleted/Modified

```
%MPLS-TP-5-CONFIG-CHANGED: Tunnel-tp<Tunnel_Num> is (Added | Updated | Deleted)
```

MPLS-TP Mid-Point Created/Deleted/Modified

```
%LSP-5-CONFIG-CHANGED: LSP <LSP_ID> is (Added | Updated | Deleted)
```

MPLS-TP Link Created/Deleted/Modified

```
%MPLS-TP-LINK-5-CONFIG-CHANGED: Link <Link_Num>, Interface <Interface_Name>, NextHop <IP
Address|MAC Address> (Added | Updated | Deleted).
```

Static MPLS Label Range updated

```
%MPLS-LABEL-5-CHANGED: (Static | Dynamic) Min/Max Label: <Min Label>/<Max Label>
```

Examples

The following example enables the display of interface or LSP state changes:

```
Router(config-mpls-tp)# logging events
```

Related Commands

Command	Description
debug mpls tp	Enables the display of MPLS-TP error messages.