

address-family

To enter the address family submode for configuring routing protocols such as Border Gateway Protocol (BGP), Routing Information Protocol (RIP), and static routing, use the **address-family** command in address family configuration submode. To disable the address family submode for configuring routing protocols, use the **no** form of this command.

VPN-IPv4 Unicast

address-family vpnv4 [unicast]

no address-family vpnv4 [unicast]

IPv4 Unicast

address-family ipv4 [unicast]

no address-family ipv4 [unicast]

IPv4 Unicast with CE router

address-family ipv4 [unicast] vrf vrf-name

no address-family ipv4 [unicast] vrf vrf-name

Syntax Description

vpnv4	Configures sessions that carry customer Virtual Private Network (VPN)-IPv4 prefixes, each of which has been made globally unique by adding an 8-byte route distinguisher.
ipv4	Configures sessions that carry standard IPv4 address prefixes.
unicast	(Optional) Specifies unicast prefixes.
vrf vrf-name	Specifies the name of a VPN routing/forwarding instance (VRF) to associate with submode commands.

Defaults

Routing information for address family IPv4 is advertised by default when you configure a BGP session using the **neighbor remote-as** command unless you execute the **no bgp default ipv4-activate** command.

Command Modes

Address family configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Using the **address-family** command puts the router in address family configuration submode (prompt: `(config-router-af)#`). Within this submode, you can configure address-family specific parameters for routing protocols, such as BGP, that can accommodate multiple Layer 3 address families.

To leave address family configuration submode and return to router configuration mode, enter the **exit-address-family** or **exit** command.

Examples

The **address-family** command in the following example puts the router into address family configuration submode for the VPNv4 address family. Within the submode, you can configure advertisement of Network Layer Reachability Information (NLRI) for the VPNv4 address family using **neighbor activate** and other related commands:

```
router bgp 100
address-family vpnv4
```

The **address-family** command in the following example puts the router into address family configuration submode for the IPv4 address family. Use this form of the command, which specifies a VRF, only to configure routing exchanges between provider edge (PE) and customer edge (CE) devices. This **address-family** command causes subsequent commands entered in the submode to be executed in the context of VRF vrf2. Within the submode, you can use **neighbor activate** and other related commands to accomplish the following:

- Configure advertisement of IPv4 NLRI between the PE and CE routers.
- Configure translation of the IPv4 NLRI (that is, translate IPv4 into VPNv4 for NLRI received from the CE, and translate VPNv4 into IPv4 for NLRI to be sent from the PE to the CE).
- Enter the routing parameters that apply to this VRF.

The following example shows how to enter the address family submode:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 unicast vrf vrf2
```

Related Commands

Command	Description
default	Exits from address family submode.
neighbor activate	Enables the exchange of information with a neighboring router.

append-after

To insert a path entry after a specified index number, use the **append-after** command in IP explicit path configuration mode.

append-after *index command*

Syntax Description	<i>index</i>	Previous index number. Valid values are from 0 to 65534.
	<i>command</i>	An IP explicit path configuration command that creates a path entry. (Use the next-address command to specify the next IP address in the explicit path.)

Defaults No path entry is inserted after a specified index number.

Command Modes IP explicit path configuration

Command History	Release	Modification
	12.0(5)S	This command was introduced.

Examples In the following example, the **next-address** command is inserted after index 5:

```
Router(config-ip-expl-path)# append-after 5 next-address 3.3.27.3
```

Related Commands	Command	Description
	index	Inserts or modifies a path entry at a specific index.
	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.

bgp default route-target filter

To enable automatic Border Gateway Protocol (BGP) route-target community filtering, use the **bgp default route-target filter** command in router configuration mode. To disable automatic BGP route-target community filtering, use the **no** form of this command.

bgp default route-target filter

no bgp default route-target filter

Syntax Description This command has no arguments or keywords.

Defaults This command is enabled.

Command Modes Router configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines Use the **bgp default route-target filter** command to control the distribution of Virtual Private Network (VPN) routing information through the list of VPN route-target communities.

When you use the **no** form of this command, all received VPN-IPv4 routes are accepted by the configured router. Accepting VPN-IPv4 routes is the desired behavior for a router configured as an autonomous system border edge router or as a customer edge (CE) BGP border edge router.

If you configure the router for BGP route-target community filtering, all received exterior BGP (EBGP) VPN-IPv4 routes are discarded when those routes do not contain a route-target community value that matches the import list of any configured VPN routing/forwarding instances (VRFs). This is the desired behavior for a router configured as a provider edge (PE) router.



Note This command is automatically disabled if a PE router is configured as a client of a common VPN-IPv4 route reflector in the autonomous system.

Examples In the following example, BGP route-target filtering is disabled for autonomous system 120:

```
Router(config)# router bgp 120
Router(config-router)# no bgp default route-target filter
```

Related Commands	Command	Description
	show tag-switching forwarding-table	Displays the contents of the LFIB.

bgp scan-time

To configure scanning intervals of Border Gateway Protocol (BGP) routers for next hop validation or to decrease import processing time of Virtual Private Network version 4 (VPNv4) routing information, use the **bgp scan-time** command in address family or router configuration mode. To return the scanning interval of a router to its default scanning interval of 15 seconds, use the **no** form of this command.

bgp scan-time [**import**] *scanner-interval*

no bgp scan-time [**import**] *scanner-interval*

Syntax Description	import	(Optional) Configures import processing of VPNv4 unicast routing information from BGP routers into routing tables.
	<i>scanner-interval</i>	Specifies the scanning interval of BGP routing information. Valid values used for selecting the desired scanning interval are from 5 to 60 seconds. The default is 15 seconds.

Defaults The default scanning interval is 15 seconds.

Command Modes Address family configuration
Router configuration

Command History	Release	Modification
	12.0(7)T	This command was introduced.

Usage Guidelines The **import** keyword is supported in address family VPNv4 unicast mode only. Entering the **no** form of this command does not disable scanning, but removes it from the output of the **show running-config** command.

Examples In the following router configuration example, the scanning interval for next hop validation of IPv4 unicast routes for BGP routing tables is set to 20 seconds:

```
router bgp 100
no synchronization
bgp scan-time 20
```

In the following address family configuration example, the scanning interval for next hop validation of address family VPNv4 unicast routes for BGP routing tables is set to 45 seconds:

```
router bgp 150
address-family vpn4 unicast
bgp scan-time 45
```

In the following address family configuration example, the scanning interval for importing address family VPNv4 routes into IP routing tables is set to 30 seconds:

```
router bgp 150
address-family vpnv4 unicast
  bgp scan-time import 30
```

Related Commands

Command	Description
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.

class (MPLS)

To configure a defined Multiprotocol Label Switching (MPLS) class of service (CoS) map that specifies how classes map to label switched controlled virtual circuits (LVCs) when combined with a prefix map, use the **class** command in CoS map submode. To remove the defined MPLS CoS map, use the **no** form of this command.

class *class* [**available** | **standard** | **premium** | **control**]

no class *class* [**available** | **standard** | **premium** | **control**]

Syntax Description

<i>class</i>	The precedence of identified traffic to classify traffic.
available	(Optional) Means low precedence (In/Out plus lower two bits = 0,4).
standard	(Optional) Means next precedence (In/Out plus lower two bits = 1,5).
premium	(Optional) Means high precedence (In/Out plus lower two bits = 2,6).
control	(Optional) Means highest precedence pair (In/Out plus lower two bits = 3,7). These bits are reserved for control traffic.

Defaults

This command is disabled.

Command Modes

CoS map submode

Command History

Release	Modification
12.0(5)T	This command was introduced.

Examples

The following example shows how to configure a CoS map:

```
Router(config)# mpls cos-map 55
Router(config-mpls-cos-map)# class 1 premium
Router(config-mpls-cos-map)# exit
```

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.
mpls cos-map	Creates a class map that specifies how classes map to LVCs when combined with a prefix map.
mpls prefix-map	Configures a router to use a specified quality of service (QoS) map when a label definition prefix matches the specified access list.
show mpls cos-map	Displays the CoS map used to assign quantity of LVCs and associated CoS of those LVCs.

clear ip route vrf

To remove routes from the Virtual Private Network (VPN) routing/forwarding instance (VRF) routing table, use the **clear ip route vrf** command in user EXEC or privileged EXEC mode.

```
clear ip route vrf vrf-name [* | network [mask]]
```

Syntax Description

<i>vrf-name</i>	Name of the VRF for the static route.
*	Indicates all routes for a given VRF.
<i>network</i>	Destination to be removed, in dotted decimal format.
<i>mask</i>	(Optional) Mask for the specified network destination, in dotted decimal format.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use this command to clear routes from the routing table. Use the asterisk (*) to delete all routes from the forwarding table for a specified VRF, or enter the address and mask of a particular network to delete the route to that network.

Examples

The following command shows how to remove the route to the network 10.13.0.0 in the vpn1 routing table:

```
Router# clear ip route vrf vpn1 10.13.0.0
```

Related Commands

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

clear mpls ldp neighbor

To forcibly reset a label distribution protocol (LDP) session, use the **clear mpls ldp neighbor** command in privileged EXEC mode.

```
clear mpls ldp neighbor [vrf vpn-name] {nbr-address | *}
```

Syntax Description		
vrf <i>vpn-name</i>	(Optional) Specifies the VPN routing and forwarding instance (<i>vpn-name</i>) for resetting an LDP session.	
<i>nbr-address</i>	Specifies the address of the LDP neighbor whose session will be reset. The neighbor address is treated as <nbr-address>:0, which means it pertains to the LDP session for the LSR's platform-wide label space.	
*	Designates that all LDP sessions will be reset.	

Defaults No default behavior or values

Command Modes Privileged EXEC

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.
	12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Usage Guidelines The **clear mpls ldp neighbor** command terminates the specified LDP sessions. The LDP sessions should be reestablished if the LDP configuration remains unchanged.

You can clear an LDP session for an interface-specific label space of an LSR by issuing the **no mpls ip** command and then the **mpls ip** command on the interface associated with the LDP session.

Examples The following example resets an LDP session:

```
Router# clear mpls ldp neighbor 12.12.12.12
```

To verify the results of the **clear mpls ldp neighbor** command, enter the **show mpls ldp neighbor** command. Notice the value in the “Up time” field.

```
Router# show mpls ldp neighbor 12.12.12.12
```

```
Peer LDP Ident: 12.12.12.12:0; Local LDP Ident 13.13.13.13:0
TCP connection: 12.12.12.12.646 - 13.13.13.13.15093
State: Oper; Msgs sent/rcvd: 142/138; Downstream
Up time: 02:16:28
LDP discovery sources:
Serial1/0, Src IP addr: 25.0.0.2
Addresses bound to peer LDP Ident:
2.0.0.129      12.12.12.12      25.0.0.2      32.1.1.0.5
```

21.7.0.1

Then enter the following **clear mpls ldp neighbor 12.12.12.12** command. With mpls ldp logging configured, the easiest way to verify the **clear mpls ldp neighbor** command is to monitor the LDP log messages.

```
Router# clear mpls ldp neighbor 12.12.12.12
```

```
1w1d: %LDP-5-CLEAR_NBRS: Clear LDP neighbors (12.12.12.12) by console
1w1d: %LDP-5-NBRCHG: LDP Neighbor 12.12.12.12:0 is DOWN
1w1d: %LDP-5-NBRCHG: LDP Neighbor 12.12.12.12:0 is UP
```

Reenter the **show mpls ldp neighbor 12.12.12.12** command. Notice that the “Up time” value has been reset.

```
Router# show mpls ldp neighbor 12.12.12.12
```

```
Peer LDP Ident: 12.12.12.12:0; Local LDP Ident 13.13.13.13:0
TCP connection: 12.12.12.12.646 - 13.13.13.13.15095
State: Oper; Msgs sent/rcvd: 125/121; Downstream
Up time: 00:00:05
LDP discovery sources:
  Serial1/0, Src IP addr: 25.0.0.2
Addresses bound to peer LDP Ident:
  2.0.0.129      12.12.12.12      25.0.0.2      32.1.0.5
  21.7.0.1
```

The following example resets all LDP sessions:

```
Router# clear mpls ldp neighbor *
```

Related Commands

Command	Description
show mpls ldp neighbor	Displays the status of the LDP sessions.

clear mpls traffic-eng auto-bw timers

To reinitialize the automatic bandwidth adjustment feature on a platform, use the **clear mpls traffic-eng auto-bw timers** command in user EXEC or privileged EXEC mode.

clear mpls traffic-eng auto-bw timers

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC
Privileged EXEC

Command History	Release	Modification
	Release 12.2(4)T	This command was introduced.

Usage Guidelines For each tunnel for which automatic bandwidth adjustment is enabled, the platform maintains information about sampled output rates and the time remaining until the next bandwidth adjustment. The **clear mpls traffic-eng auto-bw timers** command clears this information for all such tunnels. The effect is as if automatic bandwidth adjustment had just been enabled for the tunnels.

Examples The following example shows how to clear information about sampled output rates and the time remaining until the next bandwidth adjustment:

```
Router# clear mpls traffic-eng auto-bw timers

Clear mpls traffic engineering auto-bw timers [confirm]
```

Related Commands	Command	Description
	mpls traffic-eng auto-bw timers	Enables automatic bandwidth adjustment on a platform for tunnels configured for bandwidth adjustment.
	tunnel mpls traffic-eng auto-bw	Enables automatic bandwidth adjustment for a tunnel, specifies the frequency with which tunnel bandwidth can be automatically adjusted, and designates the allowable range of bandwidth adjustments.

connect (Frame Relay)

To define connections between Frame Relay permanent virtual circuits (PVCs), use the **connect** command in global configuration mode. To remove connections, use the **no** form of this command.

connect *connection-name interface dlc* {*interface dlc* | **l2transport**}

no connect *connection-name interface dlc* {*interface dlc* | **l2transport**}

Syntax Description

<i>connection-name</i>	A name for this connection.
<i>interface</i>	Interface on which a PVC connection will be defined.
<i>dlci</i>	Data-link connection identifier (DLCI) number of the PVC that will be connected.
l2transport	Specifies that the PVC will not be a locally switched PVC, but will be tunneled over the backbone network.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.0(23)S	The l2transport keyword was added.
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.

Usage Guidelines

When Frame Relay switching is enabled, the **connect** command creates switched PVCs in Frame Relay networks.

Examples

The following example shows how to define a connection called “frompls1” with DLCI 100 on serial interface 5/0.

```
connect frompls1 Serial5/0 100 l2transport
```

The following example shows how to enable Frame Relay switching and define a connection called “one” between DLCI 16 on serial interface 0 and DLCI 100 on serial interface 1.

```
frame-relay switching
connect one serial0 16 serial1 100
```

Related Commands	Command	Description
	frame-relay switching	Enables PVC switching on a Frame Relay DCE or NNI.
	mpls l2transport route	Enables routing of Frame Relay packets over a specified VC.

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. Possible values are:

- aal5**—ATM adaptation layer 5
- aal0**—ATM adaptation layer 0

Defaults

The default encapsulation is AAL5.

Command Modes

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

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.0(30)S	This command was updated to enable ATM encapsulations as part of a VC class.

Usage Guidelines

In L2transport VC configuration mode, the **pvc** command and the **encapsulation** command work together. How you use the commands for AToM is slightly different than for all other applications. The following table shows the differences in how the commands are used:

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 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**, **aal5mux**, and so on). 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 13.13.13.13 100 encapsulation mpls
```

The following example configures ATM AAL5 over MPLS in VC class configuration mode. The VC class is then 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 13.13.13.13 100 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

<i>layer-type</i>	Adaptation layer type. Possible values are:
	aal5
	aal0
	aal5snap
	aal5mux
	aal5nlpid (not on Cisco 12000 series)

Defaults

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, 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.

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 only use PVCs to transport Layer 2 packets.

The following table shows the encapsulation types supported for each transport type:

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 12transport
 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

<i>vlan-id</i>	Virtual LAN identifier. The allowed range is from 1 to 4095. 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 <i>vlan-id</i> 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.
-	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.

Release	Modification
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.

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).

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. 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 Inter-Switch Link (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.

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.

Defaults 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	EIGRP support was added.
	12.2(15)T	EIGRP support was added.

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

Examples The following example shows how to exit address family configuration mode:

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

Related Commands	Command	Description
	address-family	Enters the address family submode for configuring routing protocols, such as BGP, RIP, and static routing.
	address-family ipv4 (BGP)	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IP Version 4 address prefixes.
	address-family ipv4 (EIGRP)	Enters address family configuration mode for EIGRP.

export map

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

export map *route-map*

Syntax Description	<i>route-map</i>	Specifies the route map to be used as an export map.
---------------------------	------------------	--

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	IP VPN Routing/Forwarding configuration mode
----------------------	--

Command History	Release	Modification
	12.0(5)T	This command was introduced.

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.

Command	Description
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

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

<i>ctrl-if</i>	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.
bp x <i>bp</i> x-port-number	Specifies the associated Cisco BPX interface using the native BPX syntax. <i>slot.port</i> [<i>.virtual port</i>] You can use this form of the command only when the controlled switch is a Cisco BPX switch.
descriptor <i>vsi-descriptor</i>	Specifies the associated port by its VSI physical descriptor. The <i>vsi-descriptor</i> string must match the corresponding VSI physical descriptor.
vsi <i>vsi-port-number</i>	Specifies the associated port by its VSI port number. The <i>vsi-port-number</i> string must match the corresponding VSI physical port number.

Defaults

Extended MPLS ATM interfaces are not associated.

Command Modes

Interface configuration

Command History

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

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.

import map

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

import map *route-map*

Syntax Description	<i>route-map</i>	Specifies the route map to be used as an import route map for the VRF.
--------------------	------------------	--

Defaults No import route map is configured for a VRF.

Command Modes VRF configuration submode

Command History	Release	Modification
	12.0(5)T	This command was introduced.

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 vrf_blue
Router(config-vrf)# import map blue_import_map
```

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	
<i>index</i>	Index number at which the path entry will be inserted or modified. Valid values are from 0 to 65534.
<i>command</i>	An IP explicit path configuration command that creates or modifies a path entry. (Currently 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.

Examples The following example shows how to insert the next address at index 6:

```
Router(cfg-ip-expl-path)# index 6 next-address 3.3.29.3
```

```
Explicit Path identifier 6:
 6: next-address 3.3.29.3
```

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.

interface xtagatm

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	<i>interface-number</i>	The interface number.
---------------------------	-------------------------	-----------------------

Defaults	XTagATM interfaces are not created.	
-----------------	-------------------------------------	--

Command Modes	Global configuration	
----------------------	----------------------	--

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.

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.

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 router 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 <i>word</i>	Name of the explicit path.
identifier <i>number</i>	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

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

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-router)# 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 route static inter-vrf

To allow static routes to point to Virtual Private Network (VPN) routing/forwarding instance (VRF) interfaces in VRFs 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.

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
```

Mistakenly, the same route is 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 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.

In the following example, 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 ser1/0.0 7.0.0.1 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/ forwarding instance (VRF), 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

<i>vrf-name</i>	Name of the VPN routing/forwarding instance (VRF) for the static route.
<i>prefix</i>	IP route prefix for the destination, in dotted-decimal format.
<i>mask</i>	Prefix mask for the destination, in dotted-decimal format.
<i>next-hop-address</i>	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
<i>interface</i>	(Optional) Type of network interface to use: atm , ethernet , loopback , pos , or null .
<i>interface-number</i>	(Optional) Number identifying the network interface to use.
global	(Optional) Specifies that the given next hop address is in the non-VRF routing table.
<i>distance</i>	(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 static routes are established.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

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.

Examples

The following command shows how to reroute packets addressed to network 172.23.0.0 in VRF vpn3 to router 172.31.6.6:

```
Router(config)# ip route vrf vpn3 172.23.0.0 255.255.0.0 172.31.6.6
```

Related Commands

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

ip vrf

To define a virtual private network (VPN) routing/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

<i>vrf-name</i>	Name assigned to a VRF.
-----------------	-------------------------

Defaults

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

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.

Usage Guidelines

The **ip vrf** *vrf-name* command creates a VRF instance named *vrf-name*. To make the VRF functional, a route distinguisher 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 route distinguisher (RD) with the VRF instance named *vrf-name*.

Examples

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

```
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target both 100:2
Router(config-vrf)# 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/forwarding instance (VRF) 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		
	<i>vrf-name</i>	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.
	<i>vrf-name2</i>	(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)	This command was updated with the downstream keyword 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.

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 VRF, while others operate in the downstream VRFs. The following functions operate in the downstream VRFs:
 - Point-to-Point Protocol (PPP) peer routes are installed in the downstream VRF.
 - Authentication, Authorization, and Accounting (AAA) per-user routes are installed in the downstream VRF.
 - A Reverse Path Forwarding (RPF) check is performed in the downstream VRF.

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 X.25 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/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	<i>vrf-name</i>	Name assigned to a VRF into which you want to add the IP address of the interface.
---------------------------	-----------------	--

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	12.0(22)S	This command was introduced.
	12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

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 (CEF) table. MPLS VPNs require CEF 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 CEF 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 VRF_1 and VRF_2 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 172.16.1.3 255.255.255.252
Router(config-if)# ip vrf select source
Router(config-if)# ip vrf receive VRF_1
Router(config-if)# ip vrf receive VRF_2
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 VRF_1 and VRF_2 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 192.168.1.2 255.255.255.252
Router(config-if)# ip policy route-map PBR-VRF-SELECTION
Router(config-if)# ip vrf receive VRF_1
Router(config-if)# ip vrf receive VRF_2
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 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	<i>route-map</i>	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.
	12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S.
	12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
	12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.

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 uniquely identifies the site from which a PE router has learned a route.
-------------------------	---

Examples	The following example, beginning in global configuration mode, 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.

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.

Examples

The following example shows how to list the explicit path:

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

Explicit Path name Joe:
  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 Joe:
  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.

