



# Configuring IP Unicast Routing

- [Finding Feature Information, on page 1](#)
- [Information About Configuring IP Unicast Routing, on page 1](#)
- [Information About IP Routing, on page 2](#)
- [How to Configure IP Routing, on page 2](#)
- [How to Configure IP Addressing, on page 3](#)
- [Monitoring and Maintaining IP Addressing, on page 25](#)
- [How to Configure IP Unicast Routing, on page 26](#)
- [Information About RIP, on page 27](#)
- [How to Configure RIP, on page 28](#)
- [Information About OSPF, on page 35](#)
- [Monitoring OSPF, on page 48](#)
- [Information About EIGRP, on page 49](#)
- [How to Configure EIGRP, on page 51](#)
- [Monitoring and Maintaining EIGRP, on page 59](#)
- [Information About Multi-VRF CE, on page 59](#)
- [How to Configure Multi-VRF CE, on page 62](#)
- [Configuring Unicast Reverse Path Forwarding, on page 79](#)
- [Protocol-Independent Features, on page 80](#)
- [Monitoring and Maintaining the IP Network, on page 101](#)

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <https://cfng.cisco.com/>. An account on Cisco.com is not required.

## Information About Configuring IP Unicast Routing

This module describes how to configure IP Version 4 (IPv4) unicast routing on the switch.

Basic routing functions like static routing are available with . IP Base feature set and the IP Services feature set on Catalyst 3560-CX switches. Catalyst 2960-CX switches support only static routing.



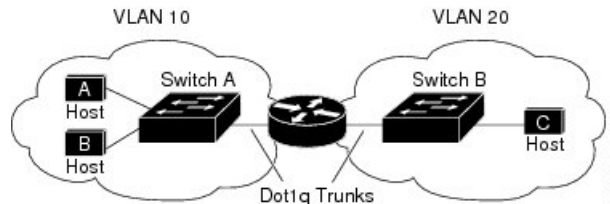
**Note** In addition to IPv4 traffic, you can also enable IP Version 6 (IPv6) unicast routing and configure interfaces to forward IPv6 traffic .

## Information About IP Routing

In some network environments, VLANs are associated with individual networks or subnetworks. In an IP network, each subnetwork is mapped to an individual VLAN. Configuring VLANs helps control the size of the broadcast domain and keeps local traffic local. However, network devices in different VLANs cannot communicate with one another without a Layer 3 device (router) to route traffic between the VLAN, referred to as inter-VLAN routing. You configure one or more routers to route traffic to the appropriate destination VLAN.

**Figure 1: Routing Topology Example**

This figure shows a basic routing topology. Switch A is in VLAN 10, and Switch B is in VLAN 20. The router



has an interface in each VLAN.

When Host A in VLAN 10 needs to communicate with Host B in VLAN 10, it sends a packet addressed to that host. Switch A forwards the packet directly to Host B, without sending it to the router.

When Host A sends a packet to Host C in VLAN 20, Switch A forwards the packet to the router, which receives the traffic on the VLAN 10 interface. The router checks the routing table, finds the correct outgoing interface, and forwards the packet on the VLAN 20 interface to Switch B. Switch B receives the packet and forwards it to Host C.

## Types of Routing

Routers and Layer 3 switches can route packets in these ways:

- By using default routing
- By using preprogrammed static routes for the traffic
- By dynamically calculating routes by using a routing protocol

The switch supports static routes and default routes. It does not support routing protocols.

## How to Configure IP Routing

By default, IP routing is disabled on the Device, and you must enable it before routing can take place.

In the following procedures, the specified interface must be one of these Layer 3 interfaces:

- A routed port: a physical port configured as a Layer 3 port by using the **no switchport** interface configuration command.
- A switch virtual interface (SVI): a VLAN interface created by using the **interface vlan** *vlan\_id* global configuration command and by default a Layer 3 interface.
- An EtherChannel port channel in Layer 3 mode: a port-channel logical interface created by using the **interface port-channel** *port-channel-number* global configuration command and binding the Ethernet interface into the channel group.



---

**Note** The switch does not support tunnel interfaces for unicast routed traffic.

---

All Layer 3 interfaces on which routing will occur must have IP addresses assigned to them.



---

**Note** A Layer 3 switch can have an IP address assigned to each routed port and SVI.

---

Configuring routing consists of several main procedures:

- To support VLAN interfaces, create and configure VLANs on the Device or switch stack, and assign VLAN membership to Layer 2 interfaces. For more information, see the "Configuring VLANs" chapter.
- Configure Layer 3 interfaces.
- Enable IP routing on the switch.
- Assign IP addresses to the Layer 3 interfaces.
- Enable selected routing protocols on the switch.
- Configure routing protocol parameters (optional).

## How to Configure IP Addressing

A required task for configuring IP routing is to assign IP addresses to Layer 3 network interfaces to enable the interfaces and allow communication with the hosts on those interfaces that use IP. The following sections describe how to configure various IP addressing features. Assigning IP addresses to the interface is required; the other procedures are optional.

- Default Addressing Configuration
- Assigning IP Addresses to Network Interfaces
- Configuring Address Resolution Methods
- Routing Assistance When IP Routing is Disabled
- Configuring Broadcast Packet Handling
- Monitoring and Maintaining IP Addressing

## Default IP Addressing Configuration

*Table 1: Default Addressing Configuration*

Feature	Default Setting
IP address	None defined.
ARP	No permanent entries in the Address Resolution Protocol (ARP) cache. Encapsulation: Standard Ethernet-style ARP. Timeout: 14400 seconds (4 hours).
IP broadcast address	255.255.255.255 (all ones).
IP classless routing	Enabled.
IP default gateway	Disabled.
IP directed broadcast	Disabled (all IP directed broadcasts are dropped).
IP domain	Domain list: No domain names defined. Domain lookup: Enabled. Domain name: Enabled.
IP forward-protocol	If a helper address is defined or User Datagram Protocol (UDP) flooding is configured, UDP flood protection is enabled on default ports. Any-local-broadcast: Disabled. Spanning Tree Protocol (STP): Disabled. Turbo-flood: Disabled.
IP helper address	Disabled.
IP host	Disabled.
IRDP	Disabled. Defaults when enabled: <ul style="list-style-type: none"> <li>• Broadcast IRDP advertisements.</li> <li>• Maximum interval between advertisements: 600 seconds.</li> <li>• Minimum interval between advertisements: 0.75 times max interval</li> <li>• Preference: 0.</li> </ul>
IP proxy ARP	Enabled.
IP routing	Disabled.
IP subnet-zero	Disabled.

## Assigning IP Addresses to Network Interfaces

An IP address identifies a location to which IP packets can be sent. Some IP addresses are reserved for special uses and cannot be used for host, subnet, or network addresses. RFC 1166, “Internet Numbers,” contains the official description of IP addresses.

An interface can have one primary IP address. A mask identifies the bits that denote the network number in an IP address. When you use the mask to subnet a network, the mask is referred to as a subnet mask. To receive an assigned network number, contact your Internet service provider.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-id</i></b> <b>Example:</b> <pre>Switch(config)# interface gigabitethernet 1/0/1</pre>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
<b>Step 4</b>	<b>no switchport</b> <b>Example:</b> <pre>Switch(config-if)# no switchport</pre>	Removes the interface from Layer 2 configuration mode (if it is a physical interface).
<b>Step 5</b>	<b>ip address <i>ip-address subnet-mask</i></b> <b>Example:</b> <pre>Switch(config-if)# ip address 10.1.5.1 255.255.255.0</pre>	Configures the IP address and IP subnet mask.
<b>Step 6</b>	<b>no shutdown</b> <b>Example:</b> <pre>Switch(config-if)# no shutdown</pre>	Enables the physical interface.
<b>Step 7</b>	<b>end</b> <b>Example:</b>	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Switch(config)# <b>end</b>	
<b>Step 8</b>	<b>show ip route</b> <b>Example:</b> Switch# show ip route	Verifies your entries.
<b>Step 9</b>	<b>show ip interface [interface-id]</b> <b>Example:</b> Switch# show ip interface gigabitethernet 1/0/1	Verifies your entries.
<b>Step 10</b>	<b>show running-config</b> <b>Example:</b> Switch# show running-config	Verifies your entries.
<b>Step 11</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## Using Subnet Zero

Subnetting with a subnet address of zero is strongly discouraged because of the problems that can arise if a network and a subnet have the same addresses. For example, if network 131.108.0.0 is subnetted as 255.255.255.0, subnet zero would be written as 131.108.0.0, which is the same as the network address.

You can use the all ones subnet (131.108.255.0) and even though it is discouraged, you can enable the use of subnet zero if you need the entire subnet space for your IP address.

Use the **no ip subnet-zero** global configuration command to restore the default and disable the use of subnet zero.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>	Enters global configuration mode.

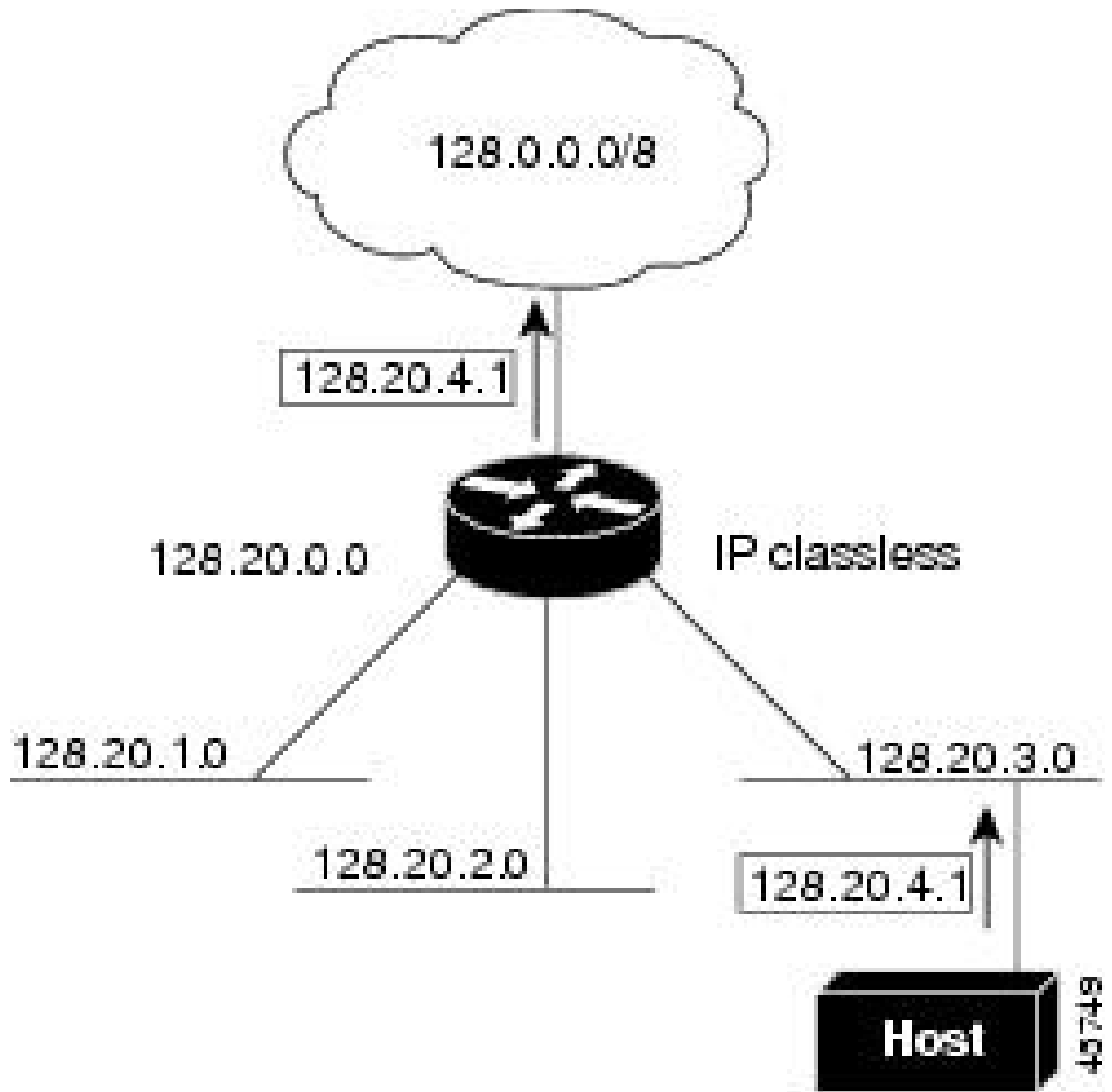
	Command or Action	Purpose
	Switch# <code>configure terminal</code>	
<b>Step 3</b>	<b>ip subnet-zero</b> <b>Example:</b> Switch(config)# <code>ip subnet-zero</code>	Enables the use of subnet zero for interface addresses and routing updates.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Switch(config)# <code>end</code>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show running-config</b> <b>Example:</b> Switch# <code>show running-config</code>	Verifies your entries.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

## Classless Routing

By default, classless routing behavior is enabled on the Device when it is configured to route. With classless routing, if a router receives packets for a subnet of a network with no default route, the router forwards the packet to the best supernet route. A supernet consists of contiguous blocks of Class C address spaces used to simulate a single, larger address space and is designed to relieve the pressure on the rapidly depleting Class B address space.

In the figure, classless routing is enabled. When the host sends a packet to 120.20.4.1, instead of discarding the packet, the router forwards it to the best supernet route. If you disable classless routing and a router receives packets destined for a subnet of a network with no network default route, the router discards the packet.

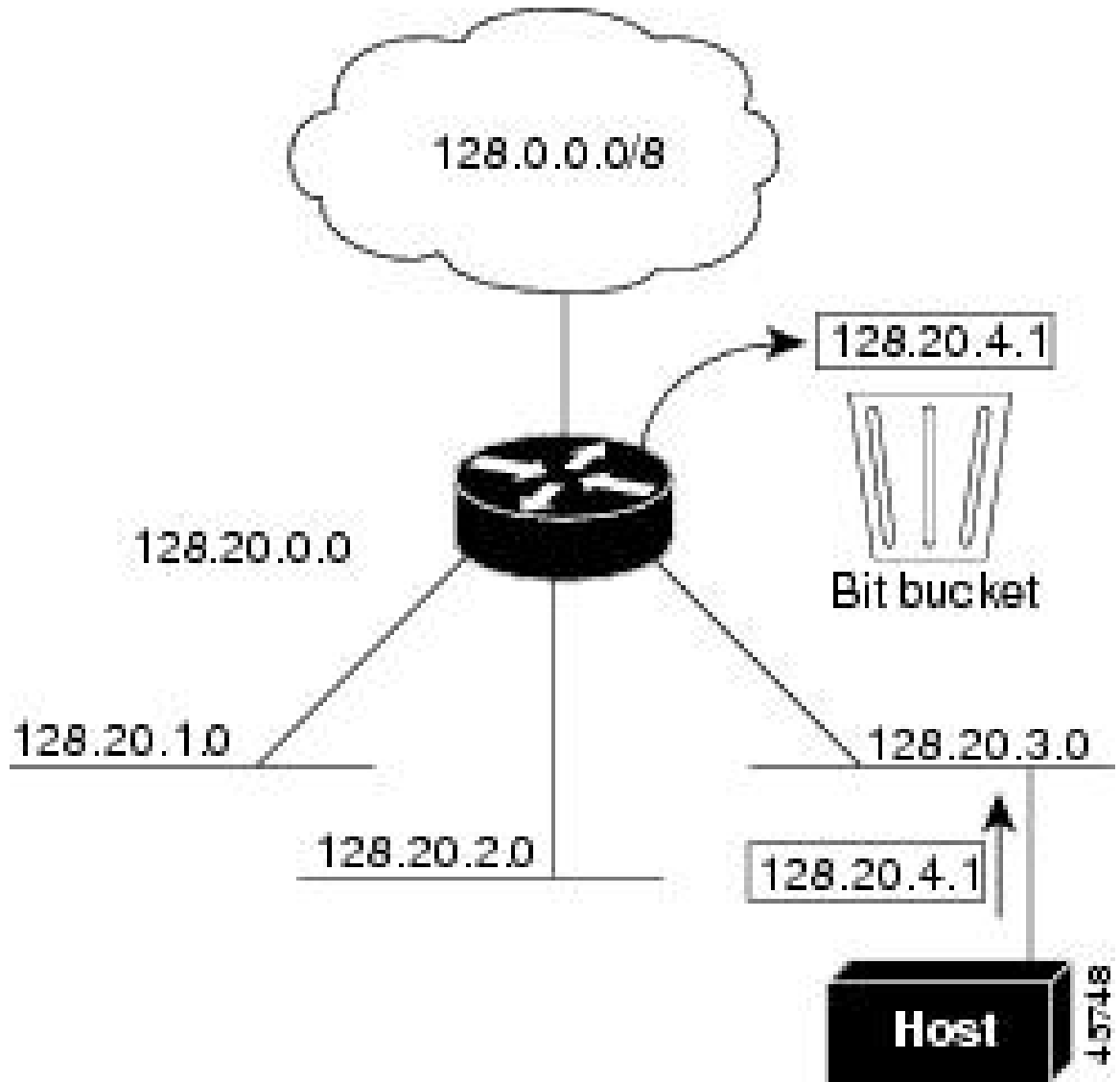
Figure 2: IP Classless Routing



In the figure, the router in network 128.20.0.0 is connected to subnets 128.20.1.0, 128.20.2.0, and 128.20.3.0. If the host sends a packet to 120.20.4.1, because there is no network default route, the router discards the packet.



Figure 3: No IP Classless Routing



To prevent the Device from forwarding packets destined for unrecognized subnets to the best supernet route possible, you can disable classless routing behavior.

## Disabling Classless Routing

To prevent the Device from forwarding packets destined for unrecognized subnets to the best supernet route possible, you can disable classless routing behavior.

### Procedure

	Command or Action	Purpose
Step 1	enable Example:	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	Switch> <b>enable</b>	
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>no ip classless</b> <b>Example:</b> Switch(config)# <b>no ip classless</b>	Disables classless routing behavior.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show running-config</b> <b>Example:</b> Switch# <b>show running-config</b>	Verifies your entries.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Configuring Address Resolution Methods

You can perform the following tasks to configure address resolution.

### Address Resolution

You can control interface-specific handling of IP by using address resolution. A device using IP can have both a local address or MAC address, which uniquely defines the device on its local segment or LAN, and a network address, which identifies the network to which the device belongs.

The local address or MAC address is known as a data link address because it is contained in the data link layer (Layer 2) section of the packet header and is read by data link (Layer 2) devices. To communicate with a device on Ethernet, the software must learn the MAC address of the device. The process of learning the MAC address from an IP address is called *address resolution*. The process of learning the IP address from the MAC address is called *reverse address resolution*.

The Device can use these forms of address resolution:

- Address Resolution Protocol (ARP) is used to associate IP address with MAC addresses. Taking an IP address as input, ARP learns the associated MAC address and then stores the IP address/MAC address association in an ARP cache for rapid retrieval. Then the IP datagram is encapsulated in a link-layer frame and sent over the network. Encapsulation of IP datagrams and ARP requests or replies on IEEE 802 networks other than Ethernet is specified by the Subnetwork Access Protocol (SNAP).
- Proxy ARP helps hosts with no routing tables learn the MAC addresses of hosts on other networks or subnets. If the Device (router) receives an ARP request for a host that is not on the same interface as the ARP request sender, and if the router has all of its routes to the host through other interfaces, it generates a proxy ARP packet giving its own local data link address. The host that sent the ARP request then sends its packets to the router, which forwards them to the intended host.

The Device also uses the Reverse Address Resolution Protocol (RARP), which functions the same as ARP does, except that the RARP packets request an IP address instead of a local MAC address. Using RARP requires a RARP server on the same network segment as the router interface. Use the **ip rarp-server address** interface configuration command to identify the server.

## Defining a Static ARP Cache

ARP and other address resolution protocols provide dynamic mapping between IP addresses and MAC addresses. Because most hosts support dynamic address resolution, you usually do not need to specify static ARP cache entries. If you must define a static ARP cache entry, you can do so globally, which installs a permanent entry in the ARP cache that the Device uses to translate IP addresses into MAC addresses. Optionally, you can also specify that the Device respond to ARP requests as if it were the owner of the specified IP address. If you do not want the ARP entry to be permanent, you can specify a timeout period for the ARP entry.

### Procedure

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
Step 3	<b>arp ip-address hardware-address type</b> <b>Example:</b> <pre>Switch(config)# ip 10.1.5.1 c2f3.220a.12f4 arpa</pre>	Associates an IP address with a MAC (hardware) address in the ARP cache, and specifies encapsulation type as one of these: <ul style="list-style-type: none"> <li>• <b>arpa</b>—ARP encapsulation for Ethernet interfaces</li> <li>• <b>snap</b>—Subnetwork Address Protocol encapsulation for Token Ring and FDDI interfaces</li> <li>• <b>sap</b>—HP's ARP type</li> </ul>

	Command or Action	Purpose
<b>Step 4</b>	<b>arp</b> <i>ip-address hardware-address type</i> [ <b>alias</b> ] <b>Example:</b>  Switch(config)# ip 10.1.5.3 d7f3.220d.12f5 arpa alias	(Optional) Specifies that the switch respond to ARP requests as if it were the owner of the specified IP address.
<b>Step 5</b>	<b>interface</b> <i>interface-id</i> <b>Example:</b>  Switch(config)# interface gigabitethernet 1/0/1	Enters interface configuration mode, and specifies the interface to configure.
<b>Step 6</b>	<b>arp</b> <i>timeout seconds</i> <b>Example:</b>  Switch(config-if)# arp 20000	(Optional) Sets the length of time an ARP cache entry will stay in the cache. The default is 14400 seconds (4 hours). The range is 0 to 2147483 seconds.
<b>Step 7</b>	<b>end</b> <b>Example:</b>  Switch(config)# end	Returns to privileged EXEC mode.
<b>Step 8</b>	<b>show interfaces</b> [ <i>interface-id</i> ] <b>Example:</b>  Switch# show interfaces gigabitethernet 1/0/1	Verifies the type of ARP and the timeout value used on all interfaces or a specific interface.
<b>Step 9</b>	<b>show arp</b> <b>Example:</b>  Switch# show arp	Views the contents of the ARP cache.
<b>Step 10</b>	<b>show ip arp</b> <b>Example:</b>  Switch# show ip arp	Views the contents of the ARP cache.
<b>Step 11</b>	<b>copy running-config startup-config</b> <b>Example:</b>  Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## Setting ARP Encapsulation

By default, Ethernet ARP encapsulation (represented by the **arpa** keyword) is enabled on an IP interface. You can change the encapsulation methods to SNAP if required by your network.

To disable an encapsulation type, use the **no arp arpa** or **no arp snap** interface configuration command.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Switch> <b>enable</b>	Enables privileged EXEC mode.  • Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-id</i></b> <b>Example:</b>  Switch(config)# <b>interface gigabitethernet 1/0/2</b>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
<b>Step 4</b>	<b>arp {arpa   snap}</b> <b>Example:</b>  Switch(config-if)# <b>arp arpa</b>	Specifies the ARP encapsulation method:  • <b>arpa</b> —Address Resolution Protocol  • <b>snap</b> —Subnetwork Address Protocol
<b>Step 5</b>	<b>end</b> <b>Example:</b>  Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show interfaces [<i>interface-id</i>]</b> <b>Example:</b>  Switch# <b>show interfaces</b>	Verifies ARP encapsulation configuration on all interfaces or the specified interface.
<b>Step 7</b>	<b>copy running-config startup-config</b> <b>Example:</b>  Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Enabling Proxy ARP

By default, the Device uses proxy ARP to help hosts learn MAC addresses of hosts on other networks or subnets.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>  Switch> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b>  Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-id</i></b> <b>Example:</b>  Switch(config)# <b>interface gigabitethernet 1/0/2</b>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
<b>Step 4</b>	<b>ip proxy-arp</b> <b>Example:</b>  Switch(config-if)# <b>ip proxy-arp</b>	Enables proxy ARP on the interface.
<b>Step 5</b>	<b>end</b> <b>Example:</b>  Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show ip interface [<i>interface-id</i>]</b> <b>Example:</b>  Switch# <b>show ip interface gigabitethernet 1/0/2</b>	Verifies the configuration on the interface or all interfaces.
<b>Step 7</b>	<b>copy running-config startup-config</b> <b>Example:</b>  Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Routing Assistance When IP Routing is Disabled

These mechanisms allow the Device to learn about routes to other networks when it does not have IP routing enabled:

- Proxy ARP
- Default Gateway

- ICMP Router Discovery Protocol (IRDP)

## Proxy ARP

Proxy ARP, the most common method for learning about other routes, enables an Ethernet host with no routing information to communicate with hosts on other networks or subnets. The host assumes that all hosts are on the same local Ethernet and that they can use ARP to learn their MAC addresses. If a Device receives an ARP request for a host that is not on the same network as the sender, the Device evaluates whether it has the best route to that host. If it does, it sends an ARP reply packet with its own Ethernet MAC address, and the host that sent the request sends the packet to the Device, which forwards it to the intended host. Proxy ARP treats all networks as if they are local, and performs ARP requests for every IP address.

## Proxy ARP

Proxy ARP is enabled by default. To enable it after it has been disabled, see the “Enabling Proxy ARP” section. Proxy ARP works as long as other routers support it.

## Default Gateway

Another method for locating routes is to define a default router or default gateway. All non-local packets are sent to this router, which either routes them appropriately or sends an IP Control Message Protocol (ICMP) redirect message back, defining which local router the host should use. The Device caches the redirect messages and forwards each packet as efficiently as possible. A limitation of this method is that there is no means of detecting when the default router has gone down or is unavailable.

### Procedure

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
Step 3	<b>ip default-gateway ip-address</b> <b>Example:</b> Switch(config)# <b>ip default gateway 10.1.5.1</b>	Sets up a default gateway (router).
Step 4	<b>end</b> <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.

	Command or Action	Purpose
<b>Step 5</b>	<b>show ip redirects</b> <b>Example:</b> <pre>Switch# show ip redirects</pre>	Displays the address of the default gateway router to verify the setting.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## ICMP Router Discovery Protocol

Router discovery allows the Device to dynamically learn about routes to other networks using ICMP router discovery protocol (IRDP). IRDP allows hosts to locate routers. When operating as a client, the Device generates router discovery packets. When operating as a host, the Device receives router discovery packets. The Device can also listen to Routing Information Protocol (RIP) routing updates and use this information to infer locations of routers. The Device does not actually store the routing tables sent by routing devices; it merely keeps track of which systems are sending the data. The advantage of using IRDP is that it allows each router to specify both a priority and the time after which a device is assumed to be down if no further packets are received.

Each device discovered becomes a candidate for the default router, and a new highest-priority router is selected when a higher priority router is discovered, when the current default router is declared down, or when a TCP connection is about to time out because of excessive retransmissions.

## ICMP Router Discovery Protocol (IRDP)

The only required task for IRDP routing on an interface is to enable IRDP processing on that interface. When enabled, the default parameters apply.

You can optionally change any of these parameters. If you change the **maxadvertinterval** value, the **holdtime** and **minadvertinterval** values also change, so it is important to first change the **maxadvertinterval** value, before manually changing either the **holdtime** or **minadvertinterval** values.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.



	Command or Action	Purpose
Step 3	<b>interface</b> <i>interface-id</i> <b>Example:</b> <pre>Switch(config)# interface gigabitethernet 1/0/1</pre>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
Step 4	<b>ip irdp</b> <b>Example:</b> <pre>Switch(config-if)# ip irdp</pre>	Enables IRDP processing on the interface.
Step 5	<b>ip irdp multicast</b> <b>Example:</b> <pre>Switch(config-if)# ip irdp multicast</pre>	(Optional) Sends IRDP advertisements to the multicast address (224.0.0.1) instead of IP broadcasts.  <b>Note</b> This command allows for compatibility with Sun Microsystems Solaris, which requires IRDP packets to be sent out as multicasts. Many implementations cannot receive these multicasts; ensure end-host ability before using this command.
Step 6	<b>ip irdp holdtime</b> <i>seconds</i> <b>Example:</b> <pre>Switch(config-if)# ip irdp holdtime 1000</pre>	(Optional) Sets the IRDP period for which advertisements are valid. The default is three times the <b>maxadvertinterval</b> value. It must be greater than <b>maxadvertinterval</b> and cannot be greater than 9000 seconds. If you change the <b>maxadvertinterval</b> value, this value also changes.
Step 7	<b>ip irdp maxadvertinterval</b> <i>seconds</i> <b>Example:</b> <pre>Switch(config-if)# ip irdp maxadvertinterval 650</pre>	(Optional) Sets the IRDP maximum interval between advertisements. The default is 600 seconds.
Step 8	<b>ip irdp minadvertinterval</b> <i>seconds</i> <b>Example:</b> <pre>Switch(config-if)# ip irdp minadvertinterval 500</pre>	(Optional) Sets the IRDP minimum interval between advertisements. The default is 0.75 times the <b>maxadvertinterval</b> . If you change the <b>maxadvertinterval</b> , this value changes to the new default (0.75 of <b>maxadvertinterval</b> ).
Step 9	<b>ip irdp preference</b> <i>number</i> <b>Example:</b> <pre>Switch(config-if)# ip irdp preference 2</pre>	(Optional) Sets a device IRDP preference level. The allowed range is -231 to 231. The default is 0. A higher value increases the router preference level.
Step 10	<b>ip irdp address</b> <i>address [number]</i> <b>Example:</b> <pre>Switch(config-if)# ip irdp address 10.1.10.10</pre>	(Optional) Specifies an IRDP address and preference to proxy-advertise.

	Command or Action	Purpose
Step 11	<b>end</b> <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 12	<b>show ip irdp</b> <b>Example:</b> <pre>Switch# show ip irdp</pre>	Verifies settings by displaying IRDP values.
Step 13	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Configuring Broadcast Packet Handling

Perform the tasks in these sections to enable these schemes:

- Enabling Directed Broadcast-to-Physical Broadcast Translation
- Forwarding UDP Broadcast Packets and Protocols
- Establishing an IP Broadcast Address
- Flooding IP Broadcasts

### Broadcast Packet Handling

After configuring an IP interface address, you can enable routing and configure one or more routing protocols, or you can configure the way the Device responds to network broadcasts. A broadcast is a data packet destined for all hosts on a physical network. The Device supports two kinds of broadcasting:

- A directed broadcast packet is sent to a specific network or series of networks. A directed broadcast address includes the network or subnet fields.
- A flooded broadcast packet is sent to every network.




---

**Note** You can also limit broadcast, unicast, and multicast traffic on Layer 2 interfaces by using the **storm-control** interface configuration command to set traffic suppression levels.

---

Routers provide some protection from broadcast storms by limiting their extent to the local cable. Bridges (including intelligent bridges), because they are Layer 2 devices, forward broadcasts to all network segments, thus propagating broadcast storms. The best solution to the broadcast storm problem is to use a single broadcast address scheme on a network. In most modern IP implementations, you can set the address to be used as the

broadcast address. Many implementations, including the one in the Device, support several addressing schemes for forwarding broadcast messages.

## Enabling Directed Broadcast-to-Physical Broadcast Translation

By default, IP directed broadcasts are dropped; they are not forwarded. Dropping IP-directed broadcasts makes routers less susceptible to denial-of-service attacks.

You can enable forwarding of IP-directed broadcasts on an interface where the broadcast becomes a physical (MAC-layer) broadcast. Only those protocols configured by using the **ip forward-protocol** global configuration command are forwarded.

You can specify an access list to control which broadcasts are forwarded. When an access list is specified, only those IP packets permitted by the access list are eligible to be translated from directed broadcasts to physical broadcasts. For more information on access lists, see the “Configuring ACLs” chapter in the Security section.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-id</i></b> <b>Example:</b> <pre>Switch(config)# interface gigabitethernet 1/0/2</pre>	Enters interface configuration mode, and specifies the interface to configure.
<b>Step 4</b>	<b>ip directed-broadcast [<i>access-list-number</i>]</b> <b>Example:</b> <pre>Switch(config-if)# ip directed-broadcast 103</pre>	Enables directed broadcast-to-physical broadcast translation on the interface. You can include an access list to control which broadcasts are forwarded. When an access list, only IP packets permitted by the access list can be translated.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> <pre>Switch(config-if)# exit</pre>	Returns to global configuration mode.
<b>Step 6</b>	<b>ip forward-protocol {udp [<i>port</i>]   nd   sdns}</b> <b>Example:</b>	Specifies which protocols and ports the router forwards when forwarding broadcast packets. <ul style="list-style-type: none"> <li>• <b>udp</b>—Forward UPD datagrams.</li> </ul>

	Command or Action	Purpose
	<code>Switch(config)# ip forward-protocol nd</code>	<p>port: (Optional) Destination port that controls which UDP services are forwarded.</p> <ul style="list-style-type: none"> <li>• <b>nd</b>—Forward ND datagrams.</li> <li>• <b>sdns</b>—Forward SDNS datagrams</li> </ul>
<b>Step 7</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 8</b>	<p><b>show ip interface</b> [<i>interface-id</i>]</p> <p><b>Example:</b></p> <pre>Switch# show ip interface</pre>	Verifies the configuration on the interface or all interfaces
<b>Step 9</b>	<p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>Switch# show running-config</pre>	Verifies your entries.
<b>Step 10</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## UDP Broadcast Packets and Protocols

User Datagram Protocol (UDP) is an IP host-to-host layer protocol, as is TCP. UDP provides a low-overhead, connectionless session between two end systems and does not provide for acknowledgment of received datagrams. Network hosts occasionally use UDP broadcasts to find address, configuration, and name information. If such a host is on a network segment that does not include a server, UDP broadcasts are normally not forwarded. You can remedy this situation by configuring an interface on a router to forward certain classes of broadcasts to a helper address. You can use more than one helper address per interface.

You can specify a UDP destination port to control which UDP services are forwarded. You can specify multiple UDP protocols. You can also specify the Network Disk (ND) protocol, which is used by older diskless Sun workstations and the network security protocol SDNS.

By default, both UDP and ND forwarding are enabled if a helper address has been defined for an interface.

## Forwarding UDP Broadcast Packets and Protocols

If you do not specify any UDP ports when you configure the forwarding of UDP broadcasts, you are configuring the router to act as a BOOTP forwarding agent. BOOTP packets carry DHCP information.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-id</i></b> <b>Example:</b> <pre>Switch(config)# interface gigabitethernet 1/0/1</pre>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
<b>Step 4</b>	<b>ip helper-address <i>address</i></b> <b>Example:</b> <pre>Switch(config-if)# ip helper address 10.1.10.1</pre>	Enables forwarding and specifies the destination address for forwarding UDP broadcast packets, including BOOTP.
<b>Step 5</b>	<b>exit</b> <b>Example:</b> <pre>Switch(config-if)# exit</pre>	Returns to global configuration mode.
<b>Step 6</b>	<b>ip forward-protocol {udp [<i>port</i>]   nd   sdns}</b> <b>Example:</b> <pre>Switch(config)# ip forward-protocol sdns</pre>	Specifies which protocols the router forwards when forwarding broadcast packets.
<b>Step 7</b>	<b>end</b> <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 8</b>	<b>show ip interface [<i>interface-id</i>]</b> <b>Example:</b> <pre>Switch# show ip interface gigabitethernet 1/0/1</pre>	Verifies the configuration on the interface or all interfaces.
<b>Step 9</b>	<b>show running-config</b> <b>Example:</b>	Verifies your entries.

	Command or Action	Purpose
	Switch# <code>show running-config</code>	
<b>Step 10</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

## Establishing an IP Broadcast Address

The most popular IP broadcast address (and the default) is an address consisting of all ones (255.255.255.255). However, the Device can be configured to generate any form of IP broadcast address.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Switch> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-id</i></b> <b>Example:</b> Switch(config)# <code>interface gigabitethernet 1/0/1</code>	Enters interface configuration mode, and specifies the interface to configure.
<b>Step 4</b>	<b>ip broadcast-address <i>ip-address</i></b> <b>Example:</b> Switch(config-if)# <code>ip broadcast-address 128.1.255.255</code>	Enters a broadcast address different from the default, for example 128.1.255.255.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Switch(config)# <code>end</code>	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	<b>show ip interface</b> [ <i>interface-id</i> ] <b>Example:</b> <pre>Switch# show ip interface</pre>	Verifies the broadcast address on the interface or all interfaces.
Step 7	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## IP Broadcast Flooding

You can allow IP broadcasts to be flooded throughout your internetwork in a controlled fashion by using the database created by the bridging STP. Using this feature also prevents loops. To support this capability, bridging must be configured on each interface that is to participate in the flooding. If bridging is not configured on an interface, it still can receive broadcasts. However, the interface never forwards broadcasts it receives, and the router never uses that interface to send broadcasts received on a different interface.

Packets that are forwarded to a single network address using the IP helper-address mechanism can be flooded. Only one copy of the packet is sent on each network segment.

To be considered for flooding, packets must meet these criteria. (Note that these are the same conditions used to consider packet forwarding using IP helper addresses.)

- The packet must be a MAC-level broadcast.
- The packet must be an IP-level broadcast.
- The packet must be a TFTP, DNS, Time, NetBIOS, ND, or BOOTP packet, or a UDP specified by the **ip forward-protocol udp** global configuration command.
- The time-to-live (TTL) value of the packet must be at least two.

A flooded UDP datagram is given the destination address specified with the **ip broadcast-address** interface configuration command on the output interface. The destination address can be set to any address. Thus, the destination address might change as the datagram propagates through the network. The source address is never changed. The TTL value is decremented.

When a flooded UDP datagram is sent out an interface (and the destination address possibly changed), the datagram is handed to the normal IP output routines and is, therefore, subject to access lists, if they are present on the output interface.

In the Device, the majority of packets are forwarded in hardware; most packets do not go through the Device CPU. For those packets that do go to the CPU, you can speed up spanning tree-based UDP flooding by a factor of about four to five times by using turbo-flooding. This feature is supported over Ethernet interfaces configured for ARP encapsulation.

## Flooding IP Broadcasts

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>ip forward-protocol spanning-tree</b> <b>Example:</b> Switch(config)# <b>ip forward-protocol spanning-tree</b>	Uses the bridging spanning-tree database to flood UDP datagrams.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show running-config</b> <b>Example:</b> Switch# <b>show running-config</b>	Verifies your entries.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.
<b>Step 7</b>	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 8</b>	<b>ip forward-protocol turbo-flood</b> <b>Example:</b>	Uses the spanning-tree database to speed up flooding of UDP datagrams.



	Command or Action	Purpose
	<code>Switch(config)# ip forward-protocol turbo-flood</code>	
<b>Step 9</b>	<b>end</b> <b>Example:</b> <code>Switch(config)# end</code>	Returns to privileged EXEC mode.
<b>Step 10</b>	<b>show running-config</b> <b>Example:</b> <code>Switch# show running-config</code>	Verifies your entries.
<b>Step 11</b>	<b>copy running-config startup-config</b> <b>Example:</b> <code>Switch# copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

## Monitoring and Maintaining IP Addressing

When the contents of a particular cache, table, or database have become or are suspected to be invalid, you can remove all its contents by using the **clear** privileged EXEC commands. The Table lists the commands for clearing contents.

**Table 2: Commands to Clear Caches, Tables, and Databases**

<b>clear arp-cache</b>	Clears the IP ARP cache and the fast-switching cache.
<b>clear host</b> { <i>name</i>   *}	Removes one or all entries from the hostname and the address.
<b>clear ip route</b> { <i>network</i> [ <i>mask</i> ]   *}	Removes one or more routes from the IP routing table.

You can display specific statistics, such as the contents of IP routing tables, caches, and databases; the reachability of nodes; and the routing path that packets are taking through the network. The Table lists the privileged EXEC commands for displaying IP statistics.

**Table 3: Commands to Display Caches, Tables, and Databases**

<b>show arp</b>	Displays the entries in the ARP table.
<b>show hosts</b>	Displays the default domain name, style of lookup service, name server, and the cached list of hostnames and addresses.
<b>show ip aliases</b>	Displays IP addresses mapped to TCP ports (aliases).
<b>show ip arp</b>	Displays the IP ARP cache.

<b>show ip interface</b> [ <i>interface-id</i> ]	Displays the IP status of interfaces.
<b>show ip irdp</b>	Displays IRDP values.
<b>show ip masks</b> <i>address</i>	Displays the masks used for network addresses and the number of subnets for each mask.
<b>show ip redirects</b>	Displays the address of a default gateway.
<b>show ip route</b> [ <i>address [mask]</i> ]   [ <i>protocol</i> ]	Displays the current state of the routing table.
<b>show ip route summary</b>	Displays the current state of the routing table in summary form.

# How to Configure IP Unicast Routing

## Enabling IP Unicast Routing

By default, the Device is in Layer 2 switching mode and IP routing is disabled. To use the Layer 3 capabilities of the Device, you must enable IP routing.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>ip routing</b> <b>Example:</b> Switch(config)# <b>ip routing</b>	Enables IP routing.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 5	<b>show running-config</b> <b>Example:</b> <pre>Switch# show running-config</pre>	Verifies your entries.
Step 6	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Example of Enabling IP Unicast Routing

This example shows how to enable IP routing on a Switch:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing

Switch(config-router)# end
```

## Information About RIP

The Routing Information Protocol (RIP) is an interior gateway protocol (IGP) created for use in small, homogeneous networks. It is a distance-vector routing protocol that uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. The protocol is documented in RFC 1058. You can find detailed information about RIP in *IP Routing Fundamentals*, published by Cisco Press.



**Note** RIP is supported in the Network Essentials feature set.

Using RIP, the Device sends routing information updates (advertisements) every 30 seconds. If a router does not receive an update from another router for 180 seconds or more, it marks the routes served by that router as unusable. If there is still no update after 240 seconds, the router removes all routing table entries for the non-updating router.

RIP uses hop counts to rate the value of different routes. The hop count is the number of routers that can be traversed in a route. A directly connected network has a hop count of zero; a network with a hop count of 16 is unreachable. This small range (0 to 15) makes RIP unsuitable for large networks.

If the router has a default network path, RIP advertises a route that links the router to the pseudonetwork 0.0.0.0. The 0.0.0.0 network does not exist; it is treated by RIP as a network to implement the default routing feature. The Device advertises the default network if a default was learned by RIP or if the router has a gateway of last resort and RIP is configured with a default metric. RIP sends updates to the interfaces in specified networks. If an interface's network is not specified, it is not advertised in any RIP update.

# How to Configure RIP

## Default RIP Configuration

*Table 4: Default RIP Configuration*

Feature	Default Setting
Auto summary	Enabled.
Default-information originate	Disabled.
Default metric	Built-in; automatic metric translations.
IP RIP authentication key-chain	No authentication. Authentication mode: clear text.
IP RIP triggered	Disabled
IP split horizon	Varies with media.
Neighbor	None defined.
Network	None specified.
Offset list	Disabled.
Output delay	0 milliseconds.
Timers basic	<ul style="list-style-type: none"> <li>• Update: 30 seconds.</li> <li>• Invalid: 180 seconds.</li> <li>• Hold-down: 180 seconds.</li> <li>• Flush: 240 seconds.</li> </ul>
Validate-update-source	Enabled.
Version	Receives RIP Version 1 and 2 packets; sends Version 1 packets.

## Configuring Basic RIP Parameters

To configure RIP, you enable RIP routing for a network and optionally configure other parameters. On the Device, RIP configuration commands are ignored until you configure the network number.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>ip routing</b> <b>Example:</b> Switch(config)# <b>ip routing</b>	Enables IP routing. (Required only if IP routing is disabled.)
<b>Step 4</b>	<b>router rip</b> <b>Example:</b> Switch(config)# <b>router rip</b>	Enables a RIP routing process, and enter router configuration mode.
<b>Step 5</b>	<b>network <i>network number</i></b> <b>Example:</b> Switch(config-router)# <b>network 12.0.0.0</b>	Associates a network with a RIP routing process. You can specify multiple <b>network</b> commands. RIP routing updates are sent and received through interfaces only on these networks.  <b>Note</b> You must configure a network number for the RIP commands to take effect.
<b>Step 6</b>	<b>neighbor <i>ip-address</i></b> <b>Example:</b> Switch(config-router)# <b>neighbor 10.2.5.1</b>	(Optional) Defines a neighboring router with which to exchange routing information. This step allows routing updates from RIP (normally a broadcast protocol) to reach nonbroadcast networks.
<b>Step 7</b>	<b>offset-list [<i>access-list number   name</i>] {<i>in</i>   <i>out</i>} <i>offset</i> [<i>type number</i>]</b> <b>Example:</b> Switch(config-router)# <b>offset-list 103 in 10</b>	(Optional) Applies an offset list to routing metrics to increase incoming and outgoing metrics to routes learned through RIP. You can limit the offset list with an access list or an interface.
<b>Step 8</b>	<b>timers <i>basic update invalid holddown flush</i></b> <b>Example:</b> Switch(config-router)# <b>timers basic 45 360 400 300</b>	(Optional) Adjusts routing protocol timers. Valid ranges for all timers are 0 to 4294967295 seconds. <ul style="list-style-type: none"> <li>• <i>update</i>—The time between sending routing updates. The default is 30 seconds.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <i>invalid</i>—The timer after which a route is declared invalid. The default is 180 seconds.</li> <li>• <i>holddown</i>—The time before a route is removed from the routing table. The default is 180 seconds.</li> <li>• <i>flush</i>—The amount of time for which routing updates are postponed. The default is 240 seconds.</li> </ul>
<b>Step 9</b>	<b>version {1   2}</b> <b>Example:</b> <pre>Switch(config-router)# version 2</pre>	(Optional) Configures the switch to receive and send only RIP Version 1 or RIP Version 2 packets. By default, the switch receives Version 1 and 2 but sends only Version 1. You can also use the interface commands <b>ip rip {send   receive} version 1   2   1 2</b> to control what versions are used for sending and receiving on interfaces.
<b>Step 10</b>	<b>no auto-summary</b> <b>Example:</b> <pre>Switch(config-router)# no auto-summary</pre>	(Optional) Disables automatic summarization. By default, the switch summarizes subprefixes when crossing classful network boundaries. Disable summarization (RIP Version 2 only) to advertise subnet and host routing information to classful network boundaries.
<b>Step 11</b>	<b>output-delay delay</b> <b>Example:</b> <pre>Switch(config-router)# output-delay 8</pre>	(Optional) Adds interpacket delay for RIP updates sent. By default, packets in a multiple-packet RIP update have no delay added between packets. If you are sending packets to a lower-speed device, you can add an interpacket delay in the range of 8 to 50 milliseconds.
<b>Step 12</b>	<b>end</b> <b>Example:</b> <pre>Switch(config-router)# end</pre>	Returns to privileged EXEC mode.
<b>Step 13</b>	<b>show ip protocols</b> <b>Example:</b> <pre>Switch# show ip protocols</pre>	Verifies your entries.
<b>Step 14</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Configuring RIP Authentication

RIP Version 1 does not support authentication. If you are sending and receiving RIP Version 2 packets, you can enable RIP authentication on an interface. The key chain specifies the set of keys that can be used on the interface. If a key chain is not configured, no authentication is performed, not even the default.

The Device supports two modes of authentication on interfaces for which RIP authentication is enabled: plain text and MD5. The default is plain text.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-id</i></b> <b>Example:</b> <pre>Switch(config)# interface gigabitethernet 1/0/1</pre>	Enters interface configuration mode, and specifies the interface to configure.
<b>Step 4</b>	<b>ip rip authentication key-chain <i>name-of-chain</i></b> <b>Example:</b> <pre>Switch(config-if)# ip rip authentication key-chain trees</pre>	Enables RIP authentication.
<b>Step 5</b>	<b>ip rip authentication mode {text   md5}</b> <b>Example:</b> <pre>Switch(config-if)# ip rip authentication mode md5</pre>	Configures the interface to use plain text authentication (the default) or MD5 digest authentication.
<b>Step 6</b>	<b>end</b> <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 7</b>	<b>show running-config</b> <b>Example:</b> <pre>Switch# show running-config</pre>	Verifies your entries.
<b>Step 8</b>	<b>copy running-config startup-config</b> <b>Example:</b>	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	Switch# <code>copy running-config startup-config</code>	

## Summary Addresses and Split Horizon

Routers connected to broadcast-type IP networks and using distance-vector routing protocols normally use the split-horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router on any interface from which that information originated. This feature usually optimizes communication among multiple routers, especially when links are broken.

## Configuring Summary Addresses and Split Horizon



**Note** In general, disabling split horizon is not recommended unless you are certain that your application requires it to properly advertise routes.

If you want to configure an interface running RIP to advertise a summarized local IP address pool on a network access server for dial-up clients, use the **ip summary-address rip** interface configuration command.



**Note** If split horizon is enabled, neither autosummary nor interface IP summary addresses are advertised.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Switch> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-id</i></b> <b>Example:</b> Switch(config)# <code>interface gigabitethernet 1/0/1</code>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.



	Command or Action	Purpose
Step 4	<b>ip address</b> <i>ip-address subnet-mask</i> <b>Example:</b>  Switch(config-if)# <b>ip address</b> 10.1.1.10 255.255.255.0	Configures the IP address and IP subnet.
Step 5	<b>ip summary-address rip</b> <i>ip-address ip-network mask</i> <b>Example:</b>  Switch(config-if)# <b>ip summary-address rip</b> 10.1.1.30 255.255.255.0	Configures the IP address to be summarized and the IP network mask.
Step 6	<b>no ip split-horizon</b> <b>Example:</b>  Switch(config-if)# <b>no ip split-horizon</b>	Disables split horizon on the interface.
Step 7	<b>end</b> <b>Example:</b>  Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
Step 8	<b>show ip interface</b> <i>interface-id</i> <b>Example:</b>  Switch# <b>show ip interface gigabitethernet 1/0/1</b>	Verifies your entries.
Step 9	<b>copy running-config startup-config</b> <b>Example:</b>  Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Configuring Split Horizon

Routers connected to broadcast-type IP networks and using distance-vector routing protocols normally use the split-horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router on any interface from which that information originated. This feature can optimize communication among multiple routers, especially when links are broken.



**Note** In general, we do not recommend disabling split horizon unless you are certain that your application requires it to properly advertise routes.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-id</i></b> <b>Example:</b> Switch(config)# <b>interface gigabitethernet 1/0/1</b>	Enters interface configuration mode, and specifies the interface to configure.
<b>Step 4</b>	<b>ip address <i>ip-address subnet-mask</i></b> <b>Example:</b> Switch(config-if)# <b>ip address 10.1.1.10 255.255.255.0</b>	Configures the IP address and IP subnet.
<b>Step 5</b>	<b>no ip split-horizon</b> <b>Example:</b> Switch(config-if)# <b>no ip split-horizon</b>	Disables split horizon on the interface.
<b>Step 6</b>	<b>end</b> <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 7</b>	<b>show ip interface <i>interface-id</i></b> <b>Example:</b> Switch# <b>show ip interface gigabitethernet 1/0/1</b>	Verifies your entries.
<b>Step 8</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Configuration Example for Summary Addresses and Split Horizon

In this example, the major net is 10.0.0.0. The summary address 10.2.0.0 overrides the autosummary address of 10.0.0.0 so that 10.2.0.0 is advertised out interface Gigabit Ethernet port 2, and 10.0.0.0 is not advertised. In the example, if the interface is still in Layer 2 mode (the default), you must enter a **no switchport** interface configuration command before entering the **ip address** interface configuration command.



**Note** If split horizon is enabled, neither autosummary nor interface summary addresses (those configured with the **ip summary-address rip** router configuration command) are advertised.

```
Switch(config)# router rip
Switch(config-router)# interface gigabitethernet1/0/2
Switch(config-if)# ip address 10.1.5.1 255.255.255.0
Switch(config-if)# ip summary-address rip 10.2.0.0 255.255.0.0
Switch(config-if)# no ip split-horizon
Switch(config-if)# exit
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
Switch(config-router)# neighbor 2.2.2.2 peer-group mygroup
Switch(config-router)# end
```

## Information About OSPF

OSPF is an Interior Gateway Protocol (IGP) designed expressly for IP networks, supporting IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets. The Cisco implementation supports RFC 1253, OSPF management information base (MIB).

The Cisco implementation conforms to the OSPF Version 2 specifications with these key features:

- Definition of stub areas is supported.
- Routes learned through any IP routing protocol can be redistributed into another IP routing protocol. At the intradomain level, this means that OSPF can import routes learned through EIGRP and RIP. OSPF routes can also be exported into RIP.
- Plain text and MD5 authentication among neighboring routers within an area is supported.
- Configurable routing interface parameters include interface output cost, retransmission interval, interface transmit delay, router priority, router dead and hello intervals, and authentication key.
- Virtual links are supported.
- Not-so-stubby-areas (NSSAs) per RFC 1587 are supported.

OSPF typically requires coordination among many internal routers, area border routers (ABRs) connected to multiple areas, and autonomous system boundary routers (ASBRs). The minimum configuration would use all default parameter values, no authentication, and interfaces assigned to areas. If you customize your environment, you must ensure coordinated configuration of all routers.

# How to Configure OSPF

## Default OSPF Configuration

*Table 5: Default OSPF Configuration*

Feature	Default Setting
Interface parameters	Cost: No default cost predefined Retransmit interval: 5 seconds. Transmit delay: 1 second. Priority: 1. Hello interval: 10 seconds. Dead interval: 4 times the hello interval. No authentication. No password specified. MD5 authentication disabled.
Area	Authentication type: 0 (no authentication). Default cost: 1. Range: Disabled. Stub: No stub area defined. NSSA: No NSSA area defined.
Auto cost	100 Mb/s.
Default-information originate	Disabled. When enabled, the default metric setting is 10, and the external route type is Type 2.
Default metric	Built-in, automatic metric translation, as appropriate for each routing protocol.
Distance OSPF	dist1 (all routes within an area): 110. dist2 (all routes from one area to another): 110. dist3 (routes from other routing domains): 110.
OSPF database filter	Disabled. All outgoing link-state advertisements (LSAs) are flooded to the interface.
IP OSPF name lookup	Disabled.
Log adjacency changes	Enabled.
Neighbor	None specified.
Neighbor database filter	Disabled. All outgoing LSAs are flooded to the neighbor.
Network area	Disabled.

Feature	Default Setting
Nonstop Forwarding (NSF) awareness	Enabled. Allows Layer 3 Device to continue forwarding packets from a neighbor NSF-capable router during hardware or software changes.
NSF capability	Disabled. <b>Note</b> The Device stack supports OSPF NSF-capable routing for IPv4.
Router ID	No OSPF routing process defined.
Summary address	Disabled.
Timers LSA group pacing	240 seconds.
Timers shortest path first (spf)	spf delay: 5 seconds.; spf-holdtime: 10 seconds.
Virtual link	No area ID or router ID defined. Hello interval: 10 seconds. Retransmit interval: 5 seconds. Transmit delay: 1 second. Dead interval: 40 seconds. Authentication key: no key predefined. Message-digest key (MD5): no key predefined.

### OSPF for Routed Access

With Cisco IOS Release 12.2(55)SE, the IP Base image supports OSPF for routed access. The IP services image is required if you need multiple OSPFv2 and OSPFv3 instances without route restrictions. Additionally, the IP services image is required to enable the multi-VRF-CE feature.

OSPF for Routed Access is specifically designed so that you can extend Layer 3 routing capabilities to the wiring closet.



**Note** OSPF for Routed Access supports only one OSPFv2 and one OSPFv3 instance with a combined total of 1000 dynamically learned routes. The IP Base image provides OSPF for routed access.

However, these restrictions are not enforced in this release.

With the typical topology (hub and spoke) in a campus environment, where the wiring closets (spokes) are connected to the distribution switch (hub) that forwards all nonlocal traffic to the distribution layer, the wiring closet Device need not hold a complete routing table. A best practice design, where the distribution Device sends a default route to the wiring closet Device to reach interarea and external routes (OSPF stub or totally stub area configuration) should be used when OSPF for Routed Access is used in the wiring closet.

For more details, see the “High Availability Campus Network Design—Routed Access Layer using EIGRP or OSPF” document.

## OSPF Nonstop Forwarding

The Device or switch stack supports two levels of nonstop forwarding (NSF):

- [OSPF NSF Awareness, on page 38](#)
- [OSPF NSF Capability, on page 38](#)

### OSPF NSF Awareness

When the neighboring router is NSF-capable, the Layer 3 Device continues to forward packets from the neighboring router during the interval between the primary Route Processor (RP) in a router crashing and the backup RP taking over, or while the primary RP is manually reloaded for a non-disruptive software upgrade.

This feature cannot be disabled.

### OSPF NSF Capability

supports the OSPFv2 NSF IETF format in addition to the OSPFv2 NSF Cisco format that is supported in earlier releases. For information about this feature, see : *NSF—OSPF (RFC 3623 OSPF Graceful Restart)*.

The also supports OSPF NSF-capable routing for IPv4 for better convergence and lower traffic loss following a stack's active switch change.



**Note** OSPF NSF requires that all neighbor networking devices be NSF-aware. If an NSF-capable router discovers non-NSF aware neighbors on a network segment, it disables NSF capabilities for that segment. Other network segments where all devices are NSF-aware or NSF-capable continue to provide NSF capabilities.

Use the **nsf** OSPF routing configuration command to enable OSPF NSF routing. Use the **show ip ospf** privileged EXEC command to verify that it is enabled.

For more information, see *Cisco Nonstop Forwarding*:

[http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-nonstp\\_fwdg.html](http://www.cisco.com/en/US/docs/ios/ha/configuration/guide/ha-nonstp_fwdg.html)

## Configuring Basic OSPF Parameters

To enable OSPF, create an OSPF routing process, specify the range of IP addresses to associate with the routing process, and assign area IDs to be associated with that range.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>router ospf process-id</b> <b>Example:</b> Switch(config)# <b>router ospf 15</b>	Enables OSPF routing, and enter router configuration mode. The process ID is an internally used identification parameter that is locally assigned and can be any positive integer. Each OSPF routing process has a unique value.

	Command or Action	Purpose
		<b>Note</b> OSPF for Routed Access supports only one OSPFv2 and one OSPFv3 instance with a maximum number of 1000 dynamically learned routes.
<b>Step 3</b>	<b>network</b> <i>address wildcard-mask</i> <b>area</b> <i>area-id</i> <b>Example:</b> Switch(config-router)# <b>network</b> 10.1.1.1 255.240.0.0 <b>area</b> 20	Define an interface on which OSPF runs and the area ID for that interface. You can use the wildcard-mask to use a single command to define one or more multiple interfaces to be associated with a specific OSPF area. The area ID can be a decimal value or an IP address.
<b>Step 4</b>	<b>end</b> <b>Example:</b> Switch(config-router)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show ip protocols</b> <b>Example:</b> Switch# <b>show ip protocols</b>	Verifies your entries.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Example: Configuring Basic OSPF Parameters

This example shows how to configure an OSPF routing process and assign it a process number of 109:

```
Switch(config)# router ospf 109
Switch(config-router)# network 131.108.0.0 255.255.255.0 area 24
```

## Configuring OSPF Interfaces

You can use the **ip ospf** interface configuration commands to modify interface-specific OSPF parameters. You are not required to modify any of these parameters, but some interface parameters (hello interval, dead interval, and authentication key) must be consistent across all routers in an attached network. If you modify these parameters, be sure all routers in the network have compatible values.



**Note** The **ip ospf** interface configuration commands are all optional.

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>interface interface-id</b> <b>Example:</b>  Switch(config)# <b>interface gigabitethernet 1/0/1</b>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
<b>Step 3</b>	<b>ip ospf cost cost</b> <b>Example:</b>  Switch(config-if)# <b>ip ospf cost 8</b>	(Optional) Explicitly specifies the cost of sending a packet on the interface.
<b>Step 4</b>	<b>ip ospf retransmit-interval seconds</b> <b>Example:</b>  Switch(config-if)# <b>ip ospf transmit-interval 10</b>	(Optional) Specifies the number of seconds between link state advertisement transmissions. The range is 1 to 65535 seconds. The default is 5 seconds.
<b>Step 5</b>	<b>ip ospf transmit-delay seconds</b> <b>Example:</b>  Switch(config-if)# <b>ip ospf transmit-delay 2</b>	(Optional) Sets the estimated number of seconds to wait before sending a link state update packet. The range is 1 to 65535 seconds. The default is 1 second.
<b>Step 6</b>	<b>ip ospf priority number</b> <b>Example:</b>  Switch(config-if)# <b>ip ospf priority 5</b>	(Optional) Sets priority to help find the OSPF designated router for a network. The range is from 0 to 255. The default is 1.
<b>Step 7</b>	<b>ip ospf hello-interval seconds</b> <b>Example:</b>  Switch(config-if)# <b>ip ospf hello-interval 12</b>	(Optional) Sets the number of seconds between hello packets sent on an OSPF interface. The value must be the same for all nodes on a network. The range is 1 to 65535 seconds. The default is 10 seconds.
<b>Step 8</b>	<b>ip ospf dead-interval seconds</b> <b>Example:</b>  Switch(config-if)# <b>ip ospf dead-interval 8</b>	(Optional) Sets the number of seconds after the last device hello packet was seen before its neighbors declare the OSPF router to be down. The value must be the same for all nodes on a network. The range is 1 to 65535 seconds. The default is 4 times the hello interval.
<b>Step 9</b>	<b>ip ospf authentication-key key</b> <b>Example:</b>	(Optional) Assign a password to be used by neighboring OSPF routers. The password can be any string of keyboard-entered characters up to 8 bytes in length. All



	Command or Action	Purpose
	Switch(config-if)# ip ospf authentication-key password	neighboring routers on the same network must have the same password to exchange OSPF information.
<b>Step 10</b>	<b>ip ospf message-digest-key</b> <i>keyid</i> <b>md5</b> <i>key</i> <b>Example:</b> Switch(config-if)# ip ospf message digest-key 16 md5 yourlpass	(Optional) Enables MDS authentication. <ul style="list-style-type: none"> <li>• <i>keyid</i>—An identifier from 1 to 255.</li> <li>• <i>key</i>—An alphanumeric password of up to 16 bytes.</li> </ul>
<b>Step 11</b>	<b>ip ospf database-filter all out</b> <b>Example:</b> Switch(config-if)# ip ospf database-filter all out	(Optional) Block flooding of OSPF LSA packets to the interface. By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives.
<b>Step 12</b>	<b>end</b> <b>Example:</b> Switch(config)# end	Returns to privileged EXEC mode.
<b>Step 13</b>	<b>show ip ospf interface</b> [ <i>interface-name</i> ] <b>Example:</b> Switch# show ip ospf interface	Displays OSPF-related interface information.
<b>Step 14</b>	<b>show ip ospf neighbor detail</b> <b>Example:</b> Switch# show ip ospf neighbor detail	Displays NSF awareness status of neighbor switch. The output matches one of these examples: <ul style="list-style-type: none"> <li>• <i>Options is 0x52</i> <i>LLS Options is 0x1 (LR)</i> When both of these lines appear, the neighbor switch is NSF aware.</li> <li>• <i>Options is 0x42</i>—This means the neighbor switch is not NSF aware.</li> </ul>
<b>Step 15</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## OSPF Area Parameters

You can optionally configure several OSPF area parameters. These parameters include authentication for password-based protection against unauthorized access to an area, stub areas, and not-so-stubby-areas (NSSAs). Stub areas are areas into which information on external routes is not sent. Instead, the area border router (ABR)

generates a default external route into the stub area for destinations outside the autonomous system (AS). An NSSA does not flood all LSAs from the core into the area, but can import AS external routes within the area by redistribution.

Route summarization is the consolidation of advertised addresses into a single summary route to be advertised by other areas. If network numbers are contiguous, you can use the **area range** router configuration command to configure the ABR to advertise a summary route that covers all networks in the range.

## Configuring OSPF Area Parameters

### Before you begin



**Note** The OSPF **area** router configuration commands are all optional.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>router ospf process-id</b> <b>Example:</b>  Switch(config)# <b>router ospf 109</b>	Enables OSPF routing, and enter router configuration mode.
<b>Step 3</b>	<b>area area-id authentication</b> <b>Example:</b>  Switch(config-router)# <b>area 1 authentication</b>	(Optional) Allow password-based protection against unauthorized access to the identified area. The identifier can be either a decimal value or an IP address.
<b>Step 4</b>	<b>area area-id authentication message-digest</b> <b>Example:</b>  Switch(config-router)# <b>area 1 authentication message-digest</b>	(Optional) Enables MD5 authentication on the area.
<b>Step 5</b>	<b>area area-id stub [no-summary]</b> <b>Example:</b>  Switch(config-router)# <b>area 1 stub</b>	(Optional) Define an area as a stub area. The <b>no-summary</b> keyword prevents an ABR from sending summary link advertisements into the stub area.
<b>Step 6</b>	<b>area area-id nssa [no-redistribution] [default-information-originate] [no-summary]</b> <b>Example:</b>	(Optional) Defines an area as a not-so-stubby-area. Every router within the same area must agree that the area is NSSA. Select one of these keywords:

	Command or Action	Purpose
	<pre>Switch(config-router)# area 1 nssa default-information-originate</pre>	<ul style="list-style-type: none"> <li>• <b>no-redistribution</b>—Select when the router is an NSSA ABR and you want the <b>redistribute</b> command to import routes into normal areas, but not into the NSSA.</li> <li>• <b>default-information-originate</b>—Select on an ABR to allow importing type 7 LSAs into the NSSA.</li> <li>• <b>no-redistribution</b>—Select to not send summary LSAs into the NSSA.</li> </ul>
<b>Step 7</b>	<p><b>area</b> <i>area-id</i> <b>range</b> <i>address mask</i></p> <p><b>Example:</b></p> <pre>Switch(config-router)# area 1 range 255.240.0.0</pre>	(Optional) Specifies an address range for which a single route is advertised. Use this command only with area border routers.
<b>Step 8</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 9</b>	<p><b>show ip ospf</b> [<i>process-id</i>]</p> <p><b>Example:</b></p> <pre>Switch# show ip ospf</pre>	Displays information about the OSPF routing process in general or for a specific process ID to verify configuration.
<b>Step 10</b>	<p><b>show ip ospf</b> [<i>process-id</i> [<i>area-id</i>]] <b>database</b></p> <p><b>Example:</b></p> <pre>Switch# show ip ospf database</pre>	Displays lists of information related to the OSPF database for a specific router.
<b>Step 11</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Other OSPF Parameters

You can optionally configure other OSPF parameters in router configuration mode.

- **Route summarization:** When redistributing routes from other protocols. Each route is advertised individually in an external LSA. To help decrease the size of the OSPF link state database, you can use the **summary-address** router configuration command to advertise a single router for all the redistributed routes included in a specified network address and mask.
- **Virtual links:** In OSPF, all areas must be connected to a backbone area. You can establish a virtual link in case of a backbone-continuity break by configuring two Area Border Routers as endpoints of a virtual link. Configuration information includes the identity of the other virtual endpoint (the other ABR) and

the nonbackbone link that the two routers have in common (the transit area). Virtual links cannot be configured through a stub area.

- **Default route:** When you specifically configure redistribution of routes into an OSPF routing domain, the route automatically becomes an autonomous system boundary router (ASBR). You can force the ASBR to generate a default route into the OSPF routing domain.
- **Domain Name Server (DNS) names for use in all OSPF `show` privileged EXEC command displays** makes it easier to identify a router than displaying it by router ID or neighbor ID.
- **Default Metrics:** OSPF calculates the OSPF metric for an interface according to the bandwidth of the interface. The metric is calculated as *ref-bw* divided by bandwidth, where *ref* is 10 by default, and bandwidth (*bw*) is specified by the **bandwidth** interface configuration command. For multiple links with high bandwidth, you can specify a larger number to differentiate the cost on those links.
- **Administrative distance** is a rating of the trustworthiness of a routing information source, an integer between 0 and 255, with a higher value meaning a lower trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. OSPF uses three different administrative distances: routes within an area (interarea), routes to another area (interarea), and routes from another routing domain learned through redistribution (external). You can change any of the distance values.
- **Passive interfaces:** Because interfaces between two devices on an Ethernet represent only one network segment, to prevent OSPF from sending hello packets for the sending interface, you must configure the sending device to be a passive interface. Both devices can identify each other through the hello packet for the receiving interface.
- **Route calculation timers:** You can configure the delay time between when OSPF receives a topology change and when it starts the shortest path first (SPF) calculation and the hold time between two SPF calculations.
- **Log neighbor changes:** You can configure the router to send a syslog message when an OSPF neighbor state changes, providing a high-level view of changes in the router.

## Configuring Other OSPF Parameters

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>router ospf <i>process-id</i></b> <b>Example:</b> Switch(config)# <code>router ospf 10</code>	Enables OSPF routing, and enter router configuration mode.

	Command or Action	Purpose
Step 3	<p><b>summary-address</b> <i>address mask</i></p> <p><b>Example:</b></p> <pre>Switch(config)# summary-address 10.1.1.1 255.255.255.0</pre>	(Optional) Specifies an address and IP subnet mask for redistributed routes so that only one summary route is advertised.
Step 4	<p><b>area</b> <i>area-id</i> <b>virtual-link</b> <i>router-id</i> [<b>hello-interval</b> <i>seconds</i>] [<b>retransmit-interval</b> <i>seconds</i>] [<b>trans</b> [<b>authentication-key</b> <i>key</i>]   <b>message-digest-key</b> <i>keyid md5 key</i>]</p> <p><b>Example:</b></p> <pre>Switch(config)# area 2 virtual-link 192.168.255.1 hello-interval 5</pre>	(Optional) Establishes a virtual link and set its parameters.
Step 5	<p><b>default-information originate</b> [<b>always</b>] [<b>metric</b> <i>metric-value</i>] [<b>metric-type</b> <i>type-value</i>] [<b>route-map</b> <i>map-name</i>]</p> <p><b>Example:</b></p> <pre>Switch(config)# default-information originate metric 100 metric-type 1</pre>	(Optional) Forces the ASBR to generate a default route into the OSPF routing domain. Parameters are all optional.
Step 6	<p><b>ip ospf name-lookup</b></p> <p><b>Example:</b></p> <pre>Switch(config)# ip ospf name-lookup</pre>	(Optional) Configures DNS name lookup. The default is disabled.
Step 7	<p><b>ip auto-cost reference-bandwidth</b> <i>ref-bw</i></p> <p><b>Example:</b></p> <pre>Switch(config)# ip auto-cost reference-bandwidth 5</pre>	(Optional) Specifies an address range for which a single route will be advertised. Use this command only with area border routers.
Step 8	<p><b>distance ospf</b> {[<b>inter-area</b> <i>dist1</i>] [<b>inter-area</b> <i>dist2</i>] [<b>external</b> <i>dist3</i>]}</p> <p><b>Example:</b></p> <pre>Switch(config)# distance ospf inter-area 150</pre>	(Optional) Changes the OSPF distance values. The default distance for each type of route is 110. The range is 1 to 255.
Step 9	<p><b>passive-interface</b> <i>type number</i></p> <p><b>Example:</b></p> <pre>Switch(config)# passive-interface gigabitethernet 1/0/6</pre>	(Optional) Suppresses the sending of hello packets through the specified interface.
Step 10	<p><b>timers throttle spf</b> <i>spf-delay</i> <i>spf-holdtime</i> <i>spf-wait</i></p> <p><b>Example:</b></p>	(Optional) Configures route calculation timers.

	Command or Action	Purpose
	Switch(config)# timers throttle spf 200 100 100	<ul style="list-style-type: none"> <li>• <i>spf-delay</i>—Delay between receiving a change to SPF calculation. The range is from 1 to 600000 in milliseconds.</li> <li>• <i>spf-holdtime</i>—Delay between first and second SPF calculation. The range is from 1 to 600000 in milliseconds.</li> <li>• <i>spf-wait</i>—Maximum wait time in milliseconds for SPF calculations. The range is from 1 to 600000 in milliseconds.</li> </ul>
<b>Step 11</b>	<b>ospf log-adj-changes</b> <b>Example:</b> Switch(config)# ospf log-adj-changes	(Optional) Sends syslog message when a neighbor state changes.
<b>Step 12</b>	<b>end</b> <b>Example:</b> Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 13</b>	<b>show ip ospf [process-id [area-id]] database</b> <b>Example:</b> Switch# show ip ospf database	Displays lists of information related to the OSPF database for a specific router.
<b>Step 14</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## LSA Group Pacing

The OSPF LSA group pacing feature allows the router to group OSPF LSAs and pace the refreshing, check-summing, and aging functions for more efficient router use. This feature is enabled by default with a 4-minute default pacing interval, and you will not usually need to modify this parameter. The optimum group pacing interval is inversely proportional to the number of LSAs the router is refreshing, check-summing, and aging. For example, if you have approximately 10,000 LSAs in the database, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

## Changing LSA Group Pacing

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>router ospf <i>process-id</i></b> <b>Example:</b>  Switch(config)# <code>router ospf 25</code>	Enables OSPF routing, and enter router configuration mode.
<b>Step 3</b>	<b>timers lsa-group-pacing <i>seconds</i></b> <b>Example:</b>  Switch(config-router)# <code>timers lsa-group-pacing 15</code>	Changes the group pacing of LSAs.
<b>Step 4</b>	<b>end</b> <b>Example:</b>  Switch(config)# <code>end</code>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show running-config</b> <b>Example:</b>  Switch# <code>show running-config</code>	Verifies your entries.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b>  Switch# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

## Loopback Interfaces

OSPF uses the highest IP address configured on the interfaces as its router ID. If this interface is down or removed, the OSPF process must recalculate a new router ID and resend all its routing information out its interfaces. If a loopback interface is configured with an IP address, OSPF uses this IP address as its router ID, even if other interfaces have higher IP addresses. Because loopback interfaces never fail, this provides greater stability. OSPF automatically prefers a loopback interface over other interfaces, and it chooses the highest IP address among all loopback interfaces.

## Configuring a Loopback Interface

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>interface loopback 0</b> <b>Example:</b>  Switch(config)# <code>interface loopback 0</code>	Creates a loopback interface, and enter interface configuration mode.
<b>Step 3</b>	<b>ip address address mask</b> <b>Example:</b>  Switch(config-if)# <code>ip address 10.1.1.5 255.255.240.0</code>	Assign an IP address to this interface.
<b>Step 4</b>	<b>end</b> <b>Example:</b>  Switch(config)# <code>end</code>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show ip interface</b> <b>Example:</b>  Switch# <code>show ip interface</code>	Verifies your entries.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b>  Switch# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

## Monitoring OSPF

You can display specific statistics such as the contents of IP routing tables, caches, and databases.

**Table 6: Show IP OSPF Statistics Commands**

<code>show ip ospf [process-id]</code>	Displays general information about OSPF processes.
--	--



<b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>router</b> ] [ <i>link-state-id</i> ]	Displays lists of information.
<b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>router</b> ] [ <b>self-originate</b> ]	
<b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>router</b> ] [ <b>adv-router</b> [ <i>ip-address</i> ]]	
<b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>network</b> ] [ <i>link-state-id</i> ]	
<b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>summary</b> ] [ <i>link-state-id</i> ]	
<b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>asbr-summary</b> ] [ <i>link-state-id</i> ]	
<b>show ip ospf</b> [ <i>process-id</i> ] <b>database</b> [ <b>external</b> ] [ <i>link-state-id</i> ]	
<b>show ip ospf</b> [ <i>process-id area-id</i> ] <b>database</b> [ <b>database-summary</b> ]	
<b>show ip ospf border-routes</b>	Displays the internal entries.
<b>show ip ospf interface</b> [ <i>interface-name</i> ]	Displays OSPF-related information.
<b>show ip ospf neighbor</b> [ <i>interface-name</i> ] [ <i>neighbor-id</i> ] <b>detail</b>	Displays OSPF neighbor information.
<b>show ip ospf virtual-links</b>	Displays OSPF-related information.

## Information About EIGRP

Enhanced IGRP (EIGRP) is a Cisco proprietary enhanced version of the IGRP. EIGRP uses the same distance vector algorithm and distance information as IGRP; however, the convergence properties and the operating efficiency of EIGRP are significantly improved.

The convergence technology employs an algorithm referred to as the Diffusing Update Algorithm (DUAL), which guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize at the same time. Routers that are not affected by topology changes are not involved in recomputations.

IP EIGRP provides increased network width. With RIP, the largest possible width of your network is 15 hops. Because the EIGRP metric is large enough to support thousands of hops, the only barrier to expanding the network is the transport-layer hop counter. EIGRP increments the transport control field only when an IP packet has traversed 15 routers and the next hop to the destination was learned through EIGRP. When a RIP route is used as the next hop to the destination, the transport control field is incremented as usual.

## EIGRP Features

EIGRP offers these features:

- Fast convergence.
- Incremental updates when the state of a destination changes, instead of sending the entire contents of the routing table, minimizing the bandwidth required for EIGRP packets.
- Less CPU usage because full update packets need not be processed each time they are received.
- Protocol-independent neighbor discovery mechanism to learn about neighboring routers.

- Variable-length subnet masks (VLSMs).
- Arbitrary route summarization.
- EIGRP scales to large networks.

## EIGRP Components

EIGRP has these four basic components:

- Neighbor discovery and recovery is the process that routers use to dynamically learn of other routers on their directly attached networks. Routers must also discover when their neighbors become unreachable or inoperative. Neighbor discovery and recovery is achieved with low overhead by periodically sending small hello packets. As long as hello packets are received, the Cisco IOS software can learn that a neighbor is alive and functioning. When this status is determined, the neighboring routers can exchange routing information.
- The reliable transport protocol is responsible for guaranteed, ordered delivery of EIGRP packets to all neighbors. It supports intermixed transmission of multicast and unicast packets. Some EIGRP packets must be sent reliably, and others need not be. For efficiency, reliability is provided only when necessary. For example, on a multiaccess network that has multicast capabilities (such as Ethernet), it is not necessary to send hellos reliably to all neighbors individually. Therefore, EIGRP sends a single multicast hello with an indication in the packet informing the receivers that the packet need not be acknowledged. Other types of packets (such as updates) require acknowledgment, which is shown in the packet. The reliable transport has a provision to send multicast packets quickly when there are unacknowledged packets pending. Doing so helps ensure that convergence time remains low in the presence of varying speed links.
- The DUAL finite state machine embodies the decision process for all route computations. It tracks all routes advertised by all neighbors. DUAL uses the distance information (known as a metric) to select efficient, loop-free paths. DUAL selects routes to be inserted into a routing table based on feasible successors. A successor is a neighboring router used for packet forwarding that has a least-cost path to a destination that is guaranteed not to be part of a routing loop. When there are no feasible successors, but there are neighbors advertising the destination, a recomputation must occur. This is the process whereby a new successor is determined. The amount of time it takes to recompute the route affects the convergence time. Recomputation is processor-intensive; it is advantageous to avoid recomputation if it is not necessary. When a topology change occurs, DUAL tests for feasible successors. If there are feasible successors, it uses any it finds to avoid unnecessary recomputation.
- The protocol-dependent modules are responsible for network layer protocol-specific tasks. An example is the IP EIGRP module, which is responsible for sending and receiving EIGRP packets that are encapsulated in IP. It is also responsible for parsing EIGRP packets and informing DUAL of the new information received. EIGRP asks DUAL to make routing decisions, but the results are stored in the IP routing table. EIGRP is also responsible for redistributing routes learned by other IP routing protocols.



---

**Note** To enable EIGRP, the Device or active switch must be running the

---

# How to Configure EIGRP

To create an EIGRP routing process, you must enable EIGRP and associate networks. EIGRP sends updates to the interfaces in the specified networks. If you do not specify an interface network, it is not advertised in any EIGRP update.



**Note** If you have routers on your network that are configured for IGRP, and you want to change to EIGRP, you must designate transition routers that have both IGRP and EIGRP configured. In these cases, perform Steps 1 through 3 in the next section and also see the “Configuring Split Horizon” section. You must use the same AS number for routes to be automatically redistributed.

## Default EIGRP Configuration

*Table 7: Default EIGRP Configuration*

Feature	Default Setting
Auto summary	Disabled.
Default-information	Exterior routes are accepted and default information is passed between processes when doing redistribution.
Default metric	Only connected routes and interface static routes can be redistributed with the default metric. The metric includes: <ul style="list-style-type: none"> <li>• Bandwidth: 0 or greater kb/s.</li> <li>• Delay (tens of microseconds): 0 or any positive number that is less than 39.1 nanoseconds.</li> <li>• Reliability: any number between 0 and 255 (255 means 100 percent reliability).</li> <li>• Loading: effective bandwidth as a number between 0 and 255 (255 means 100 percent loading).</li> <li>• MTU: maximum transmission unit size of the route in bytes. 0 or any positive integer.</li> </ul>
Distance	Internal distance: 90. External distance: 170.
EIGRP log-neighbor changes	Disabled. No adjacency changes logged.
IP authentication key-chain	No authentication provided.
IP authentication mode	No authentication provided.
IP bandwidth-percent	50 percent.

Feature	Default Setting
IP hello interval	For low-speed nonbroadcast multiaccess (NBMA) networks: 60 seconds; for other networks: 5 seconds.
IP hold-time	For low-speed NBMA networks: 180 seconds; all other networks: 15 seconds.
IP split-horizon	Enabled.
IP summary address	No summary aggregate addresses are predefined.
Metric weights	tos: 0; k1 and k3: 1; k2, k4, and k5: 0
Network	None specified.
Nonstop Forwarding (NSF) Awareness	Enabled for IPv4 on switches running the Allows Layer 3 switches to continue forwarding packets from a neighboring NSF-capable router during hardware and software changes.
NSF capability	Disabled. <b>Note</b> The Device supports EIGRP NSF-capable routing for IPv4.
Offset-list	Disabled.
Router EIGRP	Disabled.
Set metric	No metric set in the route map.
Traffic-share	Distributed proportionately to the ratios of the metrics.
Variance	1 (equal-cost load-balancing).

## EIGRP Nonstop Forwarding

The Device stack supports two levels of EIGRP nonstop forwarding:

- EIGRP NSF Awareness
- EIGRP NSF Capability

### EIGRP NSF Awareness

The Device supports EIGRP NSF Awareness for IPv4. When the neighboring router is NSF-capable, the Layer 3 Device continues to forward packets from the neighboring router during the interval between the primary Route Processor (RP) in a router failing and the backup RP taking over, or while the primary RP is manually reloaded for a nondisruptive software upgrade.

This feature cannot be disabled. For more information on this feature, see the “EIGRP Nonstop Forwarding (NSF) Awareness” section of the *Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4*.

### EIGRP NSF Capability

The Device supports EIGRP Cisco NSF routing to speed up convergence and to eliminate traffic loss after a stack's active switch changeover.

The also supports EIGRP NSF-capable routing for IPv4 for better convergence and lower traffic loss following an active switch changeover. When an EIGRP NSF-capable active switch restarts or a new active switch starts up and NSF restarts, the Device has no neighbors, and the topology table is empty. The Device must bring up the interfaces, reacquire neighbors, and rebuild the topology and routing tables without interrupting the traffic directed toward the Device stack. EIGRP peer routers maintain the routes learned from the new active switch and continue forwarding traffic through the NSF restart process.

To prevent an adjacency reset by the neighbors, the new active switch uses a new Restart (RS) bit in the EIGRP packet header to show the restart. When the neighbor receives this, it synchronizes the stack in its peer list and maintains the adjacency with the stack. The neighbor then sends its topology table to the active switch with the RS bit set to show that it is NSF-aware and is aiding the new active switch.

If at least one of the stack peer neighbors is NSF-aware, the active switch receives updates and rebuilds its database. Each NSF-aware neighbor sends an end of table (EOT) marker in the last update packet to mark the end of the table content. The active switch recognizes the convergence when it receives the EOT marker, and it then begins sending updates. When the active switch has received all EOT markers from its neighbors or when the NSF converge timer expires, EIGRP notifies the routing information database (RIB) of convergence and floods its topology table to all NSF-aware peers.

## Configuring Basic EIGRP Parameters

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>router eigrp</b> autonomous-system <b>Example:</b> Switch(config)# <code>router eigrp 10</code>	Enables an EIGRP routing process, and enter router configuration mode. The AS number identifies the routes to other EIGRP routers and is used to tag routing information.
<b>Step 3</b>	<b>nsf</b> <b>Example:</b> Switch(config-router)# <code>nsf</code>	(Optional) Enables EIGRP NSF. Enter this command on the active switch and on all of its peers.
<b>Step 4</b>	<b>network</b> network-number <b>Example:</b> Switch(config-router)# <code>network 192.168.0.0</code>	Associate networks with an EIGRP routing process. EIGRP sends updates to the interfaces in the specified networks.
<b>Step 5</b>	<b>eigrp log-neighbor-changes</b> <b>Example:</b>	(Optional) Enables logging of EIGRP neighbor changes to monitor routing system stability.

	Command or Action	Purpose
	Switch(config-router)# <b>eigrp log-neighbor-changes</b>	
<b>Step 6</b>	<b>metric weights</b> <i>tos k1 k2 k3 k4 k5</i> <b>Example:</b> Switch(config-router)# <b>metric weights 0 2 0 2 0 0</b>	(Optional) Adjust the EIGRP metric. Although the defaults have been carefully set to provide excellent operation in most networks, you can adjust them. <b>Caution</b> Setting metrics is complex and is not recommended without guidance from an experienced network designer.
<b>Step 7</b>	<b>offset-list</b> [ <i>access-list number   name</i> ] { <b>in</b>   <b>out</b> } <i>offset</i> [ <i>type number</i> ] <b>Example:</b> Switch(config-router)# <b>offset-list 21 out 10</b>	(Optional) Applies an offset list to routing metrics to increase incoming and outgoing metrics to routes learned through EIGRP. You can limit the offset list with an access list or an interface.
<b>Step 8</b>	<b>auto-summary</b> <b>Example:</b> Switch(config-router)# <b>auto-summary</b>	(Optional) Enables automatic summarization of subnet routes into network-level routes.
<b>Step 9</b>	<b>interface</b> <i>interface-id</i> <b>Example:</b> Switch(config-router)# <b>interface gigabitethernet 1/0/1</b>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
<b>Step 10</b>	<b>ip summary-address eigrp</b> <i>autonomous-system-number address mask</i> <b>Example:</b> Switch(config-if)# <b>ip summary-address eigrp 1 192.168.0.0 255.255.0.0</b>	(Optional) Configures a summary aggregate.
<b>Step 11</b>	<b>end</b> <b>Example:</b> Switch(config-if)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 12</b>	<b>show ip protocols</b> <b>Example:</b> Switch# <b>show ip protocols</b>	Verifies your entries. For NSF awareness, the output shows: *** IP Routing is NSF aware *** EIGRP NSF enabled
<b>Step 13</b>	<b>copy running-config startup-config</b> <b>Example:</b>	(Optional) Saves your entries in the configuration file.

	Command or Action	Purpose
	Switch# <code>copy running-config startup-config</code>	

## Configuring EIGRP Interfaces

Other optional EIGRP parameters can be configured on an interface basis.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>interface <i>interface-id</i></b> <b>Example:</b> Switch(config)# <code>interface gigabitethernet 1/0/1</code>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
<b>Step 3</b>	<b>ip bandwidth-percent eigrp <i>percent</i></b> <b>Example:</b> Switch(config-if)# <code>ip bandwidth-percent eigrp 60</code>	(Optional) Configures the percentage of bandwidth that can be used by EIGRP on an interface. The default is 50 percent.
<b>Step 4</b>	<b>ip summary-address eigrp <i>autonomous-system-number address mask</i></b> <b>Example:</b> Switch(config-if)# <code>ip summary-address eigrp 109 192.161.0.0 255.255.0.0</code>	(Optional) Configures a summary aggregate address for a specified interface (not usually necessary if auto-summary is enabled).
<b>Step 5</b>	<b>ip hello-interval eigrp <i>autonomous-system-number seconds</i></b> <b>Example:</b> Switch(config-if)# <code>ip hello-interval eigrp 109 10</code>	(Optional) Change the hello time interval for an EIGRP routing process. The range is 1 to 65535 seconds. The default is 60 seconds for low-speed NBMA networks and 5 seconds for all other networks.
<b>Step 6</b>	<b>ip hold-time eigrp <i>autonomous-system-number seconds</i></b> <b>Example:</b> Switch(config-if)# <code>ip hold-time eigrp 109 40</code>	(Optional) Change the hold time interval for an EIGRP routing process. The range is 1 to 65535 seconds. The default is 180 seconds for low-speed NBMA networks and 15 seconds for all other networks.  <b>Caution</b> Do not adjust the hold time without consulting Cisco technical support.

	Command or Action	Purpose
<b>Step 7</b>	<b>no ip split-horizon eigrp</b> <i>autonomous-system-number</i> <b>Example:</b>  Switch(config-if)# no ip split-horizon eigrp 109	(Optional) Disables split horizon to allow route information to be advertised by a router out any interface from which that information originated.
<b>Step 8</b>	<b>end</b> <b>Example:</b>  Switch(config)# <b>end</b>	Returns to privileged EXEC mode.
<b>Step 9</b>	<b>show ip eigrp interface</b> <b>Example:</b>  Switch# show ip eigrp interface	Displays which interfaces EIGRP is active on and information about EIGRP relating to those interfaces.
<b>Step 10</b>	<b>copy running-config startup-config</b> <b>Example:</b>  Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Configuring EIGRP Route Authentication

EIGRP route authentication provides MD5 authentication of routing updates from the EIGRP routing protocol to prevent the introduction of unauthorized or false routing messages from unapproved sources.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>interface</b> interface-id <b>Example:</b>  Switch(config)# interface gigabitethernet 1/0/1	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
<b>Step 3</b>	<b>ip authentication mode eigrp</b> <i>autonomous-system</i> <b>md5</b> <b>Example:</b>  Switch(config-if)# ip authentication mode eigrp 104 md5	Enables MD5 authentication in IP EIGRP packets.



	Command or Action	Purpose
Step 4	<p><b>ip authentication key-chain eigrp</b> <i>autonomous-system</i> <i>key-chain</i></p> <p><b>Example:</b></p> <pre>Switch(config-if)# ip authentication key-chain eigrp 105 chain1</pre>	Enables authentication of IP EIGRP packets.
Step 5	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>Switch(config-if)# exit</pre>	Returns to global configuration mode.
Step 6	<p><b>key chain</b> <i>name-of-chain</i></p> <p><b>Example:</b></p> <pre>Switch(config)# key chain chain1</pre>	Identify a key chain and enter key-chain configuration mode. Match the name configured in Step 4.
Step 7	<p><b>key</b> <i>number</i></p> <p><b>Example:</b></p> <pre>Switch(config-keychain)# key 1</pre>	In key-chain configuration mode, identify the key number.
Step 8	<p><b>key-string</b> <i>text</i></p> <p><b>Example:</b></p> <pre>Switch(config-keychain-key)# key-string key1</pre>	In key-chain key configuration mode, identify the key string.
Step 9	<p><b>accept-lifetime</b> <i>start-time</i> {<b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i>}</p> <p><b>Example:</b></p> <pre>Switch(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200</pre>	<p>(Optional) Specifies the time period during which the key can be received.</p> <p>The <i>start-time</i> and <i>end-time</i> syntax can be either <i>hh:mm:ss Month date year</i> or <i>hh:mm:ss date Month year</i>. The default is forever with the default <i>start-time</i> and the earliest acceptable date as January 1, 1993. The default <i>end-time</i> and <b>duration</b> is <b>infinite</b>.</p>
Step 10	<p><b>send-lifetime</b> <i>start-time</i> {<b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i>}</p> <p><b>Example:</b></p> <pre>Switch(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600</pre>	<p>(Optional) Specifies the time period during which the key can be sent.</p> <p>The <i>start-time</i> and <i>end-time</i> syntax can be either <i>hh:mm:ss Month date year</i> or <i>hh:mm:ss date Month year</i>. The default is forever with the default <i>start-time</i> and the earliest acceptable date as January 1, 1993. The default <i>end-time</i> and <b>duration</b> is <b>infinite</b>.</p>
Step 11	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.

	Command or Action	Purpose
<b>Step 12</b>	<b>show key chain</b> <b>Example:</b> Switch# show key chain	Displays authentication key information.
<b>Step 13</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## EIGRP Stub Routing

The EIGRP stub routing feature reduces resource utilization by moving routed traffic closer to the end user.



**Note** The device uses EIGRP stub routing at the access layer to eliminate the need for other types of routing advertisements.

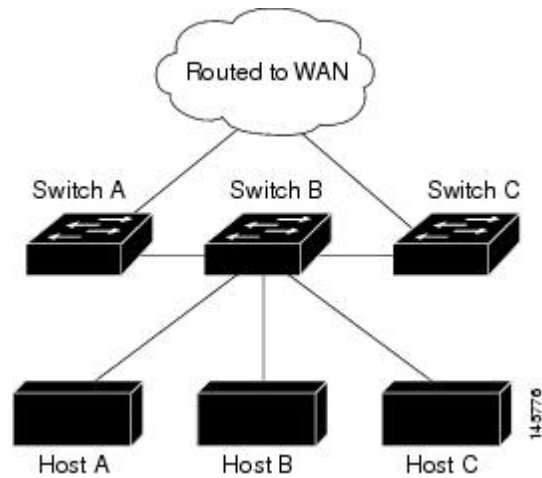
In a network using EIGRP stub routing, the only allowable route for IP traffic to the user is through a device that is configured with EIGRP stub routing. The device sends the routed traffic to interfaces that are configured as user interfaces or are connected to other devices.

When using EIGRP stub routing, you need to configure the distribution and remote routers to use EIGRP and to configure only the device as a stub. Only specified routes are propagated from the device. The device responds to all queries for summaries, connected routes, and routing updates.

Any neighbor that receives a packet informing it of the stub status does not query the stub router for any routes, and a router that has a stub peer does not query that peer. The stub router depends on the distribution router to send the proper updates to all peers.

In the figure given below, device B is configured as an EIGRP stub router. Devices A and C are connected to the rest of the WAN. Device B advertises connected, static, redistribution, and summary routes to Device A and C. Device B does not advertise any routes learned from Device A (and the reverse).

Figure 4: EIGRP Stub Router Configuration



## Monitoring and Maintaining EIGRP

You can delete neighbors from the neighbor table. You can also display various EIGRP routing statistics. The table given below lists the privileged EXEC commands for deleting neighbors and displaying statistics.

Table 8: IP EIGRP Clear and Show Commands

<b>clear ip eigrp neighbors</b> [ <i>if-address</i>   <i>interface</i> ]	Deletes neighbors from the neighbor table.
<b>show ip eigrp interface</b> [ <i>interface</i> ] [ <i>as number</i> ]	Displays information about interfaces participating in EIGRP.
<b>show ip eigrp neighbors</b> [ <i>type-number</i> ]	Displays EIGRP discovered neighbors.
<b>show ip eigrp topology</b> [ <i>autonomous-system-number</i> ]   [[ <i>ip-address</i> ] <i>mask</i> ]	Displays the EIGRP topology table.
<b>show ip eigrp traffic</b> [ <i>autonomous-system-number</i> ]	Displays the number of packets sent and received by the EIGRP process.

## Information About Multi-VRF CE

Virtual Private Networks (VPNs) provide a secure way for customers to share bandwidth over an ISP backbone network. A VPN is a collection of sites sharing a common routing table. A customer site is connected to the service-provider network by one or more interfaces, and the service provider associates each interface with a VPN routing table, called a VPN routing/forwarding (VRF) table.

The switch supports multiple VPN routing/forwarding (multi-VRF) instances in customer edge (CE) devices (multi-VRF CE) when it is running the . Multi-VRF CE allows a service provider to support two or more VPNs with overlapping IP addresses.



---

**Note** The switch does not use Multiprotocol Label Switching (MPLS) to support VPNs.

---

## Understanding Multi-VRF CE

Multi-VRF CE is a feature that allows a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs. Multi-VRF CE uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as Ethernet ports, or logical, such as VLAN SVIs, but an interface cannot belong to more than one VRF at any time.



---

**Note** Multi-VRF CE interfaces must be Layer 3 interfaces.

---

Multi-VRF CE includes these devices:

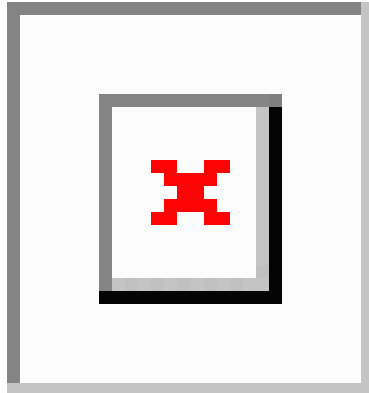
- Customer edge (CE) devices provide customers access to the service-provider network over a data link to one or more provider edge routers. The CE device advertises the site's local routes to the router and learns the remote VPN routes from it. A switch can be a CE.
- Provider edge (PE) routers exchange routing information with CE devices by using static routing or a routing protocol such as BGP, RIPv2, OSPF, or EIGRP. The PE is only required to maintain VPN routes for those VPNs to which it is directly attached, eliminating the need for the PE to maintain all of the service-provider VPN routes. Each PE router maintains a VRF for each of its directly connected sites. Multiple interfaces on a PE router can be associated with a single VRF if all of these sites participate in the same VPN. Each VPN is mapped to a specified VRF. After learning local VPN routes from CEs, a PE router exchanges VPN routing information with other PE routers by using internal BGP (IBPG).
- Provider routers or core routers are any routers in the service provider network that do not attach to CE devices.

With multi-VRF CE, multiple customers can share one CE, and only one physical link is used between the CE and the PE. The shared CE maintains separate VRF tables for each customer and switches or routes packets for each customer based on its own routing table. Multi-VRF CE extends limited PE functionality to a CE device, giving it the ability to maintain separate VRF tables to extend the privacy and security of a VPN to the branch office.

## Network Topology

The figure shows a configuration using switches as multiple virtual CEs. This scenario is suited for customers who have low bandwidth requirements for their VPN service, for example, small companies. In this case, multi-VRF CE support is required in the switches. Because multi-VRF CE is a Layer 3 feature, each interface in a VRF must be a Layer 3 interface.

**Figure 5: Switches Acting as Multiple Virtual CEs**



When the CE switch receives a command to add a Layer 3 interface to a VRF, it sets up the appropriate mapping between the VLAN ID and the policy label (PL) in multi-VRF-CE-related data structures and adds the VLAN ID and PL to the VLAN database.

When multi-VRF CE is configured, the Layer 3 forwarding table is conceptually partitioned into two sections:

- The multi-VRF CE routing section contains the routes from different VPNs.
- The global routing section contains routes to non-VPN networks, such as the Internet.

VLAN IDs from different VRFs are mapped into different policy labels, which are used to distinguish the VRFs during processing. For each new VPN route learned, the Layer 3 setup function retrieves the policy label by using the VLAN ID of the ingress port and inserts the policy label and new route to the multi-VRF CE routing section. If the packet is received from a routed port, the port internal VLAN ID number is used; if the packet is received from an SVI, the VLAN number is used.

## Packet-Forwarding Process

This is the packet-forwarding process in a multi-VRF-CE-enabled network:

- When the switch receives a packet from a VPN, the switch looks up the routing table based on the input policy label number. When a route is found, the switch forwards the packet to the PE.
- When the ingress PE receives a packet from the CE, it performs a VRF lookup. When a route is found, the router adds a corresponding MPLS label to the packet and sends it to the MPLS network.
- When an egress PE receives a packet from the network, it strips the label and uses the label to identify the correct VPN routing table. Then it performs the normal route lookup. When a route is found, it forwards the packet to the correct adjacency.
- When a CE receives a packet from an egress PE, it uses the input policy label to look up the correct VPN routing table. If a route is found, it forwards the packet within the VPN.

## Network Components

To configure VRF, you create a VRF table and specify the Layer 3 interface associated with the VRF. Then configure the routing protocols in the VPN and between the CE and the PE. BGP is the preferred routing protocol used to distribute VPN routing information across the provider's backbone. The multi-VRF CE network has three major components:

- VPN route target communities—lists of all other members of a VPN community. You need to configure VPN route targets for each VPN community member.
- Multiprotocol BGP peering of VPN community PE routers—propagates VRF reachability information to all members of a VPN community. You need to configure BGP peering in all PE routers within a VPN community.
- VPN forwarding—transports all traffic between all VPN community members across a VPN service-provider network.

## VRF-Aware Services

IP services can be configured on global interfaces, and these services run within the global routing instance. IP services are enhanced to run on multiple routing instances; they are VRF-aware. Any configured VRF in the system can be specified for a VRF-aware service.

VRF-Aware services are implemented in platform-independent modules. VRF means multiple routing instances in Cisco IOS. Each platform has its own limit on the number of VRFs it supports.

VRF-aware services have the following characteristics:

- The user can ping a host in a user-specified VRF.
- ARP entries are learned in separate VRFs. The user can display Address Resolution Protocol (ARP) entries for specific VRFs.

# How to Configure Multi-VRF CE

## Default Multi-VRF CE Configuration

*Table 9: Default VRF Configuration*

Feature	Default Setting
VRF	Disabled. No VRFs are defined.
Maps	No import maps, export maps, or route maps are defined.
VRF maximum routes	Fast Ethernet switches: 8000 Gigabit Ethernet switches: 12000.
Forwarding table	The default for an interface is the global routing table.

## Multi-VRF CE Configuration Guidelines



**Note** To use multi-VRF CE, you must have the enabled on your switch.

- A switch with multi-VRF CE is shared by multiple customers, and each customer has its own routing table.
- Because customers use different VRF tables, the same IP addresses can be reused. Overlapped IP addresses are allowed in different VPNs.
- Multi-VRF CE lets multiple customers share the same physical link between the PE and the CE. Trunk ports with multiple VLANs separate packets among customers. Each customer has its own VLAN.
- Multi-VRF CE does not support all MPLS-VRF functionality. It does not support label exchange, LDP adjacency, or labeled packets.
- For the PE router, there is no difference between using multi-VRF CE or using multiple CEs. In Figure 41-6, multiple virtual Layer 3 interfaces are connected to the multi-VRF CE device.
- The switch supports configuring VRF by using physical ports, VLAN SVIs, or a combination of both. The SVIs can be connected through an access port or a trunk port.
- A customer can use multiple VLANs as long as they do not overlap with those of other customers. A customer's VLANs are mapped to a specific routing table ID that is used to identify the appropriate routing tables stored on the switch.
- The switch supports one global network and up to 25 VRFs.
- Most routing protocols (BGP, OSPF, RIP, and static routing) can be used between the CE and the PE. However, we recommend using external BGP (EBGP) for these reasons:
  - BGP does not require multiple algorithms to communicate with multiple CEs.
  - BGP is designed for passing routing information between systems run by different administrations.
  - BGP makes it easy to pass attributes of the routes to the CE.
- Multi-VRF CE does not affect the packet switching rate.
- VPN multicast is not supported.
- You can enable VRF on a private VLAN, and the reverse.
- You cannot enable VRF when policy-based routing (PBR) is enabled on an interface, and the reverse.
- You cannot enable VRF when Web Cache Communication Protocol (WCCP) is enabled on an interface, and the reverse.

## Configuring VRFs

Perform the following steps:

## Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>ip routing</b> <b>Example:</b>  Switch(config)# ip routing	Enables IP routing.
<b>Step 3</b>	<b>ip vrf vrf-name</b> <b>Example:</b>  Switch(config)# ip vrf vpn1	Names the VRF, and enter VRF configuration mode.
<b>Step 4</b>	<b>rd route-distinguisher</b> <b>Example:</b>  Switch(config-vrf)# rd 100:2	Creates a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y)
<b>Step 5</b>	<b>route-target {export   import   both}</b> <i>route-target-ext-community</i> <b>Example:</b>  Switch(config-vrf)# route-target both 100:2	Creates a list of import, export, or import and export route target communities for the specified VRF. Enter either an AS system number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y). The <i>route-target-ext-community</i> should be the same as the <i>route-distinguisher</i> entered in Step 4.
<b>Step 6</b>	<b>import map route-map</b> <b>Example:</b>  Switch(config-vrf)# import map importmap1	(Optional) Associates a route map with the VRF.
<b>Step 7</b>	<b>interface interface-id</b> <b>Example:</b>  Switch(config-vrf)# interface gigabitethernet 1/0/1	Specifies the Layer 3 interface to be associated with the VRF, and enter interface configuration mode. The interface can be a routed port or SVI.
<b>Step 8</b>	<b>ip vrf forwarding vrf-name</b> <b>Example:</b>  Switch(config-if)# ip vrf forwarding vpn1	Associates the VRF with the Layer 3 interface.  <b>Note</b> When <b>ip vrf forwarding</b> is enabled in the Management Interface, the access point does not join.
<b>Step 9</b>	<b>end</b> <b>Example:</b>	Returns to privileged EXEC mode.



	Command or Action	Purpose
	Switch(config)# <b>end</b>	
<b>Step 10</b>	<b>show ip vrf [brief   detail   interfaces] [vrf-name]</b> <b>Example:</b> Switch# show ip vrf interfaces vpn1	Verifies the configuration. Displays information about the configured VRFs.
<b>Step 11</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Configuring VRF-Aware Services

These services are VRF-Aware:

- ARP
- Ping
- Simple Network Management Protocol (SNMP)
- Unicast Reverse Path Forwarding (uRPF)
- Syslog
- Traceroute
- FTP and TFTP

### Configuring VRF-Aware Services for ARP

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>show ip arp vrf vrf-name</b> <b>Example:</b> Switch# show ip arp vrf vpn1	Displays the ARP table in the specified VRF.

## Configuring VRF-Aware Services for Ping

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>ping vrf <i>vrf-name</i> ip-host</b></p> <p><b>Example:</b></p> <pre>Switch# ping vrf vpn1 ip-host</pre>	Displays the ARP table in the specified VRF.

## Configuring VRF-Aware Services for SNMP

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
<b>Step 2</b>	<p><b>snmp-server trap authentication vrf</b></p> <p><b>Example:</b></p> <pre>Switch(config)# snmp-server trap authentication vrf</pre>	Enables SNMP traps for packets on a VRF.
<b>Step 3</b>	<p><b>snmp-server engineID remote <i>host</i> vrf <i>vpn-instance</i> <i>engine-id string</i></b></p> <p><b>Example:</b></p> <pre>Switch(config)# snmp-server engineID remote 172.16.20.3 vrf vpn1 80000009030000B064EFE100</pre>	Configures a name for the remote SNMP engine on a switch.
<b>Step 4</b>	<p><b>snmp-server host <i>host</i> vrf <i>vpn-instance</i> traps <i>community</i></b></p> <p><b>Example:</b></p> <pre>Switch(config)# snmp-server host 172.16.20.3 vrf vpn1 traps comaccess</pre>	Specifies the recipient of an SNMP trap operation and specifies the VRF table to be used for sending SNMP traps.
<b>Step 5</b>	<p><b>snmp-server host <i>host</i> vrf <i>vpn-instance</i> informs <i>community</i></b></p> <p><b>Example:</b></p> <pre>Switch(config)# snmp-server host 172.16.20.3 vrf vpn1 informs comaccess</pre>	Specifies the recipient of an SNMP inform operation and specifies the VRF table to be used for sending SNMP informs.

	Command or Action	Purpose
Step 6	<b>snmp-server user</b> <i>user group remote host vrf vpn-instance security model</i> <b>Example:</b> <pre>Switch(config)# snmp-server user abcd remote 172.16.20.3 vrf vpn1 priv v2c 3des secure3des</pre>	Adds a user to an SNMP group for a remote host on a VRF for SNMP access.
Step 7	<b>end</b> <b>Example:</b> <pre>Switch(config-if)# end</pre>	Returns to privileged EXEC mode.

## Configuring VRF-Aware Services for HSRP

HSRP support for VRFs ensures that HSRP virtual IP addresses are added to the correct IP routing table.

For complete syntax and usage information for the commands, refer to the switch command reference for this release and the *Cisco IOS Switching Services Command Reference, Release 12.4*.

### Procedure

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
Step 2	<b>interface</b> <i>interface-id</i> <b>Example:</b> <pre>Switch(config)# interface gigabitethernet 1/0/1</pre>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
Step 3	<b>no switchport</b> <b>Example:</b> <pre>Switch(config-if)# no switchport</pre>	Removes the interface from Layer 2 configuration mode if it is a physical interface.
Step 4	<b>ip vrf forwarding</b> <i>vrf-name</i> <b>Example:</b> <pre>Switch(config-if)# ip vrf forwarding vpn1</pre>	Configures VRF on the interface.
Step 5	<b>ip address</b> <i>ip-address</i> <b>Example:</b>	Enters the IP address for the interface.

	Command or Action	Purpose
	Switch(config-if)# ip address 10.1.5.1	
<b>Step 6</b>	<b>standby 1 ip ip-address</b> <b>Example:</b> Switch(config-if)#standby 1 ip 10.1.1.254	Enables HSRP and configure the virtual IP address.
<b>Step 7</b>	<b>end</b> <b>Example:</b> Switch(config-if)# end	Returns to privileged EXEC mode.

## Configuring VRF-Aware Services for uRPF

uRPF can be configured on an interface assigned to a VRF, and source lookup is done in the VRF table.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	<b>interface interface-id</b> <b>Example:</b> Switch(config)# interface gigabitethernet 1/0/1	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
<b>Step 3</b>	<b>no switchport</b> <b>Example:</b> Switch(config-if)# no switchport	Removes the interface from Layer 2 configuration mode if it is a physical interface.
<b>Step 4</b>	<b>ip vrf forwarding vrf-name</b> <b>Example:</b> Switch(config-if)# ip vrf forwarding vpn2	Configures VRF on the interface.
<b>Step 5</b>	<b>ip address ip-address</b> <b>Example:</b> Switch(config-if)# ip address 10.1.5.1	Enters the IP address for the interface.

	Command or Action	Purpose
Step 6	<b>ip verify unicast reverse-path</b> <b>Example:</b> Switch(config-if)# ip verify unicast reverse-path	Enables uRPF on the interface.
Step 7	<b>end</b> <b>Example:</b> Switch(config-if)# end	Returns to privileged EXEC mode.

## Configuring VRF-Aware RADIUS

To configure VRF-Aware RADIUS, you must first enable AAA on a RADIUS server. The switch supports the **ip vrf forwarding** *vrf-name* server-group configuration and the **ip radius source-interface** global configuration commands, as described in the Per VRF AAA Feature Guide.

## Configuring VRF-Aware Services for Syslog

### Procedure

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> Switch# configure terminal	Enters global configuration mode.
Step 2	<b>logging on</b> <b>Example:</b> Switch(config)# logging on	Enables or temporarily disables logging of storage router event message.
Step 3	<b>logging host ip-address vrf vrf-name</b> <b>Example:</b> Switch(config)# logging host 10.10.1.0 vrf vpn1	Specifies the host address of the syslog server where logging messages are to be sent.
Step 4	<b>logging buffered logging buffered size debugging</b> <b>Example:</b> Switch(config)# logging buffered critical 6000 debugging	Logs messages to an internal buffer.
Step 5	<b>logging trap debugging</b> <b>Example:</b>	Limits the logging messages sent to the syslog server.

	Command or Action	Purpose
	Switch(config)# logging trap debugging	
<b>Step 6</b>	<b>logging facility</b> <i>facility</i> <b>Example:</b> Switch(config)# logging facility user	Sends system logging messages to a logging facility.
<b>Step 7</b>	<b>end</b> <b>Example:</b> Switch(config-if)# end	Returns to privileged EXEC mode.

## Configuring VRF-Aware Services for Traceroute

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>traceroute vrf</b> <i>vrf-name ipaddress</i> <b>Example:</b> Switch(config)# traceroute vrf vpn2 10.10.1.1	Specifies the name of a VPN VRF in which to find the destination address.

## Configuring VRF-Aware Services for FTP and TFTP

So that FTP and TFTP are VRF-aware, you must configure some FTP/TFTP CLIs. For example, if you want to use a VRF table that is attached to an interface, say E1/0, you need to configure the `ip tftp source-interface E1/0` or the `ip ftp source-interface E1/0` command to inform TFTP or FTP server to use a specific routing table. In this example, the VRF table is used to look up the destination IP address. These changes are backward-compatible and do not affect existing behavior. That is, you can use the source-interface CLI to send packets out a particular interface even if no VRF is configured on that interface.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ip ftp source-interface</b> <i>interface-type interface-number</i> <b>Example:</b> Switch(config)# ip ftp source-interface gigabitethernet 1/0/2	Specifies the source IP address for FTP connections.

	Command or Action	Purpose
<b>Step 3</b>	<b>end</b> <b>Example:</b>  Switch(config)#end	Returns to privileged EXEC mode.
<b>Step 4</b>	<b>configure terminal</b> <b>Example:</b>  Switch# configure terminal	Enters global configuration mode.
<b>Step 5</b>	<b>ip tftp source-interface interface-type interface-number</b> <b>Example:</b>  Switch(config)# ip tftp source-interface gigabitethernet 1/0/2	Specifies the source IP address for TFTP connections.
<b>Step 6</b>	<b>end</b> <b>Example:</b>  Switch(config)# end	Returns to privileged EXEC mode.

## Configuring Multicast VRFs

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ip routing</b> <b>Example:</b>  Switch(config)# ip routing	Enables IP routing mode.
<b>Step 3</b>	<b>ip vrf vrf-name</b> <b>Example:</b>  Switch(config)# ip vrf vpn1	Names the VRF, and enter VRF configuration mode.

	Command or Action	Purpose
Step 4	<b>rd</b> <i>route-distinguisher</i> <b>Example:</b> <pre>Switch(config-vrf)# rd 100:2</pre>	Creates a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y)
Step 5	<b>route-target</b> { <b>export</b>   <b>import</b>   <b>both</b> } <i>route-target-ext-community</i> <b>Example:</b> <pre>Switch(config-vrf)# route-target import 100:2</pre>	Creates a list of import, export, or import and export route target communities for the specified VRF. Enter either an AS system number and an arbitrary number (xxx:y) or an IP address and an arbitrary number (A.B.C.D:y). The <i>route-target-ext-community</i> should be the same as the <i>route-distinguisher</i> entered in Step 4.
Step 6	<b>import map</b> <i>route-map</i> <b>Example:</b> <pre>Switch(config-vrf)# import map importmap1</pre>	(Optional) Associates a route map with the VRF.
Step 7	<b>ip multicast-routing vrf</b> <i>vrf-name</i> <b>distributed</b> <b>Example:</b> <pre>Switch(config-vrf)# ip multicast-routing vrf vpn1 distributed</pre>	(Optional) Enables global multicast routing for VRF table.
Step 8	<b>interface</b> <i>interface-id</i> <b>Example:</b> <pre>Switch(config-vrf)# interface gigabitethernet 1/0/2</pre>	Specifies the Layer 3 interface to be associated with the VRF, and enter interface configuration mode. The interface can be a routed port or an SVI.
Step 9	<b>ip vrf forwarding</b> <i>vrf-name</i> <b>Example:</b> <pre>Switch(config-if)# ip vrf forwarding vpn1</pre>	Associates the VRF with the Layer 3 interface.
Step 10	<b>ip address</b> <i>ip-address</i> <b>mask</b> <b>Example:</b> <pre>Switch(config-if)# ip address 10.1.5.1 255.255.255.0</pre>	Configures IP address for the Layer 3 interface.
Step 11	<b>ip pim sparse-dense mode</b> <b>Example:</b> <pre>Switch(config-if)# ip pim sparse-dense mode</pre>	Enables PIM on the VRF-associated Layer 3 interface.
Step 12	<b>end</b> <b>Example:</b>	Returns to privileged EXEC mode.



	Command or Action	Purpose
	Switch(config)# <b>end</b>	
<b>Step 13</b>	<b>show ip vrf [brief   detail   interfaces] [vrf-name]</b> <b>Example:</b> Switch# show ip vrf detail vpn1	Verifies the configuration. Displays information about the configured VRFs.
<b>Step 14</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Configuring a VPN Routing Session

Routing within the VPN can be configured with any supported routing protocol (RIP, OSPF, EIGRP, or BGP) or with static routing. The configuration shown here is for OSPF, but the process is the same for other protocols.



**Note** To configure an EIGRP routing process to run within a VRF instance, you must configure an autonomous-system number by entering the **autonomous-system** *autonomous-system-number* address-family configuration mode command.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>router ospf process-id vrf vrf-name</b> <b>Example:</b> Switch(config)# router ospf 1 vrf vpn1	Enables OSPF routing, specifies a VPN forwarding table, and enter router configuration mode.
<b>Step 3</b>	<b>log-adjacency-changes</b> <b>Example:</b> Switch(config-router)# log-adjacency-changes	(Optional) Logs changes in the adjacency state. This is the default state.
<b>Step 4</b>	<b>redistribute bgp autonomous-system-number subnets</b> <b>Example:</b>	Sets the switch to redistribute information from the BGP network to the OSPF network.

	Command or Action	Purpose
	Switch(config-router)# redistribute bgp 10 subnets	
<b>Step 5</b>	<b>network</b> <i>network-number</i> <b>area</b> <i>area-id</i> <b>Example:</b> Switch(config-router)# network 1 area 2	Defines a network address and mask on which OSPF runs and the area ID for that network address.
<b>Step 6</b>	<b>end</b> <b>Example:</b> Switch(config-router)# end	Returns to privileged EXEC mode.
<b>Step 7</b>	<b>show ip ospf</b> <i>process-id</i> <b>Example:</b> Switch# show ip ospf 1	Verifies the configuration of the OSPF network.
<b>Step 8</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## Configuring BGP PE to CE Routing Sessions

### Procedure

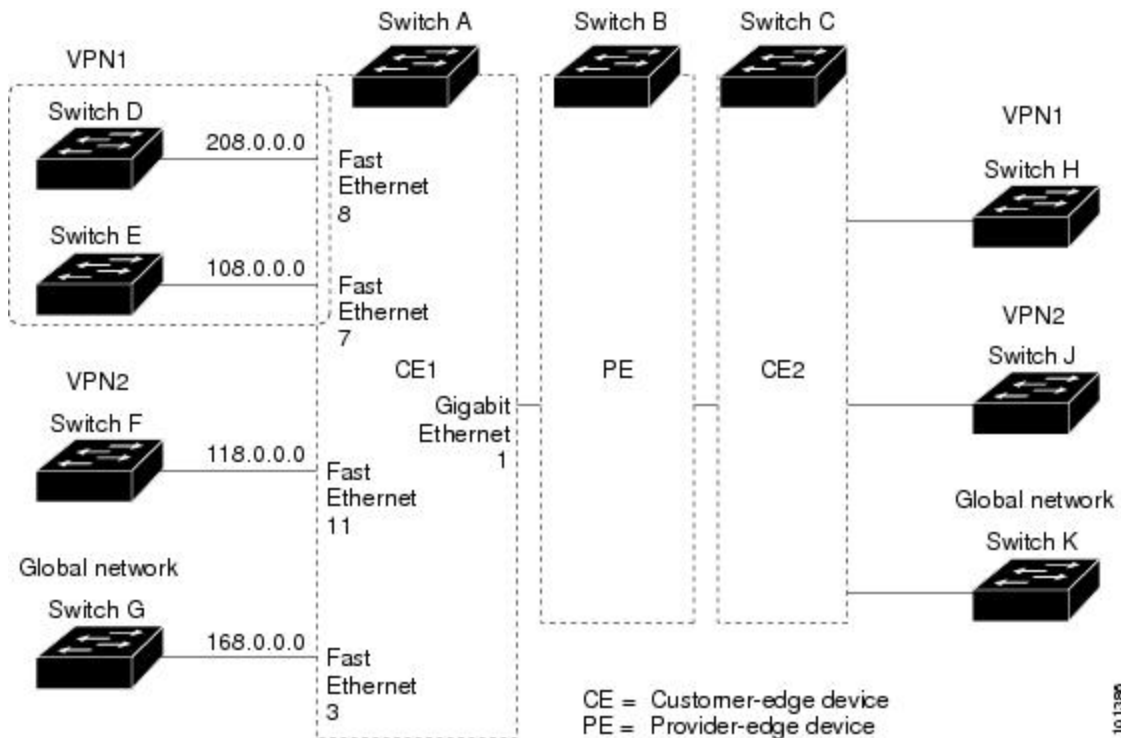
	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>router bgp</b> <i>autonomous-system-number</i> <b>Example:</b> Switch(config)# router bgp 2	Configures the BGP routing process with the AS number passed to other BGP routers, and enter router configuration mode.
<b>Step 3</b>	<b>network</b> <i>network-number</i> <b>mask</b> <i>network-mask</i> <b>Example:</b> Switch(config-router)# network 5 mask 255.255.255.0	Specifies a network and mask to announce using BGP.

	Command or Action	Purpose
Step 4	<b>redistribute ospf <i>process-id</i> match internal</b> <b>Example:</b> <pre>Switch(config-router)# redistribute ospf 1 match internal</pre>	Sets the switch to redistribute OSPF internal routes.
Step 5	<b>network <i>network-number</i> area <i>area-id</i></b> <b>Example:</b> <pre>Switch(config-router)# network 5 area 2</pre>	Defines a network address and mask on which OSPF runs and the area ID for that network address.
Step 6	<b>address-family ipv4 vrf <i>vrf-name</i></b> <b>Example:</b> <pre>Switch(config-router)# address-family ipv4 vrf vpn1</pre>	Defines BGP parameters for PE to CE routing sessions, and enter VRF address-family mode.
Step 7	<b>neighbor <i>address</i> remote-as <i>as-number</i></b> <b>Example:</b> <pre>Switch(config-router)# neighbor 10.1.1.2 remote-as 2</pre>	Defines a BGP session between PE and CE routers.
Step 8	<b>neighbor <i>address</i> activate</b> <b>Example:</b> <pre>Switch(config-router)# neighbor 10.2.1.1 activate</pre>	Activates the advertisement of the IPv4 address family.
Step 9	<b>end</b> <b>Example:</b> <pre>Switch(config-router)# end</pre>	Returns to privileged EXEC mode.
Step 10	<b>show ip bgp [<i>ipv4</i>] [<i>neighbors</i>]</b> <b>Example:</b> <pre>Switch# show ip bgp ipv4 neighbors</pre>	Verifies BGP configuration.
Step 11	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Multi-VRF CE Configuration Example

OSPF is the protocol used in VPN1, VPN2, and the global network. BGP is used in the CE to PE connections. The examples following the illustration show how to configure a switch as CE Switch A, and the VRF configuration for customer switches D and F. Commands for configuring CE Switch C and the other customer switches are not included but would be similar.

Figure 6: Multi-VRF CE Configuration Example



On Switch A, enable routing and configure VRF.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
```

Configure the loopback and physical interfaces on Switch A. Gigabit Ethernet port 1 is a trunk connection to the PE. Gigabit Ethernet ports 8 and 11 connect to VPNs:

```
Switch(config)# interface loopback1
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit
```

```

Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface gigabitethernet1/0/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

```

Configure the VLANs used on Switch A. VLAN 10 is used by VRF 11 between the CE and the PE. VLAN 20 is used by VRF 12 between the CE and the PE. VLANs 118 and 208 are used for the VPNs that include Switch F and Switch D, respectively:

```

Switch(config)# interface vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface vlan20
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit
Switch(config)# interface vlan208
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit

```

Configure OSPF routing in VPN1 and VPN2.

```

Switch(config)# router ospf 1 vrf v11
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config)# router ospf 2 vrf v12
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit

```

Configure BGP for CE to PE routing.

```

Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf v12
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit

```

```
Switch(config-router)# address-family ipv4 vrf v11
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end
```

Switch D belongs to VPN 1. Configure the connection to Switch A by using these commands.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

Switch F belongs to VPN 2. Configure the connection to Switch A by using these commands.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
```

When used on switch B (the PE router), these commands configure only the connections to the CE device, Switch A.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit
Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
```

```

Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/1/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface gigabitethernet1/1/0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf v2
Router(config-router-af)# neighbor 83.0.0.8 remote-as 800
Router(config-router-af)# neighbor 83.0.0.8 activate
Router(config-router-af)# network 3.3.2.0 mask 255.255.255.0
Router(config-router-af)# exit
Router(config-router)# address-family ipv4 vrf v1
Router(config-router-af)# neighbor 38.0.0.8 remote-as 800
Router(config-router-af)# neighbor 38.0.0.8 activate
Router(config-router-af)# network 3.3.1.0 mask 255.255.255.0
Router(config-router-af)# end

```

## Monitoring Multi-VRF CE

**Table 10: Commands for Displaying Multi-VRF CE Information**

<b>show ip protocols vrf</b> <i>vrf-name</i>	Displays routing protocol information as a VRF.
<b>show ip route vrf</b> <i>vrf-name</i> [ <b>connected</b> ] [ <i>protocol</i> [ <i>as-number</i> ]] [ <b>list</b> ] [ <b>mobile</b> ] [ <b>odr</b> ] [ <b>profile</b> ] [ <b>static</b> ] [ <b>summary</b> ] [ <b>supernets-only</b> ]	Displays IP routing table information as a VRF.
<b>show ip vrf</b> [ <b>brief</b>   <b>detail</b>   <b>interfaces</b> ] [ <i>vrf-name</i> ]	Displays information about the defined VRFs.

## Configuring Unicast Reverse Path Forwarding

The unicast reverse path forwarding (unicast RPF) feature helps to mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks, including Smurf and Tribal Flood Network (TFN), can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. For Internet service providers (ISPs) that provide public access, Unicast RPF deflects such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This action protects the network of the ISP, its customer, and the rest of the Internet.



**Note** • Unicast RPF is supported in .

# Protocol-Independent Features

This section describes IP routing protocol-independent features that are available on switches running the feature set .

## Distributed Cisco Express Forwarding

### Information About Cisco Express Forwarding

Cisco Express Forwarding (CEF) is a Layer 3 IP switching technology used to optimize network performance. CEF implements an advanced IP look-up and forwarding algorithm to deliver maximum Layer 3 switching performance. CEF is less CPU-intensive than fast switching route caching, allowing more CPU processing power to be dedicated to packet forwarding. In a switch stack, the hardware uses distributed CEF (dCEF) in the stack. In dynamic networks, fast switching cache entries are frequently invalidated because of routing changes, which can cause traffic to be process switched using the routing table, instead of fast switched using the route cache. CEF and dCEF use the Forwarding Information Base (FIB) lookup table to perform destination-based switching of IP packets.

The two main components in CEF and dCEF are the distributed FIB and the distributed adjacency tables.

- The FIB is similar to a routing table or information base and maintains a mirror image of the forwarding information in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table. Because the FIB contains all known routes that exist in the routing table, CEF eliminates route cache maintenance, is more efficient for switching traffic, and is not affected by traffic patterns.
- Nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. CEF uses adjacency tables to prepend Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries.

Because the switch or switch stack uses Application Specific Integrated Circuits (ASICs) to achieve Gigabit-speed line rate IP traffic, CEF or dCEF forwarding applies only to the software-forwarding path, that is, traffic that is forwarded by the CPU.

### How to Configure Cisco Express Forwarding

CEF or distributed CEF is enabled globally by default. If for some reason it is disabled, you can re-enable it by using the **ip cef** or **ip cef distributed** global configuration command.

The default configuration is CEF or dCEF enabled on all Layer 3 interfaces. Entering the **no ip route-cache cef** interface configuration command disables CEF for traffic that is being forwarded by software. This command does not affect the hardware forwarding path. Disabling CEF and using the **debug ip packet detail** privileged EXEC command can be useful to debug software-forwarded traffic. To enable CEF on an interface for the software-forwarding path, use the **ip route-cache cef** interface configuration command.



---

**Caution** Although the **no ip route-cache cef** interface configuration command to disable CEF on an interface is visible in the CLI, we strongly recommend that you do not disable CEF or dCEF on interfaces except for debugging purposes.

---



To enable CEF or dCEF globally and on an interface for software-forwarded traffic if it has been disabled:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>ip cef</b> <b>Example:</b>  Switch(config)# <code>ip cef</code>	Enables CEF operation on a non-stacking switch. Go to Step 4.
<b>Step 3</b>	<b>ip cef distributed</b> <b>Example:</b>  Switch(config)# <code>ip cef distributed</code>	Enables CEF operation on a active switch.
<b>Step 4</b>	<b>interface <i>interface-id</i></b> <b>Example:</b>  Switch(config)# <code>interface gigabitethernet 1/0/1</code>	Enters interface configuration mode, and specifies the Layer 3 interface to configure.
<b>Step 5</b>	<b>ip route-cache cef</b> <b>Example:</b>  Switch(config-if)# <code>ip route-cache cef</code>	Enables CEF on the interface for software-forwarded traffic.
<b>Step 6</b>	<b>end</b> <b>Example:</b>  Switch(config-if)# <code>end</code>	Returns to privileged EXEC mode.
<b>Step 7</b>	<b>show ip cef</b> <b>Example:</b>  Switch# <code>show ip cef</code>	Displays the CEF status on all interfaces.
<b>Step 8</b>	<b>show cef linecard [detail]</b> <b>Example:</b>  Switch# <code>show cef linecard detail</code>	(Optional) Displays CEF-related interface information on a non-stacking switch.

	Command or Action	Purpose
<b>Step 9</b>	<b>show cef linecard</b> [ <i>slot-number</i> ] [ <i>detail</i> ] <b>Example:</b> Switch# show cef linecard 5 detail	(Optional) Displays CEF-related interface information on a switch by stack member for all switches in the stack or for the specified switch.  (Optional) For <i>slot-number</i> , enter the stack member switch number.
<b>Step 10</b>	<b>show cef interface</b> [ <i>interface-id</i> ] <b>Example:</b> Switch# show cef interface gigabitethernet 1/0/1	Displays detailed CEF information for all interfaces or the specified interface.
<b>Step 11</b>	<b>show adjacency</b> <b>Example:</b> Switch# show adjacency	Displays CEF adjacency table information.
<b>Step 12</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## Number of Equal-Cost Routing Paths

### Information About Equal-Cost Routing Paths

When a router has two or more routes to the same network with the same metrics, these routes can be thought of as having an equal cost. The term parallel path is another way to see occurrences of equal-cost routes in a routing table. If a router has two or more equal-cost paths to a network, it can use them concurrently. Parallel paths provide redundancy in case of a circuit failure and also enable a router to load balance packets over the available paths for more efficient use of available bandwidth. Equal-cost routes are supported across switches in a stack.

Even though the router automatically learns about and configures equal-cost routes, you can control the maximum number of parallel paths supported by an IP routing protocol in its routing table. Although the switch software allows a maximum of 32 equal-cost routes, the switch hardware will never use more than 16 paths per route.

### How to Configure Equal-Cost Routing Paths

#### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>router {rip   ospf   eigrp}</b> <b>Example:</b>  Switch(config)# router eigrp	Enters router configuration mode.
<b>Step 3</b>	<b>maximum-paths <i>maximum</i></b> <b>Example:</b>  Switch(config-router)# maximum-paths 2	Sets the maximum number of parallel paths for the protocol routing table. The range is from 1 to 16; the default is 4 for most IP routing protocols, but only 1 for BGP.
<b>Step 4</b>	<b>end</b> <b>Example:</b>  Switch(config-router)# end	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show ip protocols</b> <b>Example:</b>  Switch# show ip protocols	Verifies the setting in the <i>Maximum path</i> field.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b>  Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## Static Unicast Routes

### Information About Static Unicast Routes

Static unicast routes are user-defined routes that cause packets moving between a source and a destination to take a specified path. Static routes can be important if the router cannot build a route to a particular destination and are useful for specifying a gateway of last resort to which all unroutable packets are sent.

The switch retains static routes until you remove them. However, you can override static routes with dynamic routing information by assigning administrative distance values. Each dynamic routing protocol has a default administrative distance, as listed in Table 41-16. If you want a static route to be overridden by information from a dynamic routing protocol, set the administrative distance of the static route higher than that of the dynamic protocol.

**Table 11: Dynamic Routing Protocol Default Administrative Distances**

Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced IRGP summary route	5

Route Source	Default Distance
Internal Enhanced IGRP	90
IGRP	100
OSPF	110
Unknown	225

Static routes that point to an interface are advertised through RIP, IGRP, and other dynamic routing protocols, whether or not static **redistribute** router configuration commands were specified for those routing protocols. These static routes are advertised because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. However, if you define a static route to an interface that is not one of the networks defined in a network command, no dynamic routing protocols advertise the route unless a **redistribute** static command is specified for these protocols.

When an interface goes down, all static routes through that interface are removed from the IP routing table. When the software can no longer find a valid next hop for the address specified as the forwarding router's address in a static route, the static route is also removed from the IP routing table.

## Configuring Static Unicast Routes

Static unicast routes are user-defined routes that cause packets moving between a source and a destination to take a specified path. Static routes can be important if the router cannot build a route to a particular destination and are useful for specifying a gateway of last resort to which all unroutable packets are sent.

Follow these steps to configure a static route:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>ip route prefix mask {address   interface} [distance]</b> <b>Example:</b> Device(config)# <b>ip route prefix mask gigabitethernet 1/0/4</b>	Establish a static route.
<b>Step 4</b>	<b>end</b> <b>Example:</b>	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Switch(config)# <b>end</b>	
<b>Step 5</b>	<b>show ip route</b> <b>Example:</b> Switch# <b>show ip route</b>	Displays the current state of the routing table to verify the configuration.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b> Device# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

### What to do next

Use the **no ip route** *prefix mask {address| interface}* global configuration command to remove a static route. The device retains static routes until you remove them.

## Default Routes and Networks

### Information About Default Routes and Networks

A router might not be able to learn the routes to all other networks. To provide complete routing capability, you can use some routers as smart routers and give the remaining routers default routes to the smart router. (Smart routers have routing table information for the entire internetwork.) These default routes can be dynamically learned or can be configured in the individual routers. Most dynamic interior routing protocols include a mechanism for causing a smart router to generate dynamic default information that is then forwarded to other routers.

If a router has a directly connected interface to the specified default network, the dynamic routing protocols running on that device generate a default route. In RIP, it advertises the pseudonetwork 0.0.0.0.

A router that is generating the default for a network also might need a default of its own. One way a router can generate its own default is to specify a static route to the network 0.0.0.0 through the appropriate device.

When default information is passed through a dynamic routing protocol, no further configuration is required. The system periodically scans its routing table to choose the optimal default network as its default route. In IGRP networks, there might be several candidate networks for the system default. Cisco routers use administrative distance and metric information to set the default route or the gateway of last resort.

If dynamic default information is not being passed to the system, candidates for the default route are specified with the **ip default-network** global configuration command. If this network appears in the routing table from any source, it is flagged as a possible choice for the default route. If the router has no interface on the default network, but does have a path to it, the network is considered as a possible candidate, and the gateway to the best default path becomes the gateway of last resort.

## How to Configure Default Routes and Networks

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>ip default-network <i>network number</i></b> <b>Example:</b>  Switch(config)# ip default-network 1	Specifies a default network.
<b>Step 3</b>	<b>end</b> <b>Example:</b>  Switch(config) # end	Returns to privileged EXEC mode.
<b>Step 4</b>	<b>show ip route</b> <b>Example:</b>  Switch# show ip route	Displays the selected default route in the gateway of last resort display.
<b>Step 5</b>	<b>copy running-config startup-config</b> <b>Example:</b>  Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## Route Maps to Redistribute Routing Information

### Information About Route Maps

The switch can run multiple routing protocols simultaneously, and it can redistribute information from one routing protocol to another. Redistributing information from one routing protocol to another applies to all supported IP-based routing protocols.

You can also conditionally control the redistribution of routes between routing domains by defining enhanced packet filters or route maps between the two domains. The **match** and **set** route-map configuration commands define the condition portion of a route map. The **match** command specifies that a criterion must be matched. The **set** command specifies an action to be taken if the routing update meets the conditions defined by the match command. Although redistribution is a protocol-independent feature, some of the **match** and **set** route-map configuration commands are specific to a particular protocol.

One or more **match** commands and one or more **set** commands follow a **route-map** command. If there are no **match** commands, everything matches. If there are no **set** commands, nothing is done, other than the match. Therefore, you need at least one **match** or **set** command.



**Note** A route map with no **set** route-map configuration commands is sent to the CPU, which causes high CPU utilization.

You can also identify route-map statements as **permit** or **deny**. If the statement is marked as a deny, the packets meeting the match criteria are sent back through the normal forwarding channels (destination-based routing). If the statement is marked as permit, set clauses are applied to packets meeting the match criteria. Packets that do not meet the match criteria are forwarded through the normal routing channel.

## How to Configure a Route Map

Although each of Steps 3 through 14 in the following section is optional, you must enter at least one **match** route-map configuration command and one **set** route-map configuration command.



**Note** The keywords are the same as defined in the procedure to control the route distribution.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>route-map</b> <i>map-tag</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence number</i> ] <b>Example:</b>  Switch(config)# route-map rip-to-ospf permit 4	Defines any route maps used to control redistribution and enter route-map configuration mode.  <i>map-tag</i> —A meaningful name for the route map. The <b>redistribute</b> router configuration command uses this name to reference this route map. Multiple route maps might share the same map tag name.  (Optional) If <b>permit</b> is specified and the match criteria are met for this route map, the route is redistributed as controlled by the set actions. If <b>deny</b> is specified, the route is not redistributed.  <i>sequence number</i> (Optional)— Number that indicates the position a new route map is to have in the list of route maps already configured with the same name.
<b>Step 3</b>	<b>match as-path</b> <i>path-list-number</i> <b>Example:</b>  Switch(config-route-map)#match as-path 10	Matches a BGP AS path access list.
<b>Step 4</b>	<b>match community-list</b> <i>community-list-number</i> [ <b>exact</b> ] <b>Example:</b>	Matches a BGP community list.

	Command or Action	Purpose
	Switch(config-route-map)# match community-list 150	
<b>Step 5</b>	<b>match ip address</b> { <i>access-list-number</i>   <i>access-list-name</i> } [... <i>access-list-number</i>   ... <i>access-list-name</i> ] <b>Example:</b> Switch(config-route-map)# match ip address 5 80	Matches a standard access list by specifying the name or number. It can be an integer from 1 to 199.
<b>Step 6</b>	<b>match metric</b> <i>metric-value</i> <b>Example:</b> Switch(config-route-map)# match metric 2000	Matches the specified route metric. The <i>metric-value</i> can be an EIGRP metric with a specified value from 0 to 4294967295.
<b>Step 7</b>	<b>match ip next-hop</b> { <i>access-list-number</i>   <i>access-list-name</i> } [... <i>access-list-number</i>   ... <i>access-list-name</i> ] <b>Example:</b> Switch(config-route-map)# match ip next-hop 8 45	Matches a next-hop router address passed by one of the access lists specified (numbered from 1 to 199).
<b>Step 8</b>	<b>match tag</b> <i>tag value</i> [... <i>tag-value</i> ] <b>Example:</b> Switch(config-route-map)# match tag 3500	Matches the specified tag value in a list of one or more route tag values. Each can be an integer from 0 to 4294967295.
<b>Step 9</b>	<b>match interface-type</b> <i>number</i> [... <i>type-number</i> ] <b>Example:</b> Switch(config-route-map)# match interface gigabitethernet 1/0/1	Matches the specified next hop route out one of the specified interfaces.
<b>Step 10</b>	<b>match ip route-source</b> { <i>access-list-number</i>   <i>access-list-name</i> } [... <i>access-list-number</i>   ... <i>access-list-name</i> ] <b>Example:</b> Switch(config-route-map)# match ip route-source 10 30	Matches the address specified by the specified advertised access lists.
<b>Step 11</b>	<b>match route-type</b> { <b>local</b>   <b>internal</b>   <b>external</b> [ <b>type-1</b>   <b>type-2</b> ]} <b>Example:</b> Switch(config-route-map)# match route-type local	Matches the specified <b>route-type</b> : <ul style="list-style-type: none"> <li>• <b>local</b>—Locally generated BGP routes.</li> <li>• <b>internal</b>—OSPF intra-area and interarea routes or EIGRP internal routes.</li> <li>• <b>external</b>—OSPF external routes (Type 1 or Type 2) or EIGRP external routes.</li> </ul>



	Command or Action	Purpose
Step 12	<p><b>set dampening</b> <i>halflife reuse suppress max-suppress-time</i></p> <p><b>Example:</b></p> <pre>Switch(config-route-map)# set dampening 30 1500 10000 120</pre>	Sets BGP route dampening factors.
Step 13	<p><b>set local-preference</b> <i>value</i></p> <p><b>Example:</b></p> <pre>Switch(config-route-map)# set local-preference 100</pre>	Assigns a value to a local BGP path.
Step 14	<p><b>set origin</b> {<b>igp</b>   <b>egp as</b>   <b>incomplete</b>}</p> <p><b>Example:</b></p> <pre>Switch(config-route-map)#set origin igp</pre>	Sets the BGP origin code.
Step 15	<p><b>set as-path</b> {<b>tag</b>   <b>prepend as-path-string</b>}</p> <p><b>Example:</b></p> <pre>Switch(config-route-map)# set as-path tag</pre>	Modifies the BGP autonomous system path.
Step 16	<p><b>set level</b> {<b>level-1</b>   <b>level-2</b>   <b>level-1-2</b>   <b>stub-area</b>   <b>backbone</b>}</p> <p><b>Example:</b></p> <pre>Switch(config-route-map)# set level level-1-2</pre>	Sets the level for routes that are advertised into the specified area of the routing domain. The <b>stub-area</b> and <b>backbone</b> are OSPF NSSA and backbone areas.
Step 17	<p><b>set metric</b> <i>metric value</i></p> <p><b>Example:</b></p> <pre>Switch(config-route-map)# set metric 100</pre>	Sets the metric value to give the redistributed routes (for EIGRP only). The <i>metric value</i> is an integer from -294967295 to 294967295.
Step 18	<p><b>set metric</b><i>bandwidth delay reliability loading mtu</i></p> <p><b>Example:</b></p> <pre>Switch(config-route-map)# set metric 10000 10 255 1 1500</pre>	<p>Sets the metric value to give the redistributed routes (for EIGRP only):</p> <ul style="list-style-type: none"> <li>• <i>bandwidth</i>—Metric value or IGRP bandwidth of the route in kilobits per second in the range 0 to 4294967295</li> <li>• <i>delay</i>—Route delay in tens of microseconds in the range 0 to 4294967295.</li> <li>• <i>reliability</i>—Likelihood of successful packet transmission expressed as a number between 0 and 255, where 255 means 100 percent reliability and 0 means no reliability.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <i>loading</i>—Effective bandwidth of the route expressed as a number from 0 to 255 (255 is 100 percent loading).</li> <li>• <i>mtu</i>—Minimum maximum transmission unit (MTU) size of the route in bytes in the range 0 to 4294967295.</li> </ul>
<b>Step 19</b>	<b>set metric-type {type-1   type-2}</b> <b>Example:</b> <pre>Switch(config-route-map)# set metric-type type-2</pre>	Sets the OSPF external metric type for redistributed routes.
<b>Step 20</b>	<b>set metric-type internal</b> <b>Example:</b> <pre>Switch(config-route-map)# set metric-type internal</pre>	Sets the multi-exit discriminator (MED) value on prefixes advertised to external BGP neighbor to match the IGP metric of the next hop.
<b>Step 21</b>	<b>set weight <i>number</i></b> <b>Example:</b> <pre>Switch(config-route-map)# set weight 100</pre>	Sets the BGP weight for the routing table. The value can be from 1 to 65535.
<b>Step 22</b>	<b>end</b> <b>Example:</b> <pre>Switch(config-route-map)# end</pre>	Returns to privileged EXEC mode.
<b>Step 23</b>	<b>show route-map</b> <b>Example:</b> <pre>Switch# show route-map</pre>	Displays all route maps configured or only the one specified to verify configuration.
<b>Step 24</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## How to Control Route Distribution

Although each of Steps 3 through 14 in the following section is optional, you must enter at least one **match** route-map configuration command and one **set** route-map configuration command.



**Note** The keywords are the same as defined in the procedure to configure the route map for redistribution.

The metrics of one routing protocol do not necessarily translate into the metrics of another. For example, the RIP metric is a hop count, and the IGRP metric is a combination of five qualities. In these situations, an artificial metric is assigned to the redistributed route. Uncontrolled exchanging of routing information between different routing protocols can create routing loops and seriously degrade network operation.

If you have not defined a default redistribution metric that replaces metric conversion, some automatic metric translations occur between routing protocols:

- RIP can automatically redistribute static routes. It assigns static routes a metric of 1 (directly connected).
- Any protocol can redistribute other routing protocols if a default mode is in effect.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>router { rip   ospf   eigrp }</b> <b>Example:</b>  Switch(config)# router eigrp 10	Enters router configuration mode.
<b>Step 3</b>	<b>redistribute protocol [process-id] {level-1   level-1-2   level-2} [metric metric-value] [metric-type type-value] [match internal   external type-value] [tag tag-value] [route-map map-tag] [weight weight] [subnets]</b> <b>Example:</b>  Switch(config-router)# redistribute eigrp 1	Redistributes routes from one routing protocol to another routing protocol. If no route-maps are specified, all routes are redistributed. If the keyword <b>route-map</b> is specified with no <i>map-tag</i> , no routes are distributed.
<b>Step 4</b>	<b>default-metric number</b> <b>Example:</b>  Switch(config-router)# default-metric 1024	Cause the current routing protocol to use the same metric value for all redistributed routes ( RIP and OSPF).
<b>Step 5</b>	<b>default-metric bandwidth delay reliability loading mtu</b> <b>Example:</b>  Switch(config-router)# default-metric 1000 100 250 100 1500	Cause the EIGRP routing protocol to use the same metric value for all non-EIGRP redistributed routes.
<b>Step 6</b>	<b>end</b> <b>Example:</b>  Switch(config-router)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
<b>Step 7</b>	<b>show route-map</b> <b>Example:</b> Switch# show route-map	Displays all route maps configured or only the one specified to verify configuration.
<b>Step 8</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## Policy-Based Routing

### Information About Policy-Based Routing

You can use policy-based routing (PBR) to configure a defined policy for traffic flows. By using PBR, you can have more control over routing by reducing the reliance on routes derived from routing protocols. PBR can specify and implement routing policies that allow or deny paths based on:

- Identity of a particular end system
- Application
- Protocol

You can use PBR to provide equal-access and source-sensitive routing, routing based on interactive versus batch traffic, or routing based on dedicated links. For example, you could transfer stock records to a corporate office on a high-bandwidth, high-cost link for a short time while transmitting routine application data such as e-mail over a low-bandwidth, low-cost link.

With PBR, you classify traffic using access control lists (ACLs) and then make traffic go through a different path. PBR is applied to incoming packets. All packets received on an interface with PBR enabled are passed through route maps. Based on the criteria defined in the route maps, packets are forwarded (routed) to the appropriate next hop.

- Route map statement marked as permit is processed as follows:
  - A match command can match on length or multiple ACLs. A route map statement can contain multiple match commands. Logical or algorithm function is performed across all the match commands to reach a permit or deny decision.

For example:

```
match length A B
match ip address ac11 ac12
match ip address ac13
```

A packet is permitted if it is permitted by match length A B or ac11 or ac12 or ac13

- If the decision reached is permit, then the action specified by the set command is applied on the packet .

- If the decision reached is deny, then the PBR action (specified in the set command) is not applied. Instead the processing logic moves forward to look at the next route-map statement in the sequence (the statement with the next higher sequence number). If no next statement exists, PBR processing terminates, and the packet is routed using the default IP routing table.
- For PBR, route-map statements marked as deny are not supported.

You can use standard IP ACLs to specify match criteria for a source address or extended IP ACLs to specify match criteria based on an application, a protocol type, or an end station. The process proceeds through the route map until a match is found. If no match is found, normal destination-based routing occurs. There is an implicit deny at the end of the list of match statements.

If match clauses are satisfied, you can use a set clause to specify the IP addresses identifying the next hop router in the path.

## How to Configure PBR

- To use PBR, you must have the feature set enabled on the switch or active stack.
- Multicast traffic is not policy-routed. PBR applies to only to unicast traffic.
- You can enable PBR on a routed port or an SVI.
- The switch supports PBR based on match length.
- You can apply a policy route map to an EtherChannel port channel in Layer 3 mode, but you cannot apply a policy route map to a physical interface that is a member of the EtherChannel. If you try to do so, the command is rejected. When a policy route map is applied to a physical interface, that interface cannot become a member of an EtherChannel.
- You can define a maximum of 128 IP policy route maps on the switch or switch stack.
- You can define a maximum of 512 access control entries (ACEs) for PBR on the switch or switch stack.
- When configuring match criteria in a route map, follow these guidelines:
  - Do not match ACLs that permit packets destined for a local address. PBR would forward these packets, which could cause ping or Telnet failure or route protocol flapping.
- VRF and PBR are mutually exclusive on a switch interface. You cannot enable VRF when PBR is enabled on an interface. The reverse is also true, you cannot enable PBR when VRF is enabled on an interface.
- The number of hardware entries used by PBR depends on the route map itself, the ACLs used, and the order of the ACLs and route-map entries.
- PBR based on TOS, DSCP and IP Precedence are not supported.
- Set interface, set default next-hop and set default interface are not supported.
- **ip next-hop recursive** and **ip next-hop verify availability** features are not available and the next-hop should be directly connected.
- Policy-maps with no set actions are supported. Matching packets are routed normally.
- Policy-maps with no match clauses are supported. Set actions are applied to all packets.

By default, PBR is disabled on the switch. To enable PBR, you must create a route map that specifies the match criteria and the resulting action. Then, you must enable PBR for that route map on an interface. All packets arriving on the specified interface matching the match clauses are subject to PBR.

Packets that are generated by the switch, or local packets, are not normally policy-routed. When you globally enable local PBR on the switch, all packets that originate on the switch are subject to local PBR. Local PBR is disabled by default.

### Procedure

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> Switch# configure terminal	Enters global configuration mode.
Step 2	<b>route-map</b> <i>map-tag</i> [ <b>permit</b> ] [ <i>sequence number</i> ] <b>Example:</b> Switch(config)# route-map pbr-map permit	Defines route maps that are used to control where packets are output, and enters route-map configuration mode. <ul style="list-style-type: none"> <li>• <i>map-tag</i> — A meaningful name for the route map. The <b>ip policy route-map</b> interface configuration command uses this name to reference the route map. Multiple route-map statements with the same map tag define a single route map.</li> <li>• (Optional) <b>permit</b> — If <b>permit</b> is specified and the match criteria are met for this route map, the route is policy routed as defined by the set actions.</li> <li>• (Optional) <i>sequence number</i> — The sequence number shows the position of the route-map statement in the given route map.</li> </ul>
Step 3	<b>match ip address</b> { <i>access-list-number</i>   <i>access-list-name</i> } [ <i>access-list-number</i>   ... <i>access-list-name</i> ] <b>Example:</b> Switch(config-route-map)# match ip address 110 140	Matches the source and destination IP addresses that are permitted by one or more standard or extended access lists. ACLs can match on more than one source and destination IP address.  If you do not specify a <b>match</b> command, the route map is applicable to all packets.
Step 4	<b>match length</b> <i>min max</i> <b>Example:</b> Switch(config-route-map)# match length 64 1500	Matches the length of the packet.
Step 5	<b>set ip next-hop</b> <i>ip-address</i> [... <i>ip-address</i> ] <b>Example:</b> Switch(config-route-map)# set ip next-hop 10.1.6.2	Specifies the action to be taken on the packets that match the criteria. Sets next hop to which to route the packet (the next hop must be adjacent).
Step 6	<b>set ip next-hop verify-availability</b> [ <i>next-hop-address</i> <i>sequence</i> <b>track</b> <i>object</i> ] <b>Example:</b>	Configures the route map to verify the reachability of the tracked object.

	Command or Action	Purpose
	Switch(config-route-map)# set ip next-hop verify-availability 95.1.1.2.1 track 100	<b>Note</b> This command is not supported on IPv6 and VRF.
<b>Step 7</b>	<b>exit</b> <b>Example:</b> Switch(config-route-map)# exit	Returns to global configuration mode.
<b>Step 8</b>	<b>interface</b> <i>interface-id</i> <b>Example:</b> Switch(config)# interface gigabitethernet 1/0/1	Enters interface configuration mode, and specifies the interface to be configured.
<b>Step 9</b>	<b>ip policy route-map</b> <i>map-tag</i> <b>Example:</b> Switch(config-if)# ip policy route-map pbr-map	Enables PBR on a Layer 3 interface, and identify the route map to use. You can configure only one route map on an interface. However, you can have multiple route map entries with different sequence numbers. These entries are evaluated in the order of sequence number until the first match. If there is no match, packets are routed as usual.
<b>Step 10</b>	<b>ip route-cache policy</b> <b>Example:</b> Switch(config-if)# ip route-cache policy	(Optional) Enables fast-switching PBR. You must enable PBR before enabling fast-switching PBR.
<b>Step 11</b>	<b>exit</b> <b>Example:</b> Switch(config-if)# exit	Returns to global configuration mode.
<b>Step 12</b>	<b>ip local policy route-map</b> <i>map-tag</i> <b>Example:</b> Switch(config)# ip local policy route-map local-pbr	(Optional) Enables local PBR to perform policy-based routing on packets originating at the switch. This applies to packets generated by the switch, and not to incoming packets.
<b>Step 13</b>	<b>end</b> <b>Example:</b> Switch(config)# end	Returns to privileged EXEC mode.
<b>Step 14</b>	<b>show route-map</b> [ <i>map-name</i> ] <b>Example:</b> Switch# show route-map	(Optional) Displays all the route maps configured or only the one specified to verify configuration.
<b>Step 15</b>	<b>show ip policy</b> <b>Example:</b> Switch# show ip policy	(Optional) Displays policy route maps attached to the interface.
<b>Step 16</b>	<b>show ip local policy</b> <b>Example:</b> Switch# show ip local policy	(Optional) Displays whether or not local policy routing is enabled and, if so, the route map being used.

## Filtering Routing Information

You can filter routing protocol information by performing the tasks described in this section.



**Note** When routes are redistributed between OSPF processes, no OSPF metrics are preserved.

## Setting Passive Interfaces

To prevent other routers on a local network from dynamically learning about routes, you can use the **passive-interface** router configuration command to keep routing update messages from being sent through a router interface. When you use this command in the OSPF protocol, the interface address you specify as passive appears as a stub network in the OSPF domain. OSPF routing information is neither sent nor received through the specified router interface.

In networks with many interfaces, to avoid having to manually set them as passive, you can set all interfaces to be passive by default by using the **passive-interface default** router configuration command and manually setting interfaces where adjacencies are desired.

Use a network monitoring privileged EXEC command such as **show ip ospf interface** to verify the interfaces that you enabled as passive, or use the **show ip interface** privileged EXEC command to verify the interfaces that you enabled as active.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 2</b>	<b>router { rip   ospf   eigrp }</b> <b>Example:</b>  Switch(config)# <code>router ospf</code>	Enters router configuration mode.
<b>Step 3</b>	<b>passive-interface <i>interface-id</i></b> <b>Example:</b>  Switch(config-router)# <code>passive-interface gigabitethernet 1/0/1</code>	Suppresses sending routing updates through the specified Layer 3 interface.
<b>Step 4</b>	<b>passive-interface default</b> <b>Example:</b>  Switch(config-router)# <code>passive-interface default</code>	(Optional) Sets all interfaces as passive by default.
<b>Step 5</b>	<b>no passive-interface <i>interface type</i></b> <b>Example:</b>	(Optional) Activates only those interfaces that need to have adjacencies sent.



	Command or Action	Purpose
	Switch(config-router)# no passive-interface gigabitethernet1/0/3 gigabitethernet 1/0/5	
<b>Step 6</b>	<b>network</b> <i>network-address</i> <b>Example:</b>  Switch(config-router)# network 10.1.1.1	(Optional) Specifies the list of networks for the routing process. The <i>network-address</i> is an IP address.
<b>Step 7</b>	<b>end</b> <b>Example:</b>  Switch(config-router)# end	Returns to privileged EXEC mode.
<b>Step 8</b>	<b>copy running-config startup-config</b> <b>Example:</b>  Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## Controlling Advertising and Processing in Routing Updates

You can use the **distribute-list** router configuration command with access control lists to suppress routes from being advertised in routing updates and to prevent other routers from learning one or more routes. When used in OSPF, this feature applies to only external routes, and you cannot specify an interface name.

You can also use a **distribute-list** router configuration command to avoid processing certain routes listed in incoming updates. (This feature does not apply to OSPF.)

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b>  Switch# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>router { rip   eigrp }</b> <b>Example:</b>  Switch(config)# router eigrp 10	Enters router configuration mode.
<b>Step 3</b>	<b>distribute-list {access-list-number   access-list-name} out</b> <i>[interface-name   routing process   autonomous-system-number]</i> <b>Example:</b>  Switch(config-router)# distribute-list 120 out gigabitethernet 1/0/7	Permits or denies routes from being advertised in routing updates, depending upon the action listed in the access list.

	Command or Action	Purpose
<b>Step 4</b>	<b>distribute-list</b> { <i>access-list-number</i>   <i>access-list-name</i> } <b>in</b> [ <i>type-number</i> ] <b>Example:</b> Switch(config-router)# distribute-list 125 in	Suppresses processing in routes listed in updates.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Switch(config-router)# end	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

## Filtering Sources of Routing Information

Because some routing information might be more accurate than others, you can use filtering to prioritize information coming from different sources. An administrative distance is a rating of the trustworthiness of a routing information source, such as a router or group of routers. In a large network, some routing protocols can be more reliable than others. By specifying administrative distance values, you enable the router to intelligently discriminate between sources of routing information. The router always picks the route whose routing protocol has the lowest administrative distance.

Because each network has its own requirements, there are no general guidelines for assigning administrative distances.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>configure terminal</b> <b>Example:</b> Switch# configure terminal	Enters global configuration mode.
<b>Step 2</b>	<b>router</b> { <b>rip</b>   <b>ospf</b>   <b>eigrp</b> } <b>Example:</b> Switch(config)# router eigrp 10	Enters router configuration mode.
<b>Step 3</b>	<b>distance</b> <i>weight</i> { <i>ip-address</i> { <i>ip-address mask</i> }} [ <i>ip access list</i> ] <b>Example:</b> Switch(config-router)# distance 50 10.1.5.1	Defines an administrative distance.  <i>weight</i> —The administrative distance as an integer from 10 to 255. Used alone, <i>weight</i> specifies a default administrative distance that is used when no other specification exists for a routing information source. Routes with a distance of 255 are not installed in the routing table.

	Command or Action	Purpose
		(Optional) <i>ip access list</i> —An IP standard or extended access list to be applied to incoming routing updates.
Step 4	<b>end</b> <b>Example:</b> <pre>Switch(config-router)# end</pre>	Returns to privileged EXEC mode.
Step 5	<b>show ip protocols</b> <b>Example:</b> <pre>Switch# show ip protocols</pre>	Displays the default administrative distance for a specified routing process.
Step 6	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Managing Authentication Keys

Key management is a method of controlling authentication keys used by routing protocols. Not all protocols can use key management. Authentication keys are available for EIGRP and RIP Version 2.

### Prerequisites

Before you manage authentication keys, you must enable authentication. See the appropriate protocol section to see how to enable authentication for that protocol. To manage authentication keys, define a key chain, identify the keys that belong to the key chain, and specify how long each key is valid. Each key has its own key identifier (specified with the **key number** key chain configuration command), which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use.

### How to Configure Authentication Keys

You can configure multiple keys with life times. Only one authentication packet is sent, regardless of how many valid keys exist. The software examines the key numbers in order from lowest to highest, and uses the first valid key it encounters. The lifetimes allow for overlap during key changes. Note that the router must know these lifetimes.

#### Procedure

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.

	Command or Action	Purpose
<b>Step 2</b>	<b>key chain</b> <i>name-of-chain</i> <b>Example:</b> <pre>Switch(config)# key chain key10</pre>	Identifies a key chain, and enter key chain configuration mode.
<b>Step 3</b>	<b>key number</b> <b>Example:</b> <pre>Switch(config-keychain)# key 2000</pre>	Identifies the key number. The range is 0 to 2147483647.
<b>Step 4</b>	<b>key-string</b> <i>text</i> <b>Example:</b> <pre>Switch(config-keychain)# key-string Room 20, 10th floor</pre>	Identifies the key string. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters, but the first character cannot be a number.
<b>Step 5</b>	<b>accept-lifetime</b> <i>start-time</i> { <b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i> } <b>Example:</b> <pre>Switch(config-keychain)# accept-lifetime 12:30:00 Jan 25 1009 infinite</pre>	(Optional) Specifies the time period during which the key can be received.  The <i>start-time</i> and <i>end-time</i> syntax can be either <i>hh:mm:ss Month date year</i> or <i>hh:mm:ss date Month year</i> . The default is forever with the default <i>start-time</i> and the earliest acceptable date as January 1, 1993. The default <i>end-time</i> and <b>duration</b> is <b>infinite</b> .
<b>Step 6</b>	<b>send-lifetime</b> <i>start-time</i> { <b>infinite</b>   <i>end-time</i>   <b>duration</b> <i>seconds</i> } <b>Example:</b> <pre>Switch(config-keychain)# accept-lifetime 23:30:00 Jan 25 1019 infinite</pre>	(Optional) Specifies the time period during which the key can be sent.  The <i>start-time</i> and <i>end-time</i> syntax can be either <i>hh:mm:ss Month date year</i> or <i>hh:mm:ss date Month year</i> . The default is forever with the default <i>start-time</i> and the earliest acceptable date as January 1, 1993. The default <i>end-time</i> and <b>duration</b> is <b>infinite</b> .
<b>Step 7</b>	<b>end</b> <b>Example:</b> <pre>Switch(config-keychain)# end</pre>	Returns to privileged EXEC mode.
<b>Step 8</b>	<b>show key chain</b> <b>Example:</b> <pre>Switch# show key chain</pre>	Displays authentication key information.
<b>Step 9</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

# Monitoring and Maintaining the IP Network

You can remove all contents of a particular cache, table, or database. You can also display specific statistics.

*Table 12: Commands to Clear IP Routes or Display Route Status*

Command	Purpose
<b>show ip route</b> [ <i>address</i> [ <i>mask</i> ] [ <b>longer-prefixes</b> ]]	Displays the current state of the routing table.
<b>show ip route summary</b>	Displays the current state of the routing table in summary.
<b>show platform ip unicast</b>	Displays platform-dependent IP unicast information.

