



IP Addressing Commands

clear host

To delete hostname-to-address mapping entries from one or more hostname caches, use the **clear host** command in privileged EXEC mode.

```
clear host [view view-name | vrf vrf-name | all] {hostname | *}
```

Syntax Description

view <i>view-name</i>	(Optional) The <i>view-name</i> argument specifies the name of the Domain Name System (DNS) view whose hostname cache is to be cleared. Default is the default DNS view associated with the specified or global Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf <i>vrf-name</i>	(Optional) The <i>vrf-name</i> argument specifies the name of the VRF associated with the DNS view whose hostname cache is to be cleared. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view.
all	(Optional) Specifies that hostname-to-address mappings are to be deleted from the hostname cache of every configured DNS view.
<i>hostname</i>	Name of the host for which hostname-to-address mappings are to be deleted from the specified hostname cache.
*	Specifies that all the hostname-to-address mappings are to be deleted from the specified hostname cache.

Command Default

No hostname-to-address mapping entries are deleted from any hostname cache.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.4(4)T	The vrf keyword, <i>vrf-name</i> argument, and all keyword were added.
12.4(9)T	The view keyword and <i>view-name</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command clears the specified hostname cache entries in running memory, but it does not remove the entries from NVRAM.

Entries can be removed from the hostname caches for a DNS view name, from the hostname caches for a VRF, or from all configured hostname caches. To remove entries from hostname caches for a particular DNS view name, use the **view** keyword and *view-name* argument. To remove entries from the hostname caches for a particular VRF, use the **vrf** keyword and *vrf-name* argument. To remove entries from all configured hostname caches, use the **all** keyword.

To remove entries that provide mapping information for a single hostname, use the *hostname* argument. To remove all entries, use the *** keyword.

To display the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views, use the **show hosts** command.

To define static hostname-to-address mappings in the DNS hostname cache for a DNS view, use the **ip host** command.

Examples

The following example shows how to clear all entries from the hostname cache for the default view in the global address space:

```
Router# clear host all *
```

The following example shows how to clear entries for the hostname `www.example.com` from the hostname cache for the default view associated with the VPN named `vpn101`:

```
Router# clear host vrf vpn101 www.example.com
```

The following example shows how to clear all entries from the hostname cache for the view named `user2` in the global address space:

```
Router# clear host view user2 *
```

Related Commands

Command	Description
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

clear ip route

To delete routes from the IP routing table, use the **clear ip route** command in EXEC mode.

```
clear ip route {network [mask] | *}
```

Syntax Description

<i>network</i>	Network or subnet address to remove.
<i>mask</i>	(Optional) Subnet address to remove.
*	Removes all routing table entries.

Defaults

All entries are removed.

Command Modes

EXEC

Command History

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

Examples

The following example removes a route to network 10.5.0.0 from the IP routing table:

```
Router> clear ip route 10.5.0.0
```

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

no ip address *ip-address mask* [**secondary** [**vrf** *vrf-name*]]

Syntax Description

<i>ip-address</i>	IP address.
<i>mask</i>	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. Note If the secondary address is used for a VRF table configuration with the vrf keyword, the vrf keyword must be specified also.
vrf	(Optional) Name of the VRF table. The <i>vrf-name</i> argument specifies the VRF name of the ingress interface.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(28)SB	The vrf keyword and <i>vrf-name</i> argument were introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all routers and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Routers respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.

**Note**

If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

**Note**

When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

To transparently bridge IP on an interface, you must perform the following two tasks:

- Disable IP routing (specify the **no ip routing** command).
- Add the interface to a bridge group, see the **bridge-group** command.

To concurrently route and transparently bridge IP on an interface, see the **bridge crb** command.

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for Ethernet interface 0:

```
interface ethernet 0
 ip address 192.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
 ip address 192.31.8.17 255.255.255.0 secondary
```

In the following example, Ethernet interface 0/1 is configured to automatically classify the source IP address in the VRF table vrf1:

```
interface ethernet 0/1
 ip address 10.108.1.27 255.255.255.0
 ip address 10.31.7.17 255.255.255.0 secondary vrf vrf1
 ip vrf autclassify source
```

Related Commands	Command	Description
	bridge crb	Enables the Cisco IOS software to both route and bridge a given protocol on separate interfaces within a single router.
	bridge-group	Assigns each network interface to a bridge group.
	ip vrf autoclassify	Enables VRF autoclassify on a source interface.
	match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
	route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
	set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
	show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
	show ip interface	Displays the usability status of interfaces configured for IP.
	show route-map	Displays static and dynamic route maps.

ip classless

To enable a router to forward packets, which are destined for a subnet of a network that has no network default route, to the best supernet route possible, use the **ip classless** command in global configuration mode. To disable the functionality, use the **no** form of this command.

ip classless

no ip classless

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	11.3	The default behavior changed from disabled to enabled.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines This command allows the software to forward packets that are destined for unrecognized subnets of directly connected networks. The packets are forwarded to the best supernet route.

When this feature is disabled, the Cisco IOS software discards the packets when a router receives packets for a subnet that numerically falls within its subnetwork addressing scheme, no such subnet number is in the routing table, and there is no network default route.



Note

If the supernet or default route is learned by using Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF), the **no ip classless** configuration command is ignored.

Examples The following example prevents the software from forwarding packets destined for an unrecognized subnet to the best supernet possible:

```
no ip classless
```

ip default-gateway

To define a default gateway (router) when IP routing is disabled, use the **ip default-gateway** command in global configuration mode. To disable this function, use the **no** form of this command.

ip default-gateway *ip-address*

no ip default-gateway *ip-address*

Syntax Description	<i>ip-address</i>	IP address of the router.
---------------------------	-------------------	---------------------------

Defaults	Disabled	
-----------------	----------	--

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

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

Usage Guidelines	The Cisco IOS software sends any packets that need the assistance of a gateway to the address you specify. If another gateway has a better route to the requested host, the default gateway sends an Internet Control Message Protocol (ICMP) redirect message back. The ICMP redirect message indicates which local router the Cisco IOS software should use.
-------------------------	--

Examples	The following example defines the router on IP address 192.31.7.18 as the default router: <pre>ip default-gateway 192.31.7.18</pre>
-----------------	--

Related Commands	Command	Description
	ip redirects	Enables the sending of ICMP redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received.
	show ip redirects	Displays the address of a default gateway (router) and the address of hosts for which an ICMP redirect message has been received.

ip host

To define static hostname-to-address mappings in the Domain Name System (DNS) hostname cache for a DNS view, use the **ip host** command in global configuration mode. If the hostname cache does not exist yet, it is automatically created. To remove a hostname-to-address mapping, use the **no** form of this command.

```
ip host [vrf vrf-name] [view view-name] {hostname | tmodem-telephone-number}
[tcp-port-number] {ip-address1 [ip-address2...ip-address8] | additional ip-address9
[ip-address10...ip-addressn] | [mx preference mx-server-hostname | ns nameserver-hostname |
```

```
srv priority weight port target}}
```

```
no ip host [vrf vrf-name] [view view-name] {hostname | tmodem-telephone-number}
[tcp-port-number] {ip-address1 [ip-address2...ip-address8] additional ip-address9
[ip-address10...ip-addressn] | [mx preference mx-server-hostname | ns nameserver-hostname |
```

```
srv priority weight port target}}
```

Syntax Description

vrf <i>vrf-name</i>	(Optional) The <i>vrf-name</i> argument specifies the name of the Virtual Private Network (VRF) routing and forwarding (VRF) instance associated with the DNS view whose hostname cache is to store the mappings. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view. Note More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
view <i>view-name</i>	(Optional) The <i>view-name</i> argument specifies the name of the DNS view whose hostname cache is to store the mappings. Default is the default DNS view associated with the specified or global VRF. Note More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
<i>hostname</i>	Name of the host. The first character can be either a letter or a number. If you use a number, the types of operations you can perform (such as ping) are limited.
tmodem-telephone-number	Modem telephone number that is mapped to the IP host address for use in Cisco modem user interface mode. You must enter the letter “t” before the telephone number. Note This argument is not relevant to the Split DNS feature.
<i>tcp-port-number</i>	(Optional) TCP port number to connect to when using the defined hostname in conjunction with an EXEC connect or Telnet command. The default is Telnet (port 23).
<i>ip-address1</i>	Associated host IP address.
<i>ip-address2...ip-address8</i>	(Optional) Up to seven additional associated IP addresses, delimited by a single space. Note The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.

additional <i>ip-address9</i>	The <i>ip-address9</i> argument specifies an additional IP address to add to the hostname cache. Note The use of the optional additional keyword enables the addition of more than eight IP addresses to the hostname cache.
<i>ip-address10...ip-addressn</i>	Additional associated IP addresses, delimited by a single space. Note The ellipses in the syntax description are used to indicate a range of values. Do not use ellipses when entering host IP addresses.
mx <i>preference</i> <i>mx-server-hostname</i>	Mail Exchange (MX) resource record settings for the host: <ul style="list-style-type: none"> <i>preference</i>—The order in which mailers select MX records when they attempt mail delivery to the host. The lower this value, the higher the host is in priority. Range is from 0 to 65535. <i>mx-server-hostname</i>—The DNS name of the SMTP server where the mail for a domain name should be delivered. <p>An MX record specifies how you want e-mail to be accepted for the domain specified in the <i>hostname</i> argument.</p> <p>Note You can have several MX records for a single domain name, and they can be ranked in order of preference.</p>
ns <i>nameserver-hostname</i>	Name Server (NS) resource record setting for the host: <ul style="list-style-type: none"> <i>nameserver-hostname</i>—The DNS name of the machine that provides domain service for the particular domain. Machines that provide name service do not have to reside in the named domain. <p>An NS record lists the name of the machine that provides domain service for the domain indicated by the <i>hostname</i> argument.</p> <p>Note For each domain you must have at least one NS record. NS records for a domain must exist in both the zone that delegates the domain and in the domain itself.</p>
srv <i>priority weight port</i> <i>target</i>	Server (SRV) resource record settings for the host: <ul style="list-style-type: none"> <i>priority</i>—The priority to give the record among the owner SRV records. Range is from 0 to 65535. <i>weight</i>—The load to give the record at the same priority level. Range is from 0 to 65535. <i>port</i>—The port on which to run the service. Range is from 0 to 65535. <i>target</i>—Domain name of host running on the specified port. <p>The use of SRV records enables administrators to use several servers for a single domain, to move services from host to host with little difficulty, and to designate some hosts as primary servers for a service and others as backups. Clients ask for a specific service or protocol for a specific domain and receive the names of any available servers.</p>

Command Default No static hostname-to-address mapping is added to the DNS hostname cache for a DNS view.

Command Modes Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The mx keyword and the <i>preference</i> and <i>mx-server-hostname</i> arguments were added.
12.0(7)T	The srv keyword and the <i>priority</i> , <i>weight</i> , <i>port</i> , and <i>target</i> arguments were added.
12.2(1)T	The ns keyword and the <i>nameserver-hostname</i> argument were added.
12.4(4)T	The capability to map a modem telephone number to an IP host was added for the Cisco modem user interface feature.
12.4(4)T	The vrf keyword and <i>vrf-name</i> argument were added.
12.4(9)T	The view keyword and <i>view-name</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command adds the specified hostname-to-IP address mappings as follows:

- If no VRF name and no DNS view name is specified, the mappings are added to the global hostname cache.
- Otherwise, the mappings are added to the DNS hostname cache for a specific DNS view:
 - If only a DNS view name is specified, the specified mappings are created in the view-specific hostname cache.
 - If only a VRF name is specified, the specified mappings are created in the VRF-specific hostname cache for the default view.
 - If both a VRF name and a DNS view name are specified, the specified mappings are created in the VRF-specific hostname cache for the specified view.

If the specified VRF does not exist yet, a warning is displayed and the entry is added to the hostname cache anyway.

If the specified view does not exist yet, a warning is displayed and the entry is added to the hostname cache anyway.

If the hostname cache does not exist yet, it is automatically created.

To specify the machine that provides domain service for the domain, use the **ns** keyword and the *nameserver-hostname* argument

To specify where the mail for the host is to be sent, use the **mx** keyword and the *preference* and *mx-server-hostname* arguments.

To specify a host that offers a service in the domain, use the **srv** keyword and the *priority*, *weight*, *port*, and *target* arguments.

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views, use the **show hosts** command.

**Note**

If a global or VRF-specific DNS hostname cache contains hostnames that are associated with multiple IP addresses, round-robin rotation of the returned addresses can be enabled on a DNS view-specific basis (by using the **domain round-robin** command).

Examples

The following example shows how to add three mapping entries to the global hostname cache and then remove one of those entries from the global hostname cache:

```
Router(config)# ip host www.example1.com 192.0.2.141 192.0.2.241
Router(config)# ip host www.example2.com 192.0.2.242
Router(config)# no ip host www.example1.com 192.0.2.141
```

The following example shows how to add three mapping entries to the hostname cache for the DNS view user3 that is associated with the VRF vpn101 and then remove one of those entries from that hostname cache:

```
Router(config)# ip host vrf vpn101 view user3 www.example1.com 192.0.2.141 192.0.2.241
Router(config)# ip host vrf vpn101 view user3 www.example2.com 192.0.2.242
Router(config)# no ip host vrf vpn101 view user3 www.example1.com 192.0.2.141
```

Related Commands

Command	Description
clear host	Removes static hostname-to-address mappings from the hostname cache for the specified DNS view or all DNS views.
domain round-robin	Enables round-robin rotation of multiple IP addresses in the global or VRF-specific DNS hostname cache during the TTL of the cache each time DNS lookup is performed to resolve an internally generated DNS query handled using the DNS view.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

ip hp-host

To enter into the host table the host name of a Hewlett-Packard (HP) host to be used for HP Probe Proxy service, use the **ip hp-host** global configuration command. To remove a host name, use the **no** form of this command.

ip hp-host *host-name ip-address*

no ip hp-host *host-name ip-address*

Syntax Description

<i>host-name</i>	Name of the host.
<i>ip-address</i>	IP address of the host.

Defaults

No host names are defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	This command is no longer available from Cisco IOS Mainline or Technology-based (T) releases. It may still appear in Cisco IOS S-Family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To use the HP Probe Proxy service, you must first enter the host name of the HP host into the host table using this command.

Examples

The following example specifies the name and address of an HP host, and then enables HP Probe Proxy:

```
ip hp-host BCWjo 131.108.1.27
interface fastethernet 0
ip probe proxy
```

Related Commands

Command	Description
ip probe proxy	Enables the HP Probe Proxy support, which allows the Cisco IOS software to respond to HP Probe Proxy name requests.

ip mobile arp

To enable local-area mobility, use the **ip mobile arp** command in interface configuration mode. To disable local-area mobility, use the **no** form of this command.

ip mobile arp [**timers** *keepalive hold-time*] [**access-group** *access-list-number* | *name*]

no ip mobile arp [**timers** *keepalive hold-time*] [**access-group** *access-list-number* | *name*]

Syntax Description	
timers	(Optional) Indicates that you are setting local-area mobility timers.
<i>keepalive</i>	(Optional) Frequency, in minutes, at which the Cisco IOS software sends unicast Address Resolution Protocol (ARP) messages to a relocated host to verify that the host is present and has not moved. The default keepalive time is 5 minutes (300 seconds).
<i>hold-time</i>	(Optional) Hold time, in minutes. This is the length of time the software considers that a relocated host is present without receiving some type of ARP broadcast or unicast from the host. Normally, the hold time should be at least three times greater than the keepalive time. The default hold time is 15 minutes (900 seconds).
access-group	(Optional) Indicates that you are applying an access list. This access list applies only to local-area mobility.
<i>access-list-number</i>	(Optional) Number of a standard IP access list. It is a decimal number from 1 to 99. Only hosts with addresses permitted by this access list are accepted for local-area mobility.
<i>name</i>	(Optional) Name of an IP access list. The name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid ambiguity with numbered access lists.

Defaults

Local-area mobility is disabled.

If you enable local-area mobility:

keepalive: 5 minutes (300 seconds)

hold-time: 15 minutes (900 seconds)

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Local-area mobility is supported on Ethernet, Token Ring, and FDDI interfaces only.

To create larger mobility areas, you must first redistribute the mobile routes into your Interior Gateway Protocol (IGP). The IGP must support host routes. You can use Enhanced IGRP, Open Shortest Path First (OSPF), or Intermediate System-to-Intermediate System (IS-IS); you can also use Routing Information Protocol (RIP), but RIP is not recommended. The mobile area must consist of a contiguous set of subnets.

Using an access list to control the list of possible mobile nodes is strongly encouraged. Without an access list, misconfigured hosts can be taken for mobile nodes and disrupt normal operations.

Examples

The following example configures local-area mobility on Ethernet interface 0:

```
access-list 10 permit 10.92.37.114
interface fastethernet 0
 ip mobile arp access-group 10
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
default-metric (BGP)	Sets default metric values for the BGP, OSPF, and RIP routing protocols.
default-metric (OSPF)	Sets default metric values for OSPF.
default-metric (RIP)	Sets default metric values for RIP.
network (BGP)	Specifies the list of networks for the BGP routing process.
network (IGRP)	Specifies a list of networks for the IGRP or Enhanced IGRP routing process.
network (RIP)	Specifies a list of networks for the RIP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
router eigrp	Configures the IP Enhanced IGRP routing process.
router isis	Enables the IS-IS routing protocol and specifies an IS-IS process for IP.
router ospf	Configures an OSPF routing process.

ip netmask-format

To specify the format in which netmasks are displayed in **show** command output, use the **ip netmask-format** command in line configuration mode. To restore the default display format, use the **no** form of this command.

```
ip netmask-format {bit-count | decimal | hexadecimal}
```

```
no ip netmask-format {bit-count | decimal | hexadecimal}
```

Syntax Description

bit-count	Addresses are followed by a slash and the total number of bits in the netmask. For example, 131.108.11.0/24 indicates that the netmask is 24 bits.
decimal	Network masks are displayed in dotted-decimal notation (for example, 255.255.255.0).
hexadecimal	Network masks are displayed in hexadecimal format, as indicated by the leading 0X (for example, 0XFFFFFF00).

Defaults

Netmasks are displayed in dotted-decimal format.

Command Modes

Line configuration

Command History

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

Usage Guidelines

IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 10.108.11.0 255.255.255.0.

However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 10.108.11.0 0XFFFFFF00.

The bitcount format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 10.108.11.0/24.

Examples

The following example configures network masks for the specified line to be displayed in bitcount notation in the output of **show** commands:

```
line vty 0 4
 ip netmask-format bitcount
```

ip options

To drop or ignore IP options packets that are sent to the router, use the **ip options** command in global configuration mode. To disable this functionality and allow all IP options packets to be sent to the router, use the **no** form of this command.

ip options {drop | ignore}

no ip options {drop | ignore}

Syntax Description

drop	Router drops all IP options packets that it receives.
ignore	Router ignores all options and treats the packets as though they did not have any IP options. (The options are not removed from the packet—just ignored.)
Note	This option is not available on the Cisco 10000 series router.

Defaults

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.3(19)	This command was integrated into Cisco IOS Release 12.3(19).
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 for the PRE3.

Usage Guidelines

The **ip options** command allows you to filter IP options packets, mitigating the effects of IP options on the router, and on downstream routers and hosts.

Drop and ignore modes are mutually exclusive; that is, if the drop mode is configured and you configure the ignore mode, the ignore mode overrides the drop mode.

Cisco 10720 Internet Router

The **ip options ignore** command is not supported. Only drop mode (the **ip options drop** command) is supported.

Cisco 10000 Series Router

This command is only available on the PRE3. The PRE2 does not support this command.

The **ip options ignore** command is not supported. The router supports only the **ip options drop** command.

Examples

The following example shows how to configure the router (and downstream routers) to drop all options packets that enter the network:

```
ip options drop
```

```
% Warning:RSVP and other protocols that use IP Options packets may not function in drop or ignore modes.  
end
```

ip probe proxy

To enable the HP Probe Proxy support, which allows the Cisco IOS software to respond to HP Probe Proxy name requests, use the **ip probe proxy** interface configuration command. To disable HP Probe Proxy, use the **no** form of this command.

ip probe proxy

no ip probe proxy

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(13)T	This command is no longer available from Cisco_IOS Mainline or Cisco_IOS Technology-based (T) releases. It may continue to appear in Cisco_IOS S-Family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

HP Probe Proxy Name requests are typically used at sites that have Hewlett-Packard (HP) equipment and are already using HP Probe.

To use the HP Probe Proxy service, you must first enter the host name of the HP host into the host table using the **ip hp-host** global configuration command.

Examples

The following example specifies an HP host name and address, and then enables Probe Proxy:

```
ip hp-host BCWjo 131.108.1.27
interface fastethernet 0
ip probe proxy
```

Related Commands

Command	Description
ip hp-host	Enters into the host table the host name of an HP host to be used for HP Probe Proxy service.

ip route

To establish static routes, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

```
ip route [vrf vrf-name] prefix mask { ip-address | interface-type interface-number [ip-address] }
[dhcp] [distance] [name next-hop-name] [permanent | track number] [tag tag]
```

```
no ip route [vrf vrf-name] prefix mask { ip-address | interface-type interface-number [ip-address] }
[dhcp] [distance] [name next-hop-name] [permanent | track number] [tag tag]
```

Syntax Description	
vrf <i>vrf-name</i>	(Optional) Configures the name of the VRF by which static routes should be specified.
<i>prefix</i>	IP route prefix for the destination.
<i>mask</i>	Prefix mask for the destination.
<i>ip-address</i>	IP address of the next hop that can be used to reach that network.
<i>interface-type</i> <i>interface-number</i>	Network interface type and interface number.
dhcp	(Optional) Enables a Dynamic Host Configuration Protocol (DHCP) server to assign a static route to a default gateway (option 3). Note Specify the dhcp keyword for each routing protocol.
<i>distance</i>	(Optional) Administrative distance. The default administrative distance for a static route is 1.
name <i>next-hop-name</i>	(Optional) Applies a name to the next hop route.
permanent	(Optional) Specifies that the route will not be removed, even if the interface shuts down.
track <i>number</i>	(Optional) Associates a track object with this route. Valid values for the <i>number</i> argument range from 1 to 500.
tag <i>tag</i>	(Optional) Tag value that can be used as a “match” value for controlling redistribution via route maps.

Command Default No static routes are established.

Command Modes Global configuration (config)

Command History	Release	Modification
	10.0	This command was introduced.
	12.3(2)XE	The track keyword and <i>number</i> argument were added.
	12.3(8)T	The track keyword and <i>number</i> argument were integrated into Cisco IOS Release 12.3(8)T. The dhcp keyword was added.

Release	Modification
12.3(9)	The changes made in Cisco IOS Release 12.3(8)T were added to Cisco IOS Release 12.3(9).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The establishment of a static route is appropriate when the Cisco IOS software cannot dynamically build a route to the destination.

When you specify a DHCP server to assign a static route, the interface type and number and administrative distance may be configured also.

If you specify an administrative distance, you are flagging a static route that can be overridden by dynamic information. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100. Static routes have a default administrative distance of 1.

Static routes that point to an interface on a connected router will be advertised by way of Routing Information Protocol (RIP) and EIGRP regardless of whether **redistribute static** commands are specified for those routing protocols. This situation occurs because static routes that point to an interface are considered in the routing table to be connected and hence lose their static nature. Also, the target of the static route should be included in the **network** (DHCP) command. If this condition is not met, no dynamic routing protocol will advertise the route unless a **redistribute static** command is specified for these protocols. With the following configuration:

```
rtr1 (serial 172.16.188.1/30)-----> rtr2(Fast Ethernet 172.31.1.1/30) ----->

router [rip | eigrp]
network 172.16.188.0
network 172.31.0.0
```

- RIP and EIGRP redistribute the route if the route is pointing to the Fast Ethernet interface:

```
ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
```

RIP and EIGRP do not redistribute the route with the following **ip route** command because of the split horizon algorithm:

```
ip route 172.16.188.252 255.255.255.252 serial 2/1
```

- EIGRP redistributes the route with both of the following commands:

```
ip route 172.16.188.252 255.255.255.252 FastEthernet 0/0
ip route 172.16.188.252 255.255.255.252 serial 2/1
```

With the Open Shortest Path First (OSPF) protocol, static routes that point to an interface are not advertised unless a **redistribute static** command is specified.

Adding a static route to an Ethernet or other broadcast interface (for example, `ip route 0.0.0.0 0.0.0.0 Ethernet 1/2`) will cause the route to be inserted into the routing table only when the interface is up. This configuration is not generally recommended. When the next hop of a static route points to an interface, the router considers each of the hosts within the range of the route to be directly connected through that interface, and therefore it will send Address Resolution Protocol (ARP) requests to any destination addresses that route through the static route.

A logical outgoing interface, for example, a tunnel, needs to be configured for a static route. If this outgoing interface is deleted from the configuration, the static route is removed from the configuration and hence does not show up in the routing table. To have the static route inserted into the routing table again, configure the outgoing interface once again and add the static route to this interface.

The practical implication of configuring the **ip route 0.0.0.0 0.0.0.0 ethernet 1/2** command is that the router will consider all of the destinations that the router does not know how to reach through some other route as directly connected to Ethernet interface 1/2. So the router will send an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause your router to reload.

Specifying a numerical next hop that is on a directly connected interface will prevent the router from using proxy ARP. However, if the interface with the next hop goes down and the numerical next hop can be reached through a recursive route, you may specify both the next hop and interface (for example, **ip route 0.0.0.0 0.0.0.0 ethernet 1/2 10.1.2.3**) with a static route to prevent routes from passing through an unintended interface.



Note

Configuring a default route that points to an interface, such as **ip route 0.0.0.0 0.0.0.0 ethernet 1/2**, displays a warning message. This command causes the router to consider all the destinations that the router cannot reach through an alternate route, as directly connected to Ethernet interface 1/2. Hence, the router sends an ARP request for each host for which it receives packets on this network segment. This configuration can cause high processor utilization and a large ARP cache (along with memory allocation failures). Configuring a default route or other static route that directs the router to forward packets for a large range of destinations to a connected broadcast network segment can cause the router to reload.

The **name next-hop-name** keyword and argument combination allows you to associate static routes with names in your running configuration. If you have several static routes, you can specify names that describe the purpose of each static route in order to more easily identify each one.

The **track number** keyword and argument combination specifies that the static route will be installed only if the state of the configured track object is up.

Recursive Static Routing

In a recursive static route, only the next hop is specified. The output interface is derived from the next hop.

For the following recursive static route example, all destinations with the IP address prefix address prefix 192.168.1.1/32 are reachable via the host with address 10.0.0.2:

```
ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

A recursive static route is valid (that is, it is a candidate for insertion in the IPv4 routing table) only when the specified next hop resolves, either directly or indirectly, to a valid IPv4 output interface, provided the route does not self-recurse, and the recursion depth does not exceed the maximum IPv4 forwarding recursion depth.

The following example defines a valid recursive IPv4 static route:

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
 ip route 192.168.1.1 255.255.255.255 10.0.0.2
```

The following example defines an invalid recursive IPv4 static route. This static route will not be inserted into the IPv4 routing table because it is self-recursive. The next hop of the static route, 192.168.1.0/30, resolves via the first static route 192.168.1.0/24, which is itself a recursive route (that is, it only specifies a next hop). The next hop of the first route, 192.168.1.0/24, resolves via the directly connected route via the serial interface 2/0. Therefore, the first static route would be used to resolve its own next hop.

```
interface serial 2/0
 ip address 10.0.0.1 255.255.255.252
 exit
 ip route 192.168.1.0 255.255.255.0 10.0.0.2
 ip route 192.168.1.0 255.255.255.252 192.168.1.100
```

It is not normally useful to manually configure a self-recursive static route, although it is not prohibited. However, a recursive static route that has been inserted in the IPv4 routing table may become self-recursive as a result of some transient change in the network learned through a dynamic routing protocol. If this situation occurs, the fact that the static route has become self-recursive will be detected and the static route will be removed from the IPv4 routing table, although not from the configuration. A subsequent network change may cause the static route to no longer be self-recursive, in which case it will be re-inserted in the IPv4 routing table.

**Note**

IPv4 recursive static routes are checked at one-minute intervals. Therefore, a recursive static route may take up to a minute to be inserted into the routing table once its next hop becomes valid. Likewise, it may take a minute or so for the route to disappear from the table if its next hop becomes invalid.

Examples

The following example shows how to choose an administrative distance of 110. In this case, packets for network 10.0.0.0 will be routed to a router at 172.31.3.4 if dynamic information with an administrative distance less than 110 is not available.

```
ip route 10.0.0.0 255.0.0.0 172.31.3.4 110
```

**Note**

Specifying the next hop without specifying an interface when configuring a static route can cause traffic to pass through an unintended interface if the default interface goes down.

The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6:

```
ip route 172.31.0.0 255.255.0.0 172.31.6.6
```

The following example shows how to route packets for network 192.168.1.0 directly to the next hop at 10.1.2.3. If the interface goes down, this route is removed from the routing table and will not be restored unless the interface comes back up.

```
ip route 192.168.1.0 255.255.255.0 Ethernet 0 10.1.2.3
```

The following example shows how to install the static route only if the state of track object 123 is up:

```
ip route 0.0.0.0 0.0.0.0 Ethernet 0/1 10.1.1.242 track 123
```

The following example shows that using the **dhcp** keyword in a configuration of Ethernet interfaces 1 and 2 enables the interfaces to obtain the next-hop router IP addresses dynamically from a DHCP server:

```
ip route 10.165.200.225 255.255.255.255 ethernet1 dhcp
ip route 10.165.200.226 255.255.255.255 ethernet2 dhcp 20
```

The following example shows that using the **name** *next-hop-name* keyword and argument combination for each static route in the configuration helps you remember the purpose for each static route.

```
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

The name for the static route will be displayed when the **show running-configuration** command is entered:

```
Router# show running-config | include ip route
```

```
ip route 172.0.0.0 255.0.0.0 10.0.0.1 name Seattle2Detroit
```

Related Commands

Command	Description
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

ip route vrf

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

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

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

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

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

Supported Static Route Configurations

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

Supported Static Routes in an MPLS Environment

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

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

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

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

Unsupported Static Routes in an MPLS Environment That Uses the TFIB

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

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

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

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

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

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

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

Supported Static Routes in an MPLS VPN Environment

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.
redistribute static	Redistributes routes from another routing domain into the specified domain.

ip routing

To enable IP routing, use the **ip routing** command in global configuration mode. To disable IP routing, use the **no** form of this command.

ip routing

no ip routing

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

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

Usage Guidelines To bridge IP, the **no ip routing** command must be configured to disable IP routing. However, you need not specify **no ip routing** in conjunction with concurrent routing and bridging to bridge IP.

The ip routing command is disabled on the Cisco VG200 voice over IP gateway.

Examples The following example enables IP routing:

```
ip routing
```

ip source binding

To add a static IP source binding entry, use the **ip source binding** command. Use the **no** form of this command to delete a static IP source binding entry

ip source binding *mac-address* **vlan** *vlan-id* *ip-address* **interface** *type* *mod/port*

Syntax Description		
<i>mac-address</i>	Binding	MAC address.
vlan <i>vlan-id</i>	Specifies the Layer 2 VLAN identification;	valid values are from 1 to 4094.
<i>ip-address</i>	Binding	IP address.
interface <i>type</i>	Interface type; possible valid values are	fastethernet , gigabitethernet , tengigabitethernet , port-channel <i>num</i> , and vlan <i>vlan-id</i> .
<i>mod/port</i>	Module and port number.	

Command Default No IP source bindings are configured.

Command Modes Global configuration.

Command History	Release	Modification
	12.2(33)SXH	This command was introduced.

Usage Guidelines You can use this command to add a static IP source binding entry only.

The **no** format deletes the corresponding IP source binding entry. It requires the exact match of all required parameter in order for the deletion to be successful. Note that each static IP binding entry is keyed by a MAC address and a VLAN number. If the command contains the existing MAC address and VLAN number, the existing binding entry is updated with the new parameters instead of creating a separate binding entry.

Examples This example shows how to add a static IP source binding entry:

```
Router(config)# ip source binding 000C.0203.0405 vlan 100 172.16.30.2 interface
gigabitethernet5/3
```

This example shows how to delete a static IP source binding entry:

```
Router(config)# no ip source binding 000C.0203.0405 vlan 100 172.16.30.2 interface
gigabitethernet5/3
```

Related Commands

Command	Description
ip verify source vlan dhcp snooping	Enables or disables the per 12-port IP source guard.
show ip source binding	Displays the IP source bindings configured on the system.
show ip verify source	Displays the IP source guard configuration and filters on a particular interface.

ip source-route

To allow the Cisco IOS software to handle IP datagrams with source routing header options, use the **ip source-route** command in global configuration mode. To have the software discard any IP datagram containing a source-route option, use the **no** form of this command.

ip source-route

no ip source-route

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

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

Examples The following example enables the handling of IP datagrams with source routing header options:

```
ip source-route
```

Related Commands	Command	Description
	ping (privileged)	Diagnoses basic network connectivity (in privileged EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.
	ping (user)	Diagnoses basic network connectivity (in user EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.

ip subnet-zero

To enable the use of subnet 0 for interface addresses and routing updates, use the **ip subnet-zero** command in global configuration mode. To restore the default, use the **no** form of this command.

ip subnet-zero

no ip subnet-zero

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Global configuration

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

Usage Guidelines The **ip subnet-zero** command provides the ability to configure and route to subnet 0 subnets. Subnetting with a subnet address of 0 is discouraged because of the confusion inherent in having a network and a subnet with indistinguishable addresses.

Examples The following example enables subnet zero:

```
ip subnet-zero
```

ip unnumbered

To enable IP processing on an interface without assigning an explicit IP address to the interface, use the **ip unnumbered** command in interface configuration mode or subinterface configuration mode. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered *type number*

no ip unnumbered *type number*

Syntax Description

<i>type</i>	Interface on which the router has assigned an IP address. The interface cannot be unnumbered interface. For more information, use the question mark (?) online help function.
<i>number</i>	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

IP processing on the unnumbered interface is disabled.

Command Modes

Interface configuration
Subinterface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command was modified to configure IP unnumbered support on Ethernet VLAN subinterfaces and subinterface ranges.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE. This command became available on the Supervisor Engine 720.
12.2(18)SXF	This command was modified to support Ethernet physical interfaces and switched virtual interfaces (SVIs).
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When an unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet. It also uses the address of the specified interface in determining which routing processes are sending updates over the unnumbered interface. Restrictions are as follows:

- This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

- Serial interfaces using High-Level Data Link Control (HDLC), PPP, Link Access Procedure Balanced (LAPB), Frame Relay encapsulations, and Serial Line Internet Protocol (SLIP), and tunnel interfaces can be unnumbered. It is not possible to use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.
- You cannot use the **ping EXEC** command to determine whether the interface is up because the interface has no address. Simple Network Management Protocol (SNMP) can be used to remotely monitor interface status.
- It is not possible to netboot a Cisco IOS image over a serial interface that is assigned an IP address with the **ip unnumbered** command.
- You cannot support IP security options on an unnumbered interface.

The interface you specify by the *type* and *number* arguments must be enabled (listed as “up” in the **show interfaces** command display).

If you are configuring Intermediate System-to-Intermediate System (IS-IS) across a serial line, you should configure the serial interfaces as unnumbered. This configuration allows you to comply with RFC 1195, which states that IP addresses are not required on each interface.

**Note**

Using an unnumbered serial line between different major networks (or *majornets*) requires special care. If at each end of the link there are different majornets assigned to the interfaces you specified as unnumbered, any routing protocol running across the serial line must not advertise subnet information.

Examples

In the following example, the first serial interface is given the address of Ethernet 0:

```
interface fastethernet 0
 ip address 10.108.6.6 255.255.255.0
!
interface serial 0
 ip unnumbered fastethernet 0
```

In the following example, Ethernet VLAN subinterface 3/0.2 is configured as an IP unnumbered subinterface:

```
interface fastethernet 3/0.2
 encapsulation dot1q 200
 ip unnumbered fastethernet 3/1
```

In the following example, Fast Ethernet subinterfaces in the range from 5/1.1 to 5/1.4 are configured as IP unnumbered subinterfaces:

```
interface range fastethernet5/1.1 - fastethernet5/1.4
 ip unnumbered fastethernet 3/1
```

ip verify source vlan dhcp-snooping

To enable Layer 2 IP source guard, use the **ip verify source vlan dhcp-snooping** command in the service instance mode. Use the **no** form of this command to disable Layer 2 IP source guard.

ip verify source vlan dhcp-snooping [port-security]

no ip verify source vlan dhcp-snooping [port-security]

Syntax Description	port-security Enables IP/MAC mode and applies both IP and MAC filtering.						
Command Default	Layer 2 IP source guard is disabled.						
Command Modes	Service instance (config-if-srv)						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.2(33)SXH</td> <td>This command was introduced.</td> </tr> <tr> <td>12.2(33)SRD</td> <td>The port-security keyword was added.</td> </tr> </tbody> </table>	Release	Modification	12.2(33)SXH	This command was introduced.	12.2(33)SRD	The port-security keyword was added.
Release	Modification						
12.2(33)SXH	This command was introduced.						
12.2(33)SRD	The port-security keyword was added.						
Usage Guidelines	The ip verify source vlan dhcp-snooping command enables VLANs only on the configured service instance (EVC) and looks for DHCP snooping matches only for the configured bridge domain VLAN.						
Examples	<p>This example shows how to enable Layer 2 IP source guard on an interface:</p> <pre> Router# enable Router# configure terminal Router(config)# interface GigabitEthernet7/1 Router(config-if)# no ip address Router(config-if)# service instance 71 fastethernet Router(config-if-srv)# encapsulation dot1q 71 Router(config-if-srv)# rewrite ingress tag pop 1 symmetric Router(config-if-srv)# ip verify source vlan dhcp-snooping Router(config-if-srv)# bridge-domain 10 </pre>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>service instance ethernet</td> <td>Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.</td> </tr> </tbody> </table>	Command	Description	service instance ethernet	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.		
Command	Description						
service instance ethernet	Configures an Ethernet service instance on an interface and enters Ethernet service configuration mode.						

local-ip (IPC transport-SCTP local)

To define at least one local IP address that is used to communicate with the local peer, use the **local-ip** command in IPC transport-SCTP local configuration mode. To remove one or all IP addresses from your configuration, use the **no** form of this command.

local-ip *device-real-ip-address* [*device-real-ip-address2*]

no local-ip *device-real-ip-address* [*device-real-ip-address2*]

Syntax Description

<i>device-real-ip-address</i>	IP address of the local device. The local IP addresses must match the remote IP addresses on the peer router. There can be either one or two IP addresses, which must be in global Virtual Private Network (VPN) routing and forwarding (VRF). A virtual IP (VIP) address cannot be used.
<i>device-real-ip-address2</i>	(Optional) IP address of the local device.

Defaults

No IP addresses are defined; thus, peers cannot communicate with the local peer.

Command Modes

IPC transport-SCTP local configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **local-ip** command to help associate Stream Control Transmission Protocol (SCTP) as the transport protocol between the local and remote peer.

This command is part of a suite of commands used to configure the Stateful Switchover (SSO) protocol. SSO is necessary for IP Security (IPSec) and Internet Key Exchange (IKE) to learn about the redundancy state of the network and to synchronize their internal application state with their redundant peers.

Examples

The following example shows how to enable SSO:

```
!
redundancy inter-device
  scheme standby HA-in
!
!
ipc zone default
  association 1
  no shutdown
  protocol sctp
  local-port 5000
  local-ip 10.0.0.1
  remote-port 5000
  remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-port	Defines the local SCTP port number that is used to communicate with the redundant peer.
remote-ip	Defines at least one remote IP address that is used to communicate with the redundant peer.

local-port

To define the local Stream Control Transmission Protocol (SCTP) port that is used to communicate with the redundant peer, use the **local-port** command in SCTP protocol configuration mode.

local-port *local-port-number*

Syntax Description

<i>local-port-number</i>	Local port number, which should be the same as the remote port number on the peer router (which is specified via the remote-port command).
--------------------------	---

Defaults

A local SCTP port is not defined.

Command Modes

SCTP protocol configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **local-port** command enters IPC transport-SCTP local configuration mode, which allows you to specify at least one local IP address (via the **local-ip** command) that is used to communicate with the redundant peer.

Examples

The following example shows how to enable Stateful Switchover (SSO):

```
!
redundancy inter-device
  scheme standby HA-in
!
!
ipc zone default
  association 1
  no shutdown
  protocol sctp
  local-port 5000
  local-ip 10.0.0.1
  remote-port 5000
  remote-ip 10.0.0.2
```

Related Commands

Command	Description
local-ip	Defines at least one local IP address that is used to communicate with the local peer.
remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.

remote-ip (IPC transport-SCTP remote)

To define at least one IP address of the redundant peer that is used to communicate with the local device, use the **remote-ip** command in IPC transport-SCTP remote configuration mode. To remove one or all IP addresses from your configuration, use the **no** form of this command.

```
remote-ip peer-real-ip-address [peer-real-ip-address2]
```

```
no remote-ip peer-real-ip-address [peer-real-ip-address2]
```

Syntax Description

<i>peer-real-ip-address</i>	IP address of the remote peer. The remote IP addresses must match the local IP addresses on the peer router. There can be either one or two IP addresses, which must be in the global Virtual Private Network (VPN) routing and forwarding (VRF). A virtual IP (VIP) address cannot be used.
<i>peer-real-ip-address2</i>	(Optional) IP address of the remote peer.

Defaults

No IP addresses are defined.

Command Modes

IPC transport-SCTP remote configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **remote-ip** command to help associate Stream Control Transmission Protocol (SCTP) as the transport protocol between the local and remote peer.

This command is part of a suite of commands used to configure the Stateful Switch Over (SSO) protocol. SSO is necessary for IP Security (IPSec) and Internet Key Exchange (IKE) to learn about the redundancy state of the network and to synchronize their internal application state with their redundant peers.

Examples

The following example shows how to enable SSO:

```
redundancy inter-device
  scheme standby HA-in
  !
ipc zone default
  association 1
  no shutdown
  protocol sctp
  local-port 5000
  local-ip 10.0.0.1
  remote-port 5000
  remote-ip 10.0.0.2
```

■ remote-ip (IPC transport-SCTP remote)

Related Commands	Command	Description
	local-ip	Defines at least one local IP address that is used to communicate with the local peer.
	remote-port	Defines the remote SCTP that is used to communicate with the redundant peer.

remote-port

To define the remote Stream Control Transmission Protocol (SCTP) port that is used to communicate with the redundant peer, use the **remote-port** command in SCTP protocol configuration mode.

remote-port *remote-port-number*

Syntax Description	<i>remote-port-number</i>	Remote port number, which should be the same as the local port number on the peer router (which is specified via the local-port command).
---------------------------	---------------------------	--

Defaults	A remote SCTP port is not defined.
-----------------	------------------------------------

Command Modes	SCTP protocol configuration
----------------------	-----------------------------

Command History	Release	Modification
	12.3(8)T	This command was introduced.

Usage Guidelines	The remote-port command enters IPC transport-SCTP remote configuration mode, which allows you to specify at least one remote IP address (via the remote-ip command) that is used to communicate with the redundant peer.
-------------------------	--

Examples	The following example shows how to enable Stateful Switchover (SSO):
-----------------	--

```

redundancy inter-device
  scheme standby HA-in
!
ipc zone default
  association 1
    no shutdown
    protocol sctp
    local-port 5000
    local-ip 10.0.0.1
    remote-port 5000
    remote-ip 10.0.0.2

```

Related Commands	Command	Description
	local-port	Defines the local SCTP port that is used to communicate with the redundant peer.
remote-ip	Defines at least one IP address of the redundant peer that is used to communicate with the local device.	

show hosts

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular Domain Name System (DNS) view or for all configured DNS views, use the **show hosts** command in privileged EXEC mode.

```
show hosts [vrf vrf-name] [view view-name] [all | hostname] [summary]
```

Syntax Description

vrf <i>vrf-name</i>	(Optional) The <i>vrf-name</i> argument specifies the name of the Virtual Private Network (VPN) routing and forwarding (VRF) instance associated with the DNS view whose hostname cache entries are to be displayed. Default is the global VRF (that is, the VRF whose name is a NULL string) with the specified or default DNS view. Note More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
view <i>view-name</i>	(Optional) The <i>view-name</i> argument specifies the DNS view whose hostname cache information is to be displayed. Default is the default (unnamed) DNS view associated with the specified or global VRF. Note More than one DNS view can be associated with a VRF. To uniquely identify a DNS view, specify both the view name and the VRF with which it is associated.
all	(Optional) The specified hostname cache information is to be displayed for all configured DNS views. This is the default.
<i>hostname</i>	(Optional) The specified hostname cache information displayed is to be limited to entries for a particular hostname. Default is the hostname cache information for all hostname entries in the cache.
summary	(Optional) The specified hostname cache information is to be displayed in brief summary format. Disabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2T	This command was updated to support the Cisco modem user interface feature.
12.4(4)T	The vrf , all , and summary keywords and <i>vrf-name</i> and <i>hostname</i> arguments were added.
12.4(9)T	The view keyword and <i>view-name</i> argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses specific to a particular DNS view or for all configured DNS views.

If you specify the **show hosts** command without any optional keywords or arguments, only the entries in the global hostname cache will be displayed.

If the output from this command extends beyond the bottom of the screen, press the Space bar to continue or press the Q-key to terminate command output.

Examples

The following is sample output from the **show hosts** command with no parameters specified:

```
Router# show hosts

Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 192.0.2.220
Host Flag Age Type Address(es)
EXAMPLE1.CISCO.COM (temp, OK) 1 IP 192.0.2.10
EXAMPLE2.CISCO.COM (temp, OK) 8 IP 192.0.2.50
EXAMPLE3.CISCO.COM (temp, OK) 8 IP 192.0.2.115
EXAMPLE4.CISCO.COM (temp, EX) 8 IP 192.0.2.111
EXAMPLE5.CISCO.COM (temp, EX) 0 IP 192.0.2.27
EXAMPLE6.CISCO.COM (temp, EX) 24 IP 192.0.2.30
```

The following is sample output from the **show hosts** command that specifies the VRF vpn101:

```
Router# show hosts vrf vpn101

Default domain is example.com
Domain list: example1.com, example2.com, example3.com
Name/address lookup uses domain service
Name servers are 192.0.2.204, 192.0.2.205, 192.0.2.206

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host          Port  Flags      Age Type  Address(es)
user          None (perm, OK) 0  IP    192.0.2.001
www.example.com  None (perm, OK) 0  IP    192.0.2.111
                                     192.0.2.112
```

Table 30 describes the significant fields shown in the display.

Table 30 *show hosts Field Descriptions*

Field	Description
Default domain	Default domain name to be used to complete unqualified names if no domain list is defined.
Domain list	List of default domain names to be tried in turn to complete unqualified names.
Name/address lookup	Style of name lookup service.
Name servers	List of name server hosts.

Table 30 *show hosts Field Descriptions (continued)*

Field	Description
Host	Learned or statically defined hostname. Statically defined hostname-to-address mappings can be added to the DNS hostname cache for a DNS view by using the ip hosts command.
Port	TCP port number to connect to when using the defined hostname in conjunction with an EXEC connect or Telnet command.
Flags	Indicates additional information about the hostname-to-IP address mapping. Possible values are as follows: <ul style="list-style-type: none"> temp—A temporary entry is entered by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity. perm—A permanent entry is entered by a configuration command and is not timed out. OK—Entries marked OK are believed to be valid. ??—Entries marked ?? are considered suspect and subject to revalidation. EX—Entries marked EX are expired.
Age	Number of hours since the software last referred to the cache entry.
Type	Type of address. For example, IP, Connectionless Network Service (CLNS), or X.121. If you have used the ip hp-host global configuration command, the show hosts command will display these hostnames as type HP-IP.
Address(es)	IP address of the host. One host may have up to eight addresses.

Related Commands

Command	Description
clear host	Removes static hostname-to-address mappings from the hostname cache for the specified DNS view or all DNS views.
ip host	Defines static hostname-to-address mappings in the DNS hostname cache for a DNS view.

show ip aliases

To display the IP addresses mapped to TCP ports (aliases) and Serial Line Internet Protocol (SLIP) addresses, which are treated similar to aliases, use the **show ip aliases** command in user EXEC or privileged EXEC mode.

show ip aliases

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(1)T	This command was modified. The output of the command was changed to display the dynamic and interface IP addresses, even when both the IP addresses are the same.

Usage Guidelines

To distinguish a SLIP address from a normal alias address, the command output uses the form SLIP TTY1 for the port number, where 1 is the auxiliary port. The display lists the address type, the IP address, and the corresponding port number. The output field descriptions are self-explanatory.

Examples

The following is sample output from the **show ip aliases** command:

```
Router# show ip aliases

Address Type      IP Address      Port
Interface         10.1.1.1        SLIP TTY1
Dynamic           198.51.100.1
Dynamic           198.51.100.22
Dynamic           10.0.0.0
Dynamic           10.2.2.2
Interface         10.114.11.39    SLIP TTY1
Interface         172.31.232.182  SLIP TTY1
Interface         192.0.2.11      SLIP TTY1
Dynamic           209.165.200.225
Interface         209.165.200.225
```

■ show ip aliases

Related Commands

Command	Description
show line	Displays the parameters of a terminal line.

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

```
show ip interface [type number] [brief]
```

Syntax Description	
<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Default The full usability status is displayed for all interfaces configured for IP.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(3)T	This command was expanded to include the status of the ip wccp redirect out and ip wccp redirect exclude add in commands.
	12.2(14)S	The command output was modified to display the status of NetFlow on a subinterface.
	12.2(15)T	The command output was modified to display the status of NetFlow on a subinterface.
	12.3(6)	The command output was modified to identify the downstream VPN routing and forwarding (VRF) instance in the output.
	12.3(14)YM2	The command output was modified to show the usability status of interfaces configured for Multi-Processor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.
	12.2(14)SX	This command was introduced on the Supervisor Engine 720.
	12.2(17d)SXB	This command was integrated into Cisco IOS 12.2(17d)SXB on the Supervisor Engine 2, and the command output was changed to include NDE for hardware flow status.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(31)SB2	The command output was modified to display information about the Unicast Reverse Path Forwarding (RPF) notification feature.
	12.4(20)T	The command output was modified to display information about the Unicast RPF notification feature.
	12.2(33)SXI2	This command was modified. The command output was modified to display information about the Unicast RPF notification feature.

Usage Guidelines

The Cisco IOS software automatically enters a directly-connected route in the routing table if the interface is usable (which means that it can send and receive packets). If an interface is not usable, the directly-connected routing entry is removed from the routing table. Removing the entry lets the software use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked “up.” If the interface hardware is usable, the interface is marked “up.”

If you specify an optional interface type, you see information for that specific interface. If you specify no optional arguments, you see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

You can use the **show ip interface brief** command to view a summary of the router interfaces. This command displays the IP address, the interface status, and other information.

The **show ip interface brief** command does not display any information related to Unicast RPF.

Examples

The following example shows configuration information on interface Gigabit Ethernet 0/3. In this example, the IP flow egress feature is configured on the output side (where packets go out of the interface), and the policy route-map named PBR_NAME is configured on the input side (where packets come into the interface).

```
Router# show running-config interface gigabitethernet 0/3
```

```
interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress
 ip policy route-map PBR_NAME
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end
```

The following example shows interface information on Gigabit Ethernet interface 0/3. In this example, MPF is enabled, and both features are not supported by MPF and are ignored.

```
Router# show ip interface gigabitethernet 0/3
```

```
GigabitEthernet0/3 is up, line protocol is up
 Internet address is 10.1.1.1/16
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is not set
 Inbound access list is not set
 Proxy ARP is enabled
 Local Proxy ARP is disabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is enabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
```

```

IP CEF switching is enabled
IP Feature Fast switching turbo vector
IP VPN Flow CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is enabled, using route map PBR
Network address translation is disabled
BGP Policy Mapping is disabled
IP Multi-Processor Forwarding is enabled
  IP Input features, "PBR",
    are not supported by MPF and are IGNORED
  IP Output features, "NetFlow",
    are not supported by MPF and are IGNORED

```

The following example identifies a downstream VRF instance. In the example, “Downstream VPN Routing/Forwarding “D”” identifies the downstream VRF instance.

```
Router# show ip interface virtual-access 3
```

```

Virtual-Access3 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
  Broadcast address is 255.255.255.255
  Peer address is 10.8.1.1
  MTU is 1492 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN CEF switching turbo vector
  VPN Routing/Forwarding "U"
  Downstream VPN Routing/Forwarding "D"
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled

```

The following example shows the information displayed when Unicast RPF drop-rate notification is configured:

```
Router# show ip interface ethernet 2/3

Ethernet2/3 is up, line protocol is up
  Internet address is 10.0.0.4/16
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

Unicast RPF Information

```
Input features: uRPF
  IP verify source reachable-via RX, allow default
    0 verification drops
    0 suppressed verification drops
    0 verification drop-rate
Router#
```

The following example shows how to display the usability status for a specific VLAN:

```
Router# show ip interface vlan 1

Vlan1 is up, line protocol is up
  Internet address is 10.0.0.4/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
```

```

Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Fast switching turbo vector
IP Normal CEF switching turbo vector
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled
Sampled Netflow is disabled
IP multicast multilayer switching is disabled
Netflow Data Export (hardware) is enabled

```

Table 31 describes the significant fields shown in the display.

Table 31 *show ip interface Field Descriptions*

Field	Description
Virtual-Access3 is up	Shows whether the interface hardware is usable (up). For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Broadcast address.
Peer address is	Peer address.
MTU is	MTU value set on the interface.
Helper address	Helper address, if one is set.
Directed broadcast forwarding	Shows whether directed broadcast forwarding is enabled.
Outgoing access list	Shows whether the interface has an outgoing access list set.
Inbound access list	Shows whether the interface has an incoming access list set.
Proxy ARP	Shows whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Shows whether split horizon is enabled.
ICMP redirects	Shows whether redirect messages will be sent on this interface.

Table 31 *show ip interface Field Descriptions (continued)*

Field	Description
ICMP unreachable	Shows whether unreachable messages will be sent on this interface.
ICMP mask replies	Shows whether mask replies will be sent on this interface.
IP fast switching	Shows whether fast switching is enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Shows whether Flow switching is enabled for this interface.
IP CEF switching	Shows whether Cisco Express Forwarding (CEF) switching is enabled for the interface.
Downstream VPN Routing/Forwarding "D"	Shows the VRF instance where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Shows whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast, Flow init, CEF, Ingress Flow	Shows whether NetFlow is enabled on an interface. Displays "Flow init" to specify that NetFlow is enabled on the interface. Displays "Ingress Flow" to specify that NetFlow is enabled on a subinterface using the ip flow ingress command. Shows "Flow" to specify that NetFlow is enabled on a main interface using the ip route-cache flow command.
Router Discovery	Shows whether the discovery process is enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Shows whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Shows whether compression is enabled.
WCCP Redirect outbound is disabled	Shows the status of whether packets received on an interface are redirected to a cache engine. Displays "enabled" or "disabled."
WCCP Redirect exclude is disabled	Shows the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays "enabled" or "disabled."
Netflow Data Export (hardware) is enabled	NDE hardware flow status on the interface.

The following example shows how to display a summary of the usability status information for each interface:

```
Router# show ip interface brief
```

```
Interface      IP-Address      OK? Method Status          Protocol
Ethernet0     10.108.00.5    YES NVRAM    up              up
Ethernet1     unassigned     YES unset    administratively down  down
Loopback0     10.108.200.5  YES NVRAM    up              up
Serial0       10.108.100.5  YES NVRAM    up              up
Serial1       10.108.40.5   YES NVRAM    up              up
Serial2       10.108.100.5  YES manual up          up
Serial3       unassigned     YES unset    administratively down  down
```

Table 32 describes the significant fields shown in the display.

Table 32 *show ip interface brief Field Descriptions*

Field	Description
Interface	Type of interface.
IP-Address	IP address assigned to the interface.
OK?	“Yes” means that the IP Address is currently valid. “No” means that the IP Address is not currently valid.
Method	The Method field has the following possible values: <ul style="list-style-type: none"> • RARP or SLARP—Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request. • BOOTP—Bootstrap protocol. • TFTP—Configuration file obtained from the TFTP server. • manual—Manually changed by CLI command. • NVRAM—Configuration file in NVRAM. • IPCP—ip address negotiated command. • DHCP—ip address dhcp command. • unassigned—No IP address. • unset—Unset. • other—Unknown.
Status	Shows the status of the interface. Valid values and their meanings are: <ul style="list-style-type: none"> • up—Interface is administratively up. • down—Interface is administratively down. • administratively down—Interface is administratively down.
Protocol	Shows the operational status of the routing protocol on this interface.

Related Commands	Command	Description
	ip address	Sets a primary or secondary IP address for an interface.
	ip vrf autoclassify	Enables VRF autoclassify on a source interface.
	match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
	route-map	Defines the conditions for redistributing routes from one routing protocol into another or to enable policy routing.
	set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
	show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
	show route-map	Displays static and dynamic route maps.

show ip irdp

To display ICMP Router Discovery Protocol (HRDP) values, use the **show ip irdp** command in EXEC mode.

show ip irdp

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

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

Examples The following is sample output from the **show ip irdp** command:

```
Router# show ip irdp

Ethernet 0 has router discovery enabled

Advertisements will occur between every 450 and 600 seconds.
Advertisements are valid for 1800 seconds.
Default preference will be 100.
--More--
Serial 0 has router discovery disabled
--More--
Ethernet 1 has router discovery disabled
```

As the display shows, **show ip irdp** output indicates whether router discovery has been configured for each router interface, and it lists the values of router discovery configurables for those interfaces on which router discovery has been enabled. Explanations for the less obvious lines of output in the display are as follows:

Advertisements will occur between every 450 and 600 seconds.

This indicates the configured minimum and maximum advertising interval for the interface.

Advertisements are valid for 1800 seconds.

This indicates the configured holdtime values for the interface.

Default preference will be 100.

This indicates the configured (or in this case default) preference value for the interface.

■ show ip irdp

Related Commands

Command	Description
ip irdp	Enables IRDP processing on an interface.

show ip masks

To display the masks used for network addresses and the number of subnets using each mask, use the **show ip masks** command in EXEC mode.

show ip masks *address*

Syntax Description	<i>address</i>	Network address for which a mask is required.
---------------------------	----------------	---

Command Modes	EXEC
----------------------	------

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

Usage Guidelines The **show ip masks** command is useful for debugging when a variable-length subnet mask (VLSM) is used. It shows the number of masks associated with the network and the number of routes for each mask.

Examples The following is sample output from the **show ip masks** command:

```
Router# show ip masks 172.16.0.0

Mask           Reference count
255.255.255.255 2
255.255.255.0  3
255.255.0.0     1
```

show ip route

To display the current state of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

```
show ip route [ip-address [repair-paths | next-hop-override [dhcp] | mask [longer-prefixes]] |
  protocol [process-id] | list [access-list-number | access-list-name] | static download |
  update-queue]
```

Syntax Description		
<i>ip-address</i>	(Optional) IP address about which routing information should be displayed.	
repair-paths	(Optional) Displays the repair paths.	
next-hop-override	(Optional) Displays the Next Hop Resolution Protocol (NHRP) overrides associated with a particular route, along with the corresponding default next hops.	
dhcp	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.	
<i>mask</i>	(Optional) The subnet mask.	
longer-prefixes	(Optional) Specifies that only routes matching the <i>ip-address</i> and <i>mask</i> pair should be displayed.	
<i>protocol</i>	(Optional) The name of a routing protocol, or the keyword connected , mobile , static , or summary . If you specify a routing protocol, use one of the following keywords: bgp , eigrp , hello , isis , odr , ospf , nhp , and rip .	
<i>process-id</i>	(Optional) The number used to identify a process of the specified protocol.	
list	(Optional) Filters output by an access list name or number.	
<i>access-list-number</i>	(Optional) Specific access list number for which output from the routing table should be displayed.	
<i>access-list-name</i>	(Optional) Specific access list name for which output from the routing table should be displayed.	
static	(Optional) Displays static routes.	
download	(Optional) Displays the route installed using the authentication, authorization, and accounting (AAA) route download function. This keyword is used only when AAA is configured.	
update-queue	(Optional) Displays Routing Information Base (RIB) queue updates.	

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	9.2	This command was introduced.
	10.0	The “D—EIGRP, EX—EIGRP, N1—OSPF NSSA external type 1 route” and “N2—OSPF NSSA external type 2 route” codes were added to the command output.
	10.3	The <i>process-id</i> argument was added.
	11.0	The longer-prefixes keyword was added.
	11.1	The “U—per-user static route” code was added to the command output.
	11.2	The “o—on-demand routing” code was added to the command output.
	12.2(33)SRA	This command was modified. The update-queue keyword was added.
	11.3	The output from the show ip route ip-address command was enhanced to display the origination of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
	12.0(1)T	The “M—mobile” code was added to the command output.
	12.0(3)T	The “P—periodic downloaded static route” code was added to the command output.
	12.0(4)T	The “ia—IS-IS” code was added to the command output.
	12.2(2)T	The output from the show ip route ip-address command was enhanced to display information on the multipaths to the specified network.
	12.2(13)T	The <i>egp</i> and <i>igrp</i> arguments were removed because the exterior gateway protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) are no longer available in Cisco IOS software.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
	12.3(2)T	The output was enhanced to display route tag information.
	12.3(8)T	The output was enhanced to display static routes using DHCP.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRE	This command was modified. The dhcp and repair-paths keywords were added. Support for the Border Gateway Protocol (BGP) best external and BGP additional path features was added.
	12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
	Cisco IOS XE Release 2.5	This command was modified. The next-hop-override and nhrp keywords were added.

Usage Guidelines

The **show ip route static download** command provides a way to display all dynamic static routes with name and distance information, including active and inactive ones. You can display all active dynamic static routes with both the **show ip route** and **show ip route static** commands after these active routes are added in the main routing table.

Examples

Routing Table Examples

The following examples show the standard routing tables displayed by the **show ip route** command. Use the codes displayed at the beginning of each report and the information in [Table 35](#) to understand the type of route.

The following is sample output from the **show ip route** command when entered without an address:

```
Router# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is 10.119.254.240 to network 10.140.0.0

O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E 10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E 10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E 10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E 10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E 10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E 10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E 10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E 10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E 10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E 10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E 10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E 10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

The following is sample output that includes IS-IS Level 2 routes learned:

```
Router# show ip route

Codes: L- Local R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 192.168.1.2
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.10.10.0/24 is directly connected, Vlan1
L 10.10.10.1/32 is directly connected, Vlan1
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/30 is directly connected, GigabitEthernet0
L 192.168.1.1/32 is directly connected, GigabitEthernet0
```

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes
```

```
Codes: L - Local R - RIP derived, O - OSPF derived,
        C - connected, S - static, B - BGP derived,
        * - candidate default route, IA - OSPF inter area route,
        i - IS-IS derived, ia - IS-IS, U - per-user static route,
        o - on-demand routing, M - mobile, P - periodic downloaded static route,
        D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
        E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
        N2 - OSPF NSSA external type 2 route
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.4.9.0/24 is directly connected, GigabitEthernet0/1
L       10.4.9.134/32 is directly connected, GigabitEthernet0/1
        171.69.0.0/16 is variably subnetted, 2 subnets, 2 masks
S       171.69.0.0/16 [1/0] via 10.4.9.1
S       171.69.1.129/32 [1/0] via 10.4.9.1
```

The following examples display all downloaded static routes. A P designates which route was installed using AAA route download.

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route, o - ODR, P - periodic downloaded static route
        T - traffic engineered route
```

```
Gateway of last resort is 172.21.17.1 to network 0.0.0.0
```

```
        172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1 20.0.0.0/24 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1
```

```
Router# show ip route static
```

```
        172.27.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.16.1.1/32 is directly connected, BRI0
P       172.27.4.0/8 [1/0] via 10.1.1.1, BRI0
S       172.31.0.0/16 [1/0] via 172.21.114.65, Ethernet0
S       10.0.0.0/8 is directly connected, BRI0
P       10.0.0.0/8 is directly connected, BRI0
        172.21.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.21.114.201/32 is directly connected, BRI0
S       172.21.114.205/32 is directly connected, BRI0
S       172.21.114.174/32 is directly connected, BRI0
S       172.21.114.12/32 is directly connected, BRI0
P       10.0.0.0/8 is directly connected, BRI0
P       10.1.0.0/16 is directly connected, BRI0
P       10.2.2.0/24 is directly connected, BRI0
S*      0.0.0.0/0 [1/0] via 172.21.114.65, Ethernet0
```

```
S    172.29.0.0/16 [1/0] via 172.21.114.65, Ethernet0
```

The following example shows how to use the **show ip route static download** command to display all active and inactive routes installed using AAA route download:

```
Router# show ip route static download

Connectivity: A - Active, I - Inactive

A    10.10.0.0 255.0.0.0 BRI0
A    10.11.0.0 255.0.0.0 BRI0
A    10.12.0.0 255.0.0.0 BRI0
A    10.13.0.0 255.0.0.0 BRI0
I    10.20.0.0 255.0.0.0 172.21.1.1
I    10.22.0.0 255.0.0.0 Serial0
I    10.30.0.0 255.0.0.0 Serial0
I    10.31.0.0 255.0.0.0 Serial1
I    10.32.0.0 255.0.0.0 Serial1
A    10.34.0.0 255.0.0.0 192.168.1.1
A    10.36.1.1 255.255.255.255 BRI0 200 name remotel
I    10.38.1.9 255.255.255.0 192.168.69.1
```

The following example shows how to use the **show ip route nhrp** command to enable shortcut switching on the tunnel interface:

```
Router# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP

Gateway of last resort is not set

      10.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Tunnel0
C       172.16.22.0 is directly connected, Ethernet1/0
H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
C       10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route nhrp

H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
```

The following is sample output using the **next-hop-override** keyword. When the **next-hop-override** keyword is included, the NHRP Nexthop-overrides associated with a particular route, along with the corresponding default next hops, are displayed.

```
=====
1) Initial configuration
=====
Router# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
```

```

+ - replicated route

Gateway of last resort is not set

    10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
    10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 is directly connected, Tunnel0
    10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0

Router# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set

    10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
    10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 is directly connected, Tunnel0
    10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0

Router# show ip cef

Prefix          Next Hop          Interface
.
.
.
10.2.1.255/32   receive          Loopback1
10.10.10.0/24   attached         Tunnel0 <<<<<<<<
10.11.11.0/24   attached         Ethernet0/0
127.0.0.0/8    drop
.
.
.
=====
2) Add a Nexthop-override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.1.1.1
   interface = Tunnel0
=====

Router# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

```

show ip route

```
Gateway of last resort is not set
```

```

    10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
    10.0.0.0/24 is subnetted, 1 subnets
% S     10.10.10.0 is directly connected, Tunnel0
    10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0
```

```
Router# show ip route next-hop-override
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route
```

```
Gateway of last resort is not set
```

```

    10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
    10.0.0.0/24 is subnetted, 1 subnets
% S     10.10.10.0 is directly connected, Tunnel0
           [NHO][1/0] via 10.1.1.1, Tunnel0
    10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0
```

```
Router# show ip cef
```

Prefix	Next Hop	Interface
.		
.		
.		
10.2.1.255/32	receive	Loopback110.10.10.0/24
10.10.10.0/24	10.1.1.1	Tunnel0
10.11.11.0/24	attached	Ethernet0/0
10.12.0.0/16	drop	
.		
.		
.		

```

=====
3) Delete a Nexthop-override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.11.1.1
   interface = Tunnel0
=====
```

```
Router# show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route
```

```

Gateway of last resort is not set

    10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
    10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 is directly connected, Tunnel0
    10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0

```

Router# **show ip route next-hop-override**

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

```

```

Gateway of last resort is not set

    10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
    10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 is directly connected, Tunnel0
    10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0

```

Router# **show ip cef**

Prefix	Next Hop	Interface
.		
.		
.		
10.2.1.255/32	receive	Loopback110.10.10.0/24
10.10.10.0/24	attached	Tunnel0
10.11.11.0/24	attached	Ethernet0/0
10.120.0.0/16	drop	
.		
.		
.		

Table 33 show ip route Field Descriptions

Field	Description
Codes	<p>Indicates the protocol that derived the route. It can be one of the following values:</p> <ul style="list-style-type: none"> • B—BGP derived • C—connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • i—IS-IS derived • ia—IS-IS • L—local • M—mobile • O—Open Shortest Path First (OSPF) derived • P—periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—static • U—per-user static route • o—on-demand routing • +—replicated route
Codes	<p>Type of route. It can be one of the following values:</p> <ul style="list-style-type: none"> • *—Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate which path will be used next when forwarding a nonfast-switched packet, except when the paths are equal cost. • E1—OSPF external type 1 route • E2—OSPF external type 2 route • IA—OSPF inter area route • L1—IS-IS Level 1 route • L2—IS-IS Level 2 route • N1—OSPF not-so-stubby area (NSSA) external type 1 route • N2—OSPF NSSA external type 2 route
10.110.0.0	Indicates the address of the remote network.
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next router to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

Specific Route Information

When you specify that you want information about a specific network displayed, more detailed statistics are shown. The following is sample output from the **show ip route** command when entered with the IP address 10.0.0.1:

```
Router# show ip route 10.0.0.1

Routing entry for 10.0.0.1/32
  Known via "isis", distance 115, metric 20, type level-1
  Redistributing via isis
  Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
  Routing Descriptor Blocks:
  * 10.22.22.2, from 10.191.255.247, via Serial2/3
    Route metric is 20, traffic share count is 1
    10.191.255.251, from 10.191.255.247, via Fddi1/0
    Route metric is 20, traffic share count is 1
```

When an IS-IS router advertises its link-state information, it includes one of its own IP addresses to be used as the originator IP address. When other routers calculate IP routes, they can store the originator IP address with each route in the routing table.

The preceding example shows the output from the **show ip route** command for an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine where a particular IP route has originated in your network. In the example the route to 10.0.0.1/32 was originated by a router with IP address 10.191.255.247.

[Table 36](#) describes the significant fields shown when using the **show ip route** command with an IP address.

Table 34 *show ip route with IP Address Field Descriptions*

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Tag	Integer that is used to implement the route.
type	Indicates the IS-IS route type (Level 1 or Level 2).
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes
```

```
Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
```

```
Gateway of last resort is not set
```

```
S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
    10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C    10.19.64.0 is directly connected, Ethernet0
    10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C    10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S    10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following output includes the tag 120 applied to the route 10.22.0.0/16. You must specify an IP prefix in order to see the tag value.

```
Router# show ip route 10.22.0.0
```

```
Routing entry for 10.22.0.0/16
  Known via "isis", distance 115, metric 12
  Tag 120, type level-1
  Redistributing via isis
  Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
  Routing Descriptor Blocks:
    * 172.19.170.12, from 10.3.3.3, via Ethernet2
      Route metric is 12, traffic share count is 1
      Route tag 120
```

Static Routes Using a DHCP Gateway Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.2.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate.

```
Router# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

```

Gateway of last resort is 10.0.19.14 to network 0.0.0.0

```

10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.2.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0

S* 10.0.0.0/0 [1/0] via 10.0.19.14

```

The following sample output from the **show ip route repair-paths** command shows the repair paths marked with the tag [RPR]:

Router# **show ip route repair-paths**

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP
+ - replicated route, % - next hop override

```

Gateway of last resort is not set

```

  10.0.0.0/32 is subnetted, 3 subnets
C    10.1.1.1 is directly connected, Loopback0
B    10.2.2.2 [200/0] via 172.16.1.2, 00:31:07
      [RPR][200/0] via 192.168.1.2, 00:31:07
B    10.9.9.9 [20/0] via 192.168.1.2, 00:29:45
      [RPR][20/0] via 192.168.3.2, 00:29:45
  172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C    172.16.1.0/24 is directly connected, Ethernet0/0
L    172.16.1.1/32 is directly connected, Ethernet0/0
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, Serial2/0
L    192.168.1.1/32 is directly connected, Serial2/0
B    192.168.3.0/24 [200/0] via 172.16.1.2, 00:31:07
      [RPR][200/0] via 192.168.1.2, 00:31:07
B    192.168.9.0/24 [20/0] via 192.168.1.2, 00:29:45
      [RPR][20/0] via 192.168.3.2, 00:29:45
B    192.168.13.0/24 [20/0] via 192.168.1.2, 00:29:45
      [RPR][20/0] via 192.168.3.2, 00:29:45

```

Router# **show ip route repair-paths 10.9.9.9**

```

>Routing entry for 10.9.9.9/32
> Known via "bgp 100", distance 20, metric 0
> Tag 10, type external

```

```

> Last update from 192.168.1.2 00:44:52 ago
> Routing Descriptor Blocks:
> * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>   Route metric is 0, traffic share count is 1
>   AS Hops 2
>   Route tag 10
>   MPLS label: none
> [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>   Route metric is 0, traffic share count is 1
>   AS Hops 2
>   Route tag 10
>   MPLS label: none

```

Table 35 show ip route Field Descriptions

Field	Description
O	<p>Indicates the protocol that derived the route. It can be one of the following values:</p> <p>R—Routing Information Protocol (RIP) derived</p> <p>O—Open Shortest Path First (OSPF) derived</p> <p>C—connected</p> <p>S—static</p> <p>B—Border Gateway Protocol (BGP) derived</p> <p>D—Enhanced Interior Gateway Routing Protocol (EIGRP)</p> <p>EX—EIGRP external</p> <p>i—IS-IS derived</p> <p>ia—IS-IS</p> <p>M—mobile</p> <p>P—periodic downloaded static route</p> <p>U—per-user static route</p> <p>o—on-demand routing</p>
E2	<p>Type of route. It can be one of the following values:</p> <p>*—Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate which path will be used next when forwarding a nonfast-switched packet, except when the paths are equal cost.</p> <p>IA—OSPF interarea route</p> <p>E1—OSPF external type 1 route</p> <p>E2—OSPF external type 2 route</p> <p>L1—IS-IS Level 1 route</p> <p>L2—IS-IS Level 2 route</p> <p>N1—OSPF not-so-stubby area (NSSA) external type 1 route</p> <p>N2—OSPF NSSA external type 2 route</p>
10.110.0.0	Indicates the address of the remote network.

Table 35 *show ip route Field Descriptions (continued)*

Field	Description
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next router to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

Specific Route Information

When you specify that you want information about a specific network displayed, more detailed statistics are shown. The following is sample output from the **show ip route** command when entered with the IP address 10.0.0.1:

```
Router# show ip route 10.0.0.1

Routing entry for 10.0.0.1/32
  Known via "isis", distance 115, metric 20, type level-1
  Redistributing via isis
  Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
  Routing Descriptor Blocks:
  * 10.22.22.2, from 10.191.255.247, via Serial2/3
    Route metric is 20, traffic share count is 1
    10.191.255.251, from 10.191.255.247, via Fddi1/0
    Route metric is 20, traffic share count is 1
```

When an IS-IS router advertises its link-state information, it includes one of its own IP addresses to be used as the originator IP address. When other routers calculate IP routes, they can store the originator IP address with each route in the routing table.

The example above shows the output from the **show ip route** command when looking at an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine where a particular IP route has originated in your network. In the example the route to 10.0.0.1/32 was originated by a router with IP address 10.191.255.247.

[Table 36](#) describes the significant fields shown when using the **show ip route** command with an IP address.

Table 36 *show ip route with IP Address Field Descriptions*

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Tag	Integer that is used to implement the route.
type	Indicates the IS-IS route type (Level 1 or Level 2).
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.

Table 36 *show ip route with IP Address Field Descriptions (continued)*

Field	Description
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes
```

```
Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
```

```
Gateway of last resort is not set
```

```
S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
    10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C      10.19.64.0 is directly connected, Ethernet0
    10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C      10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S      10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following output includes the tag 120 applied to the route 10.22.0.0/16. You must specify an IP prefix in order to see the tag value.

```
Router# show ip route 10.22.0.0
```

```
Routing entry for 10.22.0.0/16
  Known via "isis", distance 115, metric 12
  Tag 120, type level-1
```

```

Redistributing via isis
Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
Routing Descriptor Blocks:
  * 172.19.170.12, from 10.3.3.3, via Ethernet2
    Route metric is 12, traffic share count is 1
    Route tag 120

```

Static Routes Using a DHCP Gateway Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.2.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate.

```
Router# show ip route
```

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

```

```
Gateway of last resort is 10.0.19.14 to network 0.0.0.0
```

```

10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.2.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0

S* 10.0.0.0/0 [1/0] via 10.0.19.14

```

The following sample output from the **show ip route repair-paths** command shows the repair paths marked with the tag [RPR]:

```
Router# show ip route repair-paths
```

```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route, % - next hop override

```

```
Gateway of last resort is not set
```

```

      10.0.0.0/32 is subnetted, 3 subnets
C      10.1.1.1 is directly connected, Loopback0
B      10.2.2.2 [200/0] via 172.16.1.2, 00:31:07
      [RPR][200/0] via 192.168.1.2, 00:31:07
B      10.9.9.9 [20/0] via 192.168.1.2, 00:29:45
      [RPR][20/0] via 192.168.3.2, 00:29:45
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.16.1.0/24 is directly connected, Ethernet0/0

```

■ show ip route

```

L       172.16.1.1/32 is directly connected, Ethernet0/0
       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial2/0
L       192.168.1.1/32 is directly connected, Serial2/0
B       192.168.3.0/24 [200/0] via 172.16.1.2, 00:31:07
           [RPR][200/0] via 192.168.1.2, 00:31:07
B       192.168.9.0/24 [20/0] via 192.168.1.2, 00:29:45
           [RPR][20/0] via 192.168.3.2, 00:29:45
B       192.168.13.0/24 [20/0] via 192.168.1.2, 00:29:45
           [RPR][20/0] via 192.168.3.2, 00:29:45

```

Router# **show ip route repair-paths 10.9.9.9**

```

>Routing entry for 10.9.9.9/32
>  Known via "bgp 100", distance 20, metric 0
>  Tag 10, type external
>  Last update from 192.168.1.2 00:44:52 ago
>  Routing Descriptor Blocks:
>  * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>    Route metric is 0, traffic share count is 1
>    AS Hops 2
>    Route tag 10
>    MPLS label: none
>  [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>    Route metric is 0, traffic share count is 1
>    AS Hops 2
>    Route tag 10
>    MPLS label: none

```

Related Commands

Command	Description
show dialer	Displays general diagnostic information for interfaces configured for DDR.
show interfaces tunnel	Displays a list of tunnel interface information.
show ip route summary	Displays the current state of the routing table in summary format.

show ip source binding

To display IP-source bindings configured on the system, use the **show ip source** command in privileged EXEC mode.

```
show ip source binding [ip-address] [mac-address] [dhcp-snooping | static] [vlan vlan-id]
[interface type mod/port]
```

Syntax Description	
<i>ip-address</i>	(Optional) Binding IP address.
<i>mac-address</i>	(Optional) Binding MAC address.
dhcp-snooping	(Optional) Specifies DHCP snooping binding entry.
static	(Optional) Specifies a static binding entry.
vlan <i>vlan-id</i>	(Optional) Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
interface <i>type</i>	(Optional) Interface type; possible valid values are fastethernet , gigabitethernet , tengigabitethernet , port-channel <i>num</i> , and vlan <i>vlan-id</i> .
<i>mod/port</i>	Module and port number.

Command Default Both static and DHCP-snooping bindings are displayed.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(33)SXH	This command was introduced.

Usage Guidelines Each optional parameter is used to filter the display output.

Examples This example shows the output without entering any keywords:

```
Router# show ip source binding
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:00:00:0A:00:0B	17.16.0.1	infinite	static	10	FastEthernet6/10
00:00:00:0A:00:0A	17.16.0.2	10000	dhcp-snooping	10	FastEthernet6/11

This example shows how to display the static IP binding entry for a specific IP address:

```
Router# show ip source binding 17.16.0.1 0000.000A.000B static vlan 10 interface
gigabitethernet6/10
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:00:00:0A:00:0B	17.16.0.1	infinite	static	10	FastEthernet6/10

Table 37 describes the significant fields in the display.

Table 37 *show ip source binding Field Descriptions*

Field	Description
MAC Address	Client hardware MAC address.
IP Address	Client IP address assigned from the DHCP server.
Lease (seconds)	IP address lease time.
Type	Binding type; static bindings configured from CLI to dynamic binding learned from DHCP snooping.
VLAN	VLAN number of the client interface.
Interface	Interface that connects to the DHCP client host.

Related Commands

Command	Description
ip source binding	Adds or deletes a static IP source binding entry.
ip verify source vlan dhcp-snooping	Enables or disables the per 12-port IP source guard.
show ip verify source	Displays the IP source guard configuration and filters on a particular interface.

show ip verify source

To display the IP source guard configuration and filters on a particular interface, use the **show ip verify source** command in EXEC mode.

```
show ip verify source [interface type mod/port] [efp_id efp_id ]
```

Syntax Description	Parameter	Description
	interface type	(Optional) Specifies the interface type; possible valid values are fastethernet , gigabitethernet , tengigabitethernet , port-channel num , and vlan vlan-id .
	<i>mod/port</i>	Module and port number.
	efp_id	(Optional) Specifies the Ethernet flow point (EFP) (service instance) ID.
	<i>efp_id</i>	EFP number; range is 1 to 8000.

Defaults This command has no default settings.

Command Modes EXEC (#)

Command History	Release	Modification
	12.2(33)SXH	This command was introduced.
	12.2(33)SRD	The efp_id efp_id keyword and argument were added.

Usage Guidelines Enable port security first because the DHCP security MAC filter cannot apply to the port or VLAN.

Examples This example shows the display when DHCP snooping is enabled on VLANs 10 to 20, the interface has IP source filter mode that is configured as IP, and there is an existing IP address binding 10.0.0.1 on VLAN 10:

```
Router# show ip verify source interface gigabitethernet6/1
```

```
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----
gi6/1     ip           active       10.0.0.1        -----
gi6/1     ip           active       deny-all       11-20
```

This example shows how to display the IP source guard configuration and filters on a specific interface:

```
Router# show ip verify source interface gigabitethernet6/1
```

```
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----
gi6/1     ip           inactive-trust-port
```

This example shows the display when the interface does not have a VLAN enabled for DHCP snooping:

```
Router# show ip verify source interface gigabitethernet6/3
```

show ip verify source

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
gi6/3	ip	inactive-no-snooping-vlan			

This example shows the display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC binds 10.0.0.2/aaaa.bbbb.cccc on VLAN 10 and 10.0.0.1/aaaa.bbbb.cccd on VLAN 11:

```
Router# show ip verify source interface gigabitethernet6/4
```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
gi6/4	ip-mac	active	10.0.0.2	aaaa.bbbb.cccc	10
gi6/4	ip-mac	active	10.0.0.1	aaaa.bbbb.cccd	11
gi6/4	ip-mac	active	deny-all	deny-all	12-20

This example shows the display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC binding 10.0.0.3/aaaa.bbbb.cccc on VLAN 10, but port security is not enabled on the interface:

```
Router# show ip verify source interface gigabitethernet6/5
```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
gi6/5	ip-mac	active	10.0.0.3	permit-all	10
gi6/5	ip-mac	active	deny-all	permit-all	11-20

This example shows the display when the interface does not have IP source filter mode configured:

```
Router# show ip verify source interface gigabitethernet6/6
```

DHCP security is not configured on the interface gi6/6.

This example shows how to display all the interfaces on the switch that have DHCP snooping security enabled:

```
Router# show ip verify source
```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
gi6/1	ip	active	10.0.0.1		10
gi6/1	ip	active	deny-all		11-20
gi6/2	ip	inactive-trust-port			
gi6/3	ip	inactive-no-snooping-vlan			
gi6/4	ip-mac	active	10.0.0.2	aaaa.bbbb.cccc	10
gi6/4	ip-mac	active	11.0.0.1	aaaa.bbbb.cccd	11
gi6/4	ip-mac	active	deny-all	deny-all	12-20
gi6/5	ip-mac	active	10.0.0.3	permit-all	10
gi6/5	ip-mac	active	deny-all	permit-all	11-20

This example shows how to display all the interfaces on the switch that have DHCP snooping security enabled:

```
Router# show ip verify source interface gi5/0/0 efp_id 10
```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan	EFP ID
Gi5/0/0	ip-mac	active	123.1.1.1	00:0A:00:0A:00:0A	100	10
Gi5/0/0	ip-mac	active	123.1.1.2	00:0A:00:0A:00:0B	100	20
Gi5/0/0	ip-mac	active	123.1.1.3	00:0A:00:0A:00:0C	100	30

Related Commands	Command	Description
	ip source binding	Adds or deletes a static IP source binding entry.
	ip verify source vlan dhcp-snooping	Enables or disables the per 12-port IP source guard.
	show ip source binding	Displays the IP-source bindings configured on the system.

term ip netmask-format

To specify the format in which netmasks are displayed in **show** command output, use the **term ip netmask-format** command in EXEC configuration mode. To restore the default display format, use the **no** form of this command.

```
term ip netmask-format { bitcount | decimal | hexadecimal }
```

```
no term ip netmask-format [ bitcount | decimal | hexadecimal ]
```

Syntax Description

bitcount	Number of bits in the netmask.
decimal	Netmask dotted decimal notation.
hexadecimal	Netmask hexadecimal format.

Defaults

Netmasks are displayed in dotted decimal format.

Command Modes

EXEC

Command History

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

Usage Guidelines

IP uses a 32-bit mask that indicates which address bits belong to the network and subnetwork fields, and which bits belong to the host field. This range of IP addresses is called a *netmask*. By default, **show** commands display an IP address and then its netmask in dotted decimal notation. For example, a subnet would be displayed as 131.108.11.55 255.255.255.0.

However, you can specify that the display of the network mask appear in hexadecimal format or bit count format instead. The hexadecimal format is commonly used on UNIX systems. The previous example would be displayed as 131.108.11.55 0xFFFFFFFF00.

The bitcount format for displaying network masks is to append a slash (/) and the total number of bits in the netmask to the address itself. The previous example would be displayed as 131.108.11.55/24.

Examples

The following example specifies that network masks for the session be displayed in bitcount notation in the output of **show** commands:

```
term ip netmask-format bitcount
```

