



# Dynamic Layer-3 VPNs (RFC 2547) Support Using Multipoint GRE (mGRE) Tunnels

This feature provides a Layer-3 (L3) transport mechanism based on an enhanced multipoint Generic Routing Encapsulation (mGRE) tunneling technology for use in IP networks. This same dynamic Layer-3 tunneling transport can be used within IP networks to transport VPN traffic across service provider and enterprise networks, as well as to provide interoperability for packet transport between IP and MPLS VPNs. This feature provides support for RFC 2547 which defines the outsourcing of IP-backbone services for enterprise networks.

## Feature Specifications for Dynamic Layer-3 VPNs (RFC 2547) Support Using Multipoint GRE (mGRE) Tunnels

### Feature History

Release	Modification
12.0(23)S	This feature was introduced.

### Supported Platforms

For platforms supported in Cisco IOS Release 12.0(23)S, consult Cisco Feature Navigator.

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

**Availability of Cisco IOS Software Images**

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

## Contents

This document describes Dynamic Layer-3 VPNs (RFC 2547) Support Using Multipoint GRE (mGRE) Tunnels. It contains the following sections:

- [Restrictions for Dynamic Layer-3 VPNs \(RFC 2547\) Support Using Multipoint GRE \(mGRE\) Tunnels, page 2](#)
- [Information About Layer 3 Multipoint GRE Tunnels, page 2](#)
- [How to Deploy L3 VPN mGRE Tunnels, page 4](#)
- [Configuration Examples for Dynamic Layer-3 VPNs \(RFC 2547\) Support Using Multipoint GRE \(mGRE\) Tunnels, page 9](#)
- [Additional References, page 10](#)
- [Command Reference, page 12](#)

## Restrictions for Dynamic Layer-3 VPNs (RFC 2547) Support Using Multipoint GRE (mGRE) Tunnels

This feature is a software solution only; no hardware-assisted support is available.

## Information About Layer 3 Multipoint GRE Tunnels

By configuring mGRE tunnels, you create a multipoint tunnel network as an overlay to the IP backbone. This overlay interconnects the PE routers to transport VPN traffic through the backbone. This multipoint tunnel network uses BGP to distribute VPNv4 routing information between PE routers maintaining the peer relationship between the service provider or enterprise network and customer sites. The advertised nexthop in BGP VPNv4 triggers tunnel endpoint discovery. This feature provides the ability for multiple service providers to cooperate and offer a joint VPN service with traffic tunneled directly from the ingress PE router at one service provider directly to the egress PE router at a different service provider site.

In addition to providing the VPN transport capability, the mGRE tunnels create a full-mesh topology and reduce the administrative and operational overhead previously associated with a full mesh of point-to-point tunnels used to interconnect multiple customer sites. The configuration requirements are greatly reduced and allows the network grow with minimal additional configuration.

Dynamic L3 tunnels provide for better scaling when creating partial-mesh or full-mesh VPNs. Adding new remote VPN peers is simplified because only the new router needs to be configured. The new address is learned dynamically and propagated to the other nodes in the network. The dynamic routing capability dramatically reduces the size of configuration needed on all routers in the VPN, such that with

the use of multipoint tunnels, only one tunnel interface needs to be configured on a PE that services many VPNs. The L3 mGRE tunnels need to be configured only on the PE router. Features available with GRE are still available with mGRE, including dynamic IP routing and IP multicast and CEF switching of mGRE/NHRP tunnel traffic.

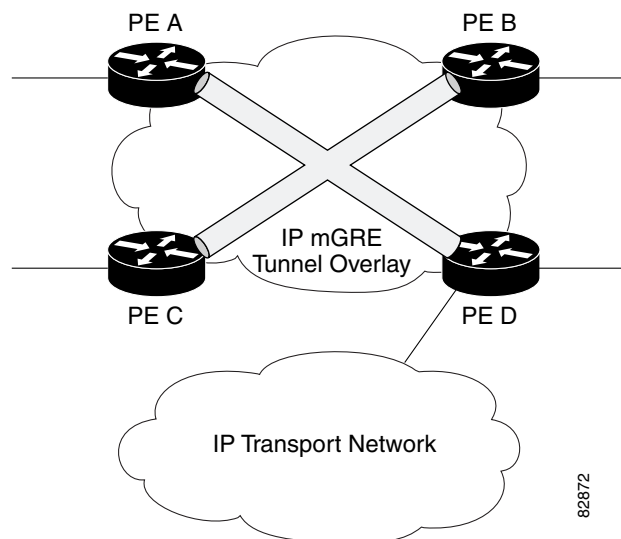
The following sections describe how the mGRE tunnels are used:

- [Interconnecting Provider Edge Routers Within an IP Network, page 3](#)
- [Packet Transport between IP and MPLS Networks, page 3](#)
- [BGP Next Hop Verification, page 4](#)

## Interconnecting Provider Edge Routers Within an IP Network

This feature allows you to create a multi-access tunnel network to interconnect the provider edge (PE) routers servicing your IP network. This tunnel network transports IP VPN traffic to all of the PE routers. [Figure 1](#) illustrates the tunnel overlay network used in an IP network to transport VPN traffic between the PE routers.

**Figure 1** mGRE Tunnel Overlay Connecting PE Routers within an IP Network

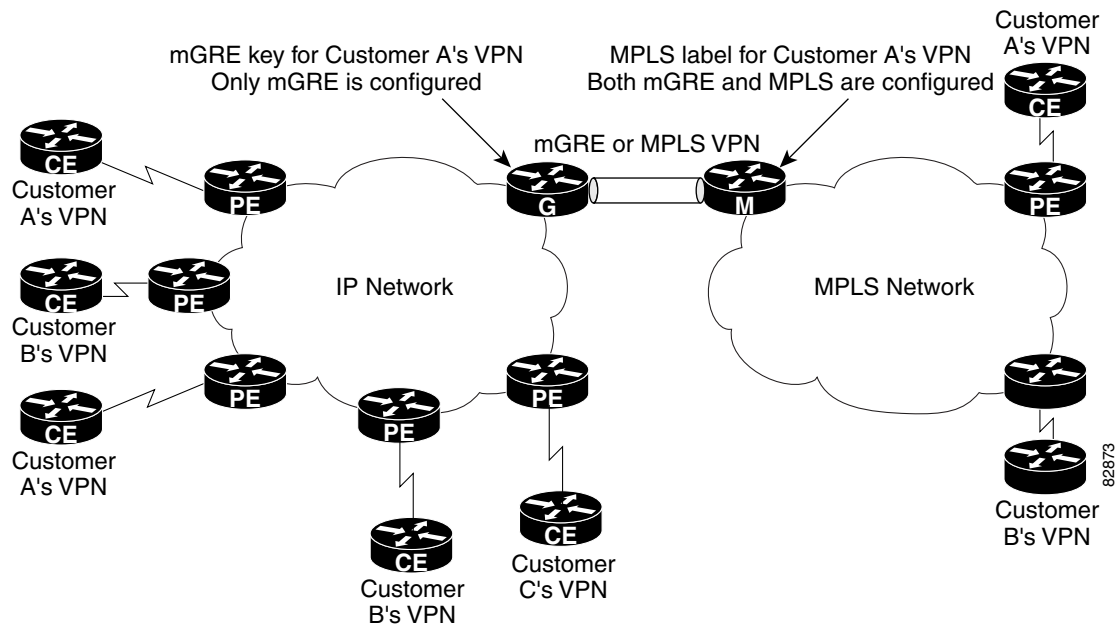


The multi-access tunnel overlay network provides full connectivity between PE routers. The PE routers exchange VPN routes using BGP as defined in RFC 2547. IP traffic is redirected through the multipoint tunnel overlay network using distinct IP address spaces for the overlay and transport networks and by changing the address space instead of changing the numerical value of the address.

## Packet Transport between IP and MPLS Networks

Layer 3 mGRE tunnels can be used as a packet transport mechanism between IP and MPLS networks. To enable the packet transport between the two different protocols, one PE router on one side of the connection between the two networks must run MPLS. [Figure 2](#) shows how mGRE tunnels can be used to transport VPN traffic between PE routers.

**Figure 2** mGRE Used to Transport VPN Traffic between IP and MPLS Network



For the packet transport to occur between the IP and MPLS network, the MPLS VPN label is mapped to the GRE key. The mapping takes place on the router where both mGRE and MPLS are configured. In [Figure 2](#) the mapping of the label to the key occurs on Router M which sits on the MPLS network.

## BGP Next Hop Verification

BGP performs the BGP path selection, or next hop verification, at the PE. For a BGP path to a network to be considered in the path selection process, the next hop for the path must be reachable in the Interior Gateway Protocol (IGP). When an IP prefix is received and advertised as the next hop IP address, the IP traffic is tunneled from the source to the destination by switching the address space of the next hop.

## How to Deploy L3 VPN mGRE Tunnels

To deploy L3 VPN mGRE tunnels you will create a VRF instance, create the mGRE tunnel, redirect the VPN IP traffic to the tunnel, and set up the BGP VPNv4 exchange so that updates are filtered through a route-map and interesting prefixes are resolved in the VRF table. The configuration steps are described in the following sections:

- [Creating the VRF and mGRE Tunnel, page 4](#)
- [Defining the Address Space and Specifying Address Resolution, page 6](#)

## Creating the VRF and mGRE Tunnel

The tunnel that transports the VPN traffic across the service provider network resides in its own address space. A special virtual route forwarding (VRF) instance must be created called Resolve in VRF (RiV). This section describes how to create the VRF and GRE tunnel.

## Prerequisites

The IP address on the interface should be the same as that of the source interface specified in the configuration. The source interface specified should match that used by BGP as a source for the VPNv4 update. The BGP configuration will include the **bgp neighbor x update-source loopback 0** command configured.

## SUMMARY STEPS

1. **enable**
2. **configure** { **terminal** | **memory** | **network** }
3. **ip vrf** *vrf-name*
4. **rd** 1:1
5. **interface** **tunnel** *n*
6. **ip address** *ip-address subnet-id*
7. **tunnel source** **loopback** *n*
8. **tunnel mode** **gre multipoint** **l3vpn**
9. **tunnel key** *gre-key*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
Step 2	<b>configure</b> { <b>terminal</b>   <b>memory</b>   <b>network</b> }  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip vrf</b> <i>vrf-name</i> <b>rd</b> 1:1  <b>Example:</b> Router#ip vrf customer_a_riv	Creates the special Resolve in VRF (RiV) VRF instance and table that will be used for the tunnel and redirection of the IP address.
Step 4	<b>interface</b> <b>tunnel</b> <i>n</i>  <b>Example:</b> interface tunnel 1	Enters Interface configuration mode to create the tunnel
Step 5	<b>ip address</b> <i>ip-address subnet-id</i>  <b>Example:</b> ipaddress 123.1.1.3 255.255.255.255	Specifies the IP address for the tunnel.

	Command or Action	Purpose
Step 6	<code>tunnel source loopback n</code>  <b>Example:</b> <code>tunnel source loopback 0</code>	Creates the loopback interface.
Step 7	<code>tunnel mode gre multipoint l3vpn</code>	Sets the mode for the tunnel as “gre multipoint l3vpn”.
Step 8	<code>tunnel key gre-key</code>	Specifies the GRE key for the tunnel.

**Example:**

```
ip vrf customer_a_riv
 rd 1:1
interface Tunnell
 ip vrf forwarding customer_a_riv
 ip address 123.1.1.3 255.255.255.255
 tunnel source Loopback0
 tunnel mode gre multipoint l3vpn
 tunnel key 123
end
```

## Defining the Address Space and Specifying Address Resolution

This configuration task described in this section sets up the BGP VPNv4 exchange so that the updates are filtered through a route-map and interesting prefixes are resolved in the VRF table.

### SUMMARY STEPS

1. **enable**
2. **configure** {terminal | memory | network}
3. **interface tunnel n**
4. **ip route vrf riv-vrf-name o.o.o.o o.o.o.o tunnel n**
5. **router bgp as-number**
6. **network network\_id**
7. **neighbor {ip-address | peer-group-name} remote-as as-number**
8. **neighbor {ip-address | peer-group-name} update-source interface-type**
9. **address-family vpnv4 [unicast]**
10. **neighbor {ip-address | peer-group-name} activate**
11. **neighbor {ip-address | peer-group-name} route-map map-name {in | out}**
12. **neighbor {ip-address | peer-group-name} route-map map-name {in | out}**
13. **set ip next-hop resolve-in-vrf vrf\_name**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables higher privilege levels, such as privileged EXEC mode.  Enter your password if prompted.
Step 2	<b>configure</b> { <b>terminal</b>   <b>memory</b>   <b>network</b> }  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface tunnel</b> <i>n</i>  <b>Example:</b> Router# interface tunnel 1	Enters Interface configuration mode for the tunnel.
Step 4	<b>ip route vrf</b> <i>riv-vrf-name</i> <i>o.o.o.o o.o.o.o</i> <b>tunnel</b> <i>n</i>  <b>Example:</b> Router (config)# ip route vrf 123.1.1.3 255.255.255.255	Sets the packet forwarding to the special Resolve-in-VRF (RiV) VRF.
Step 5	<b>router bgp</b> <i>as-number</i>  <b>Example:</b> Router (config)# router bgp 100	Specifies the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.
Step 6	<b>network</b> <i>network_id</i>  <b>Example:</b> Router (config)# network 200.0.0.3	Specifies the network ID for the networks to be advertised by the Border Gateway Protocol (BGP) and multiprotocol BGP routing processes.
Step 7	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>  <b>Example:</b> Router (config)# neighbor 123.1.1.2 remote-as 100	Adds an entry to the BGP or multiprotocol BGP neighbor table.
Step 8	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>update-source</b> <i>interface-type</i>	Specifies a specific operational interface that Border Gateway Protocol (BGP) sessions use for TCP connections.
Step 9	<b>address-family vpnv4</b> [ <b>unicast</b> ]	Specifies address family configuration mode for configuring routing sessions, such as BGP, that use standard Virtual Private Network (VPN) Version 4 address prefixes.
Step 10	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b>	Enables the exchange of information with a neighboring router, use the neighbor activate command in address family configuration or router configuration mode
Step 11	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>map-name</i> { <b>in</b>   <b>out</b> }	Applies a route map to incoming or outgoing routes. Use once for each inbound route.

	Command or Action	Purpose
Step 12	<code>neighbor {ip-address   peer-group-name}</code> <code>route-map map-name {in   out}</code>	Applies a route map to incoming or outgoing routes. Use once for each outbound route.
Step 13	<code>set ip next-hop resolve-in-vrf vrf_name</code>	Specifies that the next hop is to be resolved in the VRF table for the specified VRF.

VPN configuration is also required, but it is not described in this document. Refer to the *Cisco IOS Dial Services Configuration Guide*, Release 12.2 and the *Cisco IOS Switching Services Configuration Guide*, Release 12.2 for information about configuring VPNs.

## Troubleshooting Tips

Here are a few things you can check to make sure that the configuration is working properly.

### Check the VRF Prefix

Verify that the specified VRF prefix has been received by BGP. The BGP table entry should show that the route-map has worked and that the next hop is showing in the RiV. Use the `show ip bgp vpnv4` command as shown in this example:

```
Router_a#show ip bgp vpnv4 vrf customer 123.5.2.0
BGP routing table entry for 100:1:123.5.2.0/24, version 12
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
    123.1.1.2 in "my_riv" from 123.1.1.2 (123.1.1.2)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:1
```

Confirm that the same information has been propagated to the routing table:

```
Router_a#show ip route vrf customer 123.5.2.0
Routing entry for 123.5.2.0/24
  Known via "bgp 100", distance 200, metric 0, type internal
  Last update from 123.1.1.2 00:23:07 ago
  Routing Descriptor Blocks:
  * 123.1.1.2 (my_riv), from 123.1.1.2, 00:23:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 0
```

### CEF Switching

You can also verify that CEF switching is working as expected.

```
Router_a#show ip cef vrf customer 123.5.2.0
123.5.2.0/24, version 6, epoch 0
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Tu1, 123.1.1.2, tags imposed: {17}
  via 123.1.1.2, 0 dependencies, recursive
  next hop 123.1.1.2, Tunnel1 via 123.1.1.2/32 (my_riv)
  valid adjacency
  tag rewrite with Tu1, 123.1.1.2, tags imposed: {17}
```

### Endpoint Creation

Note that in this example display the tunnel endpoint has been created correctly:

```
Router_a#show tunnel endpoint tunnel 1
```

```
Tunnel1 running in multi-GRE/IP mode
RFC2547/L3VPN Tunnel endpoint discovery is active on Tu1
Transporting l3vpn traffic to all routes recursing through "my_riv"

Endpoint 123.1.1.2 via destination 123.1.1.2
Endpoint 123.1.1.6 via destination 123.1.1.6
```

### Adjacency

Confirm that the corresponding adjacency has been created;

```
Router_a#show adjacency Tunnel 1 int
Protocol Interface      Address
TAG      Tunnel1           123.1.1.2(4)
                               15 packets, 1980 bytes
                               4500000000000000FF2FC3C77B010103
                               7B010102000008847
                               Epoch: 0
                               Fast adjacency disabled
                               IP redirect disabled
                               IP mtu 1472 (0x0)
                               Fixup enabled (0x2)
                               GRE tunnel
                               Adjacency pointer 0x624A1580, refCount 4
                               Connection Id 0x0
                               Bucket 121
```

Note that because MPLS is being transported over mGRE, the LINK\_TAG adjacency is the relevant adjacency. The MTU reported in the adjacency is the payload length (including the MPLS label) that the packet will accept. The mac\_string shown in the adjacency display can be interpreted as follows:

```
45000000 -> Beginning of IP Header (Partially populated, t1 & chksum
00000000   are fixed up per packet)
FF2FC3C7
7B010103 -> Source IP Address in transport network 123.1.1.3
7B010102 -> Destination IP address in transport network 123.1.1.2
00008847 -> GRE Header
```

## What to Do Next

Refer to the *Cisco IOS Dial Services Configuration Guide*, Release 12.2 and the *Cisco IOS Switching Services Configuration Guide* for information about configuring VPNs

# Configuration Examples for Dynamic Layer-3 VPNs (RFC 2547) Support Using Multipoint GRE (mGRE) Tunnels

- [Configuring Layer 3 VPN mGRE Tunnels, page 9](#)

## Configuring Layer 3 VPN mGRE Tunnels

This example shows the configuration sequence for creating multipoint GRE (mGRE) tunnels. It includes the definition of the special VRF instance.

```
ip vrf my_riv
```

```

rd 1:1
interface Tunnel1
ip vrf forwarding my_riv
ip address 123.1.1.3 255.255.255.255
tunnel source Loopback0
tunnel mode gre multipoint l3vpn
tunnel key 123
end
ip route vrf my_riv 0.0.0.0 0.0.0.0 Tunnel1

router bgp 100
network 200.0.0.3
neighbor 123.1.1.2 remote-as 100
neighbor 123.1.1.2 update-source Loopback0
!
address-family vpnv4
neighbor 123.1.1.2 activate
neighbor 123.1.1.2 route-map SELECT_UPDATES_FOR_L3VPN_OVER_MGRE in
!
route-map SELECT_UPDATES_FOR_L3VPN_OVER_MGRE permit 10
set ip next-hop in-vrf my_riv

```

## Additional References

For additional information related to dynamic L3 VPN mGRE tunnels, refer to the following references:

## Related Documents

Related Topic	Document Title
VPN (Virtual Private Network) configuration	<i>Cisco IOS Dial Services Configuration Guide</i> , Release 12.2 and <i>Cisco IOS Switching Services Configuration Guide</i> , Release 12.2
CEF switching	<i>Cisco IOS Switching Services Configuration Guide</i> , Release 12.2
VPN Routing and Forwarding (VRF) instances	<i>Cisco IOS Switching Services Configuration Guide</i> , Release 12.2
Generic Routing Encapsulation (GRE)	<i>Cisco IOS Interface Configuration Guide</i> , Release 12.2

## Standards

Standards <sup>1</sup>	Title
None.	

1. Not all supported standards are listed.

## MIBs

MIBs <sup>1</sup>	MIBs Link
<ul style="list-style-type: none"> <li>None</li> </ul>	<p>To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></p>

1. Not all supported MIBs are listed.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to [cco-locksmith@cisco.com](mailto:cco-locksmith@cisco.com). An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

## RFCs

RFCs <sup>1</sup>	Title
RFC 2547	<i>BGP/MPLS VPNs</i>

1. Not all supported RFCs are listed.

## Technical Assistance

Description	Link
<p>Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.</p>	<p><a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a></p>

# Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications. The following command descriptions are included:

- [set ip next-hop \(BGP\)](#)
- [show tunnel endpoints](#)
- [tunnel mode](#)

## set ip next-hop (BGP)

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set ip next-hop** route-map configuration command. To delete an entry, use the **no** form of this command.

```
set ip next-hop ip-address [... ip-address] [peer-address] [resolve-vrf vrf-name]
```

```
no set ip next-hop ip-address [... ip-address] [peer-address]
```

Syntax Description	
<i>ip-address</i>	IP address of the next hop to which packets are output. The next hop must be an adjacent router.
<b>peer-address</b>	(Optional) Sets the next hop to be the BGP peering address.
<b>resolve-vrf</b>	(Optional) Specifies that the next hop is to be resolved in the Virtual Routing and Forwarding (VRF) table for the specified VRF instance.

Defaults	
	Disabled

Command Modes	
	Route-map configuration

Command History	Release	Modification
	11.0	This command was introduced.
	12.0	The <b>peer-address</b> keyword was added.
	12.0(23)S	The <b>resolve-vrf</b> keyword was added to support dynamic Layer 3 VPN multipoint GRE (mGRE) tunneling.

### Usage Guidelines

#### Specifying Multiple Values

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

If the interface associated with the first next hop specified with the **set ip next-hop** command is down, the optionally specified IP addresses are tried in turn.

#### Policy Routing

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria*—the conditions under which policy routing occurs. The **set** commands specify the *set actions*—the particular routing actions to perform if the criteria enforced by the **match** commands are met.

### Next Hop Inbound Routes

When the **set ip next-hop** command is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

### Next Hop Outbound Routes

When the **set ip next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ip next-hop** command has finer granularity than the per-neighbor **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

### Precendence of Set Clause Processing

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. **set ip next-hop**
2. **set interface**
3. **set ip default next-hop**
4. **set default interface**

### Examples

In the following example, three routers are on the same FDDI LAN (with IP addresses 1.1.1.1, 1.1.1.2, and 1.1.1.3). Each is in a different autonomous system. The **set ip next-hop peer-address** command specifies that traffic from the router (1.1.1.3) in remote autonomous system 300 for the router (1.1.1.1) in remote autonomous system 100 that matches the route map is passed through the router bgp 200, rather than sent directly to the router (1.1.1.1) in autonomous system 100 over their mutual connection to the LAN.

```
router bgp 200
neighbor 1.1.1.3 remote-as 300
neighbor 1.1.1.3 route-map set-peer-address out
neighbor 1.1.1.1 remote-as 100
route-map set-peer-address permit 10
set ip next-hop peer-address
```

### Related Commands

Command	Description
<b>ip policy route-map</b>	Identifies a route map to use for policy routing on an interface.
<b>match ip address</b>	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
<b>match length</b>	Bases policy routing on the Level 3 length of a packet.
<b>neighbor next-hop-self</b>	Disables next hop processing of BGP updates on the router.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
<b>set default interface</b>	Indicates where to output packets that pass a match clause of a route map for policy routing and that have no explicit route to the destination.

---

<b>set interface</b>	Indicates where to output packets that pass a match clause of a route map for policy routing.
<b>set ip default next-hop</b>	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.

---

# show tunnel endpoints

To display information about source and destination endpoints for multipoint tunnels, use the show tunnel endpoints command in EXEC mode.

**show tunnel endpoints tunnel** *interface*

<b>Syntax Description</b>	<i>interface</i>	Indicates the interface associated with the tunnel definition.
---------------------------	------------------	--

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(23)S	This command was introduced to support dynamic Layer 3 multipoint GRE (mGRE) tunnels.

## Examples

This example shows that the tunnel endpoint has been created correctly:

```
Router_a#show tunnel endpoint tunnel 1
Tunnell running in multi-GRE/IP mode
RFC2547/L3VPN Tunnel endpoint discovery is active on Tu1
Transporting l3vpn traffic to all routes recursing through "my_riv"

Endpoint 123.1.1.2 via destination 123.1.1.2
Endpoint 123.1.1.6 via destination 123.1.1.6
```

[Table 1](#) describes the significant fields shown in the display.

**Table 1** *show xxx Field Descriptions*

<b>Field</b>	<b>Description</b>
Tunnell running in multi-GRE/IP mode ... through "my_riv"	Indicates that the tunnel is active and that traffic is being routed as specified through the special VRF instance.
Endpoint 123.1.1.2 via destination 123.1.1.2	Reports the endpoint destination.

## Related Commands

<b>Command</b>	<b>Description</b>
<b>ip route vrf tunnel</b>	Sets the packet forwarding to the special Resolve-in-VRF (RiV) VRF.

# tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** interface configuration command. To set to the default, use the **no** form of this command.

```
tunnel mode {aurp | cayman | dvmrp | eon | gre ip [multipoint [l3vpn]] | ipip | nos}
```

```
no tunnel mode
```

Syntax Description		
	<b>aurp</b>	AppleTalk Update-Based Routing Protocol (AURP).
	<b>cayman</b>	Cayman Tunnel Talk AppleTalk encapsulation.
	<b>dvmrp</b>	Distance Vector Multicast Routing Protocol.
	<b>eon</b>	EON compatible Connectionless Network Service (CLNS) tunnel.
	<b>gre ip</b>	Generic routing encapsulation (GRE) protocol over IP.
	<b>multipoint</b>	(Optional) Enables a GRE tunnel to be used in a multipoint fashion. Can be used with the <b>gre ip</b> keyword only, and requires the use of the <b>tunnel key</b> command.
	<b>ipip</b>	IP over IP encapsulation.
	<b>l3vpn</b>	(Optional) Enables Layer 3 VPN tunneling. Must be used with the multipoint keyword.
	<b>nos</b>	KA9Q/network operating system (NOS) compatible IP over IP.

**Defaults** GRE tunneling

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	10.3	The <b>ipip</b> , <b>aurp</b> , and <b>dvmrp</b> keywords were introduced.
	12.0(23)S	The <b>l3vpn</b> keyword was added to support dynamic Layer 3 VPN multipoint GRE (mGRE) tunnels.

**Usage Guidelines** **Encapsulation and Loopback Interfaces**

Two tunnels cannot use the same encapsulation mode with exactly the same source and destination address. The work around is to create a loopback interface and source packets off the loopback interface.

### Cayman Tunneling

Cayman tunneling implements tunneling as designed by Cayman Systems. This enables our routers and access servers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers or between a Cisco device and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address because there is no way to ping the other end of the tunnel.

### Distance Vector Multicast Routing Protocol

Use Distance Vector Multicast Routing Protocol (DVMRP) when a router connects to an mrouter to run DVMRP over a tunnel. It is required to configure Protocol-Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

### GRE Tunneling

GRE (generic routing encapsulation) tunneling can be done between Cisco routers and access servers only. When using GRE tunneling for AppleTalk, configure the tunnel with an AppleTalk network address in order to ping the other end of the tunnel.

## Examples

For multipoint GRE tunnels, a tunnel key must be configured. Unlike other tunnels, the tunnel destination is optional. However, if the tunnel destination is supplied, it must map to an IP multicast address.

The following example enables Cayman tunneling:

```
Router(config)# interface tunnel 0
Router(config-if) tunnel source ethernet 0
Router(config-if) tunnel destination 10.108.164.19
Router(config-if) tunnel mode cayman
```

The following example enables GRE tunneling:

```
Router(config)# interface tunnel 0
Router(config-if) appletalk cable-range 4160-4160 4160.19
Router(config-if) appletalk zone Engineering
Router(config-if) tunnel source ethernet0
Router(config-if) tunnel destination 10.108.164.19
Router(config-if) tunnel mode gre ip
```

## Related Commands

Command	Description
<b>appletalk cable-range</b>	Enables an extended AppleTalk network.
<b>appletalk zone</b>	Sets the zone name for the connected AppleTalk network.
<b>tunnel destination</b>	Specifies the destination for a tunnel interface.
<b>tunnel source</b>	Sets the source address of a tunnel interface.