



Generic Routing Encapsulation on the Cisco CMTS

Revised: January 24, 2007, OL-9503-01

This document describes the Generic Routing Encapsulation (GRE) feature. This feature is a tunneling protocol that enables the encapsulation of a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

History for the Generic Routing Encapsulation Feature

Release	Modification
12.3(17a)BC	This feature was introduced.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Generic Routing Encapsulation, page 2](#)
- [Restrictions for Generic Routing Encapsulation, page 3](#)
- [Information About Generic Routing Encapsulation, page 3](#)
- [How to Configure Generic Routing Encapsulation, page 5](#)
- [Additional References, page 8](#)
- [Command Reference, page 10](#)
- [Glossary, page 10](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2006 Cisco Systems, Inc. All rights reserved.

Prerequisites for Generic Routing Encapsulation

- The Cisco uBR7246VXR or Cisco uBR10012 router must be running Cisco IOS 12.3(17a)BC or later release.
- The Cisco uBR10012 router requires the Performance Routing Engine 2 (PRE2) module for use with Generic Routing Encapsulation.
- To use GRE, you must identify the inside interfaces on your devices and specify these in the Router MC Settings configuration area. Inside interfaces are the physical interfaces on the device that connect the device to its internal subnets and networks.
- In Router MC, you must select a routing protocol whenever you enable GRE. The available routing protocols in Router MC are EIGRP and OSPF:
 - Enhanced Interior Gateway Routing Protocol (EIGRP) allows the exchange of routing information within an autonomous system and addresses some of the more difficult issues associated with routing in large, heterogeneous networks. Compared to other protocols, EIGRP provides superior convergence properties and operating efficiency. EIGRP combines the advantages of several different protocols.
 - Open Shortest Path First (OSPF) is a link-state, hierarchical protocol that features least-cost routing, multipath routing, and load balancing.
- In Router MC, you must specify an Interior Gateway Protocol (IGP) process number. This number identifies the IGP. When GRE is implemented, this IGP will be the secured IGP. See *How Does Router MC Implement GRE?* for more information about IGPs. For secure communication, the inside interfaces on peering devices in your VPN must belong to the same IGP. The IGP process number must be within the range specified in the configuration support settings under the Admin tab. If you have an existing IGP on the device that is within this range, but is different from the IGP process number specified in your GRE settings, Router MC will remove the existing IGP. If the existing IGP process number matches the one specified in your GRE settings, any networks included in the existing IGP process that do not match the specified inside interfaces, will be removed.
- If the inside interfaces on your devices are configured to use an IGP other than the IGP specified in your GRE settings (meaning that the interfaces belong to an unsecured IGP):
 - For spokes: Manually remove the inside interfaces from the unsecured IGP by means of the device CLI before configuring GRE with Router MC.
 - For hubs: If the hub inside interface is used as a network access point for Router MC, then on deployment, the interface will be published in both secured and unsecured IGPs. To ensure that the spoke peers use only the secured IGP, manually add the auto-summary command for the unsecured IGP or remove the unsecured IGP for that inside interface.
- In Router MC, you must provide a subnet that is unique and not globally-routable for loopback. This subnet must only be used to support the implementation of loopback for GRE. The loopback interfaces are created, maintained, and used only by Router MC. You should not use them for any other purpose.
- If you are using static routes instead of unsecured IGP, make sure you configure static routes on the spokes through to the hub inside interfaces

Important Notes about Configuring GRE

- You can define GRE on the Global object or on any device group (with the exception of a High Availability (HA) group).
- You can define different GRE policies for different groups of devices within your hierarchy. If you define GRE on Global, the GRE settings will be inherited by all device groups and devices in the hierarchy. You can override the Global GRE policy by defining a different GRE policy on one or more device groups.
- Peering devices must be configured with the same failover and routing policy. Therefore, if you define a specific GRE policy on a device group, both the hub and the spoke must be descendants of that device group and there must be no overriding policy on a lower level that changes the GRE policy on either the peering hub or spoke.
- Switching from IKE keepalive to GRE—If you previously used IKE keepalive for failover, and you later switch to GRE, everything outside your attached networks will no longer be a part of your VPN. Attached networks include only those networks that are directly connected to the router's inside interfaces.

Restrictions for Generic Routing Encapsulation

- To run GRE configuration, you need to have IP connectivity between the cable modems.
- The Cisco uBR10012 router requires the Performance Routing Engine 2 (PRE2) modules for use with Generic Routing Encapsulation. The GRE feature is not supported for PRE1 modules in the Cisco uBR10012 router.

Information About Generic Routing Encapsulation

To configure the Generic Routing Encapsulation feature, you should understand the following concepts:

- [Tunneling, page 3](#)
- [Generic Routing Encapsulation Overview, page 4](#)

Tunneling

Tunneling (also known as port forwarding) is a technique that enables remote access users to connect to a variety of network resources through a public data network. The tunnels established through the public network are usually point-to-point, though a multipoint tunnel is possible, and is used to link a remote user to a resource at the far end of the tunnel. Major tunneling protocols encapsulate Layer 2 traffic from the remote user and send it across the public network to the far end of the tunnel, where it is de-encapsulated and sent to its destination.

Tunneling requires three different protocols:

- Passenger protocol—The original data (IPX, NetBeui, IP) being carried.
- Encapsulating protocol—The protocol (GRE, IPSec, L2F, PPTP, and L2TP) that is wrapped around the original data.
- Carrier protocol—The protocol used by the network over which the information is traveling.

The original packet (Passenger protocol) is encapsulated inside the encapsulating protocol, which is then put inside the carrier protocol's header (usually IP) for transmission over the public network. Note that the encapsulating protocol also quite often carries out the encryption of the data. As you can see, protocols such as IPX and NetBeui, which would normally not be transferred across the Internet, can safely and securely be transmitted.

For site-to-site virtual private networks (VPNs), the encapsulating protocol is usually IPSec or Generic Routing Encapsulation (GRE). GRE includes information on what type of packet you are encapsulating and information about the connection between the client and server.

For remote-access VPNs, tunneling normally takes place using Point-to-Point Protocol (PPP). Part of the TCP/IP stack, PPP is the carrier for other IP protocols when communicating over the network between the host computer and a remote system. PPP tunneling will use one of PPTP, L2TP or Cisco's Layer 2 Forwarding (L2F).

The most significant benefit of Tunneling is that it allows for the creation of VPNs over public data networks to provide cost savings for both end users, who do not have to create dedicated networks, and for Service Providers, who can leverage their network investments across many VPN customers.

Generic Routing Encapsulation Overview

GRE Tunneling is a protocol for transporting an arbitrary network layer protocol (the payload) over another arbitrary network layer protocol (the delivery). This is achieved by encapsulating the payload packet in a delivery packet, along with a GRE header. By having both protocols encapsulate IP packets within an additional outer IP header, this enables the transport of IP multicast IP packets across a unicast-only backbone.

The following are some of the advantages of GRE tunnels:

- GRE tunnels provide multi-protocol local networks over a single-protocol backbone.
- GRE tunnels provide workarounds for networks that contain protocols with limited hop counts.
- GRE tunnels connect discontinuous sub-networks.
- GRE tunnels allow VPNs across WANs.

How to Configure Generic Routing Encapsulation

Use the following procedures to configure the GRE feature.

Before configuring the GRE feature:

- Please read the following topics:
 - [Prerequisites for Generic Routing Encapsulation, page 2](#)
 - [Important Notes about Configuring GRE, page 3](#)
- If workflow mode is enabled, make sure that you are working within the context of an open activity.

-
- Step 1** Select **Configuration > Settings**
- Step 2** Select **General VPN> Failover and Routing** in the TOC. The Failover and Routing page appears. [Table 1](#) describes the elements in the Failover and Routing page.
- Step 3** Select **GRE** in the Policy Type list box. The page refreshes to display only the fields that are relevant for GRE configuration.
- Step 4** Enter information in the displayed GRE fields, as required. Click **Advanced** to display additional GRE fields (optional). See [Table 1](#) for a description of each field.
- Step 5** Click **Apply**.
-

Table 1 *Failover and Routing: GUI Reference*

GUI Element	Description
Policy Type list box	Select the type of failover method you want to use. The page will refresh to display only the fields relevant for your selection. <ul style="list-style-type: none">• IKE Keepalive• GRE.• GRE Dynamic IP• DMVPN
GRE Elements	
Routing Protocol list box	Select either EIGRP or OSPF as the routing protocol. See Prerequisites for Configuring and Deploying GRE for more information.
Tunnel Interface IP field	Enter a private IP address, including the subnet mask in bits, which defines a subnet in your enterprise to be used to support the implementation of loopback for GRE. For example, 192.10.9.1/255.255.255.0. Router MC creates a loopback interface on the peering devices, with an IP address from this subnet. The loopback interfaces serve as the GRE tunnel endpoints.

Table 1 **Failover and Routing: GUI Reference**



GUI Element	Description
Tunnel Source IP field	<p>For GRE Dynamic IP only. Enter a private IP address, including the subnet mask in bits.</p> <p> Note To provide robust, stable tunnels, Router MC creates a static IP route using this IP address. If you change this IP address or you change the failover and routing policy, Router MC does not remove the static route from the device configuration. Please consider this if you have a problem with unstable GRE tunnels.</p>
Enable IP Multicast check box	<p>Select this check box to enable multicast transmissions across your GRE tunnels. IP multicast delivers application source traffic to multiple receivers without burdening the source or the receivers, while using a minimum of network bandwidth.</p> <p>When IP Multicast is enabled, you must specify a rendezvous point that acts as the meeting place for sources and receivers of multicast data.</p>
Rendezvous Point field	<p>This field is only editable when the IP Multicast check box is selected.</p> <p>Enter the IP address of the interface that will serve as the rendezvous point (RP) for multicast transmission. Sources send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree.</p>
Allow direct spoke to spoke tunnels check box	<p>For DMVPN only. Select this check box to enable direct communication between spokes, without going through the hub.</p> <p> Note Note With direct spoke-to-spoke communication, you must use the Main Mode Address option for preshared key negotiation.</p>
Advanced or Basic button	<p>Click the Advanced button to display additional fields for optional advanced configuration. Router MC provides default values for all the advanced options. You can change these default values if required.</p> <p>When the advanced fields are displayed, click the Basic button to display only the basic configuration fields and hide the advanced fields.</p>

Table 1 *Failover and Routing: GUI Reference*

GUI Element	Description
Process Number field	<p>Router MC adds an additional Interior Gateway Protocol (IGP) that is dedicated for IPsec and GRE secured communication. An IGP refers to a group of devices that receive routing updates from one another by means of a routing protocol, either EIGRP or OSPF. Each “routing group” is identified by a logical number, the process number.</p> <p>Enter a routing process number that will be used to identify the secured IGP that Router MC adds when configuring GRE.</p> <p>The number that you provide must be within the range specified next to the field name. The default is the lowest value in the range. This range can be changed in the Configuration Support Settings page in the Admin tab.</p>
Delay	Specify the throughput delay for the interface, in seconds.
Hello Interval EIGRP	Specify the interval between hello packets sent on the interface, from 1 to 65535 seconds. The default is 5 seconds.
Hold Time EIGRP	Specify the number of seconds the router will wait to receive a hello message before invalidating the connection. The default hold time is 15 seconds (three times the hello interval).
Tunnel Key field	For DMVPN only. Enter a number that identifies the tunnel key. The tunnel key differentiates between different multipoint GRE (mGRE) tunnel Non Broadcast Multiple Access (NBMA) networks. All mGRE interfaces in the same NBMA network must use the same tunnel key value. If there are two mGRE interfaces on the same router, they must have different tunnel key values.
Network ID (NHRP) field	For DMVPN only. All NHRP stations within one logical NBMA network must be configured with the same network identifier. Enter a globally unique, 32-bit network identifier within the range of 1 to 4294967295.
Hold Time (NHRP) field	<p>For DMVPN only. Enter the time in seconds that routers will keep information provided in authoritative Next Hop Resolution Protocol (NHRP) responses. The cached IP-to-NBMA (non-broadcast multi-access) address mapping entries are discarded after the hold time expires.</p> <p>The default is 600 seconds.</p>
Authentication (NHRP) field	For DMVPN only. Enter an authentication string that controls whether the source and destination NHRP stations allow intercommunication. All routers within the same network using NHRP must share the same authentication string. The string can be up to eight characters long.
Apply button	Click to apply your definitions.

Table 1 *Failover and Routing: GUI Reference*

GUI Element	Description
Clear button	The Clear button is only present if Global is selected in the Object Selector. Click the Clear button to remove your current definitions.
Defaults button	The Defaults button is present when any object other than Global is selected in the Object Selector. Click to remove your local definitions and restore the inherited default values.

Additional References

The following sections provide references related to the GRE feature.

- [Related Documents, page 9](#)
- [Standards, page 9](#)
- [MIBs, page 9](#)
- [RFCs, page 9](#)
- [Technical Assistance, page 10](#)

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco Broadband Cable Command Reference Guide, at the following URL: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 Configuration Guides and Command References, at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html
Configuring GRE Tunnel over Cable	<i>Configuring GRE Tunnel over Cable</i> , at the following URL: http://www.cisco.com/en/US/tech/tk86/tk89/technologies_configuration_example09186a008011520d.shtm

Standards

Standard	Title
SP-RF1v1.1-109-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1 (http://www.cablelabs.com/cablemodem/)

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1701	Generic Routing Encapsulation (GRE)
RFC 1702	Generic Routing Encapsulation over IPv4 networks
RFC 1853	IP in IP Tunneling
RFC 2003	IP Encapsulation within IP
RFC 2784	Generic Routing Encapsulation (GRE)
RFC 2890	Key and Sequence Number Extensions to GRE

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html

Command Reference

This feature uses no new or modified commands.

Glossary

EIGRP—Enhanced Interior Gateway Routing Protocol. An interior gateway protocol suited for many different topologies and media.

GRE—Generic Routing Encapsulation. A protocol for transporting an arbitrary network layer protocol (the payload) over another arbitrary network layer protocol (the delivery)

HA—High Availability.

IGP—Interior Gateway Protocol. A protocol for exchanging routing information between gateways in an autonomous network.

L2F—Layer 2 Forwarding. A Layer 2 tunneling protocol that establishes a secure tunnel across a public infrastructure (such as the Internet) that connects an ISP POP to a enterprise home gateway. This tunnel creates a virtual point-to-point connection between the user and the enterprise customer's network. L2F is the most established and stable Layer 2 tunneling protocol.

mGRE—multipoint GRE. A mGRE allows a single GRE interface to support multiple IPsec tunnels and simplifies the size and complexity of the configuration.

NBMA—Non Broadcast Multiple Access. A multiaccess network that either does not support broadcasting (such as X.25) or in which broadcasting is not feasible (for example, an SMDS broadcast group or an extended Ethernet that is too large).

NHRP—Next Hop Resolution Protocol. A protocol employed by routers on a nonbroadcast multiaccess (NBMA) network to dynamically locate MAC addresses of various hosts and routers. Systems using NHRP are able to communicate directly without requiring an intermediate hop, increasing performance in ATM, Frame Relay, X.25, and SMDS systems.

OSPF—Open Shortest Path First. A link-state, hierarchical IGP routing algorithm that includes features such as load balancing, least-cost routing, and multipath routing.

PPP—Point-to-Point Protocol. The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits.

RP—rendezvous point. A single common root placed at a chosen point of a shared distribution tree. When PIM is configured in sparse mode, you must choose one or more routers to operate as an RP.

VPNs—virtual private networks. Enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**Note**

See *[Internetworking Terms and Acronyms](#)* for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

© 2006 Cisco Systems, Inc. All rights reserved.

