Ethernet over GRE Tunnels

The Ethernet over GRE Tunnels feature allows customers to leverage existing low–end residential gateways to provide mobility services to mobile nodes using Proxy Mobile IPv6 (PMIPv6), General Packet Radio Service (GPRS) Tunneling Protocol (GTP), and Intelligent Service Gateway (ISG).

Finding Feature Information

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

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Ethernet over GRE Tunnels

- Mobile nodes can have only IPv4 addresses
- IPv6 mobile clients are not supported
- If the VLAN priority tag inside the EoGRE packet is set to a nonzero value, ISG or iWAG ignores the packet

Information About Ethernet over GRE Tunnels

The Ethernet over GRE tunnels feature allows customers to leverage existing low-end residential gateways to provide mobility services to mobile nodes.

As service provider Wi-Fi space gains popularity, Cisco customers need to provide access to the Internet and mobile services using public hotspots. A high–end RG can provide these mobility services using Proxy Mobile IPv6 (PMIPv6), Intelligent Service Gateway (ISG) or General Packet Radio Service (GPRS) Tunneling Protocol (GTP).

Low-end RGs or customer premises equipment (CPE) can be used to forward traffic from Mobile nodes to high-end devices. These RGs or CPE can be configured in bridged mode, and Ethernet over Generic Routing Encapsulation (GRE) tunnels can be used to forward Ethernet traffic to the aggregation device.

Mobile nodes access the Internet over Wi-Fi access points (APs). The APs are either autonomous or connected to a wireless LAN controller (WLC). These APs and WLCs are generically referred to as RGs or CPEs. The CPEs are located at individual or community residences and may be connected to the service–provider network through a connection mechanism like an asymmetric DSL (ADSL) modem or a cable modem. The connection mechanism is transparent to the aggregation device.

These CPEs are provided, provisioned, and managed by the service provider as a part of the broadband access service. Generally, there is extra bandwidth on the Wi-FI AP as well as the back-end pipe to the service provider, which can be used to provide mobile–Internet services to roaming customers in the vicinity.

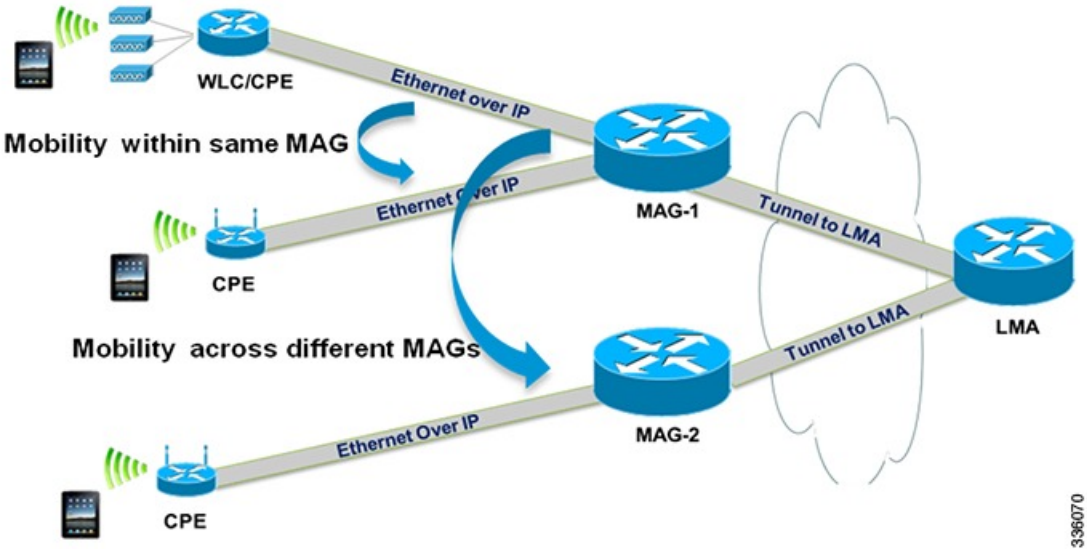
Mobility Services Using PMIPv6

You can use PMIPv6 to provide mobility services to mobile devices, but you would require high-end RGs with Mobile Access Gateways (MAG) functionality.

RGs or CPEs can also be used to forward traffic from Mobile nodes to MAG-enabled aggregation devices using Ethernet over GRE tunnels.

The aggregation device can create IP sessions and allocate IP addresses (locally or in proxy mode) in a manner similar to regular IP sessions on physical Ethernet interfaces.

Figure 1: Mobility Services Using PMIPv6



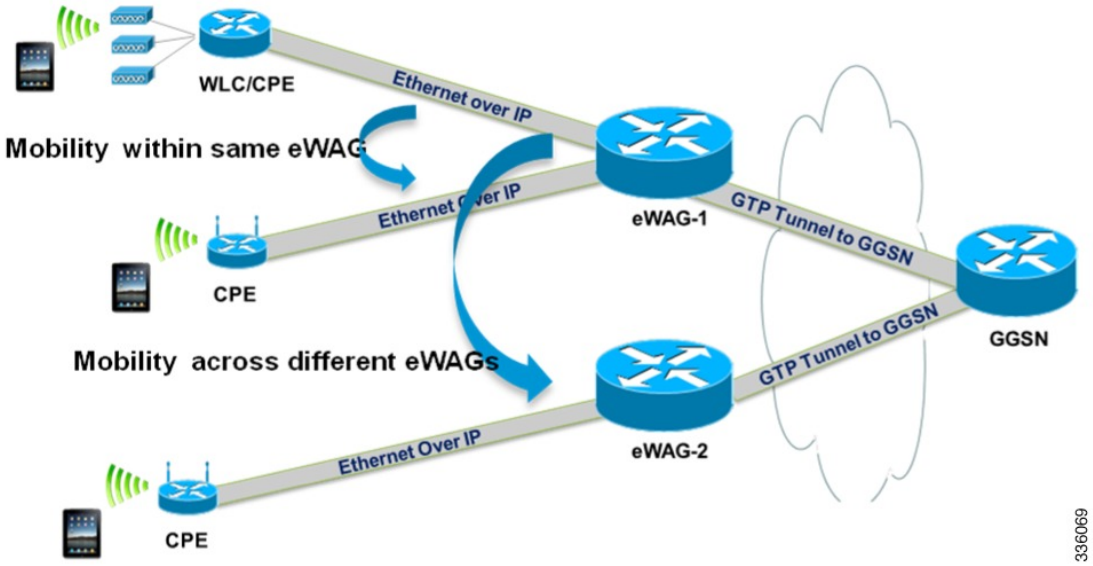
In the deployment scenario given in the above figure, MAG-1 and MAG-2 are configured to handle tunneled Ethernet traffic from access side and also have regular IP tunnels to one or more local mobility anchor (LMA).

Mobility Services Using GTP

You can use GTP to provide mobility services to mobile devices, but you would require high-end RGs with Enhanced Wireless Access Gateway functionality.

RGs or CPEs can also be used to forward traffic from Mobile nodes to Enhanced Wireless Access Gateway devices using Ethernet over GRE tunnels.

Figure 2: Mobility Services Using GTP



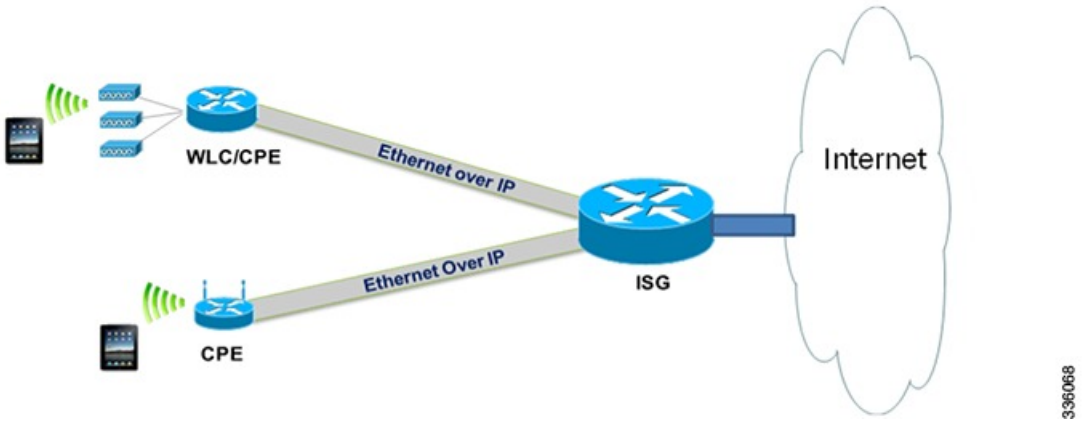
In the deployment scenario given in the above figure, eWAG-1 and eWAG-2 are configured to handle tunneled Ethernet traffic from access side and also have one or more GTP tunnels to one or more gateway Cisco General packet radio service (GPRS) support node (GGSN) devices.

Mobility Services Using ISG

You can use ISG to provide simple IP services to mobile devices but you would require a high-end RGs with ISG functionality.

RGs or CPEs can also be used to forward traffic from Mobile nodes to ISG devices using Ethernet over GRE tunnels as shown in the figure below.

Figure 3: Mobility Services Using ISG



Ethernet over GRE Tunnels Supported Functionality

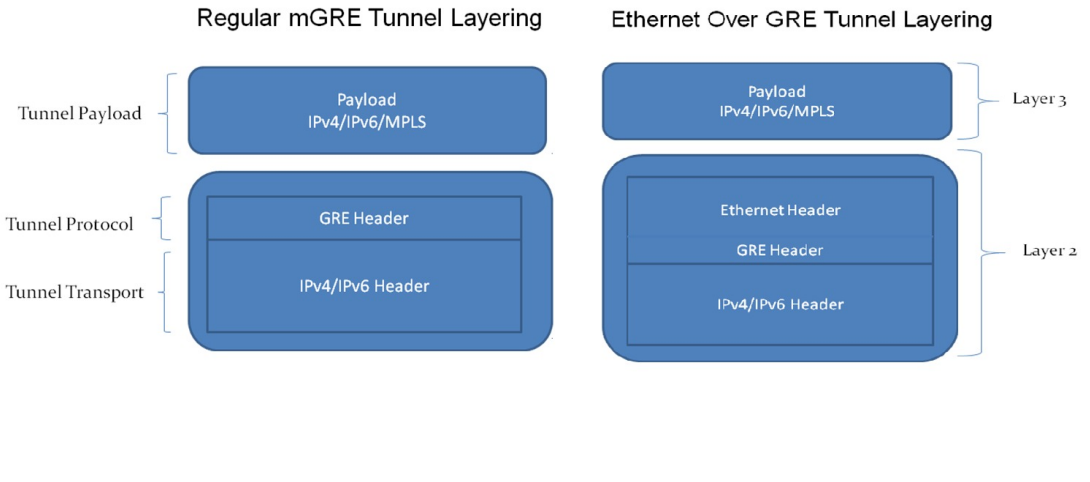
The Ethernet over GRE tunnels feature supports the following functionality:

- Mobility services can be provided to the mobile nodes using existing low-end residential gateways (RGs) using Ethernet over generic routing and encapsulation (GRE) tunnels. Intelligent Service Gateway (ISG), Proxy Mobile IPv6 (PMIPv6), and GPRS Tunneling Protocol (GTP) can be used to provide the mobility services.
- Ethernet frames can be transported over IPv6 and IPv4 infrastructures. Customer premises Equipment (CPE) is pre–configured with a point-to-point Generic Routing Encapsulation (GRE) IPv4 or IPv6 tunnel. The tunnel destination is a well-known IPv4 or IPv6 address of an aggregation device.
- Tunnels can be configured to be part of a single VLAN—The CPE may insert a VLAN tag in the Ethernet frame. Only a single VLAN tag is supported.
- Tunnels can be configured with a statically configured, symmetric GRE key. You can use the **tunnel key** command to configure this key.
- Sessions can be created with DHCP for IPv4 (DHCPv4), unclassified MAC, and Address Resolution Protocol (ARP) Detecting Network Attachments for IPv4 (DNAv4).

Tunnel Encapsulation in Ethernet over GRE tunnels

Tunnel encapsulation in Ethernet over GRE tunnels is similar to tunnel encapsulation in multipoint Generic Routing Encapsulation (mGRE) tunnels, given in the below figure.

Figure 4: Comparison of Ethernet over GRE tunnels and mGRE tunnels



The mGRE tunnel is a nonbroadcast multiAccess (NBMA) interface that can handle multiple tunnel endpoints. The mGRE tunnel can forward payloads like IPv4, IPv6, and Multiprotocol Label Switching (MPLS) in GRE–encapsulated IPv4/IPv6 transport frames from different endpoints, which can then be sent to specific endpoints. While transmitting, the mGRE tunnel interface encapsulates the payload with GRE and transports IPv4/IPv6 headers. On the receiving end, the mGRE tunnel interface strips the GRE and transport header and forwards the payload.

In Ethernet over GRE tunnels, the Ethernet header is included in the tunnel encapsulation along with GRE and transport header.

The tunnel modes used for Ethernet over GRE IPv4 transport can be set using the **tunnel mode ethernet gre ipv4** command.

Similarly, the tunnel modes used for Ethernet over GRE IPv6 transport can be set using the **tunnel mode ethernet gre ipv6** command.

You can see the source of the tunnel by using the **show tunnel source tracking** command.

Although the Ethernet over GRE tunnel simulates regular Ethernet behavior for all practical purposes, the interface is an NBMA interface at the data-link layer. As there may be many mobile nodes and CPE connected to the Ethernet over GRE tunnel, broadcasting a packet is not supported. Even if an aggregation device like the Mobile Access Gateway (MAG) needs to use a broadcast MAC address in the downstream packet frame, the message is unicast to only the respective CPE. Similarly, multicast messages are also sent as unicast messages to the mobile nodes.

Virtual MAC Address

An Ethernet over GRE tunnel is configured with a virtual MAC address. When a packet enters the tunnel, the tunnel accepts the packet only if the destination MAC address of the packet matches the virtual MAC address of the tunnel or the broadcast MAC address. Otherwise, the packet is dropped.

Note If the tunnel interface is configured to handle multicast traffic for specific multicast groups, the corresponding MAC addresses are also accepted by the tunnel.

If PMIPv6 or GTP is enabled on the tunnel, the protocols provide a virtual MAC address that is used as the source MAC address of packets exiting the tunnel. If PMIPv6 or GTP is not enabled, the virtual MAC address of the tunnel interface is used as the source MAC address of the exiting packets.

Virtual MAC addresses are associated with the tunnel using the **mac-address** command. You can use the **show tunnel mac-table** command to see MAC table entries. You can use the **test tunnel mac-address** command to test the addition of MAC addresses to the MAC table of a tunnel interface.

VLAN on the Tunnel Interface

Mobile nodes connect to the wireless access points (APs). These APs have Service Set Identifiers (SSIDs) provided by the service provider. The SSID of a CPE is the VLAN identifier. The CPE can be configured to insert VLAN tags in Ethernet frames received from the mobile nodes before forwarding them on the GRE tunnel. Similarly, for downstream traffic, the GRE tunnel can be configured to insert a VLAN tag in all Ethernet frames sent to the MN.

A tunnel interface supports only one VLAN tag.

You can associate a VLAN with an Ethernet over GRE tunnel by using the **tunnel vlan** command.

How to Configure an Ethernet over GRE tunnel

Configuring an Ethernet over GRE Tunnel

SUMMARY STEPS

1. **interface tunnel** *tunnel-number*
2. **mac-address** *mac-address*
3. Do one of the following:
   - **ip address dhcp**
   - **ip address** *ip-address mask*
4. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
5. **tunnel mode ethernet gre** {**ipv4 | ipv6**}
6. **tunnel key** *key*
7. **tunnel vlan** *vlan-id*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface tunnel** *tunnel-number* **Example:** `Device(config)# interface tunnel 1`	Configures a tunnel interface and enters interface configuration mode.
Step 2	**mac-address** *mac-address* **Example:** `Device(config-if)# mac-address 0000.0000.0001`	(Optional) Specifies a MAC address for the tunnel.

Step 3	Do one of the following:
	• **ip address dhcp**
	• **ip address** *ip-address mask*
	Example:
	`Device(config-if)# ip address 192.168.4.3 255.255.255.0`
	Example:
	`Device(config-if)# ip address dhcp`
		• Specifies that the IP address of the mobile node is allocated by DHCP when it connects to the network.
		• Specifies the IPv4 address of the mobile node.

Step 4	**tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} **Example:** `Device(config-if)# tunnel source loopback 2`	Sets the source address of a tunnel interface.

	Command or Action	Purpose
Step 5	**tunnel mode ethernet gre** {**ipv4** | **ipv6**} **Example:** `Device(config-if)# tunnel mode ethernet gre ipv4`	Sets the encapsulation mode of the tunnel to Ethernet over GRE IPv4 or GRE IPv6.
Step 6	**tunnel key** *key* **Example:** `Device(config-if)# tunnel key 1`	Enables an key identifier for the tunnel interface.
Step 7	**tunnel vlan** *vlan-id* **Example:** `Device(config-if)# tunnel vlan 1`	Associates a VLAN identifier with the Ethernet over GRE tunnel.
Step 8	**end** **Example:** `end`	Exits to privileged EXEC mode.

What to do next

Verify the tunnel.

Verifying Ethernet Over GRE Tunnel

Before you begin

Configure the Ethernet over GRE tunnel.

SUMMARY STEPS

1. **show interface tunnel**
2. **show tunnel mac-table**
3. **show tunnel endpoints**

DETAILED STEPS

Step 1 **show interface tunnel**

This command displays information about the tunnel.

Example:

```
Device# show interface tunnel 1

Tunnel1 is up, line protocol is up
Hardware is Tunnel
Internet address is 11.1.1.1/24
MTU 17846 bytes, BW 100 Kbit/sec, DLY 50000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
```

```
Tunnel source 10.0.0.1
Tunnel MAC address 0000.5e00.5213
Tunnel Vlan-id 1
Tunnel protocol/transport Ethernet-GRE/IP Key 0x1, sequencing disabled Checksumming of packets disabled
Tunnel TTL 255
Tunnel transport MTU 1454 bytes
Tunnel transmit bandwidth 8000 (kbps) Tunnel receive bandwidth 8000 (kbps)
Last input 00:48:08, output never, output hang never
Last clearing of "show interface" counters 00:48:26
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 107
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1867 packets input, 161070 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
43 packets output, 4386 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out ind-uut#
--- 22:03:51 ---
44: 2013-01-30T22:03:51: %SCRIPT-6-INFO: {_haExecCmd: Executing cmd exec with ind-uut-a}


Device# show interface tunnel 2

Tunnel2 is up, line protocol is up
Hardware is Tunnel
Internet address is 10.1.1.1/24
MTU 1434 bytes, BW 100 Kbit/sec, DLY 50000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation TUNNEL, loopback not set
Keepalive not set
Tunnel source 10::1
Tunnel MAC address 0000.5e00.5213
Tunnel Vlan-id 2
Tunnel protocol/transport Ethernet-GRE/IPv6
Key 0x2, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255
Path MTU Discovery, ager 10 mins, min MTU 1280
Tunnel transport MTU 1434 bytes
Tunnel transmit bandwidth 8000 (kbps) Tunnel receive bandwidth 8000 (kbps)
Last input never, output never, output hang never
Last clearing of "show interface" counters 00:48:28
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 106
Queueing strategy: fifo
Output queue: 0/0 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
```

Step 2 **show tunnel mac-table**

This command displays MAC table entries associated with a tunnel.

Example:

```
Device# show tunnel mac-table tunnel0

CPE IP 1.1.1.1 Refcount 2 Base 0x2A98DD0000
    mac-address 0122.0111.0111 vlan 1
    mac-address 0011.1111.0001 vlan 2
CPE IP 3.3.3.3 Refcount 2 Base 0x12345678
   mac-address 1234.5678.9011 vlan 1
```

Step 3 **show tunnel endpoints**

This command displays tunnel endpoints and verifies if the tunnel has been created correctly.

Example:

```
Device# show tunnel endpoints

Tunnel0 running in Ethernet-GRE/IP mode

Endpoint transport 10.1.1.1 Refcount 3 Base 0x2A98DD03C0 Create Time 3d02h
   overlay 10.1.1.1 Refcount 2 Parent 0x2A98DD03C0 Create Time 3d02h
 Endpoint transport 3.3.3.3 Refcount 3 Base 0x2A98DD0300 Create Time 3d02h
   overlay 10.1.1.3 Refcount 2 Parent 0x2A98DD0300 Create Time 3d02h
```

Configuration Examples for Ethernet over GRE Tunnels

Example: Configuring Ethernet over GRE Tunnels

Configuring Ethernet over GRE tunnels on the Mobile Node

```
! Configure the topology
mobile-node1(config-if)# interface GigabitEthernet0/1
mobile-node1(config-if)# ip address 10.21.1.1 255.255.255.0
mobile-node1(config-if)# no shut
mobile-node1(config-if)# exit
mobile-node1(config)# ip route 10.0.0.1 255.255.255.255 10.21.1.2

! Configuring the interface used as the source of the tunnel
mobile-node1(config)# interface Loopback0
mobile-node1(config-if)# ip address 10.40.0.1 255.255.255.0
mobile-node1(config-if)# ipv6 address 2001:db8:2:40::1/64
mobile-node1(config-if)# no shutdown

! Configuring the Ethernet over GRE IPv4 Tunnel
mobile-node1(config-if)# interface Tunnel1
mobile-node1(config-if)# mac-address 0000.0000.0001
mobile-node1(config-if)# ip dhcp client client-id ascii MN1@cisco.com
mobile-node1(config-if)# ip address dhcp
mobile-node1(config-if)# no ip redirects
mobile-node1(config-if)# no ip route-cache
mobile-node1(config-if)# tunnel source Loopback0
mobile-node1(config-if)# tunnel mode ethernet gre ipv4
mobile-node1(config-if)# tunnel key 1
mobile-node1(config-if)# tunnel vlan 1
```

```
mobile-node1(config-if)# no shutdown
```

Configuring Ethernet over GRE tunnel on the MAG

```
! Configure the topology
MAG(config)# interface FastEthernet1/1/5
MAG(config-if)# ip address 10.21.1.2 255.255.255.0
MAG(config-if)# ipv6 address 2001:db8:2:21::2/64
MAG(config-if)# no shut
MAG(config)# ip route 10.40.0.1 255.255.255.255 10.21.1.1

! Configure the interface used as source of the tunnel
MAG(config-if)# interface Loopback0
MAG(config-if)# ip address 10.0.0.1 255.255.255.0
MAG(config-if)# no shutdown

! Configuring the Ethernet over GRE IPv4 Tunnel
MAG(config)# interface Tunnel1
MAG(config-if)# ip address 10.11.1.1 255.255.255.0
MAG(config-if)# tunnel mode ethernet gre ipv4
MAG(config-if)# tunnel source 10.0.0.1

! Configuring a static GRE and VLAN ID for the tunnel
MAG(config-if)# tunnel key 1
MAG(config-if)# tunnel vlan 1

! Associating the service policy control with the tunnel
MAG(config-if)# service-policy type control DHCP1

! Enable ISG on the tunnel
MAG(config-if)# ip subscriber l2-connected
MAG(config-subscriber)# initiator unclassified mac-address
Please unconfigure existing command before configuring.
MAG(config-subscriber)# initiator dhcp class-aware
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*Cisco IOS IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

Standards and RFCs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Ethernet over GRE Tunnels

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Ethernet over GRE Tunnels

Feature Name	Releases	Feature Information
Ethernet over GRE Tunnels	Cisco IOS XE Release 3.9S	The Ethernet over GRE tunnels feature allows customers to leverage existing low–end residential gateways to provide mobility services to mobile nodes using Proxy Mobile IPv6 (PMIPv6), GPRS Tunneling Protocol (GTP) and Intelligent Service Gateway (ISG). The following command was modified to add the Ethernet over GRE tunnel mode for IPv4 and IPv6: **tunnel mode ethernet gre**. The following commands were introduced:**tunnel vlan**, **show tunnel mac-table**, **show tunnel source tracking**, **test tunnel mac-address**.