IPv4 Unicast Generic Routing Encapsulation Tunnel Overview

IPv4 unicast Generic Routing Encapsulation Tunnel (GRE) tunneling protocol provides a simple generic approach to transport packets of one protocol over another protocol by means of encapsulation. The term GRE tunnels in this document implies only unicast IPv4 GRE tunnel that supports IPv4 payload.

GRE encapsulates a payload, that is, an inner packet that needs to be delivered to a destination network inside an outer IP packet. GRE tunnel endpoints send payloads through GRE tunnels by routing encapsulated packets through intervening IP networks. Other IP routers along the way do not parse the payload (the inner packet); they only parse the outer IP packet as they forward it towards the GRE tunnel endpoint. Upon reaching the tunnel endpoint, GRE encapsulation is removed and the payload is forwarded to it's ultimate destination.

Prior to Cisco IOS XE Gibraltar Release 16.12.x, GRE tunnels could provide a speed of 520 kbps for unidirectional and 250 kbps for bidirectional traffic. Starting with Cisco IOS XE Gibraltar Release 16.12.x, GRE tunnels enable the traffic to pass at a speed according to the size of the interface.

The IPv4 unicast GRE tunnels work on the following conditions:

• The unicast GRE tunnels work only with IPv4 as the transport protocol.

• The payload protocol is of type IPv4.

• SDM templates are supported only by the Metro Aggregation Services license. The license to use should be either **advancedmetroipaccess** or **metroaggrservices**.

IPv4 unicast GRE tunnels provide support to transport multiple protocols and packet types over the core network. More importantly, GRE tunnels can be used to form VPN networks by encapsulating the private addressing packets as payload with the tunnel header to transport the packet to the remote end. In the remote end, the packet is decapsulated and then routed based on private routing table. GRE tunnels can also carry multiple packet types such as unicast and multicast.

The tunnel comprises of the following three components:

1. Payload packet or the passenger protocol

2. GRE header or the carrier protocol

3. Delivery header or the transport protocol

Figure 1: Packet Format in GRE Network

The following image shows a typical topology using GRE tunnel where IPv4 acts as both the transport protocol and the payload protocol.

Figure 2: Typical Unicast IPv4 GRE Topology
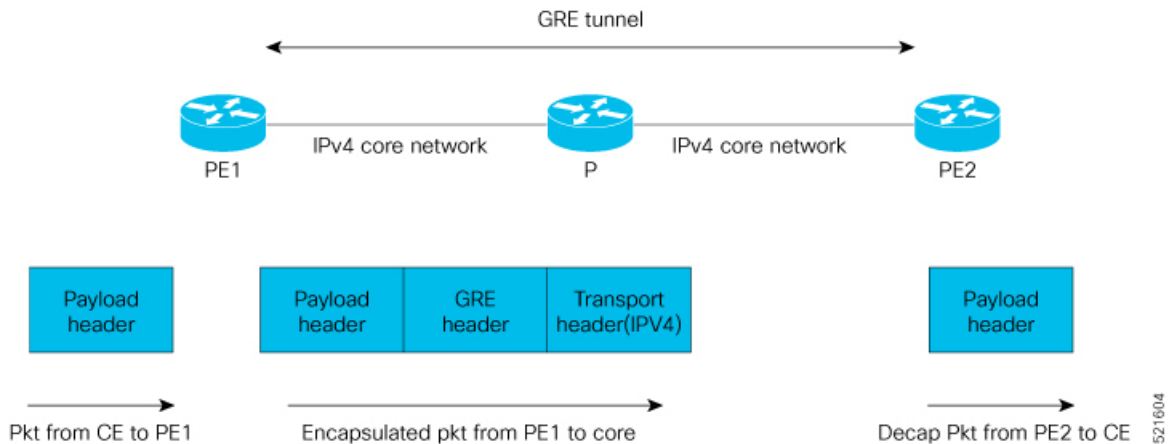
Restrictions

- Tunnel destination under VRF and command **tunnel vrf** is *not* supported. Tunnel destination prefix must be in global routing table for IPV4 unicast GRE to be functional.

- Convergence lesser than 50 msec is not guaranteed.

- Maximum supported GRE scale is 510.

- Tunnel key is *not* supported. Hence, you must configure unique pair of source or destination IP address per tunnel.

- ACL and QoS are *not* supported over GRE tunnel.

- Time To Live (TTL) and Type of Service (TOS) are supported in Pipe mode.

- Tunnel Interface Statistics is *not* supported.

- Maximum Transmission Unit (MTU) is *not* supported for GRE tunnel and hence path MTU is also *not* supported.

- Recursive routing is *not* supported as control plane support is not available.

- Netflow and Policy-Based Routing (PBR) are *not* supported over the GRE tunnel.

- GRE over Virtual Private LAN Services (VPLS) or PW is *not* supported.

- GRE with indirection LB, Prefix Independent Convergence (PIC) core or PIC Edge, is *not* supported.

- GRE over Traffic Engineering (TE) tunnel core (mid-chain pointing to mid-chain support) is *not* supported.

- Equal-Cost Multi-Path Routing (ECMP) or load balancing between GRE tunnels is *not* supported. But, when you can configure LB paths for a single GRE tunnel, the tunnel uses only one of the paths.

- Bidirectional Forwarding Detection (BFD) over IPv4 unicast tunnel is *not* supported.

- MPLS over GRE tunnel and GRE over MPLS are *not* supported.

- GRE over MPLS core is supported provided **explicit null** command is disabled on the tunnel end routers.

How to Configure IPv4 GRE Tunnel

- Each IP address should be learned in global routing table.

- The IPv4 GRE tunnel can be established using any routing protocols enabled between Provider Edge 1 (PE1) router and PE2 router.

- Tunnel number should be identical in both the nodes.

Configure IPv4 Unicast Generic Routing Encapsulation Tunnel

Before You Begin

Bring up any routing process between two PEs.

Configure IPv4 GRE tunnel with a destination IP address:

```
interface Tunnel10
   ip address 10.1.1.1 255.255.255.255
   tunnel source 16.1.1.1
   tunnel destination 17.1.1.1
  end
```

Bring Up IGP over GRE Tunnel :

```
router ospf 100
   router-id 1.1.1.51
   nsr
   nsf ietf

  interface Tunnel10
  ip ospf network point-to-point
  ip ospf 100 area 100
end
```

Verification of IPv4 Unicast Generic Routing Encapsulation Tunnel Configuration

Use **show interface tunnel**10 command to verify IPv4 unicast GRE tunnel configuration.

```
Router#show interface Tunnel10
   Tunnel10 is up, line protocol is up
     Hardware is Tunnel
     Internet address is 10.1.1.1/32
     MTU 17916 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 linestate evaluation up
     Tunnel source 16.1.1.1, destination 17.1.1.1
     Tunnel protocol/transport GRE/IP
       Key disabled, sequencing disabled
       Checksumming of packets disabled
     Tunnel TTL 255, Fast tunneling enabled
     Tunnel transport MTU 9178 bytes
     Tunnel transmit bandwidth 8000 (kbps)
     Tunnel receive bandwidth 8000 (kbps)
     Last input 00:00:00, output 00:00:01, output hang never
     Last clearing of "show interface" counters 3d08h
     Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
     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
        41447 packets input, 4841002 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
        44429 packets output, 5043980 bytes, 0 underruns
        Output 0 broadcasts (0 IP multicasts)
        0 output errors, 0 collisions, 0 interface resets
        0 unknown protocol drops
        0 output buffer failures, 0 output buffers swapped out
```

Establish GRE Tunnel over VRF Routes

Table 1: Feature History

Feature Name	Release Information	Description
Establish GRE Tunnel over VRF Routes	Cisco IOS XE Bengaluru 17.6.1	This feature establishes GRE tunnels over Virtual Route Forward (VRF) routes.

Starting with Cisco IOS XE Bengaluru Release 17.6.1, you can establish GRE tunnels over Virtual Route Forward (VRF) routes or IPv4 and VPNv4 routes.

Limitations

- VRF GRE tunnel is supported only with **max-ipv4-tunnel** SDM template.

- From Cisco IOS XE 17.16.x, GRE tunnel is supported only with **max-ipv4-tunnel** SDM template. This is the maximum line rate the router can achieve under optimal conditions.

- Per-vrf label allocation mode is mandatory to operate VRF GRE tunnels for a particular VRF.

- Once you configure a VRF GRE tunnel for a VRF, only tunnel traffic works for that particular VRF. L3VPN traffic from core may get dropped at PE node if the packets are ingressed via non-tunnel interface.

- The source and destination addresses of the VRF GRE tunnel must *only* be present in the VRF routing table.

- Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) cannot be established over VRF GRE tunnels. Use static routes to route traffic over the tunnel.

- VRF GRE tunnels cannot process fragmented IP packets.

- VRF GRE supports a maximum of 256 tunnels.

- You cannot establish OSPF, ISIS over VRF GRE tunnels.

Configure GRE Tunnel over VRF Routes

VRF Configuration:

To configure VRF:

```
ip vrf vpn1
rd 100:1
route-target export 100:1
route-target import 100:1
```

GRE Tunnel over VRF Routes Configuration:

To configure GRE tunnel over VRF routes at PE1:

```
interface Loopback1
ip vrf forwarding vpn1
ip address 22.22.22.22 255.255.255.255


interface Tunnel1
ip vrf forwarding vpn1
ip address 192.168.1.1 255.255.255.0
tunnel source Loopback1
tunnel destination 33.33.33.33
tunnel vrf vpn1
```

To configure GRE tunnel over VRF routes at PE2:

```
interface Loopback1
ip vrf forwarding vpn1
ip address 33.33.33.33 255.255.255.255

interface Tunnel1
ip vrf forwarding vpn1
ip address 192.168.1.2 255.255.255.0
tunnel source Loopback1
tunnel destination 22.22.22.22
tunnel vrf vpn1
```