GRE Tunneling Feature Guide

Cisco Services

GRE Tunneling Feature Guide

TABLE OF CONTENTS

Contents

Introduction | Plan | Configure | Monitor | Troubleshoot | Resources | Contents

Introduction

Generic Route Encapsulation (GRE) is a protocol used for the encapsulation of a network layer protocol inside another network layer protocol. This form of encapsulation is often referred to as tunneling. GRE is primarily intended to allow devices running a given network layer protocol to communicate over a network running a different network layer protocol.

A network receives a native packet from its logical *attachment circuit* and encapsulates the native packet into another network protocol and sends the encapsulated packet towards its de-encapsulation point. The encapsulation point is called tunnel entry and the decapsulation point is called tunnel exit. Tunnels are typically point-to-point dedicated virtual links to transport packets from one endpoint to another.

Key Benefits

The following are several situations in which encapsulating traffic in another network layer protocol is beneficial:

- To provide multiprotocol local networks over a single-protocol backbone.
- To provide communication path for networks containing protocols that have limited hop counts. If the path between two computers has more than 15 hops, the computers cannot communicate with each other. However, it is possible to hide some of the hops inside the network using a tunnel.
- To connect distant subnetworks.
- To allow virtual private networks across WANs.

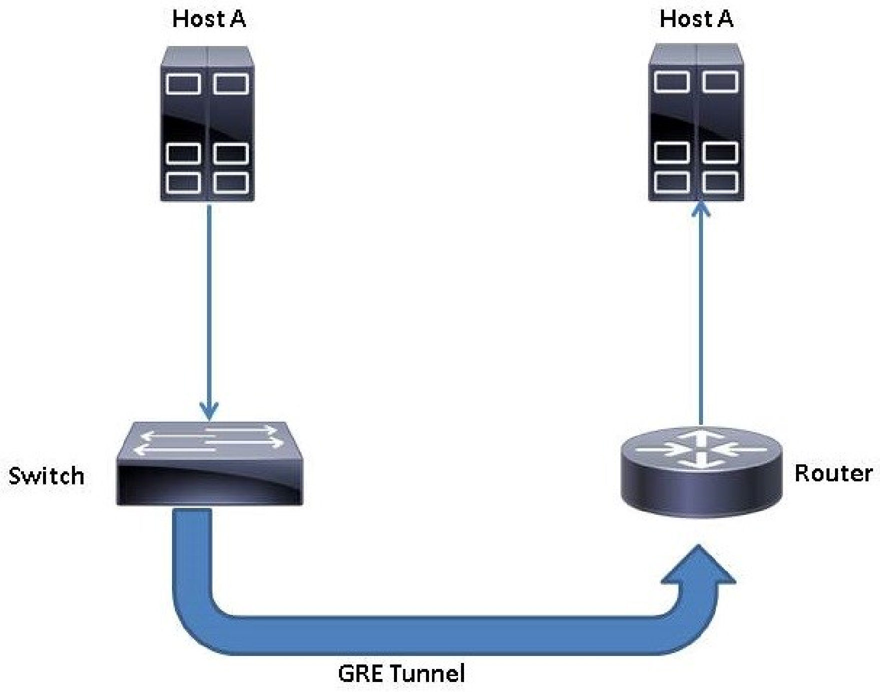
A tunneled packet logically consists of:

- Payload Data—Specifies the data that is being tunneled.
- Encapsulation Header—Provides additional control information about the payload being carried, or about the forwarding behavior to be applied to the tunneled packet on decapsulation, or both.
- Delivery or Transport Header—Indicates how the encapsulated payload data is transported or delivered to the other end of the tunnel.

Planning for Deployment

Existing and Supported Topology

Figure 1 displays the GRE Tunneling topology



Guidelines and Limitations for Configuring GRE Tunneling

The following are some of the limitations pertaining to GRE tunneling on Cisco IOS XE Release Denali 16.3.1:

- Hardware-switching of the packets occurs when GRE is configured without any tunneling options such as checksum and sequence number.
- Support is available only for encapsulation; support for encryption is not available.
- Support for this feature on Cisco Catalyst 3650 and Cisco Catalyst 3850 Series switches is available with IP Base and IP Services licenses.
- Support is available only for IPv4 tunnels; IPv6 tunneling is not supported.
- Vulnerable to fragmented packet attacks.
- Support for GRE services that are defined in header fields, such as those used to specify checksums, keys, or sequencing is not available. If any packet that is received that specifies the use of these services will be dropped.
- Support is available for Virtual Routing and Forwarding-aware tunnels. However the **tunnel vrf** *<vrf_name>* command is not supported. This also means that tunnel source and egress interface of GRE packets are in global VRF.
- Support is available for Static, Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) routing protocols over GRE interface.
- Support is available for **gre ip** tunnel mode. The tunnel source can

be loopback and Layer 3 (physical or Etherchannel) interfaces only.

- Support is available for up to 10 tunnels.
- Support is available for GRE tunnel keepalive.
- Support is available for IPv4 Multicast over Point-to-Point Generic Routing Encapsulation (GRE) Tunnels.
- Support is not available for the following features in IOS XE 16.3
  - Multipoint GRE
  - Tunnel counters
  - Crypto support
  - Access Control Lists (ACL) and Quality of Service (QoS)
  - Fragmentation
  - Cisco Discovery Protocol (CDP)
  - Internet Protocol Security (IPsec)
  - Storm Control, Port Security, and Netflow features on GRE Tunnel interface

Configuring GRE Tunneling

Beginning in privileged EXEC mode, perform the following steps:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface tunnel** *number*	Enters tunnel interface configuration mode.
Step 3	**ip address ip_address** *subnet_mask*	Configures IP address and IP subnet.
Step 4	**tunnel source** {*ip-address* | *interface-name*}	Configures the source address for the IP tunnel.
Step 5	**tunnel destination** {*ip-address* | *host-name*}	Configures the destination address for the IP tunnel.
Step 6	**end**	Exits configuration mode.
Step 7	**copy running-config startup config**	Saves your configuration changes to NVRAM.
Step 8	**show running-config interface tunnel**	Verifies the configuration.

Configuration Example for Configuring a GRE Tunnel

The following example shows how to configure a logical Layer 3 GRE tunnel interface tunnel 2 in a global or non-VRF environment.
Note: In the example configuration, the 10.10.10.1 network is in global VRF.

```
Switch> enable
Switch# config terminal
Switch(config)# interface tunnel 2
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# tunnel source 10.10.10.1
Switch(config-if)# tunnel destination 10.10.10.2
Switch(config-if)# end
```

The following example shows how to configure a logical Layer 3 GRE tunnel interface tunnel 2 in VRF environment. This example uses the **vrf definition** <*vrf_name*> and **vrf forwarding** <*vrf_name*> commands to create and apply VRF.

```
Switch(config)# vrf definition RED
Switch(config-vrf)#  address-family ipv4
Switch(config-vrf-af)# exit-address-family
Switch(config-vrf)#  exit
Switch(config)# interface tunnel 2
Switch(config)# vrf forwarding RED
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)# tunnel source 10.10.10.1
Switch(config-if)# tunnel destination 10.10.10.2
Switch(config-if)# end
```

Monitoring

Viewing Tunnel Interface Status

To view the status of a tunnel interface, use the **show interface tunnel** command in privileged EXEC mode.
show interface tunnel *number*

Syntax Description

number	Number of the tunnel interface that you want to display the information for. The range is from 0 to 2147483647.

Examples

```
switch# show interface tunnel 10
Tunnel10 is up, line protocol is up
Hardware is Tunnel
Internet address is 201.1.1.2/24
MTU 17900 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 200.1.1.2, destination 200.1.1.1
Tunnel protocol/transport GRE/IP
Key disabled, sequencing disabled
Checksumming of packets disabled
Tunnel TTL 255, Fast tunneling enabled
Tunnel transport MTU 1476 bytes
Tunnel transmit bandwidth 8000 (kbps)
Tunnel receive bandwidth 8000 (kbps)
Last input 00:00:00, output 00:00:02, output hang never
Last clearing of "show interface" counters 2d17h
Input  queue:  0/75/0/0  (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
50908 packets input, 3771192 bytes
```

Troubleshooting GRE Tunnels

This section explains how to troubleshoot issues pertaining to GRE tunnel. Common GRE issues include the following:

- GRE source IP address not reachable by remote host
- GRE destination IP address not reachable by local host
- Recursive routing

Using Show and Debug Commands

debug tunnel

Enables you to get tunnel debugging information and events related to a tunnel.

debug tunnel packet

Enables you to get tunnel packet debugging information and events related to tunnel packets.

show interface tunnel number

Enables you to view the interface status, tunnel IP address, tunnel mode, tunnel source and destination.

.

Resources and Support Information

Obtaining Documentation, Obtaining Support, and Security Guidelines
For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service.

TOMORROW
starts here.

11/15