GRE

Generic Routing Encapsulation (GRE) is a protocol designed for performing encapsulation of one network layer protocol (for example, IP or IPX) over another network layer protocol (for example, IP). GRE uses the tunneling technology and serves as a Layer 3 tunneling protocol of virtual private network (VPN).

A tunnel is a virtual point-to-point connection for transferring encapsulated packets. Packets are encapsulated at one end of the tunnel and decapsulated at the other end.

Operation of GRE

A packet transferred through a tunnel undergoes an encapsulation process and a decapsulation process. Figure 1 depicts the network used to illustrate these two processes.

Figure 1 IPX networks interconnected through the GRE tunnel

I. Encapsulation process

1) After receiving an IPX packet through the interface connected to IPX network Group 1, Router A submits it to the IPX module for processing.
2) The IPX module checks the destination address field in the IPX header to determine how to route the packet.
3) If the packet must be tunneled to reach its destination, Router A sends it to the tunnel interface.
4) Upon receipt of the packet, the tunnel interface encapsulates it in a GRE packet and submits to the IP module.
5) The IP module encapsulates the packet in an IP packet, and then forwards the IP packet out through the corresponding network interface based on its destination address and the routing table.

II. Format of an encapsulated packet

Figure 2 shows the format of an encapsulated packet.

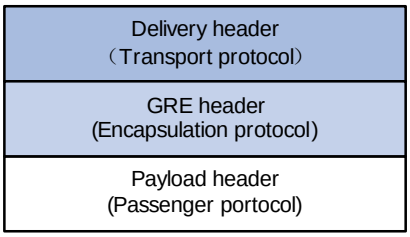

Figure 2 Format of an encapsulated packet

As an example, Figure 3 shows the format of an IPX packet encapsulated for transmission over an IP tunnel.

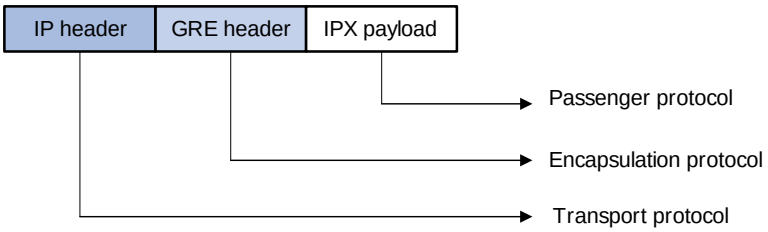

Figure 3 Format of an IPX packet encapsulated for transmission over an IP tunnel

These are the involved terms:

- Payload: Packet that needs to be encapsulated and routed.
- Passenger protocol: Protocol that the payload packet uses, IPX in the example.
- Encapsulation or carrier protocol: Protocol used to encapsulate the payload packet, that is, GRE.
- Delivery or transport protocol: Protocol used to encapsulate the GRE packet and to forward the resulting packet to the other end of the tunnel, IP in this example.

Depending on the transport protocol, two tunnel modes are present: GRE over IPv4 and GRE over IPv6.

III. Decapsulation process

Decapsulation is the reverse process of encapsulation:

1) Upon receiving an IP packet from the tunnel interface, Router B checks the destination address.
2) If the destination is itself, Router B strips off the IP header of the packet and submits the resulting packet to the GRE module.
3) The GRE module checks the key, checksum and sequence number, and then strips off the GRE header and submits the payload to the IPX module.
4) The IPX module performs the subsequent forwarding processing for the packet.

Note:

Encapsulation and decapsulation processes on both ends of the GRE tunnel and the resulting increase in data volumes will degrade the forwarding efficiency for the GRE-enabled device to some extent.

GRE Security Options

For the purpose of tunnel security, GRE provides two options: tunnel interface key and end-to-end checksum.

According to RFC 1701,

- If the Key Present field of a GRE packet header is set to 1, the Key field will carry the key for the receiver to authenticate the source of the packet. This key must be the same at both ends of a tunnel. Otherwise, packets delivered over the tunnel will be discarded.
- If the Checksum Present bit of a GRE packet header is set to 1, the Checksum field contains valid information. The sender calculates the checksum for the GRE header and the payload and sends the packet containing the checksum to the peer. The receiver calculates the checksum for the received packet and compares it with that carried in the packet. If the checksums are the same, the receiver considers the packet intact and continues to process the packet. Otherwise, the receiver discards the packet.

Note:

Due to the GRE encapsulation/decapsulation process respectively executed on both ends of the tunnels and the resulting increase in data volume, the forwarding efficiency of routers using GRE is degraded to some extent.

GRE Applications

GRE supports these types of applications:

- Multi-protocol communications through a single-protocol backbone
- Scope enlargement of the network running a hop-limited protocol
- VPN creation by connecting discontinuous subnets
- GRE-IPSec tunnel application

I. Multi-protocol communications through a single-protocol backbone

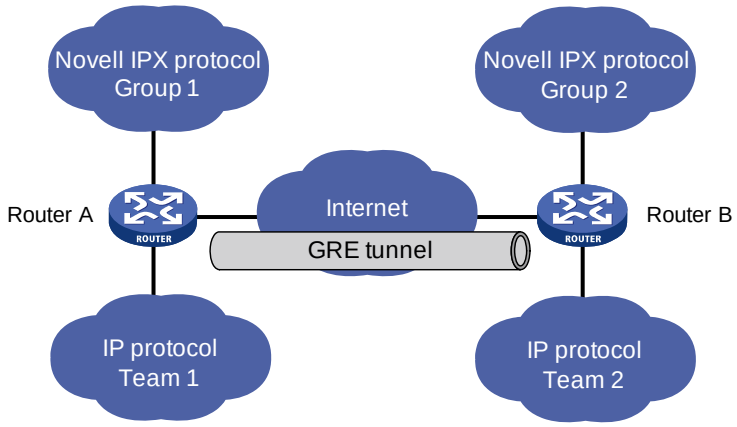

Figure 4 Multi-protocol communications through a single-protocol backbone

In the example as shown in Figure 4, Group 1 and Group 2 are local networks running Novell IPX, while Team 1 and Team 2 are local networks running IP. Through the GRE tunnel between Router A and Router B, Group 1 can communicate with Group 2 and Team 1 can communicate with Team 2. They will not interfere with each other.

II. Scope enlargement of the network running a hop-limited protocol

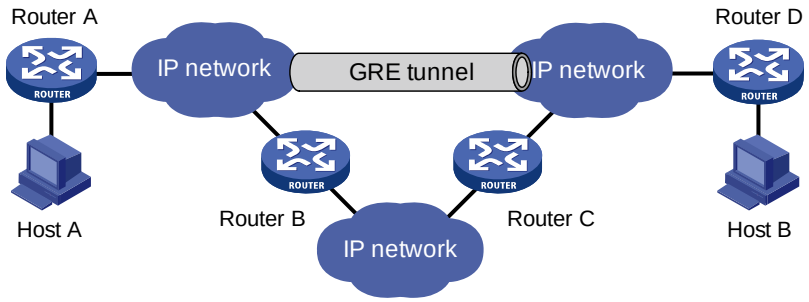

Figure 5 Scope enlargement of the network

When the hop count between two terminals exceeds 15, the terminals cannot communicate with each other. Using GRE, you can hide some hops so as to enlarge the scope of the network.

III. VPN creation by connecting discontinuous subnets

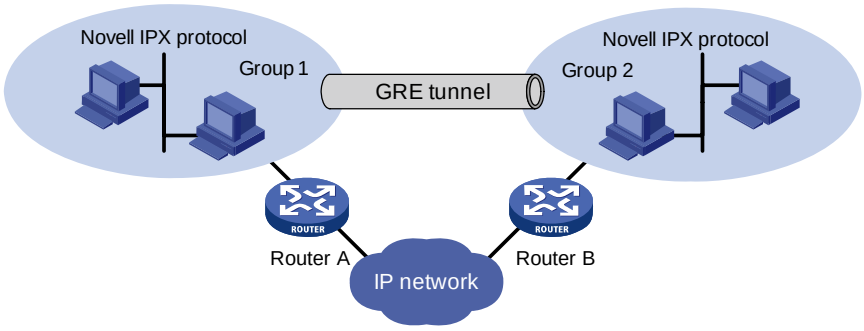

Figure 6 Connect discontinuous subnets with a tunnel to form a VPN

In the example as shown in Figure 6, Group 1 and Group 2 running Novell IPX are deployed in different cities. They can constitute a trans-WAN virtual private network (VPN) through the tunnel.

IV. GRE-IPSec tunnel application

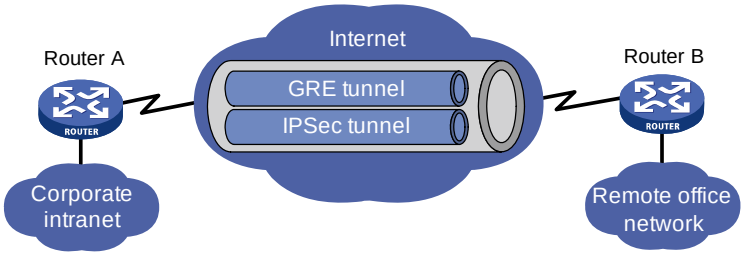

Figure 7 GRE-IPSec tunnel application

Working with IPSec, GRE allows data packets like routing protocol, voice, and video packets to be first encapsulated by GRE and then encrypted by IPSec.

Note:

IPSec support of GRE varies with devices.
