



Networkforyou

Subscribe to our
You Tube Channel



Networkforyou



**Welcome
To
Network for you
GRE**



Networkforyou

Email us:
networkforyou4@gmail.com

1 of 4

WhatsApp Us : +918143809578



Generic Routing Encapsulation:

- GRE stand for the **Generic Routing Encapsulation**.
- Generic Routing Encapsulation (GRE) is a **tunneling protocol developed by Cisco Systems** that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links or point-to-multipoint links over an Internet Protocol network.
- **GRE is the mechanism that encapsulate one protocol in another protocol.**
- **Tunneling is a concept where we put 'packets into packets' so that they can be transported over certain networks. We also call this encapsulation.**
- Tunneling is used to hide the packet and transported over certain networks. In GRE basically, tunneling is a concept where to put packets into packets.
- GRE tunnels are used to create point-to-point connections between two networks.
- Generic Routing Encapsulation is a method to **tunnel IP packets between two end points.**
- Generic Routing Encapsulation supports **encapsulating IPv4 broadcast & multicast traffic.**
- GRE does **not encrypt packets**; it can be used along with **IPsec to encrypt the packets.**

GRE Configuration Steps:

Step 1:

Create tunnel interfaces on R1 and R2 using the interface tunnel number command.

Step 2:

Choose a subnet to be used on tunnel interfaces and assign an IP address from the subnet to both end points.

Step 3:

Configure the source IP address of the tunnel interface using the tunnel source interface or the tunnel source ip-address command. The source interface or IP address must be the one that connects the router to the public part of the network.

Step 4:

Configure the destination IP address of the tunnel interface using the tunnel destination ip-address command. The destination IP address must be the remote one that connects the router to the public part of the network.

Step 5:

Configure the routers to use the tunnel interfaces to reach remote subnets. Use either static routing or a dynamic routing protocol to enable on tunnel interfaces to achieve that.

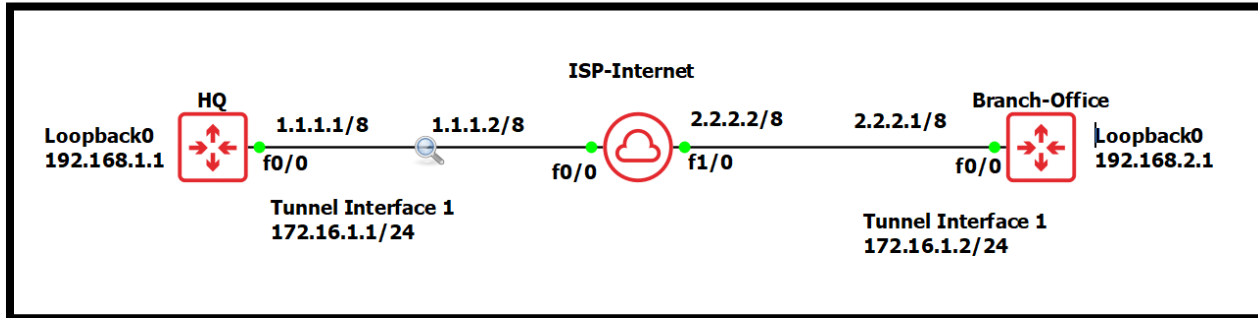
Email us:
networkforyou4@gmail.com

2 of 4

WhatsApp Us : **+918143809578**



Let do Lab for GRE:



!HQ Basic Configuration:	!Branch-Office Basic Configuration:
<pre>en config t hostname HQ interface FastEthernet0/0 ip address 1.1.1.1 255.0.0.0 no shutdown ! interface Loopback0 ip address 192.168.1.1 255.255.255.0</pre>	<pre>en config t hostname BO interface FastEthernet0/0 ip address 2.2.2.1 255.0.0.0 no shutdown ! interface Loopback0 ip address 192.168.2.1 255.255.255.0</pre>
!HQ GRE Configuration:	!BO GRE Configuration:
<pre>config t interface Tunnel1 ip address 172.16.1.1 255.255.255.0 tunnel source 1.1.1.1 tunnel destination 2.2.2.1 ! ip route 0.0.0.0 0.0.0.0 1.1.1.2 router eigrp 1 no auto-summary network 192.168.1.0 network 172.16.1.0</pre>	<pre>config t interface Tunnel1 ip address 172.16.1.2 255.255.255.0 tunnel source 2.2.2.1 tunnel destination 1.1.1.1 ! ip route 0.0.0.0 0.0.0.0 2.2.2.2 router eigrp 1 no auto-summary network 192.168.2.0 network 172.16.2.0</pre>
!Internet(ISP Router)Basic Configuration:	Verification Commands
<pre>en config t hostname ISP interface FastEthernet0/0 ip address 1.1.1.2 255.0.0.0</pre>	<pre>HQ#traceroute 192.168.2.1 BO#traceroute 192.168.1.1 HQ#ping 192.168.2.1 source loopback 0 BO#ping 192.168.1.1 source loopback 0 HQ#show ip eigrp neighbors</pre>

Email us:
networkforyou4@gmail.com

3 of 4

WhatsApp Us : +918143809578



```
no shutdown
!  
interface FastEthernet1/0  
ip address 2.2.2.2 255.0.0.0  
no shutdown
```

```
BO#show ip eigrp neighbors
```

IPsec Over GRE:

!HQ Basic Configuration:	!Branch-Office Basic Configuration:
<pre>crypto isakmp policy 1 encr 3des hash md5 authentication pre-share group 2 lifetime 86400 exit crypto isakmp key cisco address 2.2.2.1 crypto ipsec transform-set TS esp-3des esp-md5- hmac mode transport exit crypto ipsec profile abc set security-association lifetime seconds 86400 set transform-set TS exit interface Tunnel 1 tunnel protection ipsec profile abc</pre>	<pre>crypto isakmp policy 1 encr 3des hash md5 authentication pre-share group 2 lifetime 86400 exit crypto isakmp key cisco address 1.1.1.1 crypto ipsec transform-set TS esp-3des esp-md5- hmac mode transport exit crypto ipsec profile abc set security-association lifetime seconds 86400 set transform-set TS exit interface Tunnel 1 tunnel protection ipsec profile abc</pre>

Email us:
networkforyou4@gmail.com

4 of 4

WhatsApp Us : +918143809578