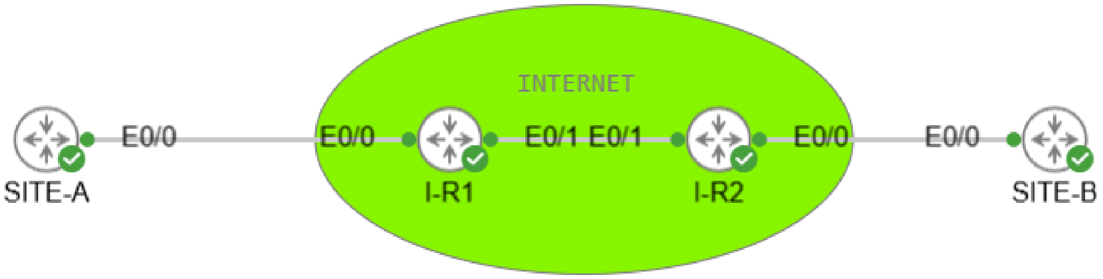
VPN TUNNEL

TOPOLOGY



INITIAL CONFIGURATION

-INTERNET-

I-R1

```
#int e0/0
#ip address 200.200.200.1 255.255.255.252
#no shutdown
#int e0/1
#ip address 200.200.200.5 255.255.255.252
#no shutdown
```

I-R2

```
#int e0/0
#ip address 200.200.200.9 255.255.255.252
#no shutdown
#int e0/1
#ip address 200.200.200.6 255.255.255.252
#no shutdown
```

-SITES-

SITE-A

```
#int e0/0
#ip address 200.200.200.2 255.255.255.252
#no shutdown
#int e0/3
#description SITE-A-Network
#ip address 10.10.10.1 255.255.255.0
#no shutdown
```

SITE-B

```
#int e0/0
#ip address 200.200.200.10  255.255.255.252
#no shutdown
#int e0/3
#description SITE-B-Network
#ip address 20.20.20.1 255.255.255.0
#no shutdown
```

TUNNEL CONFIGURATION

SITE-A

```
#interface tunnel 1
# ip mtu 1400
# ip tcp adjust-mss 1360
#ip address 192.168.1.1 255.255.255.252
#tunnel source 200.200.200.2
#tunnel destination 200.200.200.10
```

SITE-B

```
#interface tunnel 1
# ip mtu 1400
# ip tcp adjust-mss 1360
#ip address 192.168.1.2 255.255.255.252
#tunnel source 200.200.200.10
#tunnel destination 200.200.200.2
```

ROUTING CONFIGURATION

I-R1

```
#ip route 200.200.200.8 255.255.255.252 200.200.200.6
```

I-R2

```
#ip route 200.200.200.0 255.255.255.252 200.200.200.5
```

SITE-A

```
#ip route 0.0.0.0 0.0.0.0 200.200.200.2
```

SITE-B

```
#ip route 0.0.0.0 0.0.0.0 200.200.200.9
```

- With this configuration, SITE-A and SITE-B cannot ping each other from 10.10.10.1 and 20.20.20.1 vice versa.
- SITE-A and SITE-B can ping 200.200.200.10 and 200.200.200.2 respectively

TROUBLESHOOTING

- We are expecting a connection between the tunnels, when I ping 192.168.1.2 from SITE-A it failed and so is SITE-B to 192.168.1.1 even though their connection is up/up suggesting that the GRE tunnel is established.

Tunnel Updated Configuration

SITE-A

```
#interface tunnel 1
# ip mtu 1400
# ip tcp adjust-mss 1360
#ip address 172.16.1.1 255.255.255.252
#tunnel source 200.200.200.2
#tunnel destination 200.200.200.10
```

SITE-B

```
#interface tunnel 1
# ip mtu 1400
# ip tcp adjust-mss 1360
#ip address 172.16.1.2 255.255.255.252
#tunnel source 200.200.200.10
#tunnel destination 200.200.200.2
```

- With this adjustment SITE-A and SITE-B can ping both tunnel interfaces.
- Another problem is the ping to the Internal network of both side which is 10.10.10.0 and 20.20.20.0, still has no connection

UPDATED ROUTING CONFIGURATION

SITE-A

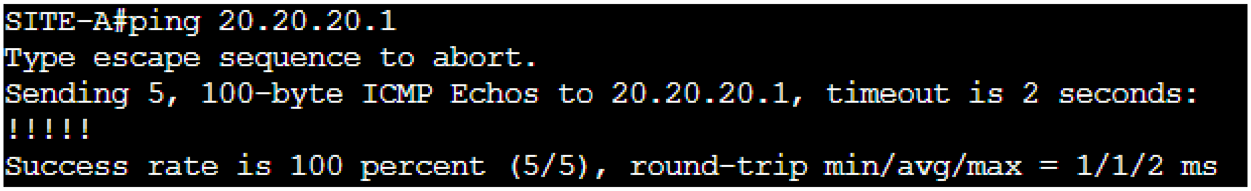
```
#ip route 0.0.0.0 0.0.0.0 200.200.200.2
#ip route 20.20.20.0 255.255.255.0 tunnel 1
```

SITE-B

```
#ip route 0.0.0.0 0.0.0.0 200.200.200.9
#ip route 10.10.10.0 255.255.255.0 tunnel 1
```

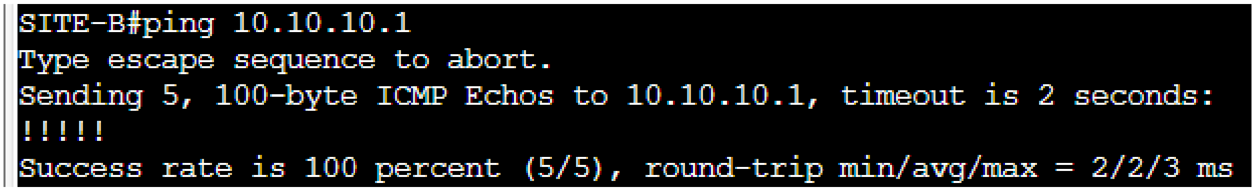
- With this configuration the they can both ping the internal network

SITE-A



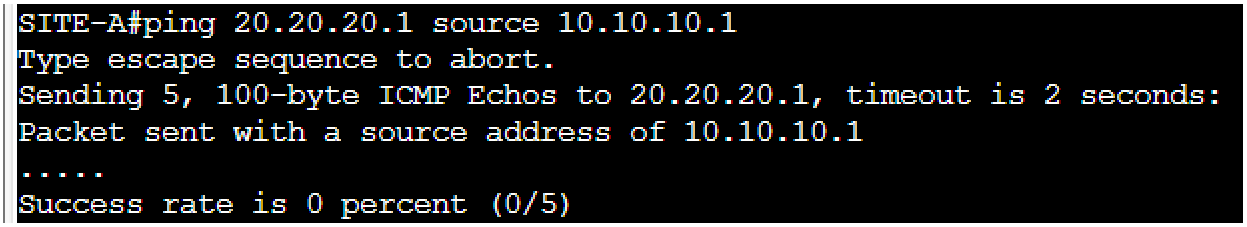
```
SITE-A#ping 20.20.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

SITE-B



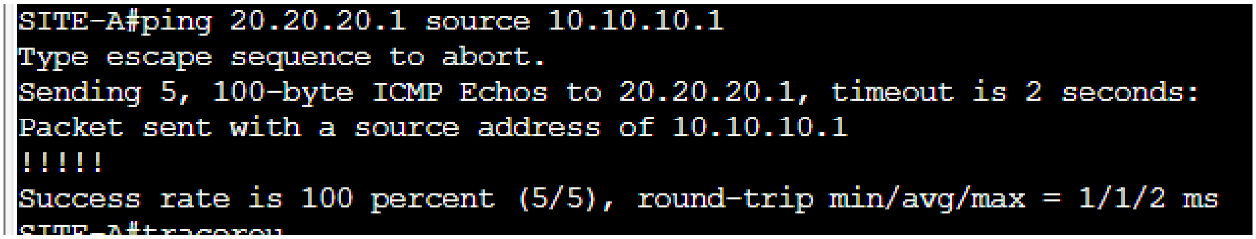
```
SITE-B#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

- After trying to another ping, from SITE-A, ping 20.20.20.1 source 10.10.10.1, ping the 20.20.20.0 network using the internal network of SITE-A, the ping failed and vice versa



```
SITE-A#ping 20.20.20.1 source 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.1
.....
Success rate is 0 percent (0/5)
```

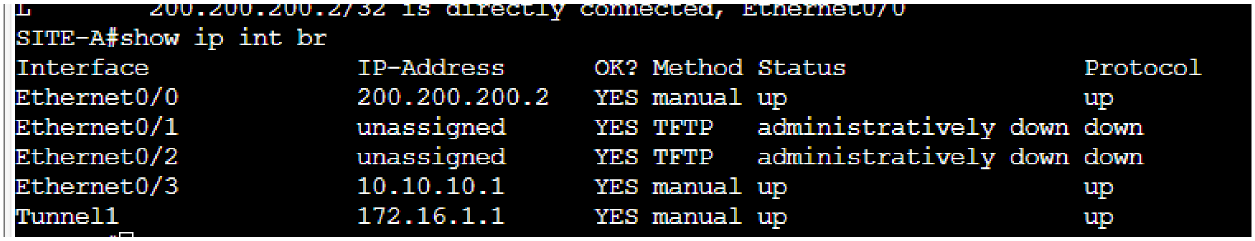
- After wiping and trying the same configuration on the routers ping 20.20.20.1 with source is fixed



```
SITE-A#ping 20.20.20.1 source 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
SITE-A#tracerou
```

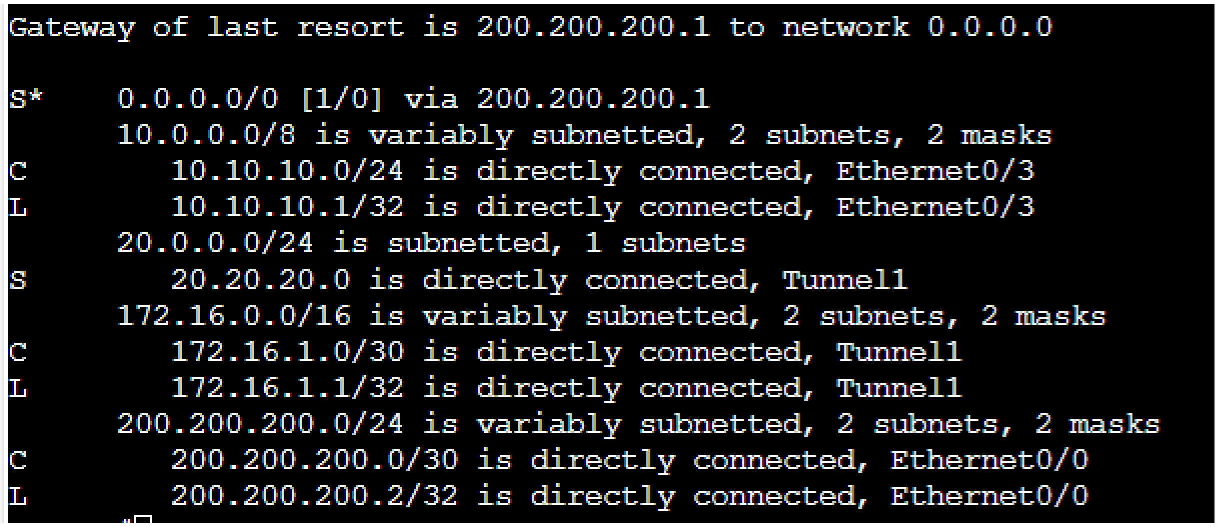
VERIFICATION AND RESULTS

SITE-A ROUTER



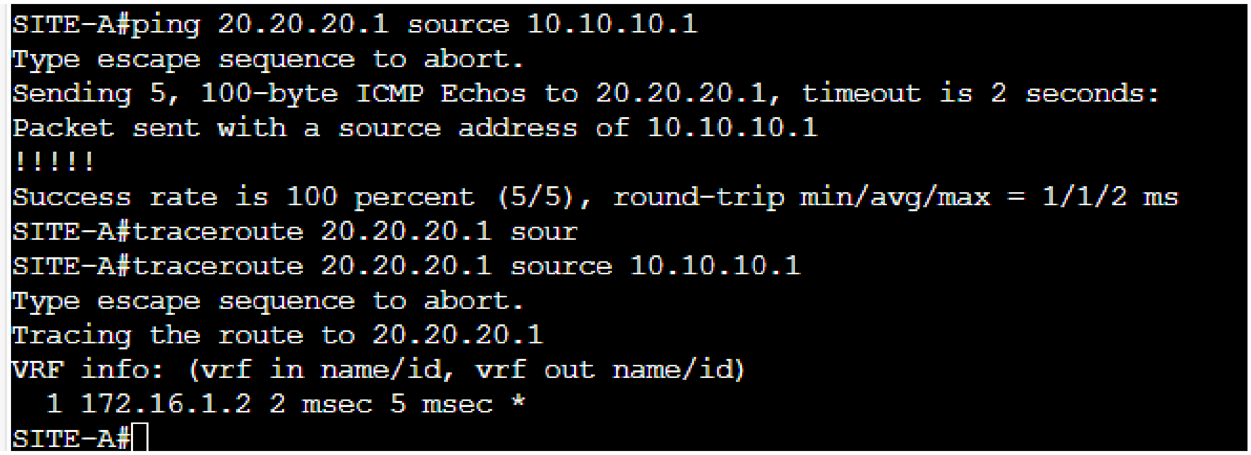
```
L        200.200.200.2/32 is directly connected, Ethernet0/0
SITE-A#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            200.200.200.2   YES manual up                    up
Ethernet0/1            unassigned      YES TFTP   administratively down down
Ethernet0/2            unassigned      YES TFTP   administratively down down
Ethernet0/3            10.10.10.1      YES manual up                    up
Tunnel1                172.16.1.1      YES manual up                    up
```

IP ROUTE



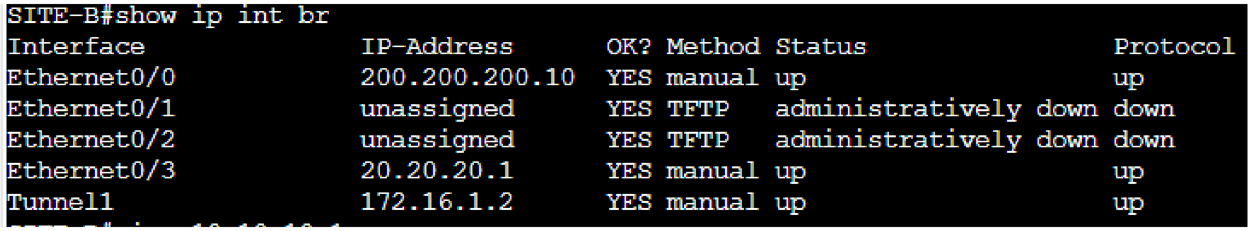
```
Gateway of last resort is 200.200.200.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 200.200.200.1
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.10.10.0/24 is directly connected, Ethernet0/3
L        10.10.10.1/32 is directly connected, Ethernet0/3
      20.0.0.0/24 is subnetted, 1 subnets
S        20.20.20.0 is directly connected, Tunnel1
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/30 is directly connected, Tunnel1
L        172.16.1.1/32 is directly connected, Tunnel1
      200.200.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        200.200.200.0/30 is directly connected, Ethernet0/0
L        200.200.200.2/32 is directly connected, Ethernet0/0
```

PING and TRACEROUTE



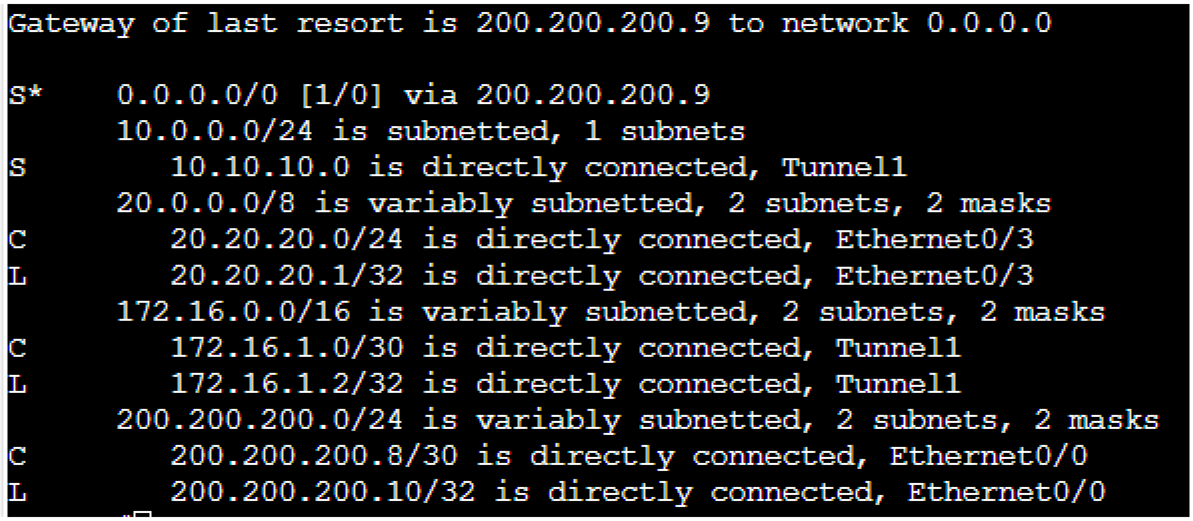
```
SITE-A#ping 20.20.20.1 source 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.1, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
SITE-A#traceroute 20.20.20.1 sour
SITE-A#traceroute 20.20.20.1 source 10.10.10.1
Type escape sequence to abort.
Tracing the route to 20.20.20.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.2 2 msec 5 msec *
SITE-A#
```

SITE-B



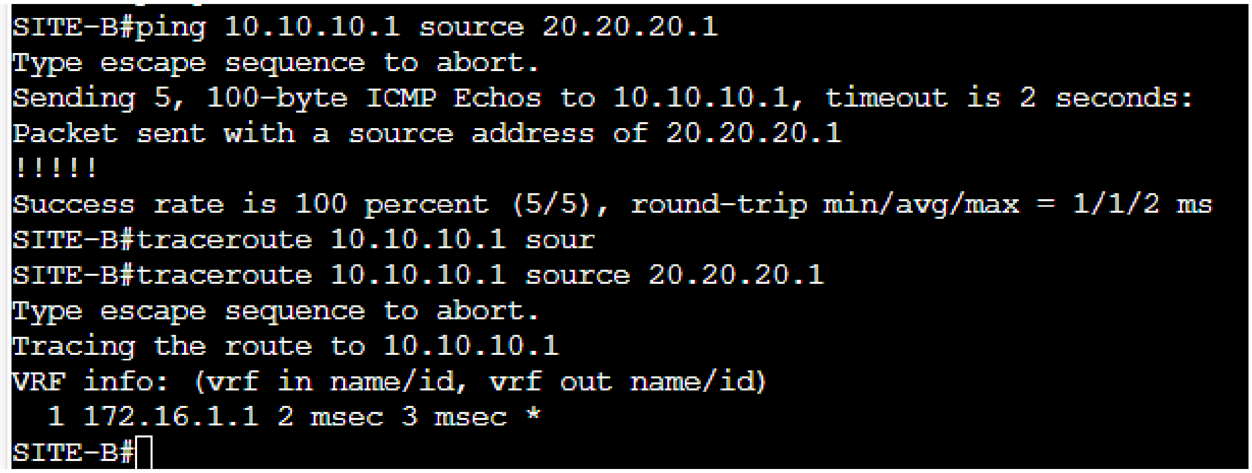
```
SITE-B#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
Ethernet0/0            200.200.200.10  YES manual up                    up
Ethernet0/1            unassigned      YES TFTP   administratively down down
Ethernet0/2            unassigned      YES TFTP   administratively down down
Ethernet0/3            20.20.20.1      YES manual up                    up
Tunnel1                172.16.1.2      YES manual up                    up
```

IP ROUTE



```
Gateway of last resort is 200.200.200.9 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 200.200.200.9
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel1
      20.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        20.20.20.0/24 is directly connected, Ethernet0/3
L        20.20.20.1/32 is directly connected, Ethernet0/3
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/30 is directly connected, Tunnel1
L        172.16.1.2/32 is directly connected, Tunnel1
      200.200.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        200.200.200.8/30 is directly connected, Ethernet0/0
L        200.200.200.10/32 is directly connected, Ethernet0/0
```

PING and TRACEROUTE



```
SITE-B#ping 10.10.10.1 source 20.20.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
Packet sent with a source address of 20.20.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
SITE-B#traceroute 10.10.10.1 sour
SITE-B#traceroute 10.10.10.1 source 20.20.20.1
Type escape sequence to abort.
Tracing the route to 10.10.10.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.1.1 2 msec 3 msec *
SITE-B#
```

KEY NOTES:

1. Why does when I use 192.168.1.1 and 192.168.1.2 in the tunnel interface, we cannot ping the tunnels?
2. What is the purpose of (ip mtu 1400) and (ip tcp adjust-mss 1360)?
3. What are some key concepts to make this happen?
4. What is supposed to happen if we don't have the GRE tunnel?
5. What is the purpose of GRE tunneling?\
6. How does the GRE work?
7. What is an overhead error?
8. Key things to take note about?

ANSWER

1. After searching the web regarding this, I found out that it might be the cause of default behaviour related to IP address range and routing.
   Chances are:

- The router is treating the 192.168.x.x range as internal traffic
- Implicit filtering of RFC1918 IPs, it means that the routers might be silently blocking the ip traffic of 192.168.x.x across WAN interfaces.

2. The reason we use ip mtu 1400 and ip tcp adjust-mss 1360 is because most transport MTUs are 1500 bytes and since we are using GRE we have an added overhead, we must reduce the MTU to account for the extra overhead. Also mtu of 1400 is a common practice and will ensure unnecessary packet fragmentation is kept to a minimum

3. During this laboratory, the key concepts that I learn is routing, and tunneling

- I found out that routing is necessary to establish a connection.
- After establishing a route the ip 10.10.10.1 and 20.20.20.1 is still not reachable, thus simulating a internet environment.
- The route 10.10.10.0/20.20.20.0 255.255.255.0 tunnel 1 is necessary, to force the packet to move thru the GRE tunnel.

4. Without GRE tunnel, in order to achieve this feat, we have to configure a route using BGP in order for us to connect router site to site

5. It provides a mechanism to transport packets from one protocol to another.

- GRE is a layer 3 tunneling protocol that allows private or non-IP traffic to travel across an IP-based network.
- It's like a VPN without encryption.
- This is a core foundation for DMVPN, IPsec VPN, SD-WAN

6. How it work step-by-step

    1. SITE-A receive an IP packet destined for SITE-B
    2. The original packet is encapsulated with GRE header (Protocol 47)
    3. The new ip header will use the public WAN IP (200.200.200.2 - source IP in the tunnel configuration)
    4. Packet traverse to the Internet where it see the outer IP header (200.200.200.10 - destination IP)
    5. SITE-B removes the GRE header and forwards the original packet to the destination.

7. In simple terms if you have an overhead error you will receive a packet loss, most ethernet networks have a default MTU of 1500 bytes, because of GRE-encapsulation the packet sometimes exceeds this limit causing packet fragmentation, and or potential packet loss.

8.
    a. It better to take into account the performance, since GRE encapsulation add overhead (especially with large packet).
    b. Take note of misconfiguration, especially recursive routing.
    c. Take note of Protocol 47 filtering, maybe the ISP is blocking port 47 traffic because it’s not encrypted.

END
EMERSON INTING