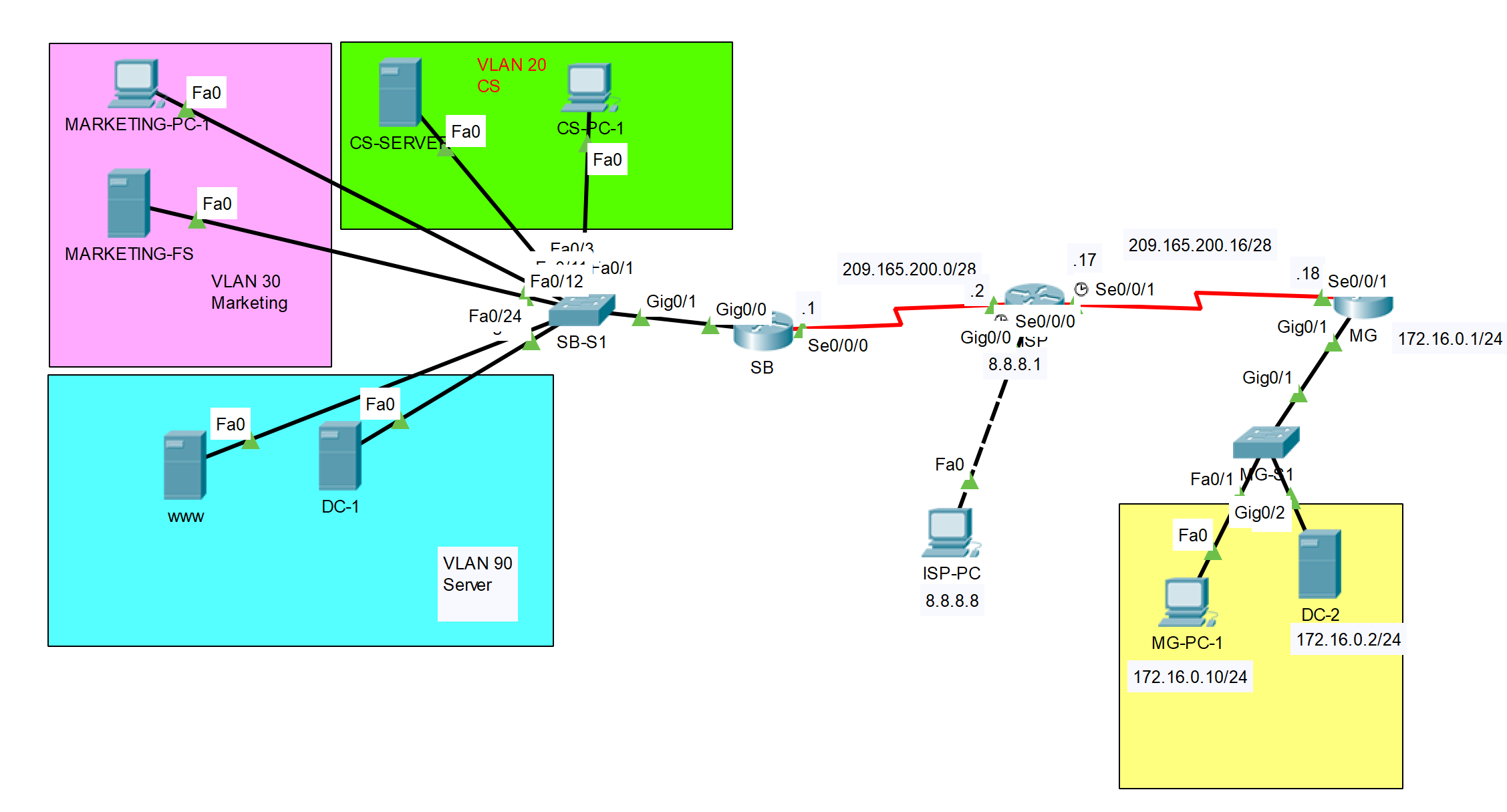
# Lab 4 VPN GRE Tunnel Instructions



| Device | Interface | IP Address/Prefix | Default Gateway |
| --- | --- | --- | --- |
| SB Router | S0/0/0 | 209.165.200.1/28 |  |
|  | Tunnel 0 | 172.16.12.1/30 |  |
| ISP | S0/0/0 | 209.165.200.2/28 |  |
|  | S0/0/1 | 209.165.200.17/28 |  |
|  | G0/0 | 8.8.8.1/8 |  |
| MG Router | S0/0/1 | 209.165.200.18/28 |  |
|  | Tunnel 0 | 172.16.12.2/30 |  |
|  | G0/1 | 172.16.0.1/24 |  |
| ISP-PC | Fastether port | 8.8.8.8/8 |  |
| MG-PC-1 | Fastether port | 172.16.0.10/24 | 172.16.0.1/24 |
| DC-2 | Fastether port | 172.16.0.2/24 | 172.16.0.1/24 |

In this lab, a VPN via GRE tunnel is going to be deployed on the router SB and MG. SB is symbolizing the head office of Mavis company in South Bank. MG is symbolizing the branch office of Mavis company in Mt Gravatt. When the lab is finished, any end devices from the SB Router’s LAN side should be able to ping any devices on the MG Router’s LAN side. This is because a GRE tunnel is set up in between the two edge routers SB and MG. Eventhough ZBF is still blocking the traffic initiated from the Internet, ZBF is putting the tunnel as the trusted interface, Inside.

## Part 1: Setup the network environment as in Lab 3

**Step 1**. Cable the network as the topology above.

**Note**: In each subnet, the PC and the Server can be running as VMs on a same physical host.

**Step 2**. Import the backup running-config files from Lab 3 to the network devices.

| SB-S1 | SB | ISP | MG |
| --- | --- | --- | --- |
| en  conf t  int g0/1  ip address 10.10.10.1 255.255.255.0  no shut  exit  exit  copy tftp://10.10.10.10/sb-s1-confg running-config | en  conf t  int g0/0  ip address 10.10.10.1 255.255.255.0  no shut  exit  exit  copy tftp://10.10.10.10/sb-confg running-config | en  conf t  int g0/0  ip address 10.10.10.1 255.255.255.0  no shut  exit  exit  copy tftp://10.10.10.10/isp-confg running-config | en  conf t  int g0/0  ip address 10.10.10.1 255.255.255.0  no shut  exit  exit  copy tftp://10.10.10.10/mg-confg running-config |

**Step 3**. Import the backup vlan.dat from Lab 3 into SB-S1.

**Step 4**. Configure the end devices IP address as in Lab 3.

**Step 5**. Verify the network connection.

* Pings from the SB router LAN side to the MG router LAN side should fail.
* Pings from the SB router LAN side to the ISP-PC should be successful.
* Pings from the MG router LAN side to the ISP-PC should be successful.
* Pings from the MG router LAN side to the static public IP 209.165.200.10 of WWW server located on SB site should be unsuccessful.

## Part 2: Configure the GRE tunnel interface

**Step 1**. Configure the tunnel interface on the router SB. Use S0/0/0 on SB Router as the tunnel source interface and MG Router’s s0/0/1 interface IP as the tunnel destination on SB.

| Device | Interface | IP Address/Prefix | Default Gateway |
| --- | --- | --- | --- |
| SB | Tunnel 0 | 172.16.12.1/30 |  |
| MG | Tunnel 0 | 172.16.12.2/30 |  |

**Step 2**. Configure the tunnel interface on the MG. Use S0/0/1 on MG as the tunnel source interface and SB Router’s s0/0/0 interface IP as the tunnel destination on the MG.

**Note**: For the tunnel source command, either the interface name or the IP address can be used as the source.

**Step 3**. Configure the tunnel interface as trusted Inside zone-member security on both router SB and MG.

**Step 4**. Verify that the GRE tunnel is functional.

* Verify the status of the tunnel interface on both router SB and MG by issuing the command “**show ip interface brief**”. The Tunnel 0 interface should be up on both routers.
* Pings from the SB to the MG tunnel interface IP should be successful and vice versa.

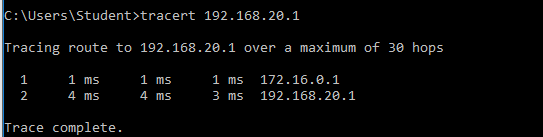


|  |  |
| --- | --- |

## Part 3: Enable Routing over the GRE Tunnel

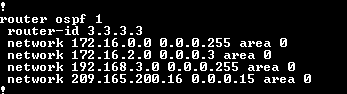
In Part 3, you will configure OSPF routing so that the LANs on SB site and the LANs on the MG site can communicate using the GRE tunnel.

**Note: You do not need to configure OSPF on the ISP router as the ISP router is not participating in this routing process**.

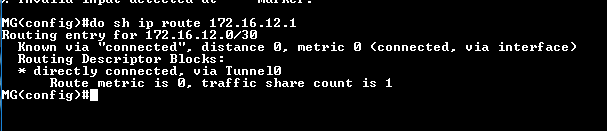


**Step 1**. Configure OSPF process ID 1 using area 0 on both SB and MG. Configure the router-id as 1.1.1.1 on router SB and 2.2.2.2 on router MG. Advertise the directly connected networks in OSPF on both routers except for the WAN link network.

**Note: If you advertise the WAN link network in OSPF on the routers, it will disturb the GRE tunnel negotiation and lead to a failure of OSPF neighbour forming.**

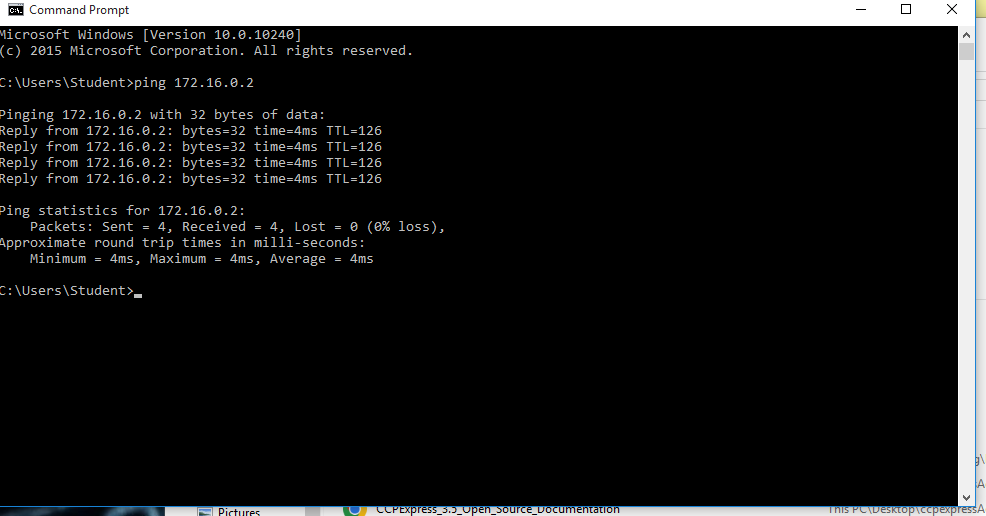
****

**Step 2**. Verify OSPF routing.

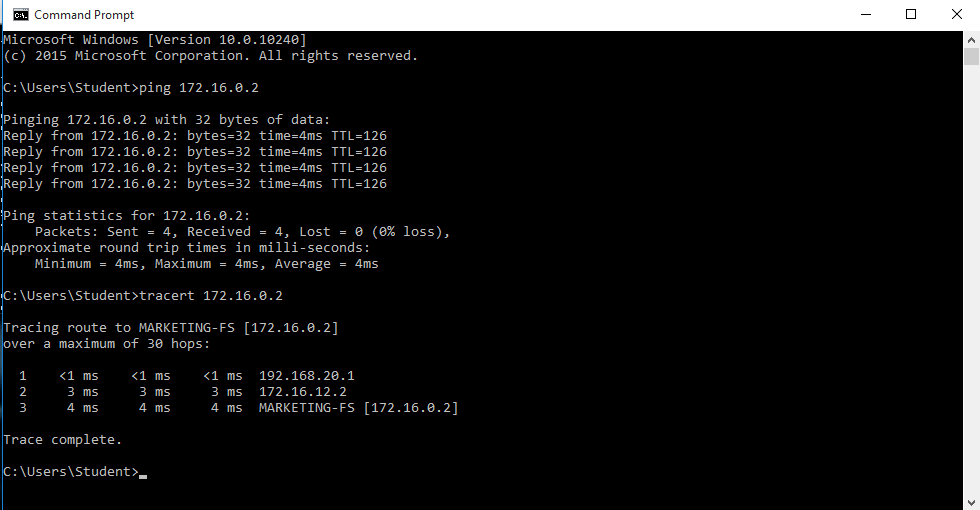
* From router SB, issue the command **show ip route** to verify that the route to 172.16.0.0/24 LAN on the MG Router is via 172.16.12.2.
* From router MG, issue the command **show ip route** to verify that the route to the LANs on the SB site is via 172.16.12.1.
* 

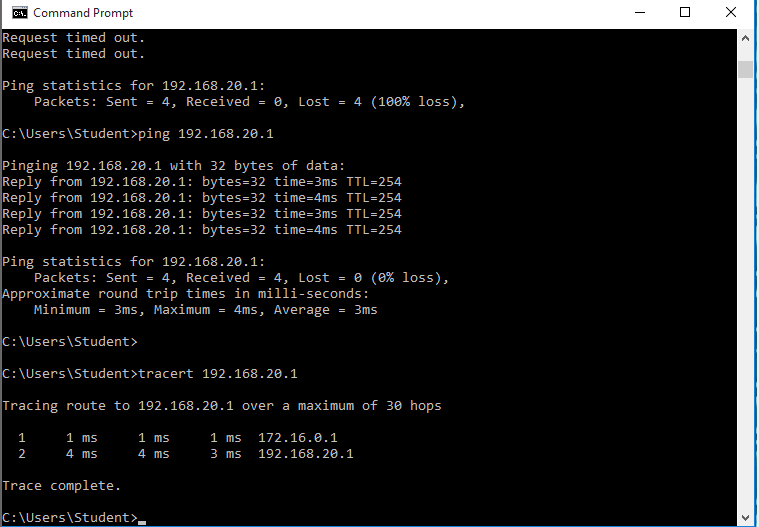
**Step 3**. Verify end-to-end connectivity.

* Ping from any end devices on the SB LAN side to any end devices on the MG LAN side should be successful.



* Ping from any end devices on the MG LAN side to any end devices on the SB LAN side should be successful.

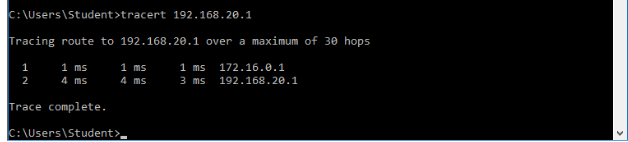




**Note: The pings coming from the MG LAN side is not prohibited by the ZBF on the router SB any more. This is because the pings packets are travelling through the GRE tunnel on SB which penetrate the firewall. The SB’s LAN and the MG’s LAN are viewed as if they are in the same intranet.**

* Trace route from CS-PC-1 to MG-PC-1 and notice the path is via the Tunnel Interface on the MG Router:

192.168.1.1 > 172.16.12.2 > 172.16.0.10



* From any end devices on the MG’s LAN, browsing the web page on the WWW Server using its

private ip address 192.168.x.x should be successful. This is because the web traffic going through the GRE tunnel and is not subject to the NAT any more.

* Ping from ISP-PC to any end devices on the SB site or MG site should fail. This is because the traffic initiated from the Internet is blocked by the ZBF on both router SB and MG.

## Part 4: Demonstration, Mark off, and Backup Network Configuration

1. Demonstrate the following to your instructor and ask for mark off:

* From MG-PC-1 or DC-2, trace route to any end devices on the SB’s LAN should be successful via the Tunnel Interface IP on SB 172.16.12.1.

* From any end devices on router SB’s LAN, trace route to the MG-PC-1 or DC-2 should be successful via the Tunnel Interface IP on router MG 172.16.12.2;
* Display the routing table by issuing the **show ip route** command on router SB and the router MG. Take the screenshots from SB and MG then paste them to AT4 Part 2 template.
* Ping from ISP-PC to CS-PC-1.
* Ping from ISP-PC to MG-PC-1.

1. Backup the running-config on the router SB.

* Backup the router SB’s running-config in plain text files for the future practical labs.
* Backup the ISP’s running-config in plain text files for the future practical labs.
* Backup the router MG’s running-config in plain text files for the future practical labs.
* Backup the SB-S1’s running-config and SB-S1’s VLAN.dat into plain text files for the future practical labs.