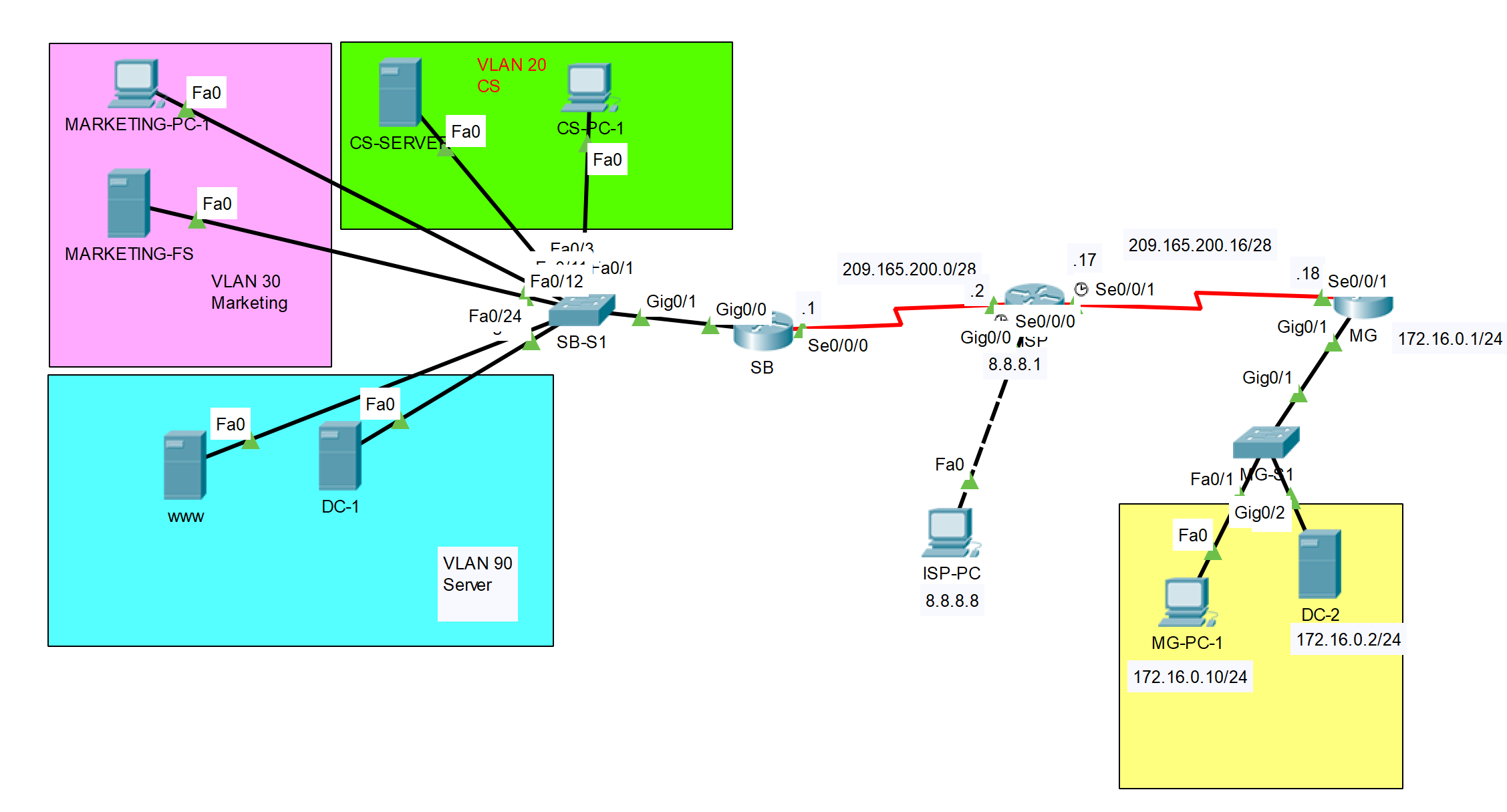
# Lab 3 Zone-Based Firewall Instructions

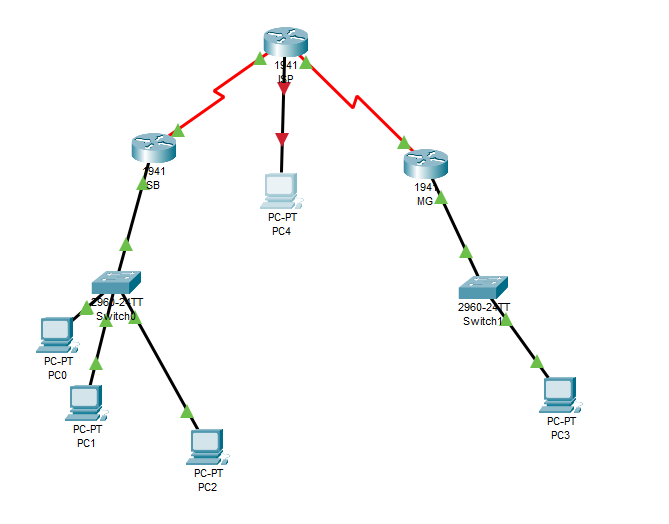


| Device | Interface | IP Address/Prefix | Default Gateway |
| --- | --- | --- | --- |
| SB Router | S0/0/0 | 209.165.200.1/28 |  |
| ISP | S0/0/0 | 209.165.200.2/28 |  |
|  | S0/0/1 | 209.165.200.17/28 |  |
|  | G0/0 | 8.8.8.1/8 |  |
| MG Router | S0/0/0 | 209.165.200.18/28 |  |
|  | G0/0 | 172.16.0.1/24 |  |
| 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, ZBF is going to be deployed on the SB router and MG router. SB is symbolizing the head office of Mavis company in South Bank. MG is symbolizing the branch office of Mavis company in Mt Gravatt. OSPF is going to be removed from all three routers. When the lab is finished, any end devices from the SB Router’s LAN side should not be able to ping any devices on the MG Router’s LAN side. This is because ZBF on the SB Router put the WAN interface S0/0/0 as untrusted. So as in the MG Router.

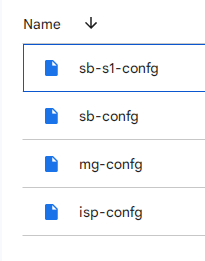
## Part 1: Setup the network environment as in Lab 2 and setup NAT on MG

**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.

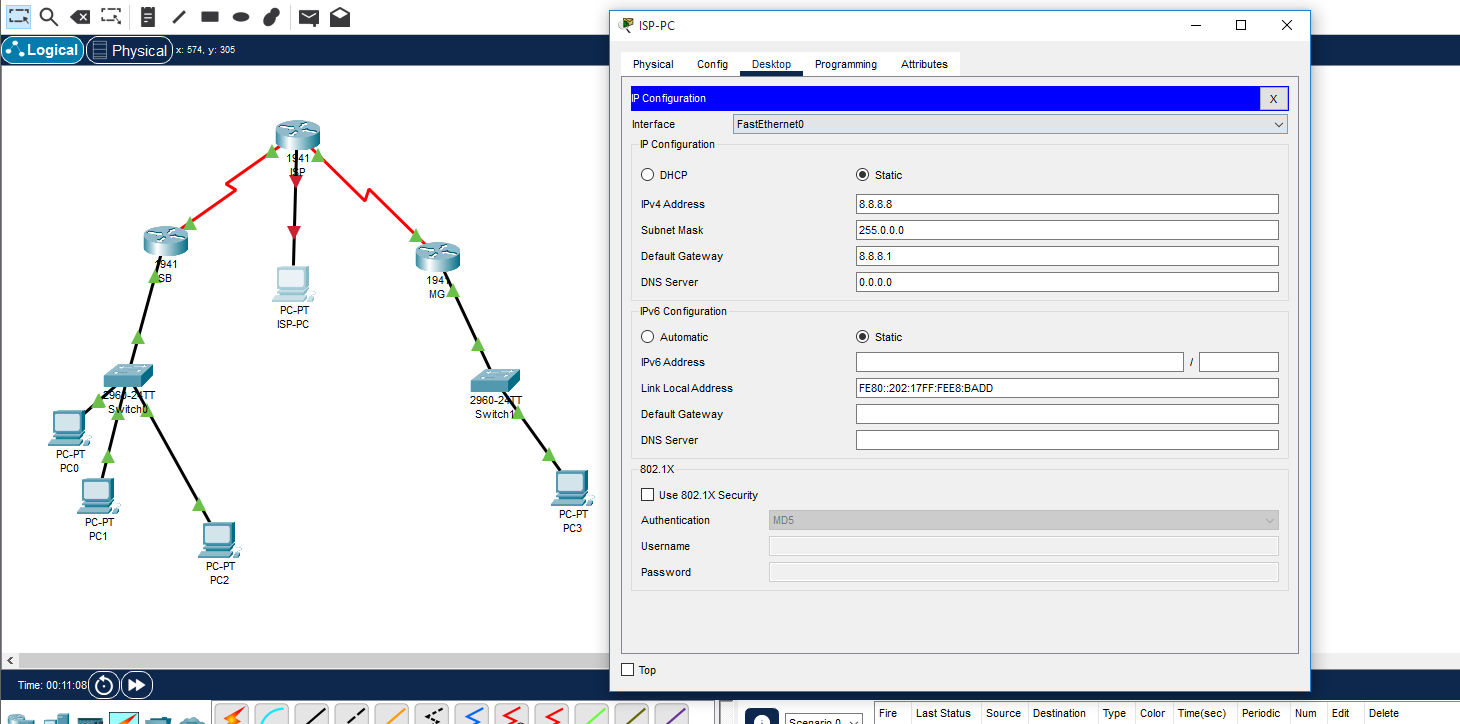
**Step 2**. Import the backup running-config files from Lab 2 to the network devices.



**Step 3**. Import the backup vlan.dat from Lab 2 into SB-S1 .

**Step 4**. Configure the end devices IP address as in Lab 2.

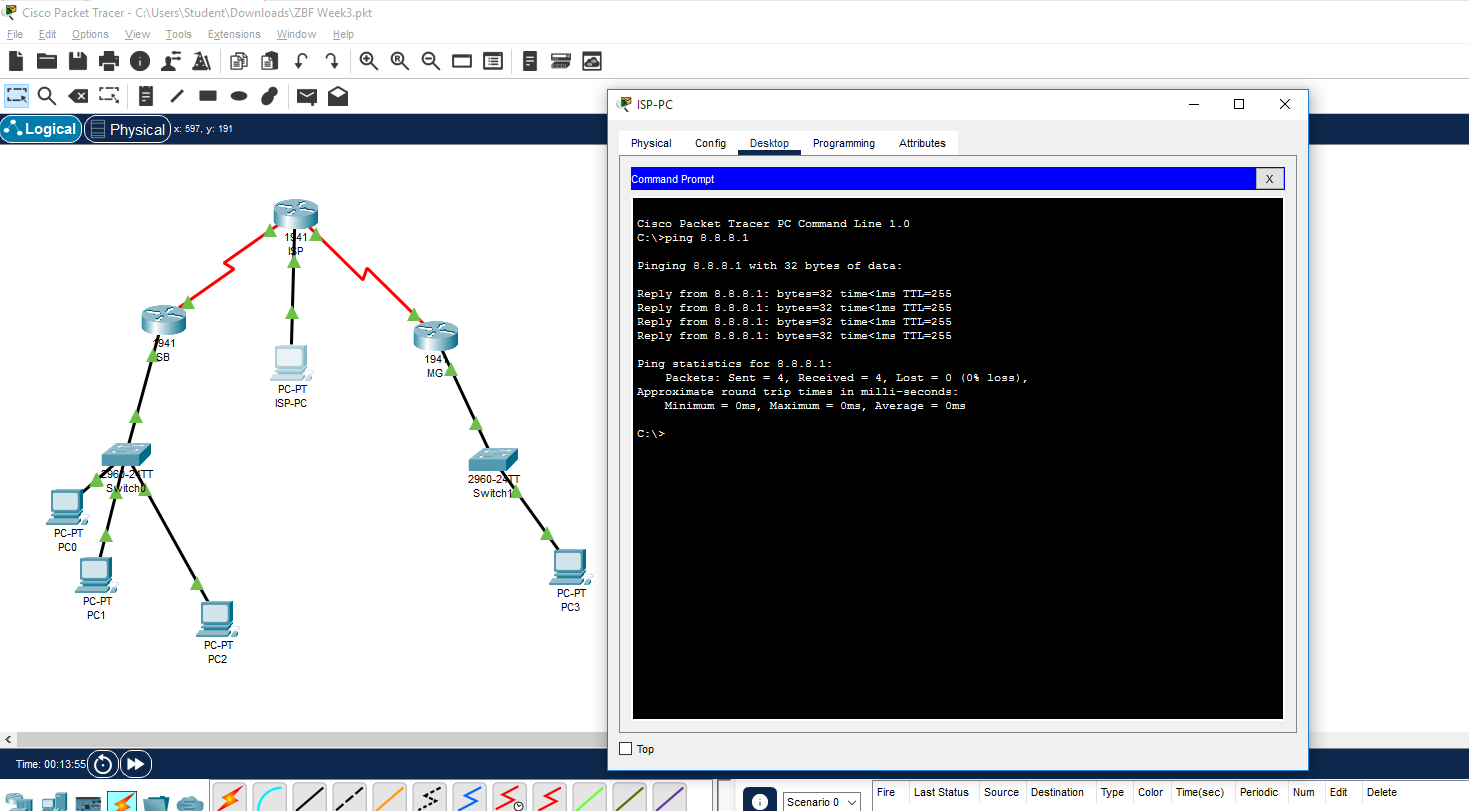
**Step 5**. Configure ISP-PC with the IP address configurations as shown in the IP address table above.

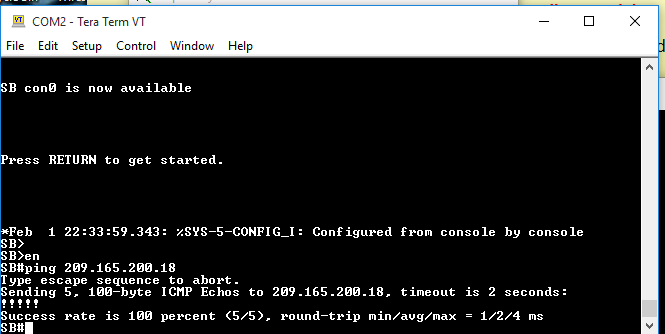


**Step 6**. Configure interface G0/0 on router ISP with the IP address configuration as shown in the IP address table above.

| ISP |
| --- |
| !###Configure interface G0/0 on router ISP with the IP address configuration###!  en  conf t  int g0/0  ip address 8.8.8.1 255.0.0.0  no shut  exit |

**Step 7**. Verify the network connection. Pings from the SB router LAN side to the MG router LAN side should be successful.





**Step 8**. Remove the OSPF settings on both ISP and MG.

| ISP | MG |
| --- | --- |
| !###Removing OSPF settings on ISP###! en  conf t  router ospf 1  no network 209.165.200.0 0.0.0.31 area 0  exit | !###Removing OSPF settings on MG###! en  conf t  router ospf 1  no network 209.165.200.16 0.0.0.15 area 0  no network 172.16.0.0 0.0.0.255 area 0  exit |

**Step 9**. Configure a default route on MG pointing towards ISP.

| **MG** |
| --- |
| !### Configuring a default route MG -> ISP.###!  en  conf t  int s0/0/0  ip route 0.0.0.0 0.0.0.0 0.0.0.0 |

**Step 10**. Configure PAT on MG by overloading the WAN interface connecting to the Internet.

1. Create a standard ACL to capture the traffic initiated from the LAN side on MG:

| **MG** |
| --- |
| !### Configure ACL list for capturing outgoing ISP traffic###!  en  conf t  access-list 2 permit 172.16.0.0 0.0.0.255  exit |

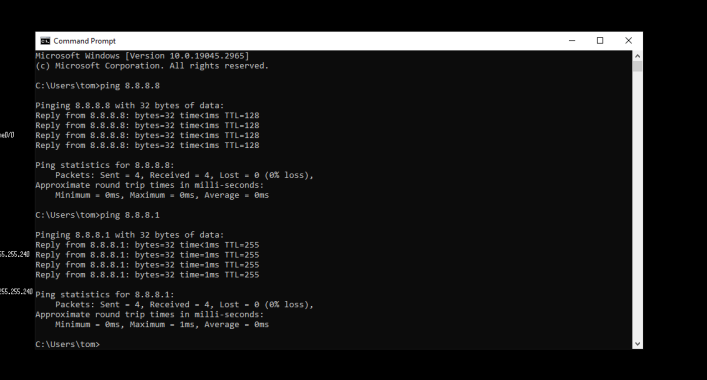
1. Configure PAT by overloading the serial interface on MG.

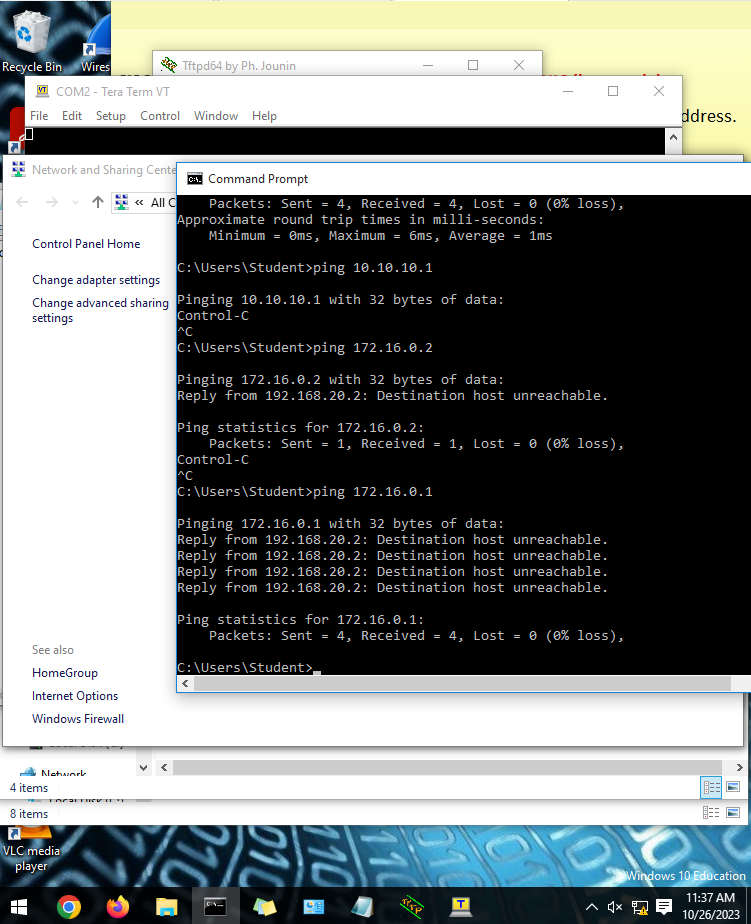
| **MG** |
| --- |
| !### Configuring NAT on MG Router###!  en  conf t  ip nat pool NAT\_POOL 209.165.200.18 209.165.200.18 netmask 255.255.255.240  ip nat inside source list 2 interface s0/0/0 overload |

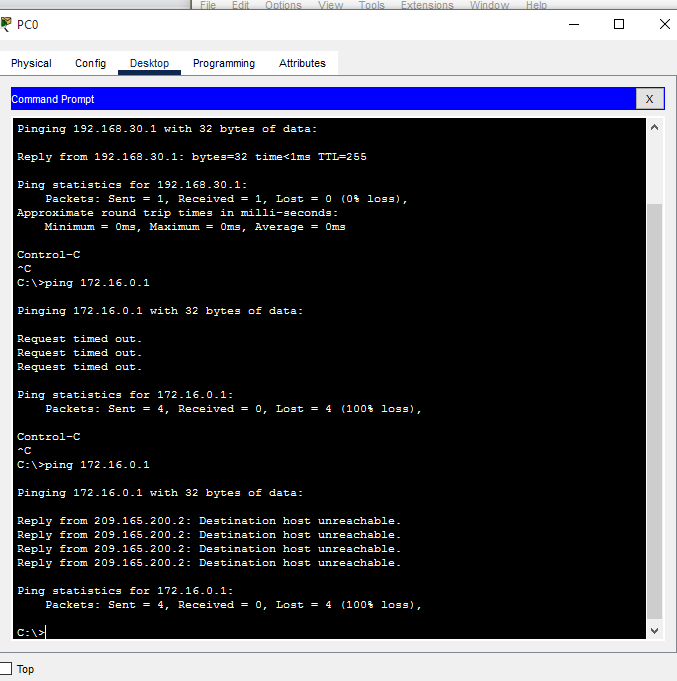
1. Assign inside/outside interfaces on MG router properly.

| **MG** |
| --- |
| !### Assigning Inside/Outside interfaces for NAT###!  int s0/0/0  ip nat outside  no shut  exit  int g0/0  ip nat inside  no shut  exit |

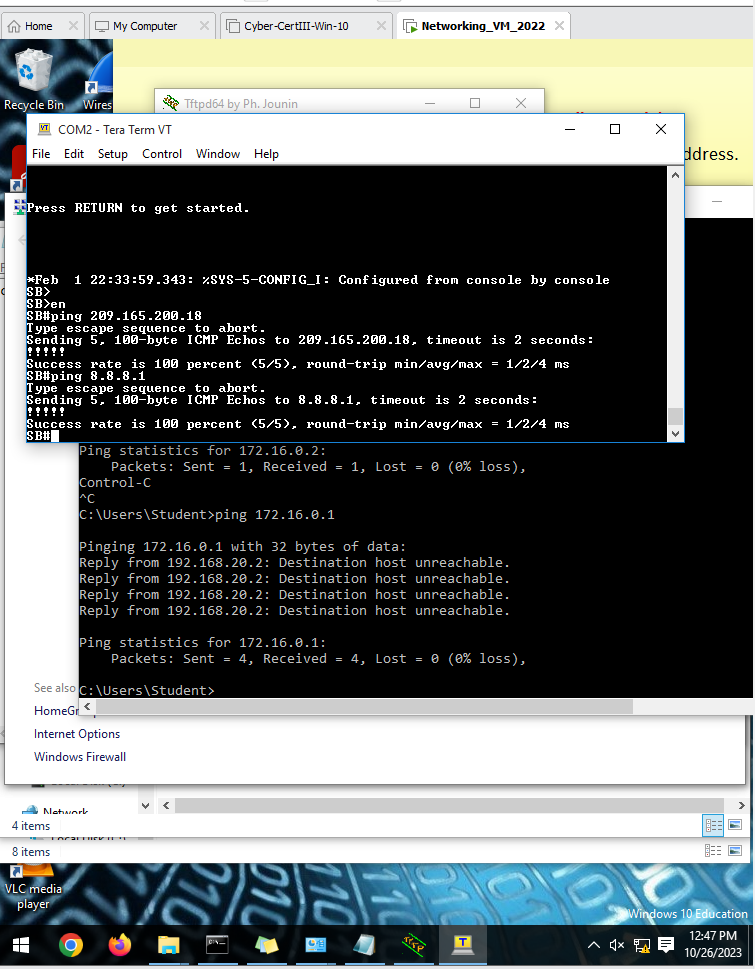
**Step 11**. Verify the network connection.

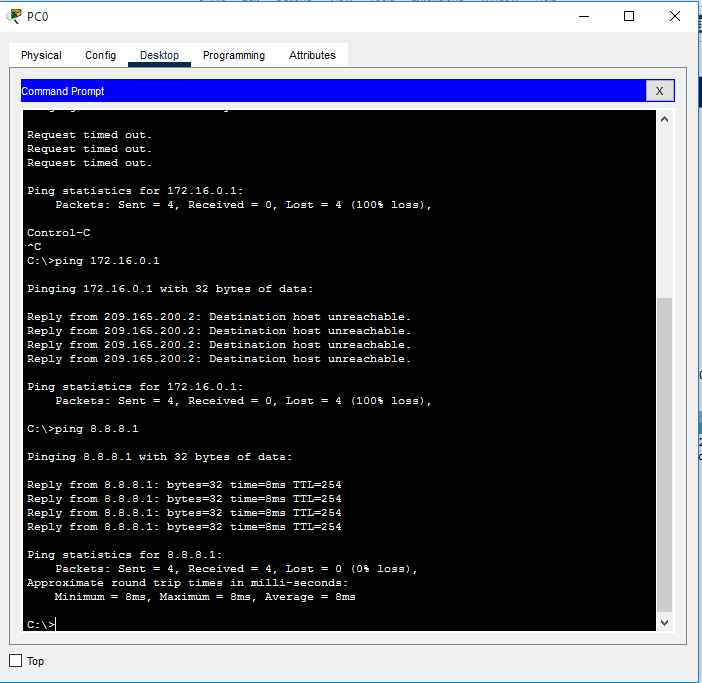


* Pings from the SB router LAN side to the MG router LAN side should fail.
* 

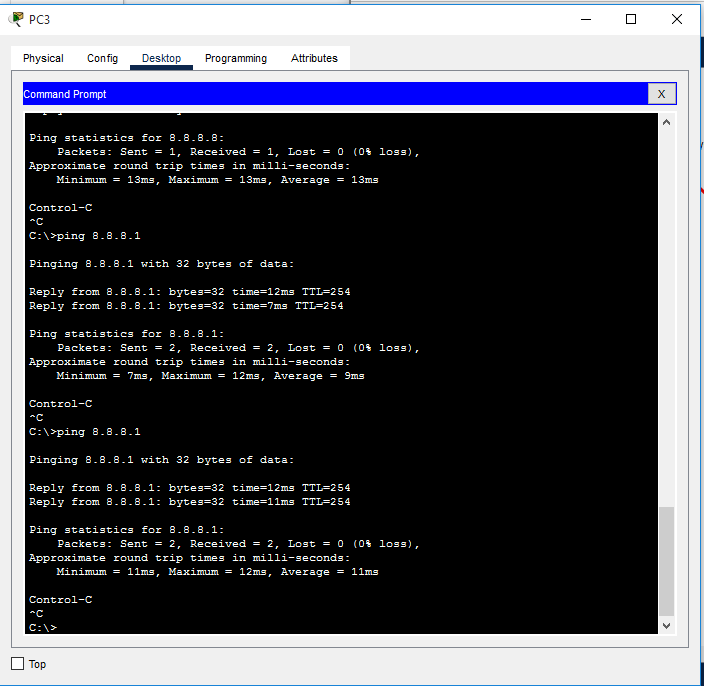


* Pings from the SB router LAN side to the ISP-PC should be successful.

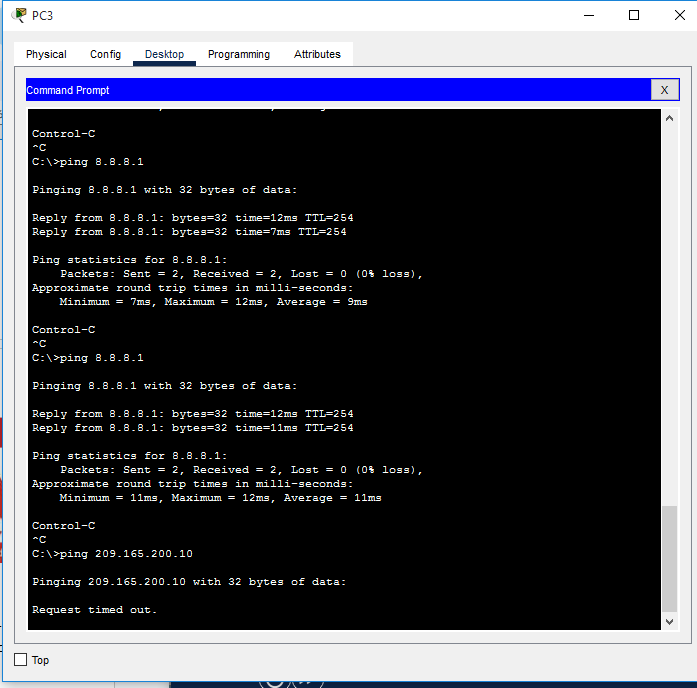




* Pings from the MG router LAN side to the ISP-PC should be successful.



* 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 a ZBF on router SB and MG

In this part, you will create a zone-based policy firewall on SB Router, making it act not only as a router but also as a firewall. SB is currently responsible for routing packets for the four networks connected to it. SB’s interface roles are configured as follows: Serial 0/0/0 is connected to the Internet. Because this is a public network, it is considered an untrusted network and should have the lowest security level. Sub-interfaces G0/0.20, G0/0.30, and G0/0.90 are connected to the internal network. Only authorized users have access to these networks. In addition, vital institution resources also reside in these networks. The internal networks are to be considered as trusted networks and should have the highest security level. The security policy to be enforced by SB when it is acting as a firewall dictates that: • No traffic initiated from the Internet should be allowed into the internal networks. • Returning Internet traffic (return packets coming from the Internet into the SB site, in response to requests originating from any of the SB internal networks) should be allowed. • Computers in the SB internal network are considered trusted and are allowed to initiate any type traffic (TCP, UDP or ICMP based traffic).

**Step 1**. **Create the security zones**.

A security zone is a group of interfaces with similar security properties and requirements. For example, if a router has three interfaces connected to internal networks, all three interfaces can be placed under the same zone named “internal”. Because all security properties are configured to the zone instead of to the individual router interfaces, the firewall design is much more scalable. In this lab, the SB site has four interfaces; three sub-interfaces connected to the internal trusted networks, the serial interface connected to the Internet. Because the internal network and the Internet have different security requirements and properties, we will create two different security zones.

C. INITIAL CONFIGURATION TO RUN ZBF AND ZONE COMMANDS - NEED TO RUN THE LICENCES

| SB | MG |
| --- | --- |
| !### Enabling securityk9 package###!  !### This allows ZBF to be configured properly :)###!  en  conf t  license boot module c1900 technology-package securityk9  yes  !### Need to reload switch to enable the licence properly###!  do write memory  do copy running-config startup-config  !###Press enter manually after this so it reloads###!  do reload | !### Enabling securityk9 package###!  !### This allows ZBF to be configured properly :)###!  en  conf t  license boot module c1900 technology-package securityk9  yes  !### Need to reload switch to enable the licence properly###!  do write memory  do copy running-config startup-config  !###Press enter manually after this so it reloads###!  do reload |

1. Security zones are created in global configuration mode, and the command allows for zone name definition. Create two zones named Inside and Internet on both router SB and MG:

| **SB** | **MG** |
| --- | --- |
| en  sh lic feat  !### creating security zones###!  conf t  zone security Inside  zone security Internet  end  show run | section zone  !## | en  sh lic feat  !### creating security zones###!  en  conf t  zone security Inside  zone security Internet  end  show run | section zone  !## |

**Step 2**. **Create Security Policies**.

1. Create an inspect class-map to match traffic to be allowed from the Inside zone to the Internet zone. Because we trust the Inside zone, we allow all the main protocols, including tcp, udp, and icmp.

| SB | MG |
| --- | --- |
| conf t  class-map type inspect match-any cmap-inside  match protocol tcp  match protocol udp  match protocol icmp  end | conf t  class-map type inspect match-any cmap-inside  match protocol tcp  match protocol udp  match protocol icmp  end |

The class-map name is up to your choice. In this lab, please name the class-map from Inside zone to Internet zone as “cmap-inside”. Created the class-map named “cmap-inside” on both router SB and MG.

1. Create an inspect policy-map named Inside-to-Internet on both router SB and MG. The policy map is to decide the fate of the selected traffic captured by a class-map.

| SB | MG |
| --- | --- |
| conf t  policy-map type inspect Inside-to-Internet  class cmap-inside  inspect  end | conf t  policy-map type inspect Inside-to-Internet  class cmap-inside  inspect  end |

**Step 3**. **Create the Zone Pairs**.

A zone pair allows you to specify a unidirectional firewall policy between two security zones. In this lab, there is only one zone pair is required, **Inside to Internet**. This zone-pair defines unidirectional traffic flowing from Inside to Internet and allowing the returning traffic in response to the traffic originating from the Inside to flow through, in the direction of Internet to Inside. If **Internet-initiated** traffic needs to flow in the **Internet-to-Inside** direction, another zone-pair must be created.

1. **Create the zone-pair named Inside-to-Internet on both router SB and MG with the source is Inside and destination is Internet.**

**Note**: the source and the destination must be consistent with the security zones name (case sensitive).

| **SB** | **MG** |
| --- | --- |
| !###Defining a zone-pair for traffic flowing from Inside to Internet###!  conf t  zone-pair security Inside-to-Internet source Inside destination Internet  end | !###Defining a zone-pair for traffic flowing from Inside to Internet###!  conf t  zone-pair security Inside-to-Internet source Inside destination Internet  end |

1. Verify the zone-pairs were correctly created by issuing the **show zone-pair security** command. Notice that no policies are associated with the zone-pairs yet. The security policies will be applied to zone-pairs in the next step.

| **SB** | **MG** |
| --- | --- |
| show zone-pair security | show zone-pair security |

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

**Step 4**. **Applying Security Policies**.

1. Associate the policy-maps to the zone-pairs on both the SB router and MG router:

**Note**: the inspected policy name must be consistent with the policy map defined before (case sensitive).

| **SB** | **MG** |
| --- | --- |
| conf t  zone-pair security Inside-to-Internet source Inside destination Internet  service-policy type inspect Inside-to-Internet  end | conf t  zone-pair security Inside-to-Internet source Inside destination Internet  service-policy type inspect Inside-to-Internet  end |

1. Verify the zone-pairs again by issuing the **show zone-pair security** command. Notice that the policies associated with the zone-pairs are now displayed.

| **SB** | **MG** |
| --- | --- |
| show zone-pair security | show zone-pair security |

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

1. To obtain more information about the zone-pairs, their policy-maps, the class-maps and match counters, use the **show policy-map type inspect zone-pair** command.

| **SB** | **MG** |
| --- | --- |
| show policy-map type inspect zone-pair  !###Aforementioned command will not work as the zone-pair is not specified as its a one to many attribute###! !###Using this instead…###!  show policy-map type inspect zone-pair Inside-to-Internet  !###doesnt work still so i just show the generic sessions###! show policy-map type inspect zone-pair sessions | show policy-map type inspect zone-pair  !###Aforementioned command will not work as the zone-pair is not specified as its a one to many attribute###! !###Using this instead…###!  show policy-map type inspect zone-pair Inside-to-Internet  !###doesnt work still so i just show the generic sessions###! show policy-map type inspect zone-pair sessions |

**Step 5**. **Assign Interfaces to the Proper Security Zones**.

Interfaces (physical and logical) are assigned to security zones with the **zone-member security** interface command**.**

1. Assign the LAN interfaces to the Inside zone on both router SB and MG. **On SB router, make sure the zone-member security should be configured on each subinterface, not the physical interface**:

**Note**: the security zone name must be consistent with the security zones defined before (case sensitive).

**Note**: If you need to troubleshoot with the network connectivity and not sure whether it is caused by the ZBF or the other network configuration problems, you can simply unassign the interfaces to the security zones to deactivate the ZBF and exclude the ZBF caused factors.

| **MG** | **SB** |
| --- | --- |
| conf t  interface GigabitEthernet0/0.20  zone-member security Inside  interface GigabitEthernet0/0.30  zone-member security Inside  interface GigabitEthernet0/0.90  zone-member security Inside  end | conf t  interface GigabitEthernet0/0  zone-member security Inside  end |

1. Assign the WAN interfaces to the Internet zone on both router SB and MG:

| **SB** | **MG** |
| --- | --- |
| conf t  interface s0/0/0  zone-member security Internet  end | conf t  interface s0/0/0  zone-member security Internet  end |

**Step 6**. **Verify Zone Assignment**.

1. Issue the **show zone security** command on both router SB and MG to ensure the zones are properly created, and the interfaces were correctly assigned:

**Note**: The “self” zone is a special default security zone. This zone relates to traffic that originates in or is destined to the control plane of the router itself (eg. Routing protocols, SSH, SNMP, etc.). By default, all traffic is allowed into the self zone.



## Part 3: Demonstration, Mark off, and Backup Network Configuration

1. Demonstrate the following to your instructor and ask for mark off:
   * 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.
   * Issue the **show zone security** command on both router SB and MG to demonstrate the zones are properly created, and the interfaces were correctly assigned. Take the screenshots from SB and MG then paste them to the AT4 Part 2 template.
   * Issue the **show policy-map type inspect zone-pair** command to demonstrate the zone-pairs, their policy-maps, the class-maps and match counters. Take the screenshot of the output from SB and paste it to AT4 Part 2 template.
2. Backup the running-config on the routers.

* Backup all routers’ running-config in plain text files for the future practical labs.