Report 2

VLAN

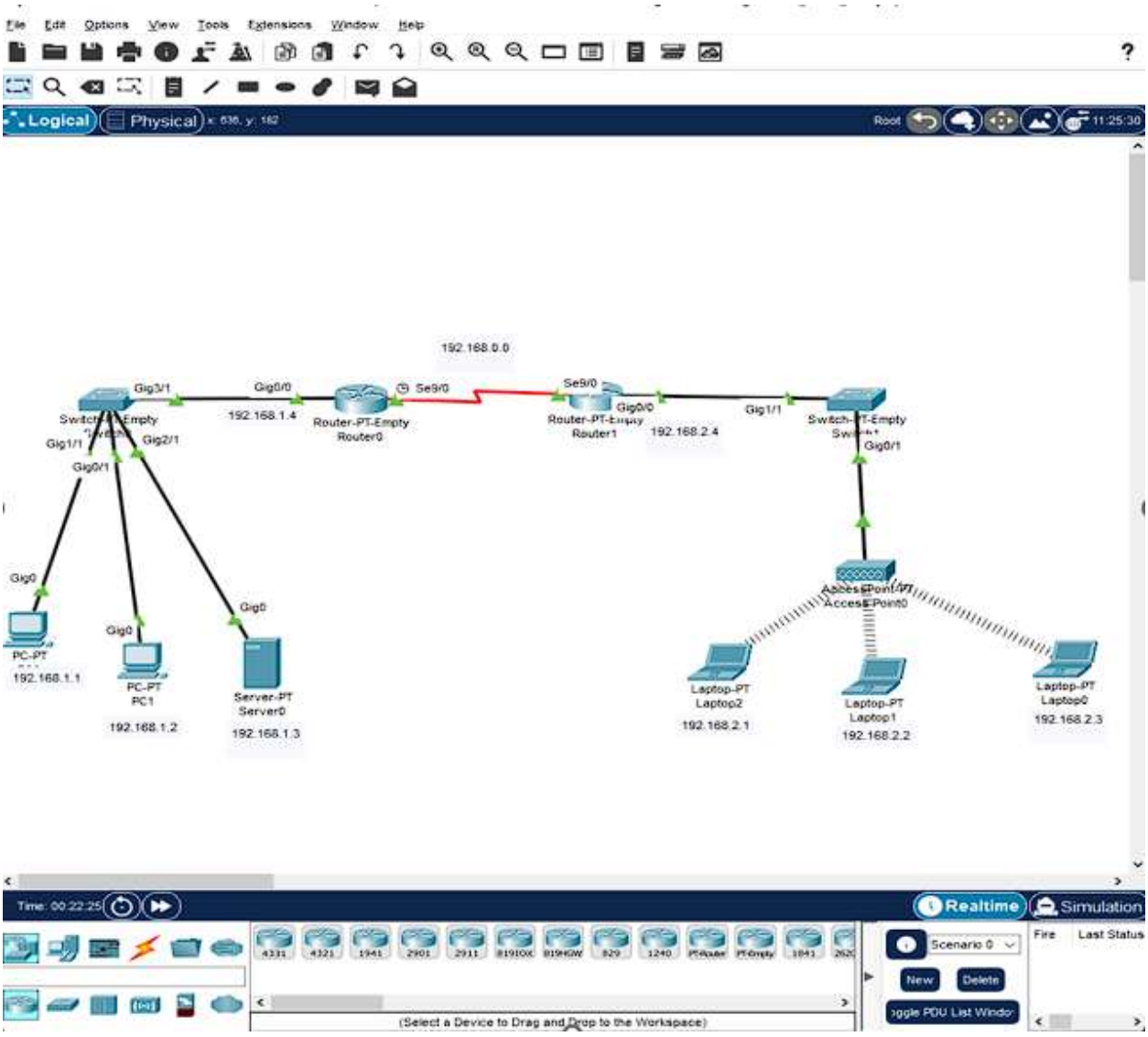
Utsav Shakya

Introduction

The goal of this assignment is to connect a PC in one VLAN to another VLAN. This is possible through connecting the two VLAN with the help of routers. Inter-VLAN communication is very important in network configurations because it enhances security through controlling network traffic between different segments. VLANs are also excellent is sharing resources, as it enables devices from different devices connected in different VLAN utilize resources between them.

Equipment/Software Setup:

For this assignment, devices are separated into two sections, one for each VLANs. For VLAN 10, a switch (Switch0) is taken. Two PCs and a server are connected to it through GCE cable, and the switch is connected to a router (Router0). For VLAN 20, another switch (Switch1) is taken. It is connected with a router (Router1) and an Access Point through GCE cable. Three laptops are connected to the Access Point wirelessly. Then both routers are connected through series9 cable.



VLAN Configuration:

For VLAN 10, it is set on Switch0. After creating the VLAN 10 in the switch, it is named Main as it is the Main VLAN for this assignment. Then both PCs and the Server are connected to the VLAN through the CGE cable. Interface Gig1/1, Gig0/1 and Gig2/1 is added to the VLAN so that all three devices can communicate with each other. PC0, PC1 and Server0 were assigned 192.168.1.1, 192.168.1.2, 192.168.1.3 IP-address respectively within the subnet 192.168.1.0/24.

For VLAN 20, it is set on Switch1. Then, a wireless access point is connected to the Switch. WPA2-PSK authentication was used for security and the “Guest” was set for its SSID so that not all wireless devices could access the WAP. The password was set as “Zxcvbnm12345!”. Now only people with the password were able to access the WAP. For VLAN 20, it was named “Guest”, as it was only for guest users. Three laptops were connected to the WAP with the help of wireless module set in it. We used WAP so that all three laptops were able to connect to the

Guest VLAN. Laptop0, Laptop1 and Laptop2 were assigned 192.168.2.1, 192.168.2.2, 192.168.2.3 IP-address respectively within the subnet 192.168.2.0/24.

The main reason to why the devices are set within same subnet is for efficient routing, as devise within same subnet could communicate with each other without another router, and since all devices within same subnet belong to same broadcast domain, it prevents unnecessary traffic in the network.

Router Configuration:

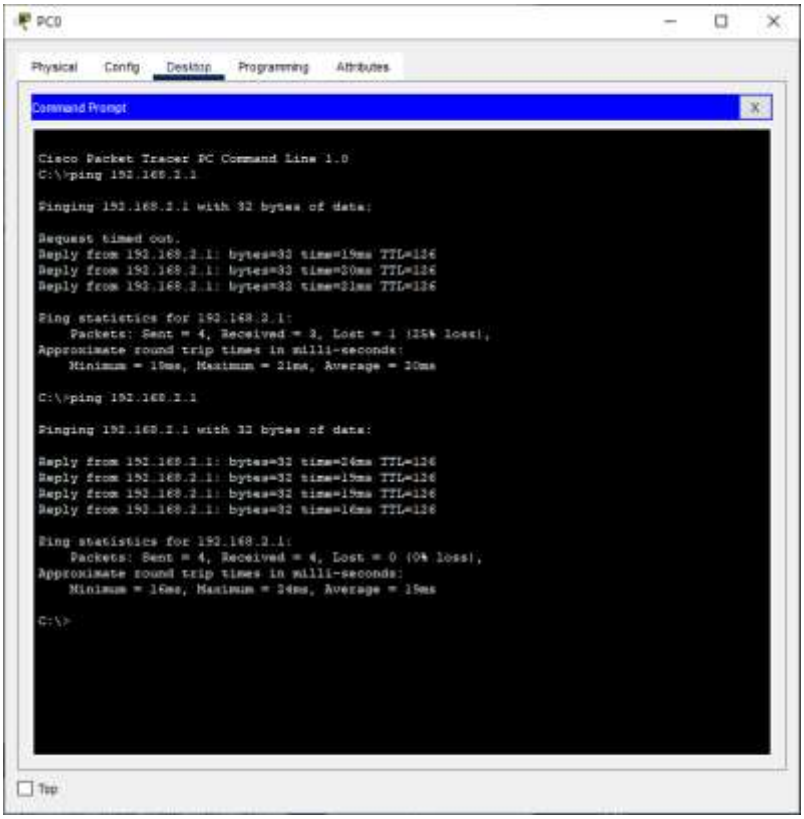
After setting up both the VLANs, we take two routers (Router0 and Router1) and connect with the VLANs respectively. Both routers have connected with a GCE to connect with the switch and NM-1SS module to connect with the other router. The IP address for Router0 ethernet is set to 192.168.1.4, within the 192.168.1.0/24 range and 192.168.0.1 for its serial9/0. For Router1 the IP address for Router0 ethernet is set to 192.168.2.4, within the 192.168.2.0/24 range and 192.168.0.2 for its serial9/0. We set Ip address for seriral9/0 so that we could connect to the other router and IP address for the gig ethernet because it is used as a default gateway for the devices connected to it through a switch for routing, inter-network communication and proper network functionality.

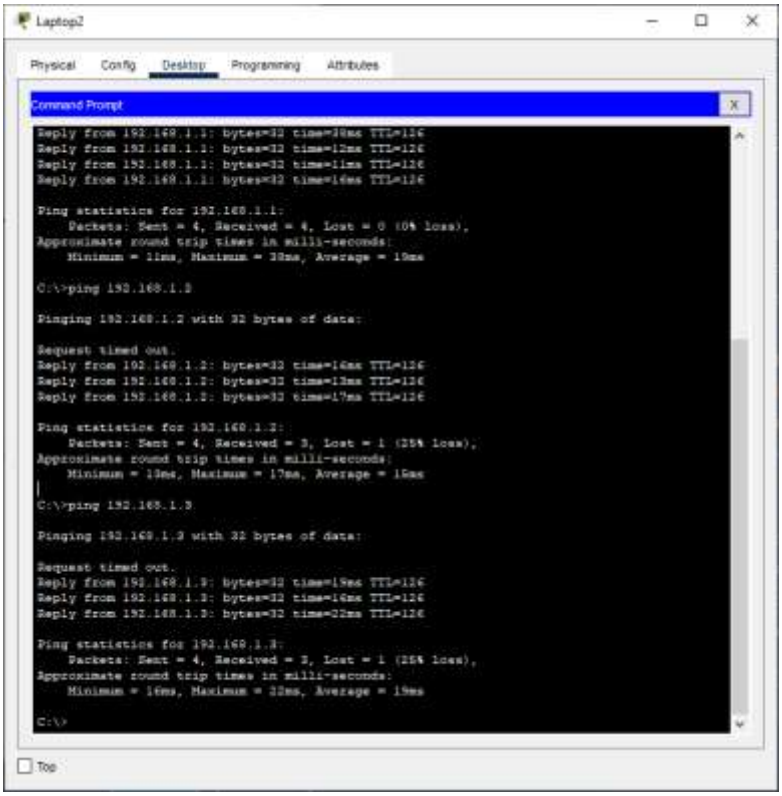
Then we enable static routing by adding network (entering the supposed to connect network), mask (255.255.255.0) and next hop (the IP address of the serial9/0 of the other router that Is to be connected). For Router0 static Routes, network, mask, and next Hop are set as 192.168.2.0, 255.255.255.0,192.168.0.2 respectively and for Router1 static Routes, network, mask and next Hop are set as 192.168.1.0, 255.255.255.0,192.168.0.1 respectively. If done successfully, PCs could connect with PCs from VLAN 10 to VLAN 20.

Test and Results:

After completely all the setup successfully, the computer from VLAN 10 was able to ping Laptops in VLAN 20 and vice versa. It was tested by going to the command prompt for each PCs and pinging to other PCs in the same VLAN first to confirm that they could ping each other. Then Pinging devices from VLAN10 to devices of VLAN20. This step is done to all the PCs. After completing this test, when ping PCs in same VLAN, there was no packet loss for both VLANs. But when connecting to PCs in different VLANs, some packet losses were discovered.

From the image below, you can see that when I pinged from PC0 of VLAN10(192.168.1.1) to Laptop2 of VLAN20(192.168.2.1), there was 25% of packet loss at first, but when performed again, there was no packet loss.





From 2 images, we can also see that, when pinging from a device for the first time, there was a 25% packet loss, but when pinging again, no packet loss was to be found.

Discussion:

From the images we can see that routing is very effective and reliable but there still is a chance of loss of data. For this assignment, when I pinged to a device to another device from the first time, I usually saw 25% packet loss (happened when ping PC1 to Laptop2 and Laptop2 to PC2 and Server0). Then if the process was repeated, there was no packet loss.

The main problem I faced was to also connect the gigabit Ethernet connecting the router and switch to include in the VLAN server for both VLANs. This was very easy to miss and took a long time of debugging to figure out.

The main importance of inter-VLAN communication in practical network scenarios would be that they would provide proper security as it is one of the very important factors in real life scenarios. The other is that inter-VLAN communication ensures that critical applications and services receive necessary bandwidth as it is excellent in handling resource which is also another important factor in practical scenarios.

Conclusion:

From this assignment, we can conclude that, to be able to connect PCs from one VLAN server to another VLAN server, routing is needed. Both servers should have a router for routing to work and that routing is very effective in but there will still be chance of losing data when transferring.