CSCI 31082 - Systems and Network Administration

Lab Report of Mid Examination

2020/2021

R.P.T.W. Randunu
CS/2018/033

Contents

List of Figures

List of Tables

Mid Examination Lab Session – Inter-VLAN Routing

1.1 First Scenario of the Lab Session

1.1.1 IP Addressing Table of Devices

Table 1 - IP Addressing Table 1

Device Name	IP Address of the device	Subnet Mask of the device	Default Gateway
PC1	192.168.10.10	255.255.255.0	192.168.10.1
PC2	192.168.10.20	255.255.255.0	192.168.20.1
PC3	192.168.10.100	255.255.255.0	192.168.10.1
PC4	192.168.10.200	255.255.255.0	192.168.20.1

1.1.2 Topology

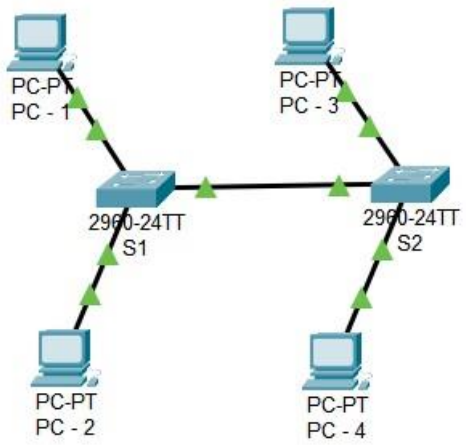

Figure 1 – Topology of first scenario

1.1.3 Set Up the network topology.

- **Step 1** – First we Set Up the devices, then cable them together as shown in Figure 1.
- **Step 2** – Then we Initialize the switches and then reload the switches.

1.1.4 Configure the PCs and verify the connectivity among them.

- **Step 3** – After reloading the switches we configure all the PCs according to the IP addressing table.

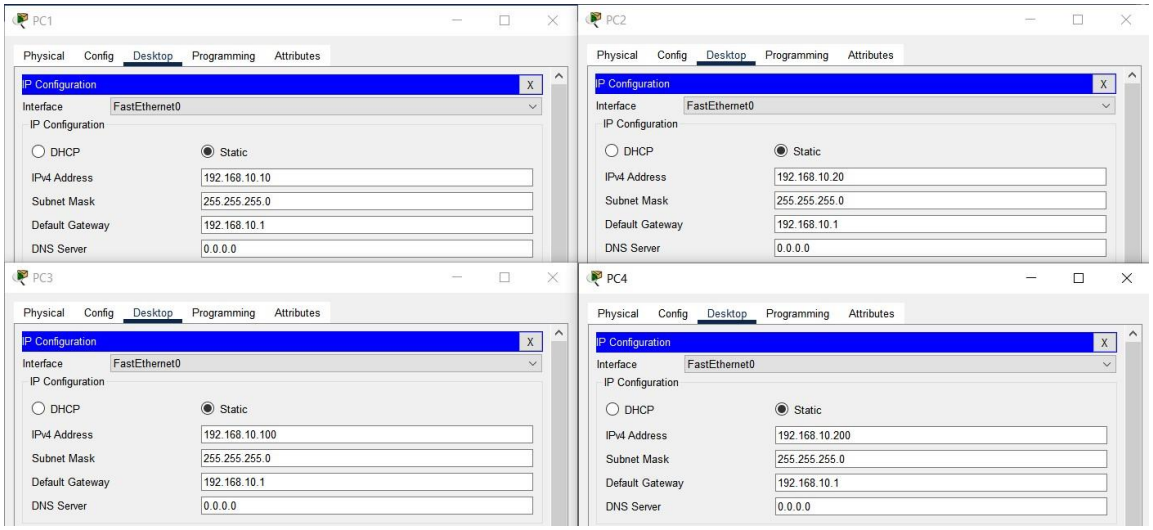

Figure 2 - IP Configurations of PCs

- **Step 4** – Then we verified all connectivity of all the PCs by giving ping commands. For that we send ping from PC1 to PC2, PC1 to PC3 and PC1 to PC4. Since it was successful, we were able confirm that each device is connected successfully. All the ping commands shown in the below figures.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.20

Pinging 192.168.10.20 with 32 bytes of data:

Reply from 192.168.10.20: bytes=32 time<1ms TTL=128
Reply from 192.168.10.20: bytes=32 time=4ms TTL=128
Reply from 192.168.10.20: bytes=32 time<1ms TTL=128
Reply from 192.168.10.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms

C:\>
```

Figure 3 - Ping PC1 to PC2

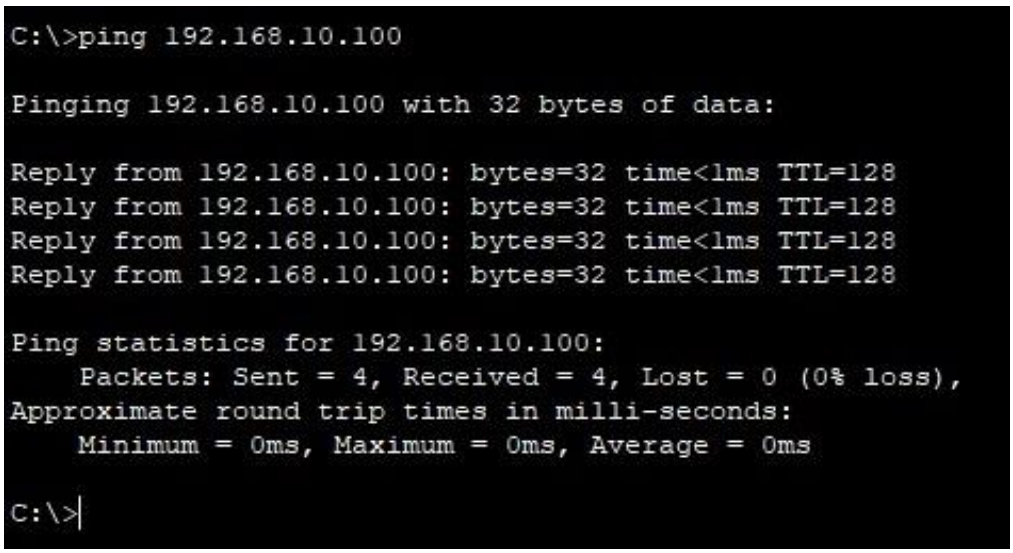

Figure 4 - Ping PC1 to PC3

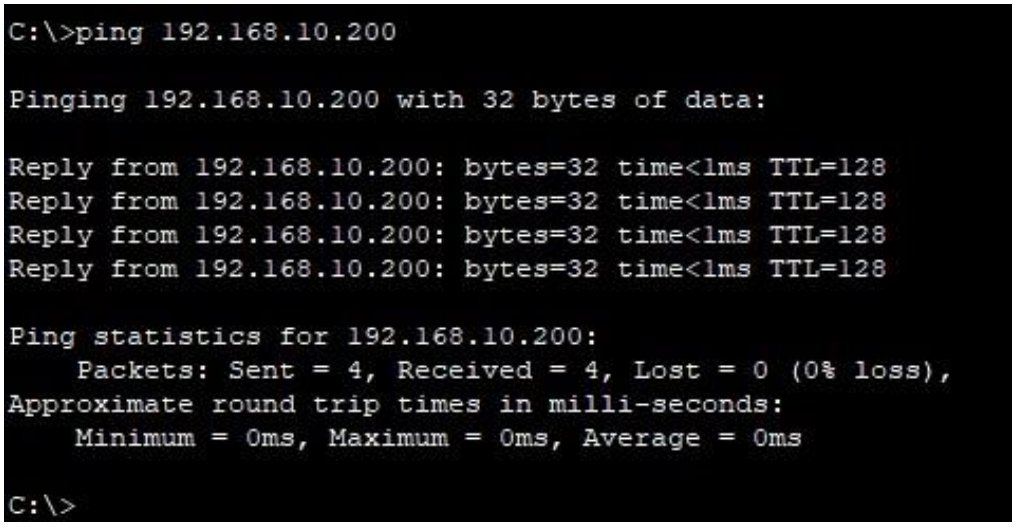

Figure 5 - Ping PC1 to PC4

1.2 Second scenario of the Lab Session

1.2.1 Topology

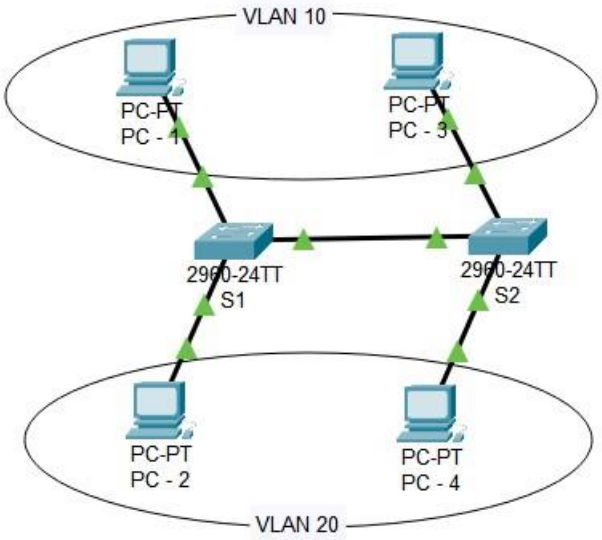

Figure 6 – Topology of second scenario

1.2.2 Configure both VLANs on Switch S1 and S2.

- **Step 1** – Connect switch S1 and PC1 by a console cable. Switches doesn't have interface to configure, so when ever we need to configure a switch, we connect the switch to pc or laptop via a console cable. Then we configure the switch with our pc or laptop. Console cable is light blue cable which can be identify easily.
- **Step 2** – After connecting the Switch to our PC we configure switch S1 then we configure switch S2. We did that at the same time. We configure switch S1 by PC1 and switch S2 by PC3.
- **Step 3** – When we configure the switch, first we use 'enable' command to activate 'EXEC' mode. Then we use 'configure terminal' command to activate 'config' mode, so we can change things like host name. And we can create VLANs in this mode.

```
Switch> enable
Switch#
Switch# config terminal
Switch(config)#
Switch(config)# hostname S1
S1(config)# no ip domain-lookup
```

- **Step 4** – Then we create our VLANs on switch S1. Then we gave names for the VLANs.

```
S1(config)#vlan 10
S1(config-vlan)#name VLAN-10
S1(config)#vlan 20
S1(config-vlan)#name VLAN-20
```

- **Step 5** – Then we did the same process to S2. Gave the same names for VLANs.

1.2.3 Configure interfaces of PCs to the correct VLAN

- **Step 6** – Then we Assigned switch ports to VLANs on switch S1.

```
S1(config)#interface fa0/1
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#interface fa0/2
S1(config-if-range)#switchport access vlan 20

S1#show vlan brief
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
10   VLAN0010                         active    Fa0/1
20   VLAN0020                         active    Fa0/2
```

- **Step 7** – Then we did the the same process to S2

1.2.4 Configure a Trunk port between switch S1 and S2.

```
S1(config)#interface fa0/3
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk allowed vlan 10,20

S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      1



Port        Vlans allowed on trunk
Fa0/3       10,20

Port        Vlans allowed and active in management domain
Fa0/3       10,20

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/3       10,20
```

- **Step 8** – Then we did the same process to S2

1.2.5 Check connectivity of the PCs

- **Step 9** – Give ping command from PC1 to PC3. Both of PC1 and PC2 are in the same VLAN.

  C:\>ping 192.168.10.100

  Pinging 192.168.10.100 with 32 bytes of data:

  Reply from 192.168.10.100: bytes=32 time=10ms TTL=128
  Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
  Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
  Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

  Ping statistics for 192.168.10.100:
  Packets: Sent = 4, Received = 4, Lost = 0 (0%
  loss), Approximate round trip times in milli-
  seconds:
  Minimum = 0ms, Maximum = 10ms, Average = 2ms

- **Step 10** – Then we gave ping command from PC1 to PC2. PC1 and PC2 are in different VLANs.

  C:\>ping 192.168.10.20

  Pinging 192.168.10.20 with 32 bytes of data:

  Request timed out.
  Request timed out.
  Request timed out.
  Request timed out.

  Ping statistics for 192.168.10.20:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

- **Step 11** – Packets didn't travel through different VLANs. So we connected the router.

1.3 Third Scenario of the Lab Session

1.3.1 Addressing Table

Table 2 – IP Addressing Table 2

Device Name	VLAN ID	IP Address of device	Subnet Mask of device	Default Gateway
R1	VLAN 10	192.168.10.1	255.255.255.0	N/A
	VLAN 20	192.168.20.1	255.255.255.0	N/A
PC1	VLAN 10	192.168.10.10	255.255.255.0	192.168.10.1
PC2	VLAN 20	192.168.20.20	255.255.255.0	192.168.20.1
PC3	VLAN 10	192.168.10.100	255.255.255.0	192.168.10.1
PC4	VLAN 20	192.168.20.200	255.255.255.0	192.168.20.1

- **Step 1** – Due to the connection of the router, we must change the IP addresses of the PCs. This matter is explained in the ‘Problem that occurred during the lab session’.

1.3.2 Topology

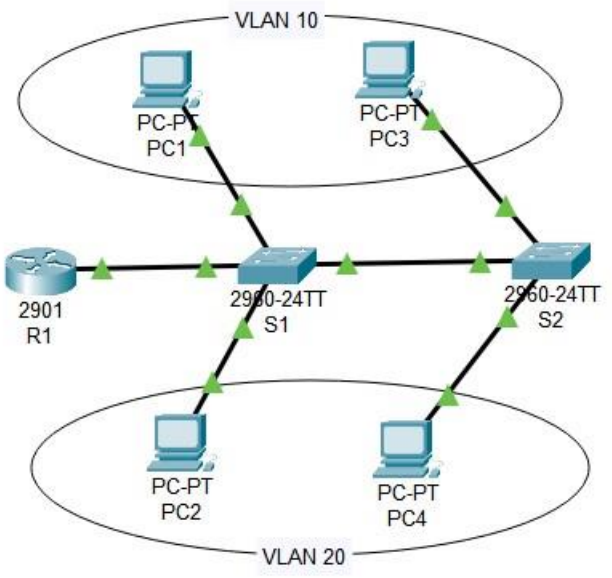

Figure 7 – Topology of third scenario

- **Step 2** – Connect the router R1 to the Network.

1.3.3 Configure a Trunk port that connects the router.

```
S1(config)#interface gig0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan 10,20
```

1.3.4 Configure sub-interfaces on router.

- **Step 3** – Connect the Router and PC1 by a console cable. Routers don't have graphical interface. So, if we want to configure a router, we must connect the router to our PC or laptop via console cable. After that we can configure the router through the PC or laptop.
- **Step 4** – After connecting the router to the PC by a console cable we Configured the Router. We use same console cable to configure the switches.
- **Step 5** – First we use 'enable' command to activate the 'EXEC' mode. Then we use 'configure terminal' command to activate 'config' mode, so we can change things like host name.

```
Router> enable
Router#
Router# config terminal
Router(config)#
Router(config)# hostname R1
R1(config)# no ip domain-lookup
```

- **Step 6** – Then we create sub-interfaces for Inter VLAN Routing. We did that while we are in the 'config' mode.

```
R1(config)#interface gig0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#interface gig0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
```

- **Step 7** – Then we 'State Up' the Router sub-interfaces.

```
R1(config)#interface gig0/0
R1(config-if)#no shutdown
```

(With 'no shutdown' command we can state up the ports of the router, if we want to down any port we can use 'shutdown' command).

- **Step 8** – Then we checked the connectivity of routing. With show IP route command.

```
R1#show ip route

Gateway of last resort is not set

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0.10
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0.20
```

1.3.5 Check the routing by pinging from each PC

- **Step 9** – Ping PC1 to PC3 which is in same VLAN.

```
C:\>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time=10ms TTL=128
Reply from 192.168.10.100: bytes=32 time=5ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms

C:\>
```

Figure 8 - Ping PC1 to PC3 - Same VLAN

- **Step 10** – Ping PC1 to PC2 which is in different VLAN.

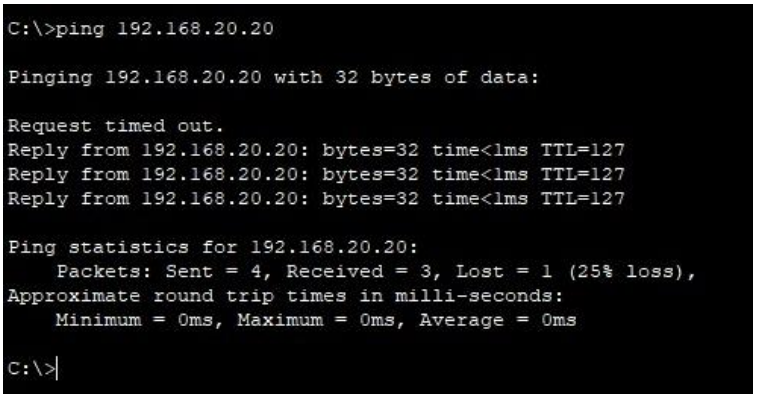

Figure 9 - Ping PC1 to PC2 - Different VLAN

- **Step 11** – Ping PC1 to PC4 which is in different VLAN.

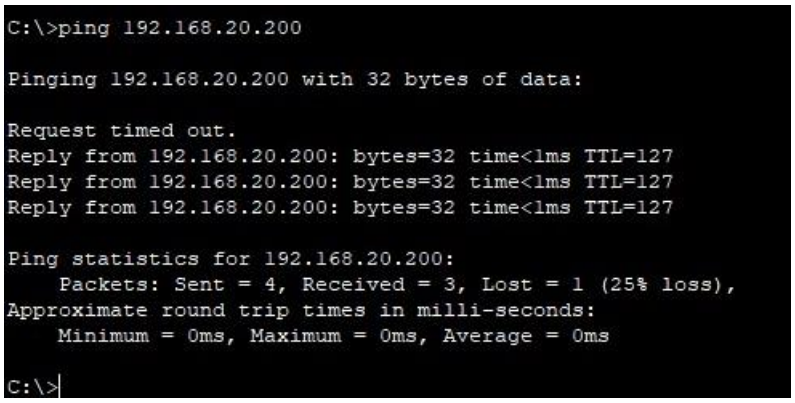

Figure 10 - Ping PC1 to PC4 - Different VLAN

- **Step 12** – Check the ping command with each PC and confirm success.

1.4 Problems that occurred during the Lab session

1.4.1 Inter-VLAN ping command failure

- Many modern PCs have built-in firewalls that are designed to protect the PC from external threats, and these firewalls may block incoming ping requests by default. As a solution for this problem, we had to disable Windows Defender Firewall manually on each PC. In the real world this solution does not suit well. Because the firewall can help to improve network security, prevent network congestion, and enforce network security policies.

1.4.2 VLAN interface configuration failure

- Traffic can be routed between the different VLANs by the router. When using a router on stick configuration, it is important to properly configure the VLAN interfaces on the router. This typically involves assigning each VLAN interface with an IP address and subnet mask and enabling routing on the router. If the VLAN interfaces are not properly configured, VLAN routing may not work properly. Firstly, we used IP addresses in the range of 192.168.100.0 – 192.168.100.255 for all configurations in this lab which is same and one network. Because VLAN routing doesn't work at all, and our sir was kind enough to show our mistake and troubleshoot this problem. Then we use 2 different networks. In the 1st and 2nd Scenarios we used the same network IP address for the two VLANs. But in the 3rd Scenario that does not work due to the connection of the router. For the router the two VLANs should be in separate networks. So as the solution we configured the PCs of the two VLANs with different network IP addresses.

1.5 Important Points that I learned from the Lab Session

- The purpose and benefits of using a router on stick configuration in a network.
- The steps involved in setting up and configuring a router on stick configuration.
- The limitations and potential issues that can arise when using a router on stick configuration.
- How to troubleshoot common problems with a router on stick configuration.
- The importance of proper planning, design, and configuration in ensuring the success of a router on stick configuration.
- The value of hands-on experience in learning about network technologies and concepts.

1.6 Conclusion

- After conducting the experiment on inter-VLAN routing, it can be concluded that interVLAN routing is an effective method for allowing communication between different VLANs within a network. In conclusion, a router on stick configuration is a networking setup where a single router is connected to a switch using a single Ethernet cable, or "stick." This allows the router to route traffic between multiple network segments that are connected to the switch, providing inter-VLAN routing capabilities. The decision to use a router on stick configuration in a network will depend on the specific requirements and constraints of the network. In some cases, a router on stick configuration may be the best option due to its simplicity, cost effectiveness, and flexibility. In other cases, a dedicated layer 3 switch may be a better option due to its higher performance and scalability.

1.7 References

[1] "Inter-VLAN Routing," catchpoint, [Online]. Available: https://www.catchpoint.com/network-admin-guide/inter-vlanrouting#:~:text=Inter%2DVLAN%20routing%20is%20the,2%20based%20on%20MAC%20 addresses..

[2] E. Harmoush, "Routing Between VLANs & Layer 3 Switches," Practical Networking, 30 August 2022. [Online]. Available: https://www.practicalnetworking.net/standalone/routing-between-vlans/.