Enterprise Network Design Analysis Report

Prepared By : Bihanga Rathnayaka
Date : 2024.10.28

Contents

1. Introduction

This report demonstrates the practical application of network design concepts and protocols by analyzing and configuring the network models using Cisco Packet Tracer. The objective of this report is to highlight the understanding of network structures, through constructing a network with dynamic routing, implementing VLAN configurations and by evaluating Layer 2 and Layer 3 addresses at router interfaces.

2. Task 1 – SMTP protocol Analysis

2.1 Introduction to SMTP protocol

Sending an email is the most common thing in the present world but that requires some protocols. The Simple Mail Transfer Protocol (SMTP) is the primary protocol used for sending emails in most of the cases (Riabov, 2006). It establishes a Transmission Control Protocol (TCP) connection between client and server, allowing data of the email to be exchanged in a reliable way. SMTP makes communication between mail servers by allowing them to transfer messages between users on different networks (Klensin, 2008).

2.2 Purpose and the Functionality of SMTP protocol

As mentioned above, the primary purpose of the SMTP protocol is to facilitate the reliability and transmission efficiency of emails. When operating at the TCP/IP models' application layer, SMTP establishes a connection between an email client and a server to send a message, typically via the port 25 (Riabov, 2006). The SMTP client sends a set of commands to the server to start a session, and the server replies with status codes to show faults and confirm whether the process was successful or not. Effective mail sending and receiving is made possible by the smooth communication between mail servers made possible by the SMTP request-response technology.

Also SMTP supports the transmission of various data types through extensions like Multipurpose Internet Mail Extensions (MIME), which allows emails to include multimedia content such as images and audio files (Klensin, 2008). This flexibility of SMTP makes it more integral to the modern email system. Because of efficient management of message routing and addressing of potential delivery failures, SMTP ensures that communication between emails remain consistent and dependable across diverse network environments (GeeksForGeeks, 2024). The SMTP mechanism offers a solid foundation for electronic communication by offering a stable framework for email exchange.

3. Task 2 – Network Design and Plan

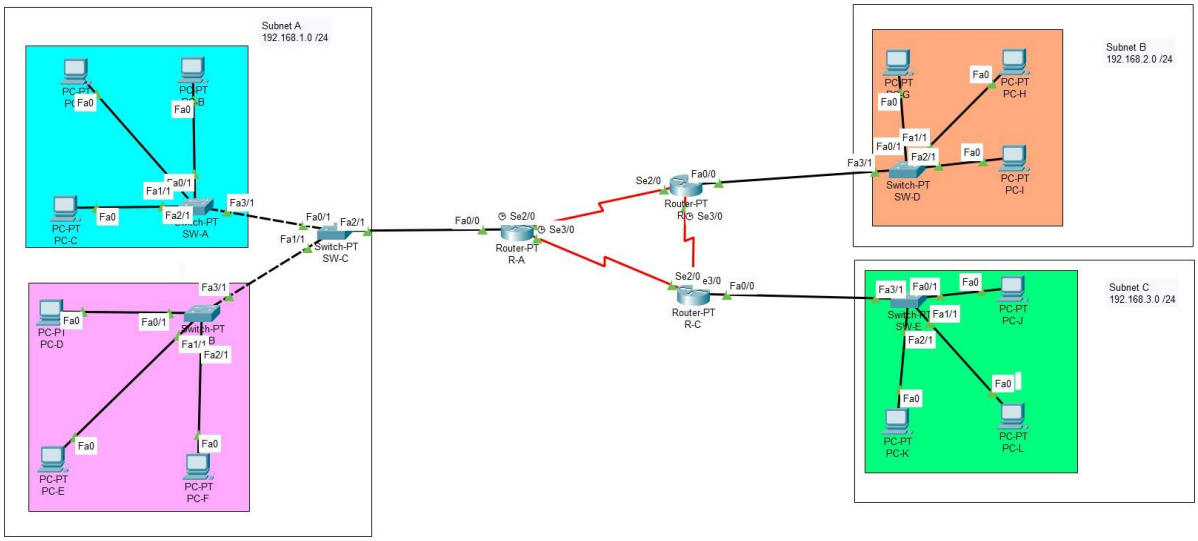


Figure 1 - Network Topology

3.1 IP ranges of Subnets

The following table depicts the IP ranges, and the subnet masks used for each of the subnets.

Table 1 - IP ranges of Subnets

Subnet	Network Address	Subnet Mask	IP range	Proofs
Subnet A	192.168.1.0	255.255.255.0	192.168.1.1 – 192.168.1.254	Figure 2
Subnet B	192.168.2.0	255.255.255.0	192.168.2.1 – 192.168.2.254	Figure 3
Subnet C	192.168.3.0	255.255.255.0	192.168.3.1 – 192.168.3.254	Figure 4

```
Router#show ip dhcp pool

Pool A_POOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 6
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.1          192.168.1.1      - 192.168.1.254     6    / 0     / 254
```

Figure 2 - IP range of Subnet A

```
Router#show ip dhcp pool

Pool B_POOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 3
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.2.1          192.168.2.1      - 192.168.2.254     3    / 0     / 254
```

Figure 3 - IP range of Subnet B

```
Router#show ip dhcp pool

Pool C_POOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 3
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.3.1          192.168.3.1      - 192.168.3.254     3    / 0     / 254
```

Figure 4 - IP range of Subnet C

Why were the above IP ranges chosen?

1. Because when using an adjoining IP range, the network can be easily documented and managed.
2. Because each subnet provides 254 usable IP addresses, the network can be easily expanded.

3. Because 192.168.0.0 range is within the private IP space, internal networks can be configured without using global routable addresses.

3.2 Routing between Subnets

The Open Shortest Path First (OSPF) protocol was selected for routing between subnets.

OSPF was chosen as the protocol for routing between subnets because of the following reasons.

1. OSPF helps to scale well with larger networks and supports hierarchical designs with multiple areas (Agarwal et al., 2023). Even though this network is not much complex, OSPF provides flexibility to future expansions.
2. OSPF helps for faster coverage than distance-vector protocols like RIP. If a network change occurs, OSPF will quickly recalculate the routes for faster routing between networks (Majid & Fuada, 2020).
3. OSPF sends updates only when there is a change in the network. This helps to conserve the bandwidth when compared with the periodic updates used by RIP(Majid & Fuada, 2020).

Given below the proofs of configurations of routing between subnets using OSPF protocol.

```
Router#show ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    10.0.0.0 0.0.0.3 area 0
    10.0.0.4 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.1           110      00:09:10
    192.168.2.1           110      00:09:10
    192.168.3.1           110      00:09:10
  Distance: (default is 110)
```

Figure 5 - OSPF in Router A

```
Router#show ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.2.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.2.0 0.0.0.255 area 0
    10.0.0.0 0.0.0.3 area 0
    10.0.0.8 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.1           110      00:11:18
    192.168.2.1           110      00:11:18
    192.168.3.1           110      00:11:18
  Distance: (default is 110)
```

Figure 6 - OSPF in Router B

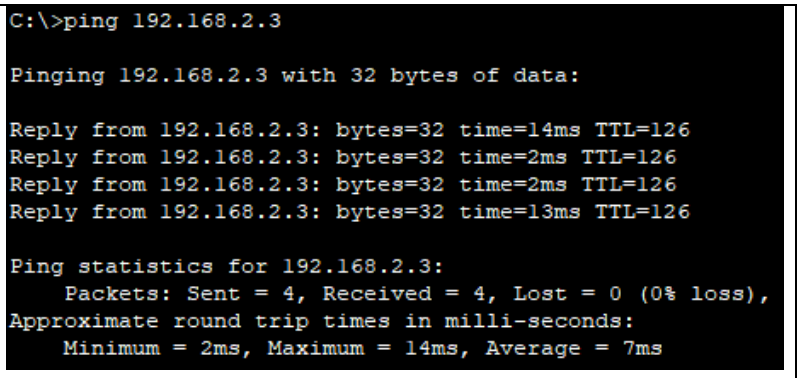
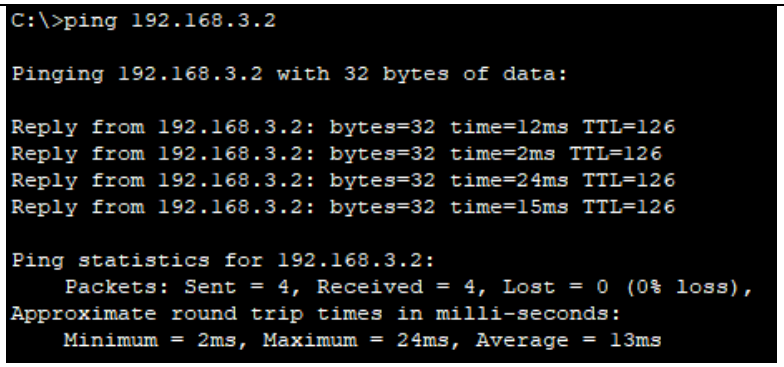
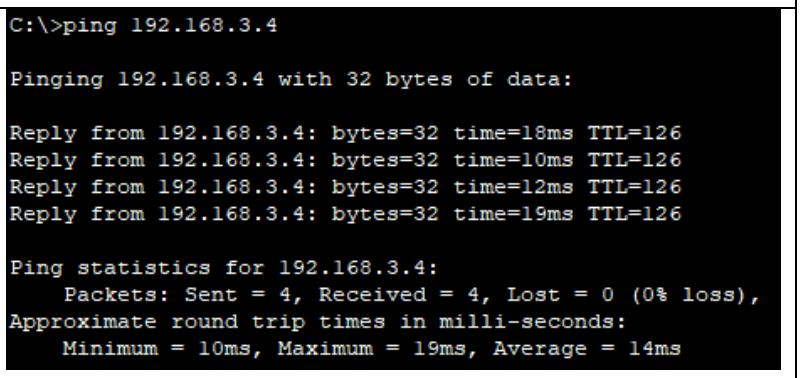
```
Router#show ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.3.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.3.0 0.0.0.255 area 0
    10.0.0.4 0.0.0.3 area 0
    10.0.0.8 0.0.0.3 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.1.1           110      00:12:20
    192.168.2.1           110      00:12:20
    192.168.3.1           110      00:12:20
  Distance: (default is 110)
```

Figure 7 - OSPF in Router C

3.3 Network Behavior Analysis with Simulation

Table 2 - Ping of Intra Subnets and Inter Subnets

Type of the ping	Source	Destination	Status
Intra Subnet ping – Subnet A	PC-A 192.168.1.5	PC-E 192.168.1.6	Cisco Packet Tracer PC Command Line 1.0 C:\>ping 192.168.1.6 Pinging 192.168.1.6 with 32 bytes of data: Reply from 192.168.1.6: bytes=32 time=1ms TTL=128 Reply from 192.168.1.6: bytes=32 time=1ms TTL=128 Reply from 192.168.1.6: bytes=32 time<1ms TTL=128 Reply from 192.168.1.6: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.1.6: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms
Intra Subnet ping – Subnet B	PC-G 192.168.2.4	PC-I 192.168.2.3	Cisco Packet Tracer PC Command Line 1.0 C:\>ping 192.168.2.3 Pinging 192.168.2.3 with 32 bytes of data: Reply from 192.168.2.3: bytes=32 time<1ms TTL=128 Reply from 192.168.2.3: bytes=32 time<1ms TTL=128 Reply from 192.168.2.3: bytes=32 time<1ms TTL=128 Reply from 192.168.2.3: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.2.3: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
Intra Subnet ping – Subnet C	PC-J 192.168.3.3	PC-K 192.168.3.4	Cisco Packet Tracer PC Command Line 1.0 C:\>ping 192.168.3.4 Pinging 192.168.3.4 with 32 bytes of data: Reply from 192.168.3.4: bytes=32 time<1ms TTL=128 Reply from 192.168.3.4: bytes=32 time<1ms TTL=128 Reply from 192.168.3.4: bytes=32 time<1ms TTL=128 Reply from 192.168.3.4: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.3.4: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms

Inter Subnet ping (Subnet A – Subnet B)	PC-C 192.168.1.2	PC-I 192.168.2.3	
Inter Subnet ping (Subnet A – Subnet C)	PC-D 192.168.1.3	PC-L 192.168.3.2	
Inter Subnet ping (Subnet B – Subnet C)	PC-H 192.168.2.2	PC-K 192.168.3.4	

3.3.1 Simulation Analysis of sending a message between PC-A to PC-H

The following figure depicts the simulation of sending a message between PC-A and PC when there is a link between Router A and Router B.

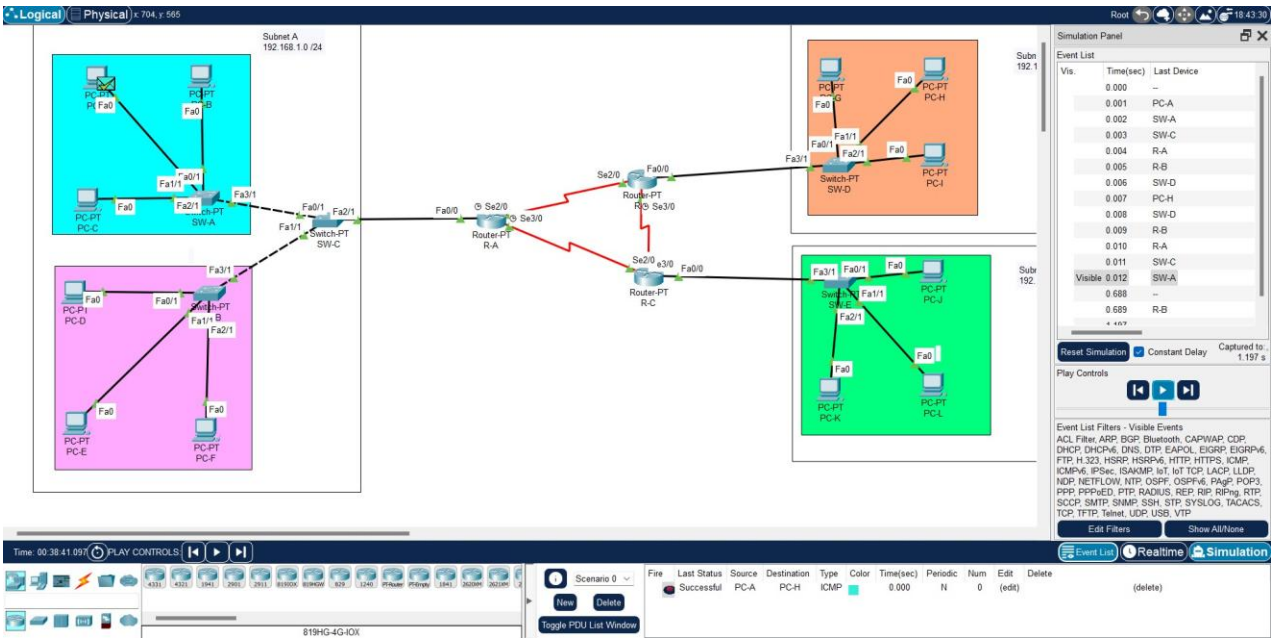


Figure 8 - Sending a message from PC-A to PC-H

The following figure depicts the simulation of sending a message between PC-A and PC-H when link between Router A and Router B is disabled.

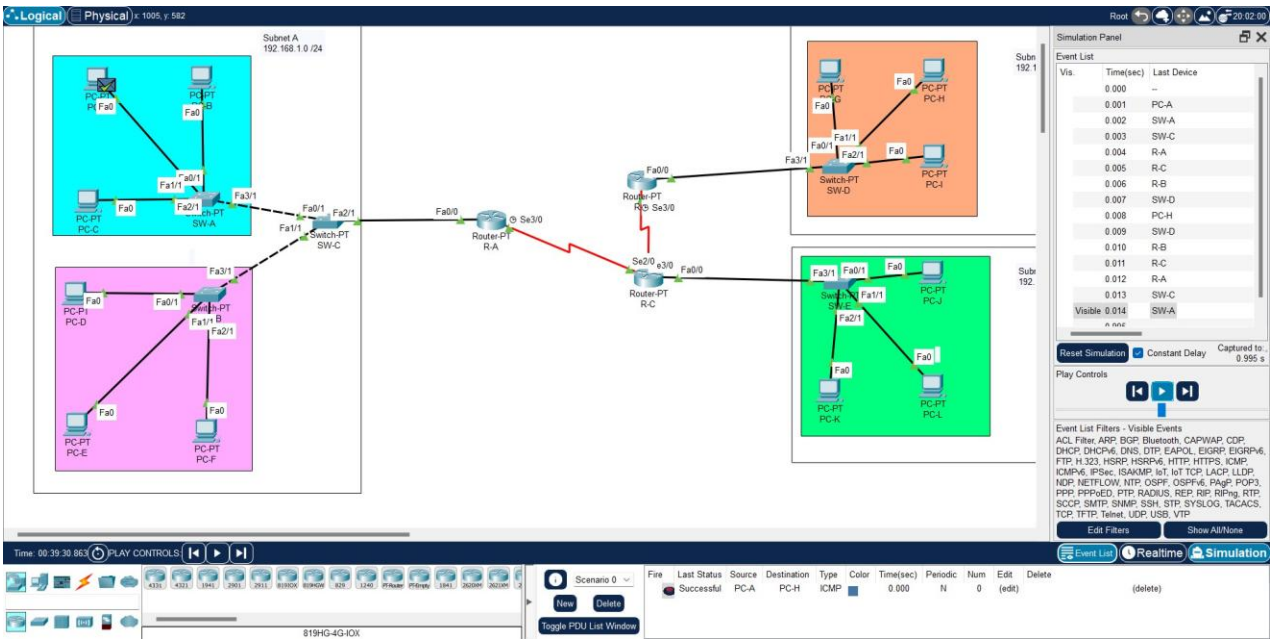


Figure 9 - Sending a message from PC-A to PC-H

The following figure depicts the event list of sending a message between PC-A and PC-H when link between Router A and Router B is disabled.

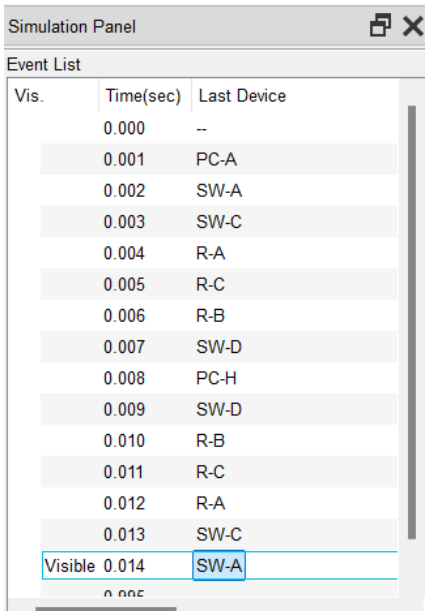


Figure 10 - Event list of sending message from PC-A to PC-H without R-A and R-B link

As in figure 8, when sending a message from PC-A to PC-H, the packet travels through Router-A to Router-B based on OSPF routing. When observe the simulation mode, the packet successfully delivered from PC-A to Router-A, then from Router-A to Router-B and finally to the PC-H.

But when the link between Router-A and Router-B is disabled, the packet travels through the Router-A to Router-C because OSPF recalculate and finds an alternative path for the packet. It can be clearly observed through figure 10. This demonstrates the flexibility of the OSPF protocol. Also, the communication between PC-A to PC-H remained intact because of this rerouting.

3.3.2 Shortcomings of the Network Design

When sending the message from PC-A to PC-H, if the path between Router-A to Router C also fails, then there would be no connection between the Subnet A and Subnet B. Therefore, implementing redundant links or additional routers can be helpful to improve the reliability of the network.

Also, when the direct link between Router-A and Router-B fails, all the traffic from Subnet A to Subnet B must pass through the Router-C, this can result in an increase of traffic load on Router-C. So, this network design might not be most suitable for networks with high traffic load.

4. Task 3 – (OSI) Layer 2 Implementation and Analysis

4.1 Introduction to VLAN

A Virtual Local Area Network (VLAN) is a technology that divides a physical network into multiple, isolated virtual networks. In VLAN even if the devices are connected to the same physical switch, they are grouped into different logical networks, which behave as if they are on separate switches. This isolation in VLAN enhances the security of the network by restricting broadcast traffic and limiting sensitive data.

VLAN can also be used to simplify network management by allowing devices to be grouped into different networks based on function, department, or application, regardless of their physical location. This flexibility of VLAN is useful to reassign users to different networks or implement access control. Also, VLAN can be used to better utilize resources by dividing large networks into small manageable units.

4.2 Configuration of VLAN

The following table depicts the IP ranges and the masks for each subnet.

Subnet	Network Address	Subnet Mask
VLAN 75	192.168.10.128	255.255.255.192
VLAN 150	192.168.10.192	255.255.255.192
VLAN 225	192.168.10.0	255.255.255.128

The following figures depict the VLAN configurations on switches and the router.

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa4/1, Fa5/1
75   VLAN_75                          active    Fa1/1
150  VLAN_150                         active    Fa0/1, Fa2/1
225  VLAN_225                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 11- VLAN brief of SW-A

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa4/1, Fa5/1
75   VLAN_75                          active    Fa0/1, Fa2/1
150  VLAN_150                         active    Fa1/1
225  VLAN_225                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 12- VLAN brief of SW-B

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa4/1, Fa5/1
75   VLAN_75                          active
150  VLAN_150                         active
225  VLAN_225                         active    Fa3/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Figure 13- VLAN brief of SW-C

According to the above figures 11,12 and 13, it is clear that PC-A, PC-D and PC-F are assigned to the VLAN 75 and all the other PCs are assigned to VLAN 150. The laptops which are connected to the access point are assigned to the VLAN 225.

```
Router#show ip dhcp pool

Pool A_POOL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.1.1          192.168.1.1      - 192.168.1.254     0    / 0     / 254

Pool VLAN75 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 3
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.10.129       192.168.10.129   - 192.168.10.190    3    / 0     / 62

Pool VLAN_75 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 0
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.10.129       192.168.10.129   - 192.168.10.190    0    / 0     / 62

Pool VLAN_150 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 62
 Leased addresses               : 3
 Excluded addresses             : 0
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.10.193       192.168.10.193   - 192.168.10.254    3    / 0     / 62

 Pool VLAN_225 :
  Utilization mark (high/low)    : 100 / 0
  Subnet size (first/next)       : 0 / 0
  Total addresses                : 126
  Leased addresses               : 2
  Excluded addresses             : 0
  Pending event                  : none

  1 subnet is currently in the pool
  Current index        IP address range                      Leased/Excluded/Total
  192.168.10.1         192.168.10.1     - 192.168.10.126     2    / 0     / 126
```

Figure 14- VLAN DHCP pool of R-A

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet0/0.75     192.168.10.129  YES manual up                    up
FastEthernet0/0.150    192.168.10.193  YES manual up                    up
FastEthernet0/0.225    192.168.10.1    YES manual up                    up
FastEthernet1/0        unassigned      YES unset  administratively down down
Serial2/0              10.0.0.1        YES manual up                    up
Serial3/0              10.0.0.5        YES manual up                    up
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
```

Figure 15- IP interface brief of R-A

```
Router#show ip protocol

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.193
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.0 0.0.0.255 area 0
    10.0.0.0 0.0.0.3 area 0
    10.0.0.4 0.0.0.3 area 0
    192.168.10.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.1           110      00:03:45
    192.168.3.1           110      00:03:46
    192.168.10.193        110      00:03:44
  Distance: (default is 110)
```

Figure 16- IP protocol used in R-A

According to the above figures 14,15 and 16, how routers are configured and how the DHCP is set up can be clearly seen. So, when configuring router for the sub interfaces router-on-a-stick configuration was used. Using that a single physical interface fa0/0 was used to create multiple sub interfaces associated with VLANs. In this case, the router R-A connected to the switch that hosts the VLANs are using a trunk port. For each VLAN sub interfaces were created on the main physical interface. Each subnet was tagged with a corresponding VLAN ID and an assigned IP address as below.

Fa0/0.75 → Assigned to VLAN 75 with IP 192.168.1.1/26
Fa0/0.150 → Assigned to VLAN 150 with IP 192.168.1.65/26
Fa0/0.225 → Assigned to VLAN 225 (Wi-Fi) with IP 192.168.1.129/25

And OSPF protocol was used for routing between the VLANs to enable dynamic routing between the subnets created for each VLAN.

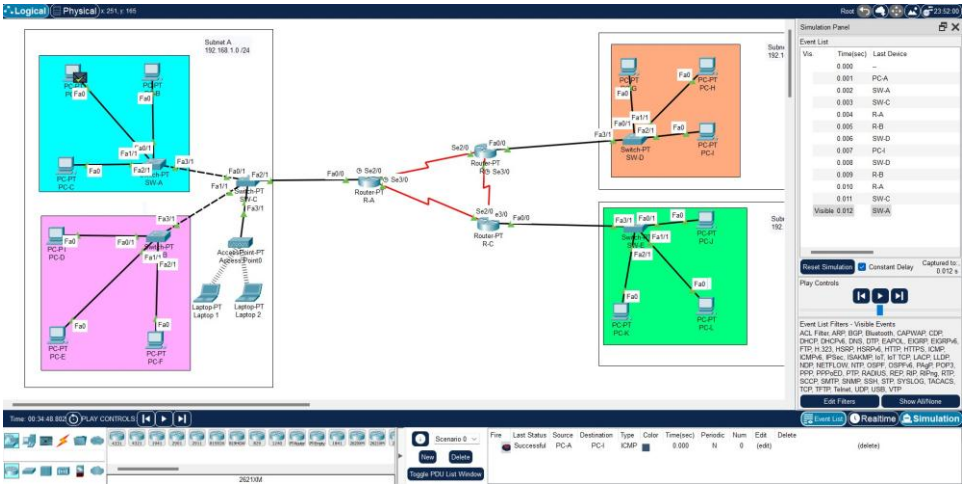
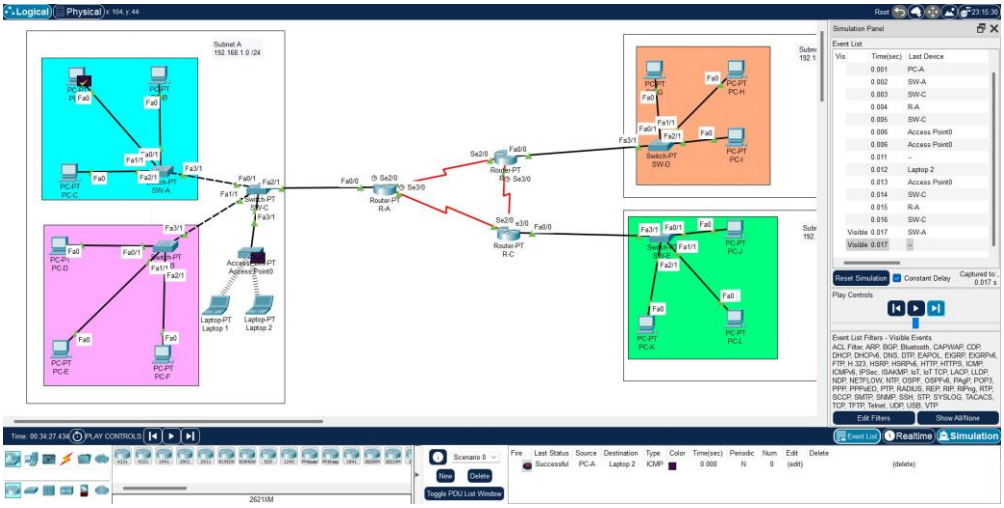
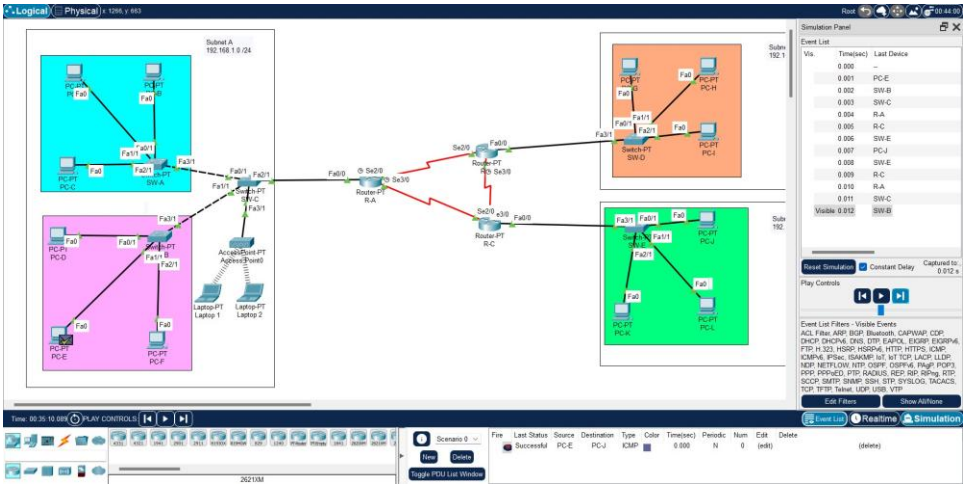
4.3 Checking connectivity within the same and different VLANs

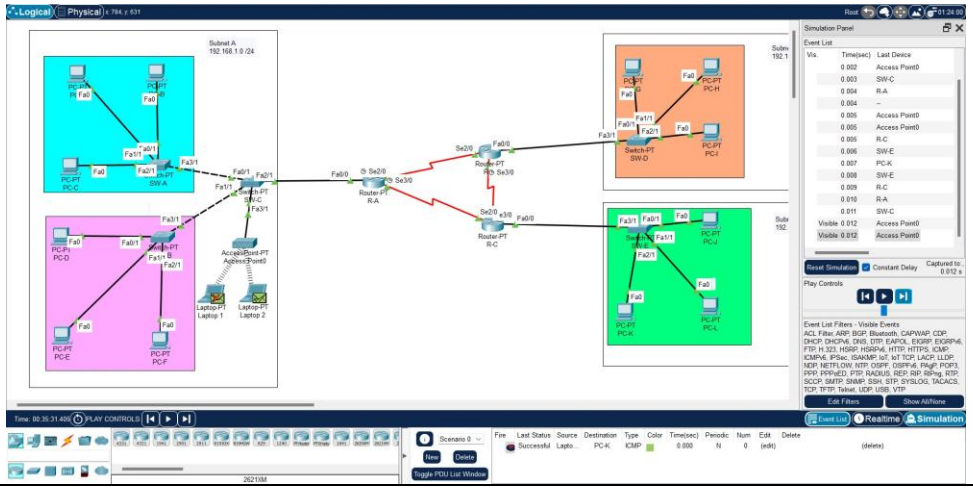
Table 3- Ping between inter and intra VLANs

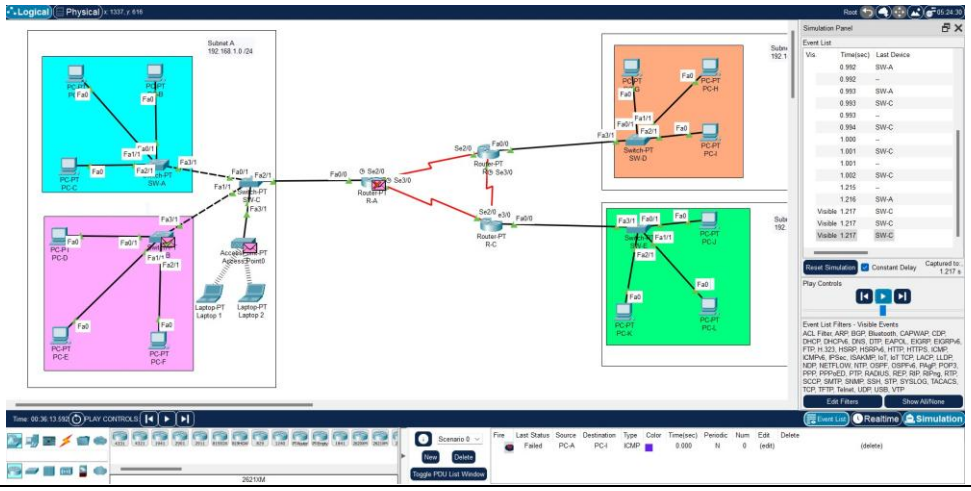
Type of the ping	Source	Destination	Status
Intra VLAN ping – VLAN 75	PC-A 192.168.10.131	PC-F 192.168.10.130	Cisco Packet Tracer PC Command Line 1.0 C:\>ping 192.168.10.130 Pinging 192.168.10.130 with 32 bytes of data: Reply from 192.168.10.130: bytes=32 time<1ms TTL=128 Reply from 192.168.10.130: bytes=32 time<1ms TTL=128 Reply from 192.168.10.130: bytes=32 time=6ms TTL=128 Reply from 192.168.10.130: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.10.130: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 6ms, Average = 1ms
Intra VLAN ping – VLAN 150	PC-C 192.168.10.196	PC-E 192.168.10.195	Cisco Packet Tracer PC Command Line 1.0 C:\>ping 192.168.10.195 Pinging 192.168.10.195 with 32 bytes of data: Reply from 192.168.10.195: bytes=32 time<1ms TTL=128 Reply from 192.168.10.195: bytes=32 time<1ms TTL=128 Reply from 192.168.10.195: bytes=32 time<1ms TTL=128 Reply from 192.168.10.195: bytes=32 time<1ms TTL=128 Ping statistics for 192.168.10.195: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
Intra VLAN ping – VLAN 225	Laptop 1 192.168.10.3	Laptop 2 192.168.10.2	Cisco Packet Tracer PC Command Line 1.0 C:\>ping 192.168.10.2 Pinging 192.168.10.2 with 32 bytes of data: Reply from 192.168.10.2: bytes=32 time=54ms TTL=128 Reply from 192.168.10.2: bytes=32 time=26ms TTL=128 Reply from 192.168.10.2: bytes=32 time=24ms TTL=128 Reply from 192.168.10.2: bytes=32 time=18ms TTL=128 Ping statistics for 192.168.10.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 18ms, Maximum = 54ms, Average = 30ms

Inter Subnet ping (VLAN 75 – VLAN 150)	PC-D 192.168.10.132	PC-B 192.168.10.194	C:\>ping 192.168.10.194 Pinging 192.168.10.194 with 32 bytes of data: Reply from 192.168.10.194: bytes=32 time<1ms TTL=127 Reply from 192.168.10.194: bytes=32 time<1ms TTL=127 Reply from 192.168.10.194: bytes=32 time<1ms TTL=127 Reply from 192.168.10.194: bytes=32 time<1ms TTL=127 Ping statistics for 192.168.10.194: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms
Inter Subnet ping (VLAN 75 – VLAN 225)	PC-F 192.168.10.130	Laptop 2 192.168.10.2	C:\>ping 192.168.10.2 Pinging 192.168.10.2 with 32 bytes of data: Reply from 192.168.10.2: bytes=32 time=10ms TTL=127 Reply from 192.168.10.2: bytes=32 time=19ms TTL=127 Reply from 192.168.10.2: bytes=32 time=16ms TTL=127 Reply from 192.168.10.2: bytes=32 time=19ms TTL=127 Ping statistics for 192.168.10.2: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 10ms, Maximum = 19ms, Average = 16ms
Inter Subnet ping (VLAN 150 – VLAN 225)	PC-C 192.168.10.196	Laptop 1 192.168.10.3	C:\>ping 192.168.10.3 Pinging 192.168.10.3 with 32 bytes of data: Reply from 192.168.10.3: bytes=32 time=19ms TTL=127 Reply from 192.168.10.3: bytes=32 time=1ms TTL=127 Reply from 192.168.10.3: bytes=32 time=15ms TTL=127 Reply from 192.168.10.3: bytes=32 time=21ms TTL=127 Ping statistics for 192.168.10.3: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 21ms, Average = 14ms

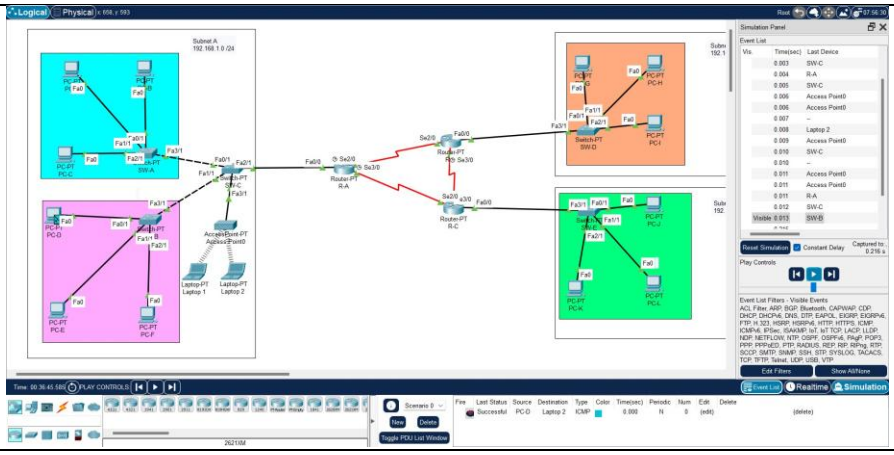
Table 4- Analysis of ping between VLANs

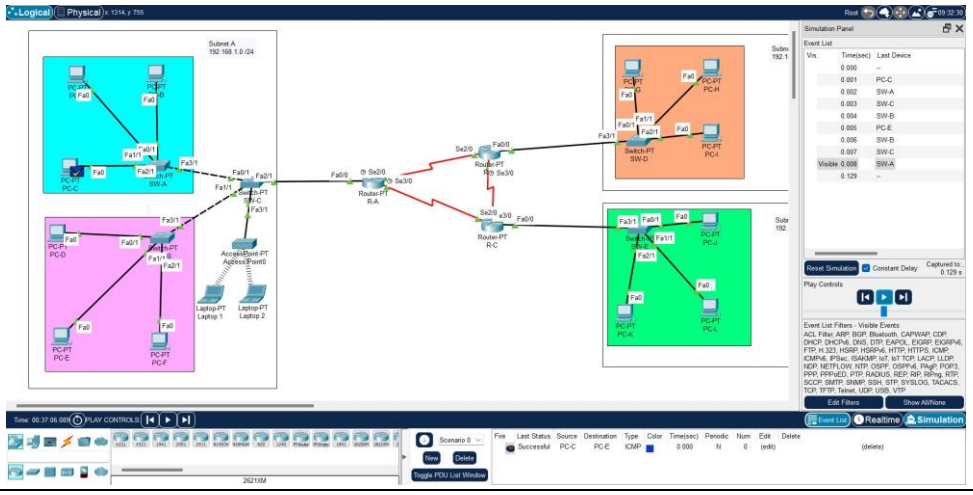
Ping	Status	Why successful or failed?
VLAN 75 to subnet B	Successful 	Because different VLANs can communicate via the router's inter-VLAN routing configuration
VLAN 75 to VLAN 225	Successful 	Because different VLANs can communicate via the router's inter-VLAN routing configuration
VLAN 150 to Subnet C	Successful 	Because different VLANs can communicate via the router's inter-VLAN routing configuration

VLAN 225 to Subnet C	Successful 	Because different VLANs can communicate via the router's inter-VLAN routing configuration

VLAN 75 to subnet B	Failed
	`Router(config)#interface fa0/0.75`
	`Router(config-subif)#shutdown`
	
	`Router(config-subif)#`
	`%LINK-5-CHANGED: Interface FastEthernet0/0.75, changed state to administratively down`
	
	`%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.75, changed state to down`
	 
		Because of the lack of OSPF redundancy, the connection between VLAN 75 and Subnet B fails when interface fa0/0.75 disables.

VLAN 75 to VLAN 225	Successful
	`Router(config-subif)#interface f0/0.150`
	`Router(config-subif)#shutdown`
	
	`Router(config-subif)#`
	`Router(config-subif)#`
	`%LINK-5-CHANGED: Interface FastEthernet0/0.150, changed state to administratively down`
	
	`%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.150, changed state to down`
		Because of the OSPF updates and reroutes, even though router interface f0/0.150 disables communication between VLAN 75 and VLAN 225 still carries on.

VLAN 150 to VLAN 150	Successful
	`Router(config-subif)#interface fa0/0.150`
	`Router(config-subif)#shutdown`
	
	`Router(config-subif)#`
	`%LINK-5-CHANGED: Interface FastEthernet0/0.150, changed state to administratively down`
	
	`%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.150, changed state to down`
	 
		Because of the OSPF updates and reroutes, even though router interface f0/0.150 disables communication between VLAN 75 and VLAN 225 still carries on.

4.4 Shortcomings of the Network Design

1. In this design, inter VLAN routing is heavily based on Router-A. So, if that fails, inter-VLAN communication also would fail completely. Therefore, to avoid that implementation of redundant routers for inter VLAN routing are recommended.

2. Since this design uses Router-on-a-Stick configuration, all VLAN traffic Is going through a single physical interface of the router. This interface may become a bottleneck if a larger amount of inter VLAN traffic is required. So, as the traffic grows, router's physical link might not be able to handle the bandwidth. Therefore, the bandwidth of the trunk links must increase to improve the network design.

3. The current network design is scalable to a certain extent, yet there are limitations. Adding more VLANs using Router-on-a-Stick could limit router resources, so adding a layer 3 switch or an additional router is a most recommended method to improve the performance of the network. Also, the subnet expansion must be planned carefully to avoid any reconfiguration issues as the network grows.

5. Task 4 – (OSI) Layer 2 & 3 Evaluation

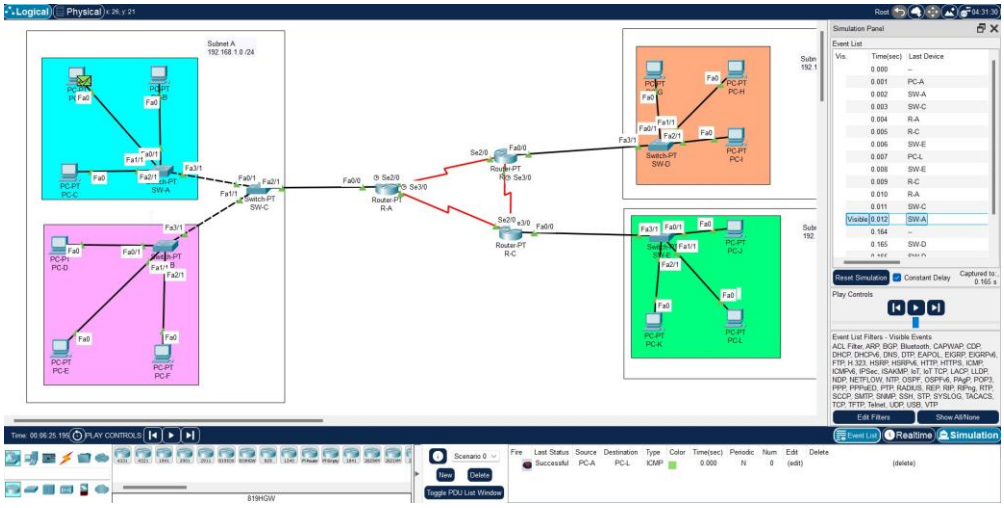


Figure 17- Ping from PC-A to PC-L

Layer 2 (L2) addresses are represented by the MAC addresses in Ethernet networks, and they are used for communication thin the same local network segment.

Layer 3 (L3) addresses are the IP addresses, which are used to route data packets across different networks.

5.1 Simulation Analysis

Initial packet flow from PC-A to R-A

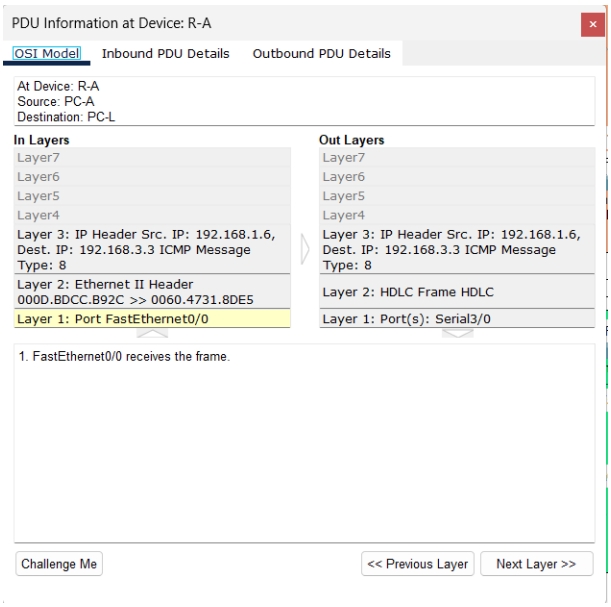


Figure 18- Packet flow from PC-A to R-A

1. Ingress on R-A

Layer 3 – The IP header of the packet shows the source IP as 192.168.1.6 (PC-A) and the IP of the destination as 192.168.3.3 (PC-L), identifying the endpoints of the communication.
Layer 2 – The Ethernet II header shows the MAC address as 0000.BDCC.B92C (PC-A) and the MAC address of the destination as 0060.4731.8DE5 (interface MAC on R-A). These MAC addresses are valid only within the local network segment connecting PC-A to R-A.

2. Egress on R-A
   Layer 3 – The IP addresses of the source and destination remains same, ensuring the continuity of end-to-end routing.
   Layer 2 – The Layer 2 encapsulation changes to an HDLC frame on the serial3/0 interface. This occurs because HDLC is typically used on point to point of WAN links. The MAC addresses are removed, because HDLC does not use MAC addressing.

Packet flow from R-A to R-C

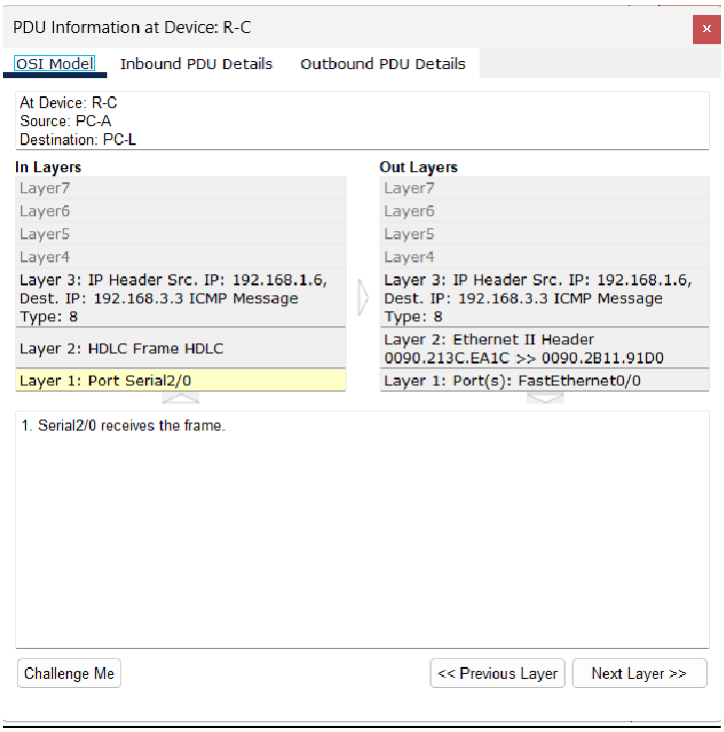


Figure 19- Packet flow from R-A to R-C

1. Ingress on R-C
   Layer 3 – The IP header continues to show the source as 192.168.1.6 and the destination as 192.168.3.3
   Layer 2 – The incoming frame is encapsulated in HDLC, matching the format expected on serial interfaces between routers.

2. Egress on R-C

Layer 3 – The IP header remains unchanged, with source IP as 192.168.1.6 and destination IP as 192.168.3.3
Layer 2 – The packet is re-capsulated in an Ethernet II frame for transmission on the fa0/0 interface. The new source MAC address is 0090.213C.EA1C (interface on R-C) and the destination MAC address is 0090.2B11.91D0, which is the MAC addresses of the switch E.

According to the above information about the simulation analysis, the summary of the findings is as follows,

Layer 3 Addressing – When the data packet travels from PC-A to PC-L the IP addresses remain unchanged. This is because the IP addressing operating at L3 provides end-to-end routing. Routers use these addresses to forward packets preserving the original source and destination addresses.

Layer 2 Addressing – At each router interface, L2 addresses are updated based on the type of the network segment,

- On Ethernet segments, MAC addresses are used to identify the source and destination within the local network segment.
- On serial links, HDLC is used instead of MAC addresses, as these point-to-point links do not require unique MAC addresses for each device.

Each router removes the incoming header of L2 and applied a new header based on the interface type of the outgoing. This ensures compatibility with the specific link or medium being used.

6. Reflection of the assignment

This assignment improved the understanding of how to configure a network with DHCP protocol and VLAN. The most challenging part was the configuration of VLAN subnets, as it was trickier. To manage that breaking it down into a step-by-step configuration was helpful to accomplish the task. So, when considering about the overall gain of this assignment, it improved the analyzing and evaluating of a network and was able to gain knowledge on how to formulate a network design in small scale and how to expand it.

7. References

Agarwal, A., Sharma, S., & Xavier, E. T. (2023). Performance Evaluation of HSRP and GLBP Over OSPF and RIP Routing Protocols. In (pp. 173-186). Springer Nature Singapore. https://doi.org/10.1007/978-981-99-1312-1_14

GeeksForGeeks. (2024). *Simple Mail Transfer Protocol (SMTP)*. https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp/

Klensin, J. (2008). Simple Mail Transfer Protocol. *RFC 5321*. https://www.rfc-editor.org/rfc/pdfrfc/rfc5321.txt.pdf

Majid, N. W. A., & Fuada, S. (2020). RIP VS. OSPF ROUTING PROTOCOLS: WHICH ONE IS THE BEST FOR A REAL-TIME COMPUTER NETWORK? *Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, *11*(1), 249-256. https://doi.org/10.24176/simet.v11i1.3796

Riabov, V. (2006). Simple Mail Transfer Protocol (SMTP). In H. Bidgoli (Ed.), *Handbook of Information Security*. John Wiley & Sons. https://www.researchgate.net/publication/236855917_Simple_Mail_Transfer_Protocol_SMTP