আন্তর্জাতিক ইসলামী বিশ্ববিদ্যালয় চট্টগ্রাম
الجامعة الإسلامية العالمية شيتاغونغ
International Islamic University Chittagong

Department Of Computer Science & Engineering

Course Title : Computer Networks Lab
Course Code: CSE - 3634
Section : 7AM
Semester : Spring- 2024

A Project Report on

Optimizing Corporate Network Efficiency: Design and Implementation of Multiprotocol Label Switching (MPLS) Protocol Using GNS3

Authors:

Team Name: IIUC_DWIP_ELITE

Members:

1.C211017 – Abdullah Al- Noman ***(Team Leader)***

2. C211001 – Md Anamul Haque

3. C211002 – Hossain Mohammad Meraj

4. C211019 – Meharaz Hossain

5. C211030 – Manjur Ahmed Chowdhury

Course Instructor:	**Course TA**
Abdullahil Kafi Assistant Professor Department of CSE, IIUC	Mohammad Abdul Kader Student Department of CSE, IIUC

Submission Date: Tuesday, 25 June, 2024

Abstract

MPLS is a traffic engineering technology that improves network performance, scalability, and reliability. It works by assigning short labels to packets, which are then used by routers to forward packets along specific paths through the network.

In this project, MPLS was implemented using the Resource Reservation Protocol (RSVP) as the control plane protocol and Constrained Route Tunneling (CR-T) as the traffic engineering technique. The following results were obtained:

- Improved network performance: MPLS reduced latency and improved throughput.
- Increased network scalability: MPLS allowed the network to handle more traffic without sacrificing performance.
- Improved network reliability: MPLS provided resilience to failures by routing traffic around failed links.

Acknowledgements

We would like to express our sincere gratitude to Abdullahil Kafi, Assistant Professor, and Ali Khatami, Teaching Assistant, for their invaluable guidance, support, and expertise throughout the entire duration of the "Enhancing Corporate Office System Efficiency: Design and Implementation of an MPLS Network Protocol" project.

Abdullahil Kafi's insightful recommendations, academic mentorship, and commitment to excellence have been instrumental in shaping the strategic direction of our project. His dedication to fostering a deep understanding of networking concepts and technologies has greatly enriched our learning experience.

We extend our appreciation to Mohammad Abdul Kader for his unwavering assistance, technical insights, and hands-on support during the implementation phase of the MPLS network protocol. His commitment to helping us overcome challenges and his enthusiasm for the subject matter significantly contributed to the success of our project.

We are also grateful to our fellow team members whose collaboration and teamwork were pivotal in the successful completion of this project. Their collective efforts, diverse perspectives, and shared commitment to excellence have made this project a rewarding and enriching experience.

Thank you once again to Abdullahil Kafi, Mohammad Abdul Kader, and our fellow team members for their contributions, guidance, and collaborative spirit, which have significantly enhanced the efficiency of our corporate office system.

Table of Contents

1. Introduction:

In the ever-evolving landscape of corporate technology, where efficiency and adaptability are paramount, our final project report delves into the successful culmination of our endeavor: "Optimizing Corporate Network Efficiency: Design and Implementation of Multiprotocol Label Switching (MPLS) Protocol Using GNS3"

As we navigate the intricacies of contemporary business environments, the significance of a seamless and high-performing corporate office system becomes increasingly evident. Our project has been driven by the core objective of not just meeting but surpassing the demands of our dynamic corporate ecosystem. Through meticulous design and implementation, we aimed to elevate the efficiency and reliability of our network infrastructure, contributing to the overall success of our organization.

Having maintained an efficient and secure network infrastructure over the years, our organization recognized the imperative for evolution in the face of rapid operational expansion and the growing complexity of our IT landscape. The project builds upon the foundation of our existing network architecture, integrating the latest technologies and industry best practices in network administration. Drawing on our accumulated knowledge and hands-on experience, we embarked on this journey fully equipped to craft a system that seamlessly aligns with the specific requirements of our organization.

This report chronicles the journey from proposal to implementation, detailing the challenges encountered, strategies employed, and the ultimate outcomes achieved in the pursuit of a more efficient and resilient corporate office system. Through collaborative efforts and a commitment to excellence, our team has not only met the objectives set forth but has also laid the groundwork for sustained success in the dynamic realm of corporate networking.

2. Background:

- **Importance of the Project:**

1. Operational Efficiency: The project holds significant importance in enhancing the operational efficiency of the corporate office system. By implementing an MPLS network protocol, we aimed to streamline communication, optimize data flow, and reduce latency, ultimately leading to a more efficient and responsive corporate environment.

2. Scalability: As our organization experiences rapid growth, scalability becomes a critical factor. The project addresses this need by implementing MPLS, a technology known for its scalability. This ensures that the network infrastructure can easily accommodate the increasing demands of users, devices, and applications.

3. Quality of Service (QoS): The project's focus on MPLS brings about improvements in quality of service, allowing for prioritization of critical applications. This is vital for ensuring a consistent and high-quality user experience, particularly for real-time applications such as video conferencing and voice communication.

4. Network Security: The implementation of Virtual Private Networks (VPNs) through MPLS contributes to enhanced network security. By segmenting and isolating different departments and sensitive data, the project reinforces the confidentiality and integrity of critical information within the corporate network.

5. Reliability and Resilience: The project contributes to the overall reliability and resilience of the network infrastructure. MPLS features such as built-in resiliency mechanisms and fast reroute capabilities help minimize downtime and ensure continuous connectivity even in the face of link or node failures.

6. End-to-End Connectivity: Achieving seamless end-to-end connectivity between geographically dispersed corporate offices is crucial for modern businesses. The project addresses this need by leveraging MPLS to establish reliable circuits across diverse network topologies.

➢ Tools and Methods Used:

1. Multiprotocol Label Switching (MPLS): MPLS serves as the cornerstone of our project, providing a versatile and efficient framework for packet forwarding, traffic engineering, and quality of service support.

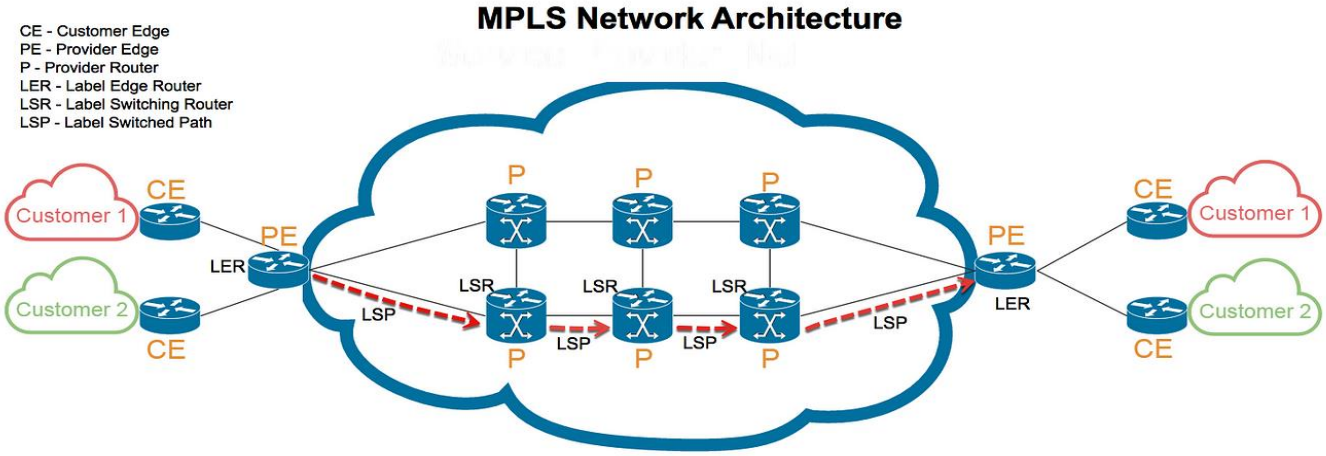


Figure: MPLS

2. GNS3 (Graphical Network Simulator 3): GNS3 was instrumental in the design and simulation phases of the project. This graphical network simulator allowed us to create a virtualized environment for testing and refining the MPLS-based network architecture before actual implementation.

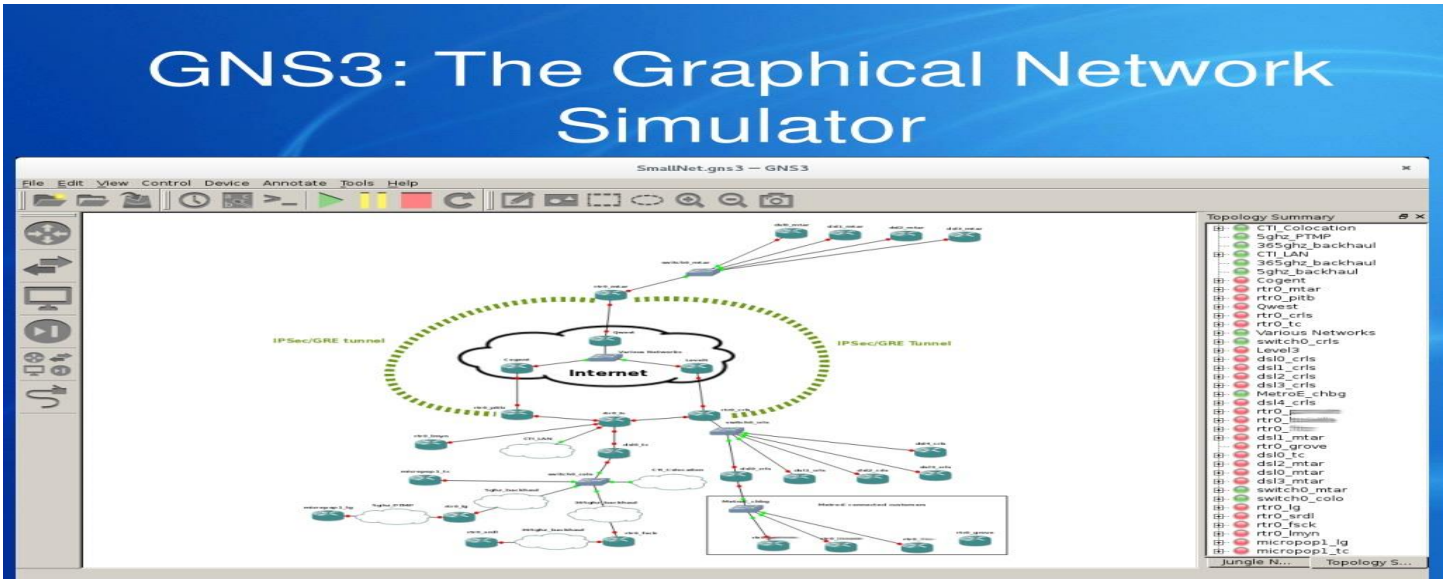


Figure: GNS3

3. Cisco C7200 Router: The Cisco C7200 router played a pivotal role in the implementation of MPLS. Its advanced features and compatibility with MPLS protocols facilitated the deployment of label-switched paths and the configuration of routing tables to optimize network traffic.

Figure: Cisco C7200 router

4. PC: Personal computers were used for network management, configuration, and monitoring purposes. These devices were essential for interacting with routers, switches, and other network components during the implementation phase.

Figure: PC

5. Ethernet Switch: Ethernet switches were employed to establish local area network (LAN) connections within the corporate office system. These switches enabled the efficient transfer of data between devices and contributed to the overall network performance.

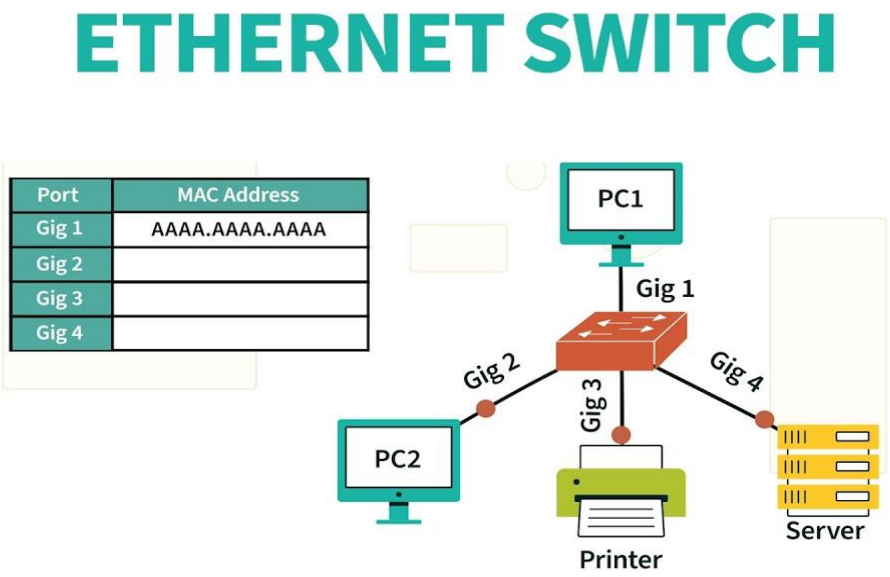


Figure: Ethernet switches

6. Ethernet Port and Serial Port: Ethernet and serial ports were utilized for connecting routers, switches, and PCs within the network topology. These physical interfaces played a crucial role in establishing the communication links necessary for the proper functioning of the MPLS-based network.

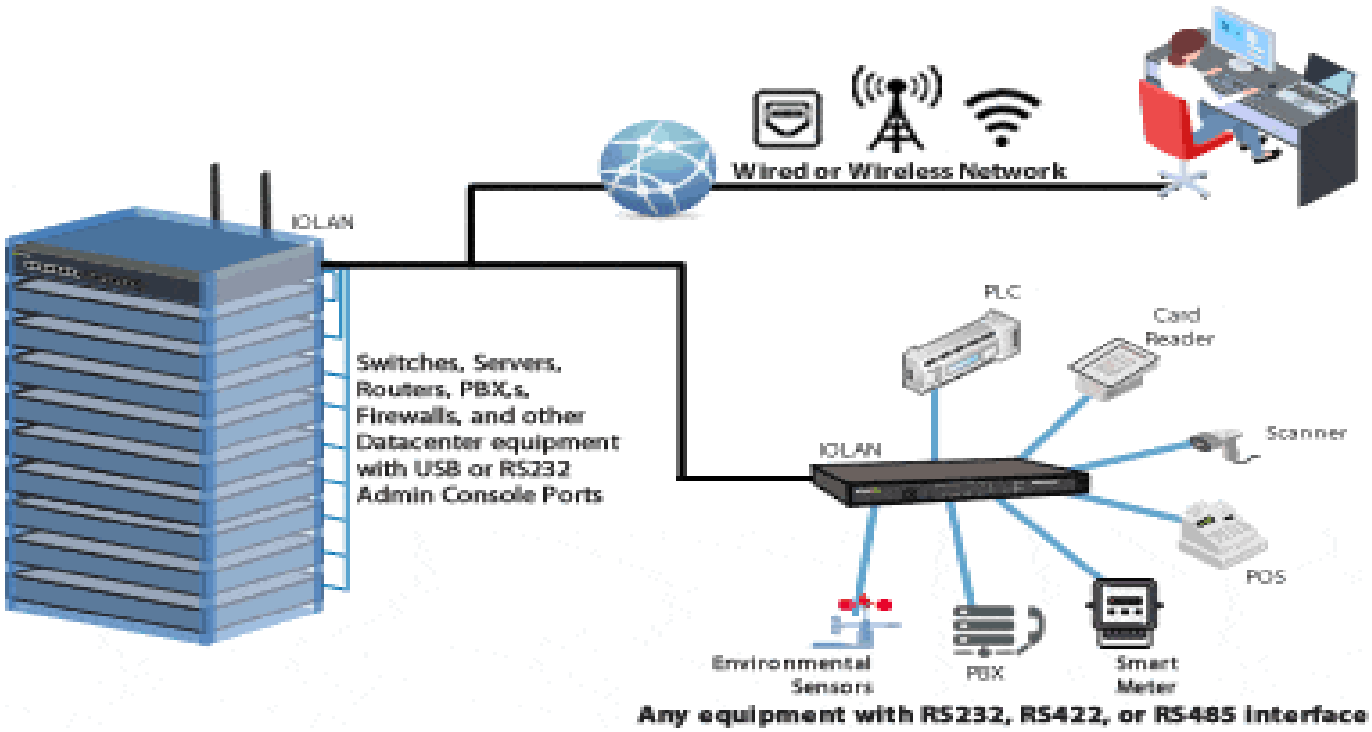


Figure: Ethernet and serial ports

7. Testing and Monitoring Tools: Various testing and monitoring tools, both software-based and hardware-based, were employed to evaluate the performance of the MPLS network. Bandwidth monitoring tools, fault detection mechanisms, and performance analysis tools were utilized to ensure the network met the desired criteria.

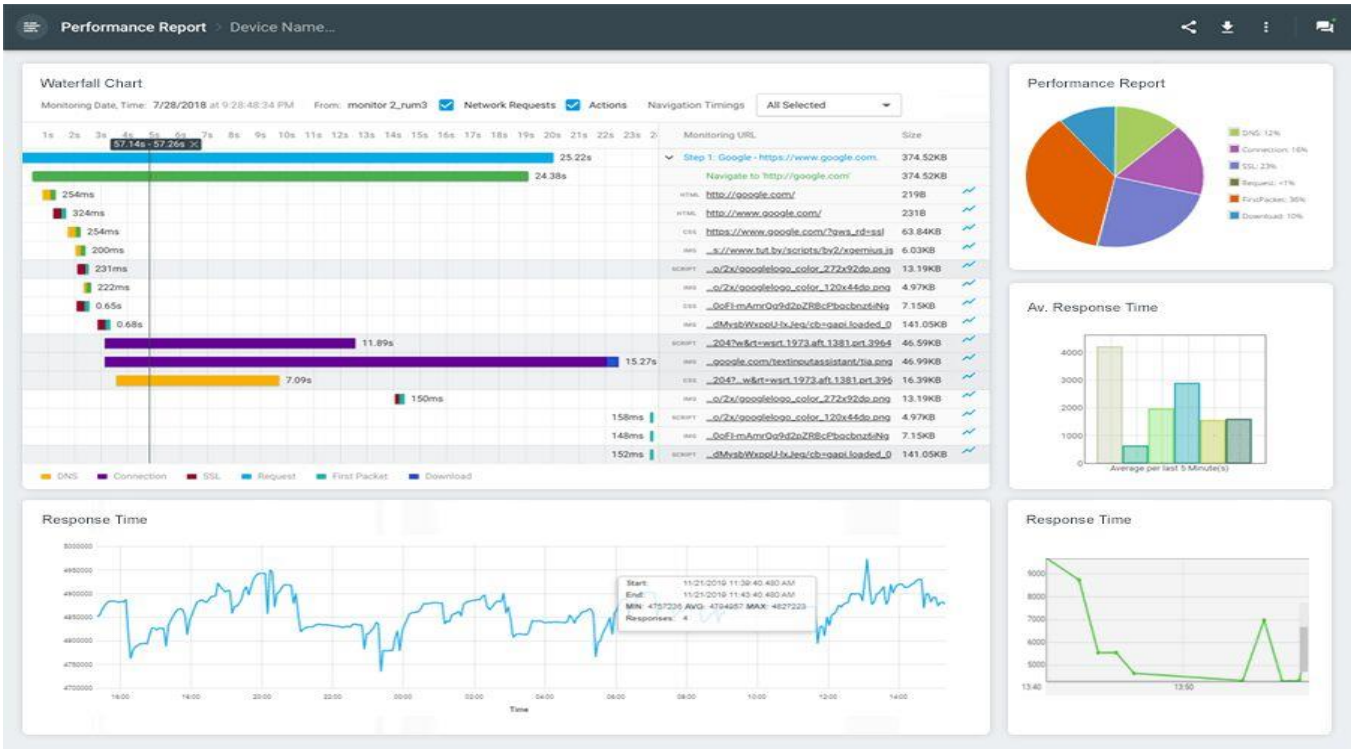


Figure: Testing and Monitoring Tools

8. Security Protocols for VPNs: Security protocols and encryption methods were implemented on the Cisco C7200 router to establish secure Virtual Private Networks (VPNs) within the MPLS framework. This ensured the confidentiality and integrity of data transmitted across the network.

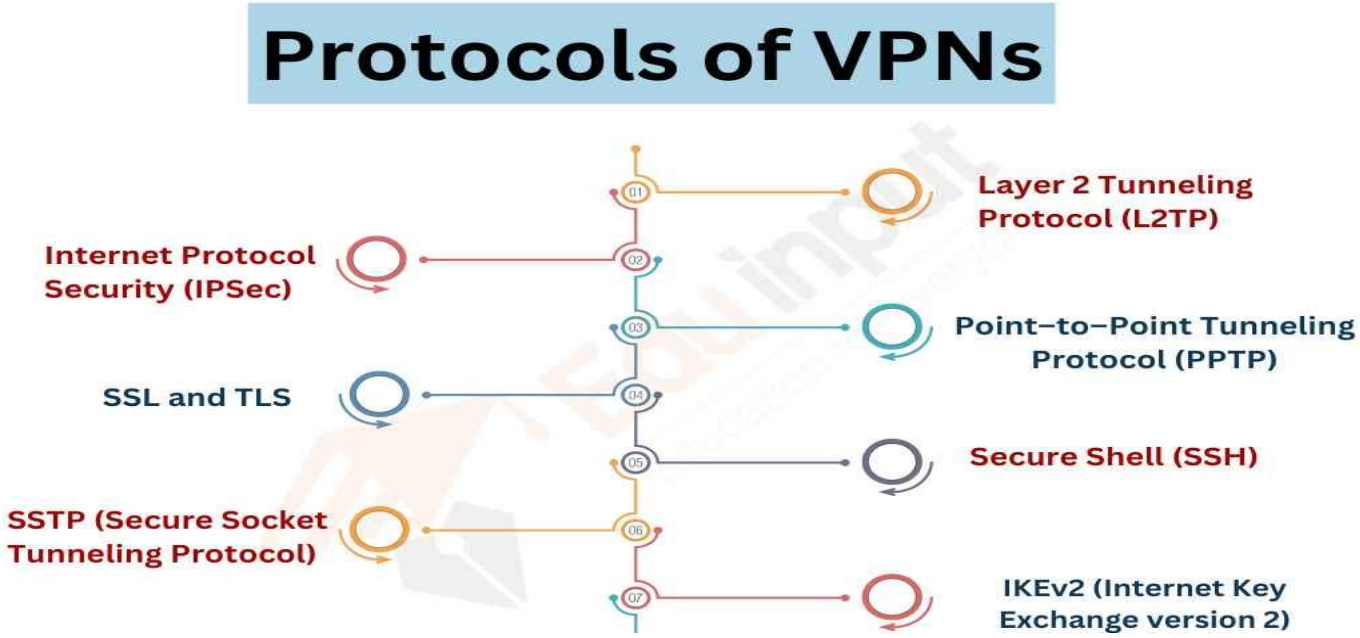


Figure: Security Protocols for VPNs

Incorporating these specific tools and methods into the discussion provides a more detailed and accurate representation of the technical aspects involved in the design and implementation of the MPLS network protocol for the corporate office system.

In summary, the project's significance lies in its ability to elevate the efficiency, scalability, and security of the corporate office system through the strategic implementation of MPLS and associated tools and methods. This initiative not only addresses the current needs of our organization but also establishes a foundation for sustained growth and adaptability in the dynamic landscape of corporate networking.

3. Literature

3.1. Campus Network

A campus network is a private computer network that interconnects devices within a limited area, such as a university, college, or corporate headquarters. Campus networks typically provide a variety of services, including email, file sharing, and internet access. They are designed to be easy to use and manage, and to provide a high level of performance and reliability.

3.2. IPv4 and VLSM

IPv4 (Internet Protocol Version 4) is the fourth version of the Internet Protocol (IP). It is the most widely used IP protocol today, and it is responsible for routing data packets across the internet. IPv4 addresses are 32 bits long, which means that there are a total of 2^32 (approximately 4.3 billion) unique IPv4 addresses.

VLSM (Variable-Length Subnet Masking) is a technique for dividing an IP address space into smaller subnets of different sizes. This is a more efficient use of IP addresses than fixed-length subnetting, which requires all subnets to be the same size. VLSM allows you to create subnets of the size that you need, based on the number of hosts on each subnet.

3.3. GNS3

GNS3 (Graphical Network Simulator-3) is a network simulation software package that allows you to create and test virtual networks. GNS3 is a popular tool for learning about networking, and it is also used by professionals to test and deploy new network designs.

3.4. Routing

Routing in computer networks refers to the process of determining the optimal path for data packets to travel from a source to a destination across a network. It involves making decisions at each network device (usually routers) about the next hop or intermediary destination based on routing algorithms and protocols. The goal of routing is to efficiently forward data while considering factors such as the network topology, link costs, and current network conditions.

In essence, routing is like providing a set of directions for network traffic. Different routing protocols, such as RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol), govern how routers exchange information about the network and make decisions about the best paths to reach destinations. These decisions are influenced by metrics like distance, bandwidth, and latency.

3.5. Cisco Images

Cisco images are software files that are used to configure Cisco routers and switches. Cisco images contain the software that is necessary for the router or switch to operate, including the operating system, the routing protocols, and the configuration settings. Cisco images are typically downloaded from the Cisco website and then loaded onto the router or switch using a variety of methods, such as TFTP (Trivial File Transfer Protocol) or SCP (Secure Copy Protocol).

4. Problem Statement:

The current corporate office network infrastructure faces challenges in terms of scalability, performance, and efficient traffic management. As the organization continues to grow, there is a need to enhance the network to support a larger number of users, applications, and services while ensuring optimal performance and reliability. The existing network lacks the necessary mechanisms for traffic engineering, quality of service (QoS) support, and seamless connectivity between geographically dispersed offices. Moreover, security concerns mandate the implementation of a robust and isolated network environment for different departments and sensitive data. To address these issues, the organization aims to implement Multiprotocol Label Switching (MPLS) within its corporate office system. The goal is to leverage the advantages of MPLS, including efficient packet forwarding, traffic engineering capabilities, and support for quality of service, to enhance the overall network infrastructure. The implementation of MPLS should provide a scalable, secure, and reliable solution that accommodates the current and future needs of the organization.

➢ Key Objectives:

- Scalability: Implement MPLS to support the increasing number of users, devices, and services within the corporate network while ensuring efficient resource utilization.
- Performance Optimization: Utilize MPLS traffic engineering capabilities to optimize the flow of network traffic, reducing latency and ensuring consistent performance for critical applications.
- Quality of Service (QoS): Implement MPLS to support QoS mechanisms, prioritizing traffic based on application requirements and providing a seamless experience for real-time communication and mission-critical applications.
- Traffic Segmentation and Isolation: Utilize MPLS to create Virtual Private Networks (VPNs) for different departments and segments within the organization, enhancing security and ensuring the isolation of sensitive data.
- Reliability and Resiliency: Design the MPLS network with built-in resiliency features to minimize downtime and ensure uninterrupted connectivity between corporate offices, even in the event of link or node failures.
- End-to-End Connectivity: Implement MPLS to establish end-to-end circuits across diverse network topologies, providing seamless connectivity between geographically dispersed corporate offices.
- Simplified Management: Leverage the simplicity of MPLS for network management and troubleshooting, aiming to reduce operational overhead and streamline the resolution of network-related issues.

By addressing these objectives through the implementation of MPLS, the organization seeks to transform its corporate office network into a robust, scalable, and high-performance infrastructure that meets the evolving needs of the business while ensuring the security and reliability of critical services and data.

➢ Specific Design Considerations

- IPv4 subnetting: The network will be divided into subnets to improve network performance and security
- Number of networks: Four routers will be used to create a total of Four networks.
- Routing: MPLS will be used as the routing protocol to dynamically forward the data packet between network destinations. In our project topology MPLS configuration in R1,R2,R3,R4 router. Here R3,R2 config as a provider router and R1,R4 config as a provider edge router .
- Gateways: Four gateways will be used to connect the different networks together.

➢ Outcomes

The implementation of the proposed network design is expected to result in the following outcomes:

- Improved network performance: Reduced latency, increased throughput, and decreased packet loss.
- Increased network scalability: Ability to handle more traffic, support for a larger number of devices, and simplified network management.
- Improved network reliability: Increased resilience to failures, reduced downtime, and improved fault tolerance.
- Additional benefits: Enhanced security, improved traffic engineering, and reduced costs.

5. Designs

5.1 VLSM:

VLSM (Variable Length Subnet Masking) is a technique for subdividing a network into subnets using different subnet mask lengths. This allows for more efficient use of IP addresses and can help to improve network performance.

In this case, the network has been divided into eight subnets, each with a different subnet mask length. The subnets are as follows:

Subnet	Network Address	Subnet Mask	Broadcast Address	Number of Hosts
1	192.168.106.0/26	255.255.255.192	192.168.106.63	62
2	20.0.0.0/30	255.255.255.252	20.0.0.3	4
3	30.0.0.0/30	255.255.255.252	30.0.0.3	4
4	10.0.0.0/30	255.255.255.252	10.0.0.3	4
5	60.0.0.0/30	255.255.255.252	60.0.0.3	4
6	70.0.0.0/30	255.255.255.252	70.0.0.3	4
7	80.0.0.0/30	255.255.255.0	80.0.0.255	4
8	192.168.106.64/26	255.255.255.192	192.168.106.127	62
9	192.168.106.128/26	255.255.255.192	192.168.106.191	62
10	192.168.106.192/26	255.255.255.192	192.168.106.255	62

5.2 Calculations

The following calculations were used to determine the subnet mask lengths and the number of hosts in each subnet:

Subnet Mask Length = Number of Bits in the Subnet Mask - Number of Bits in the Network Address

Number of Hosts = 2^(32 - Subnet Mask Length) – 2

Subnet 1:

Subnet Mask Length: 32 (total number of bits in an IP address) - 26 (number of bits in the network address) = 6 bits
Number of Hosts: 2^(32 - Subnet Mask Length) - 2 = 2^(32 - 26) - 2 = 62

A	B	C	D
Subnet	Subnet Mask	IP Range	useable Hosts
192.168.106.0/26	255.255.255.192	192.168.106.0 - 192.168.106.63	64
192.168.106.64/26	255.255.255.192	192.168.106.64 - 192.168.106.127	64
192.168.106.128/26	255.255.255.192	192.168.106.128 - 192.168.106.191	64
192.168.106.192/26	255.255.255.192	192.168.106.192 - 192.168.106.255	64

Subnet 2

Subnet Mask Length: 32 (number of bits in the subnet mask) - 30 (number of bits in the network address) = 2 bits
Number of Hosts: 2^(32 - Subnet Mask Length) - 2 = 2^(32 - 30) - 2 = 4

Subnet	Subnet Mask	IP Range	Total Hosts
10.0.0.0/30	255.255.255.252	10.0.0.0 - 10.0.0.3	2
20.0.0.0/30	255.255.255.252	20.0.0.0 - 20.0.0.3	2
30.0.0.0/30	255.255.255.252	30.0.0.0 - 30.0.0.3	2
40.0.0.0/30	255.255.255.252	40.0.0.0 - 40.0.0.3	2
50.0.0.0/30	255.255.255.252	50.0.0.0 - 50.0.0.3	2
60.0.0.0/30	255.255.255.252	60.0.0.0 - 60.0.0.3	2
70.0.0.0/30	255.255.255.252	70.0.0.0 - 70.0.0.3	2
80.0.0.0/30	255.255.255.252	80.0.0.0 - 80.0.0.3	2

5.3 IP Tables:

- End device IP table :

End Device	Assign IP
Server	192.168.106.3
Phone	192.168.106.2
Printer_b	192.168.106.66
laptop_1	192.168.106 .67
laptop_2	192.168.106.130
PC6	192.168.106.131
printer_g	192.168.106.195
PC7	192.168.106.194

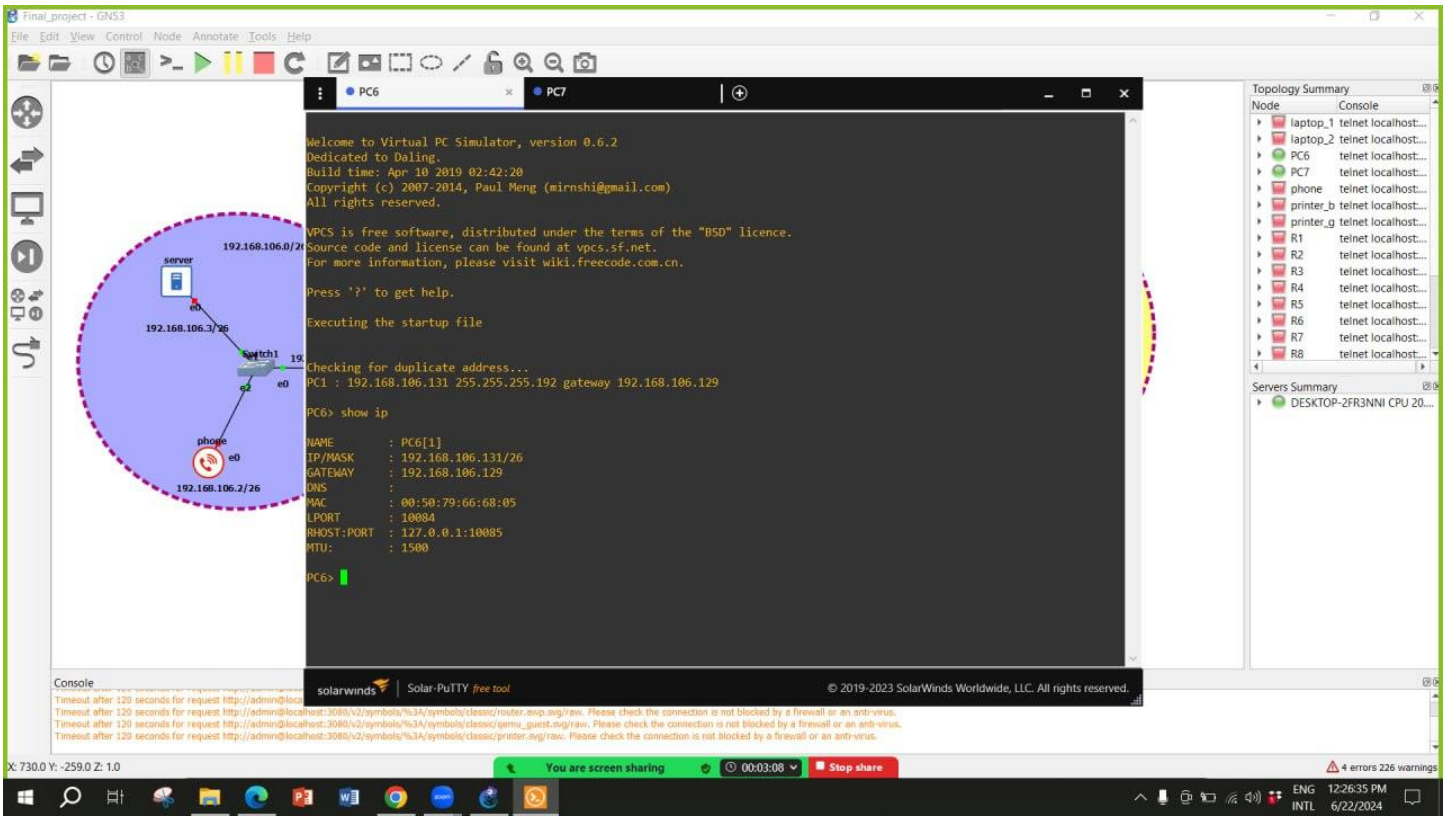


Figure: Show ip PC6[1]

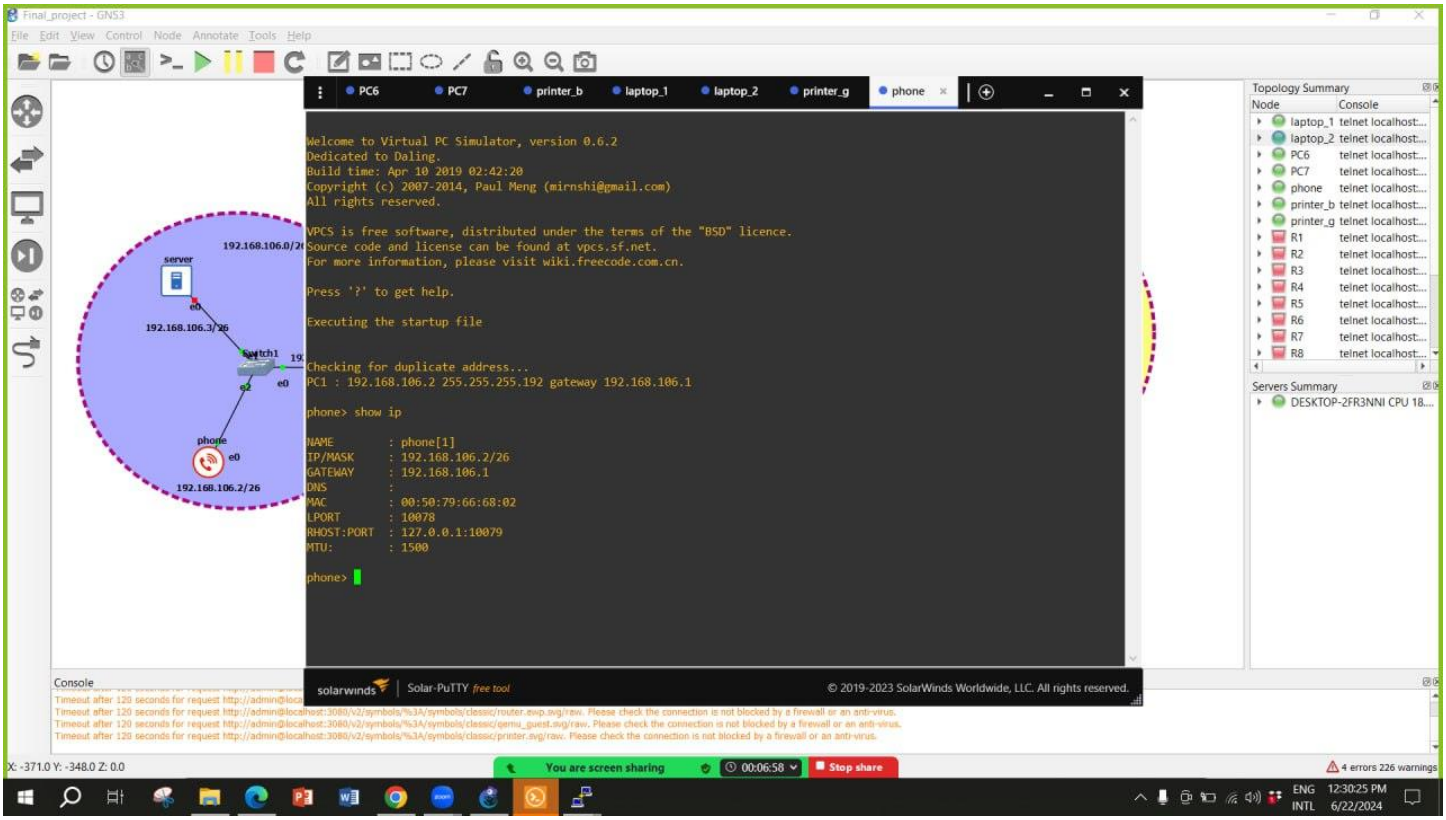


Figure: Show ip Phone[1]

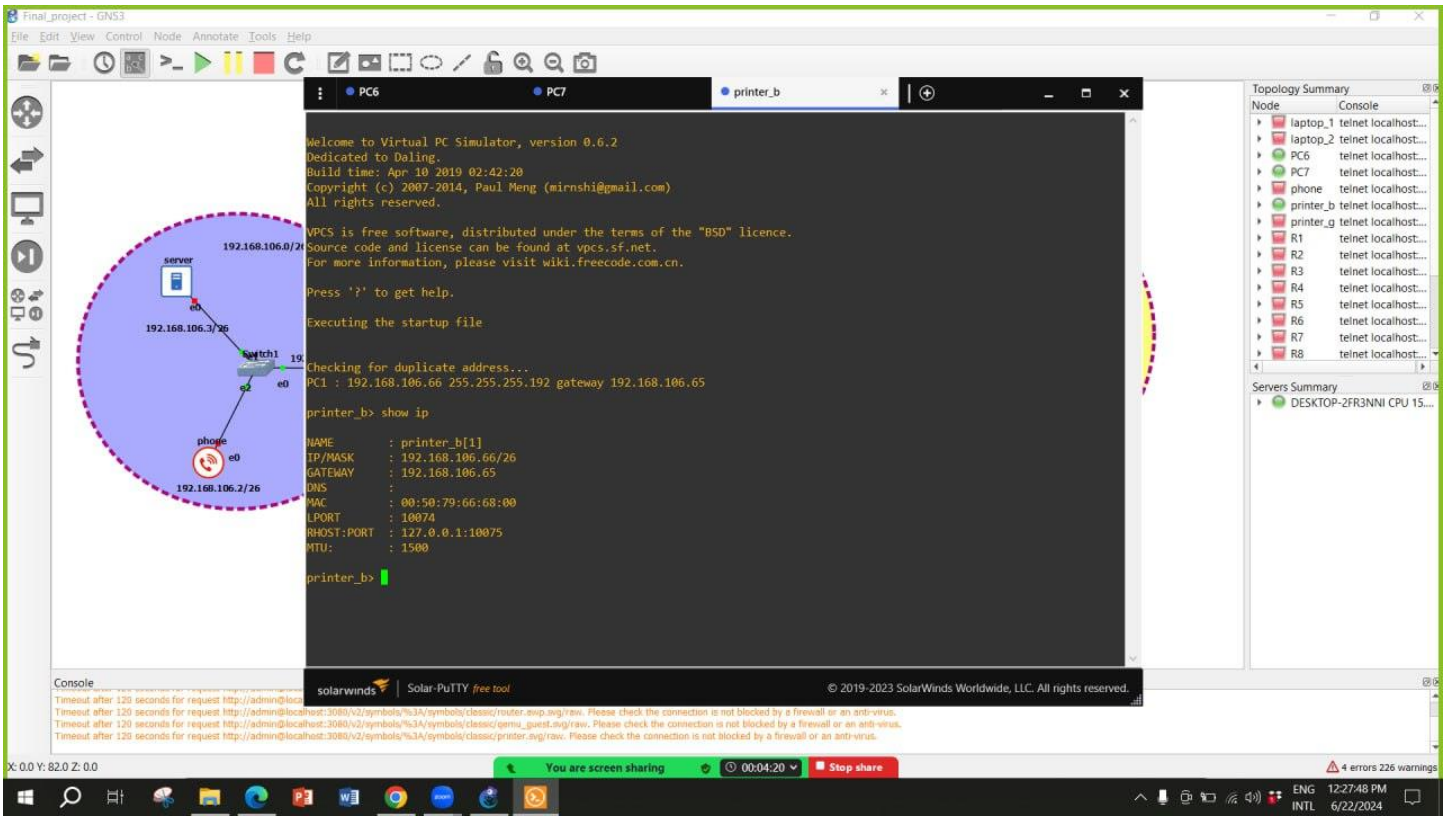


Figure: Show ip printer_b[1]

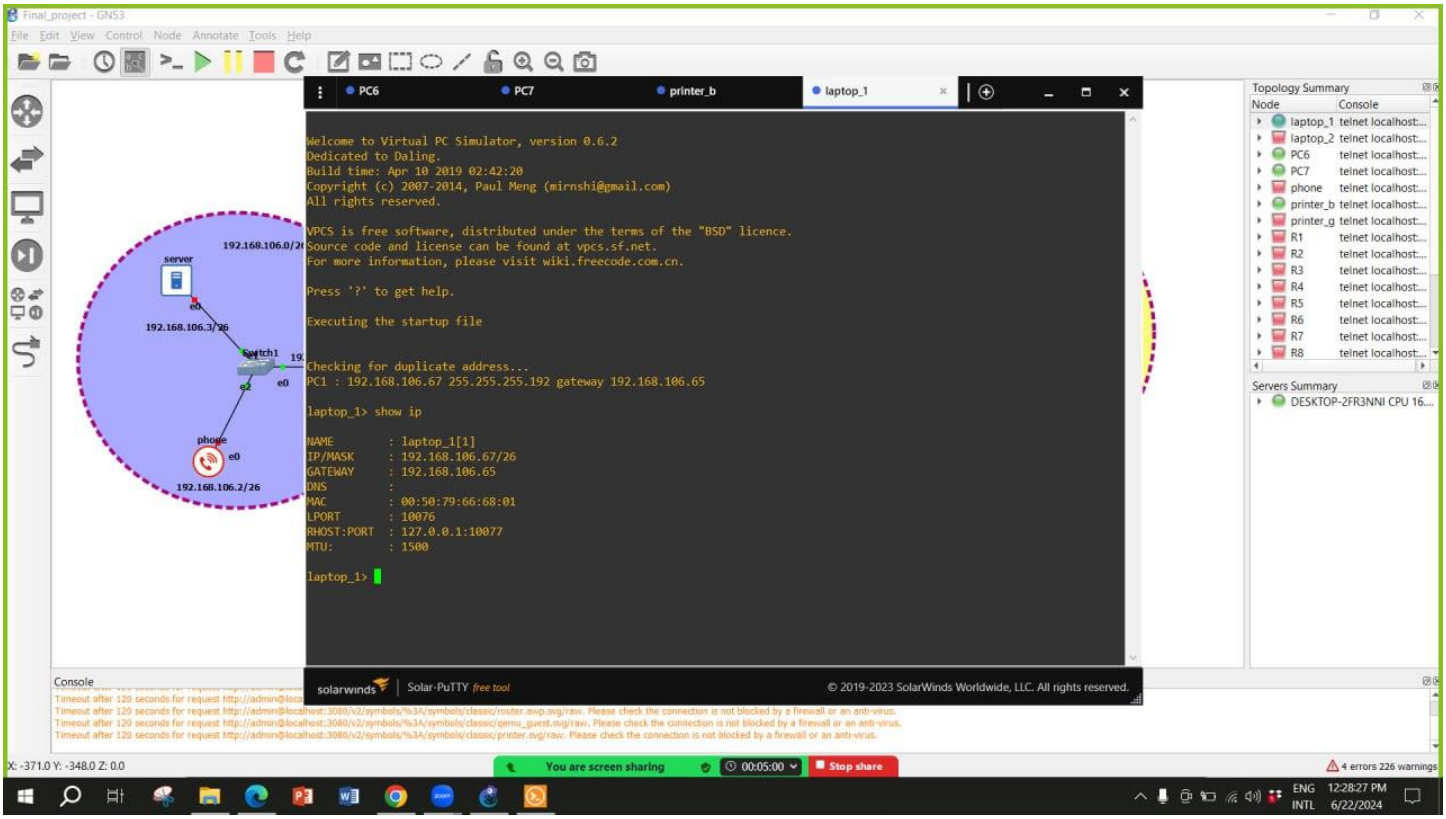


Figure: Show ip laptop_1[1]

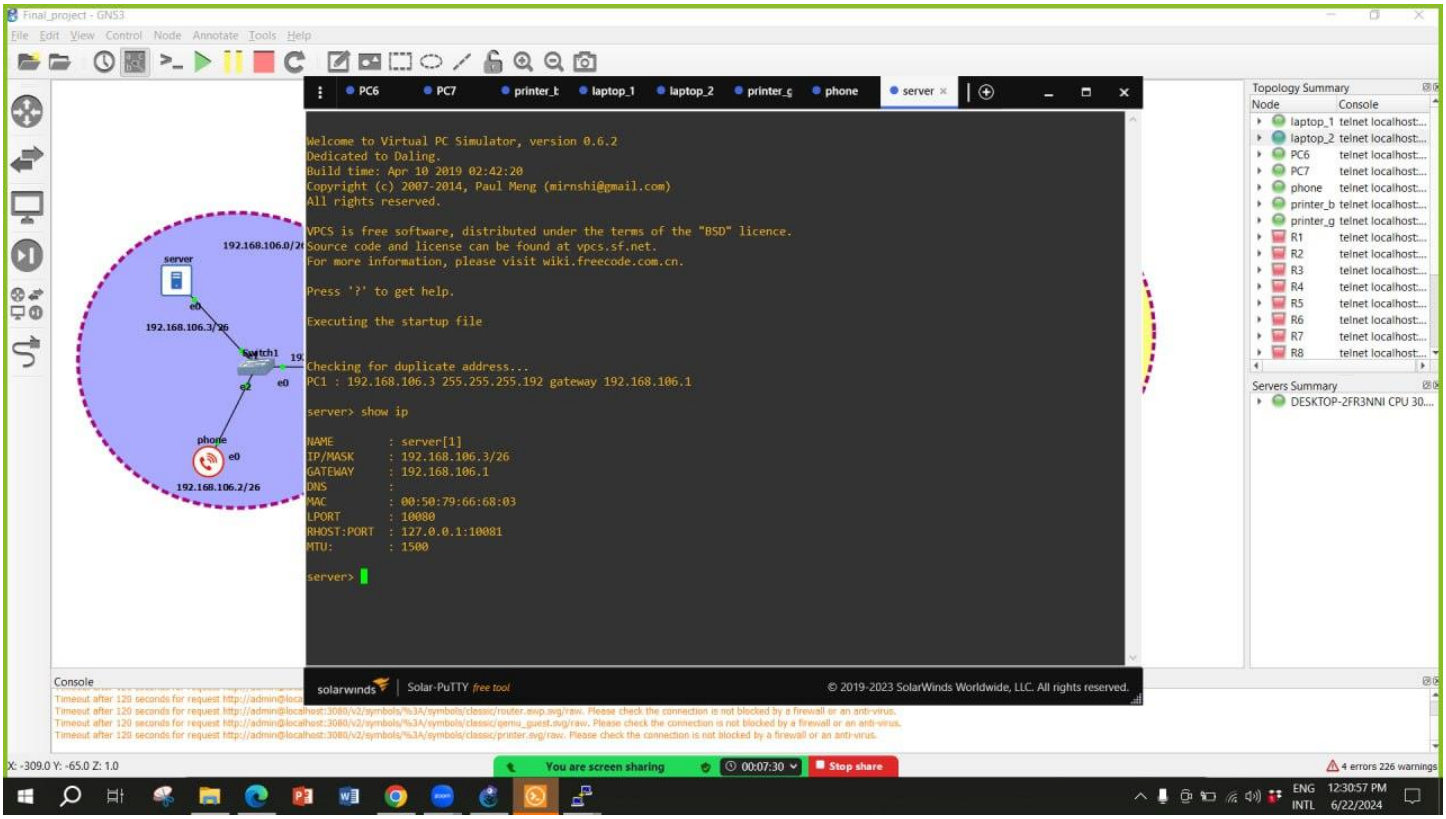


Figure: Show ip Server[1]

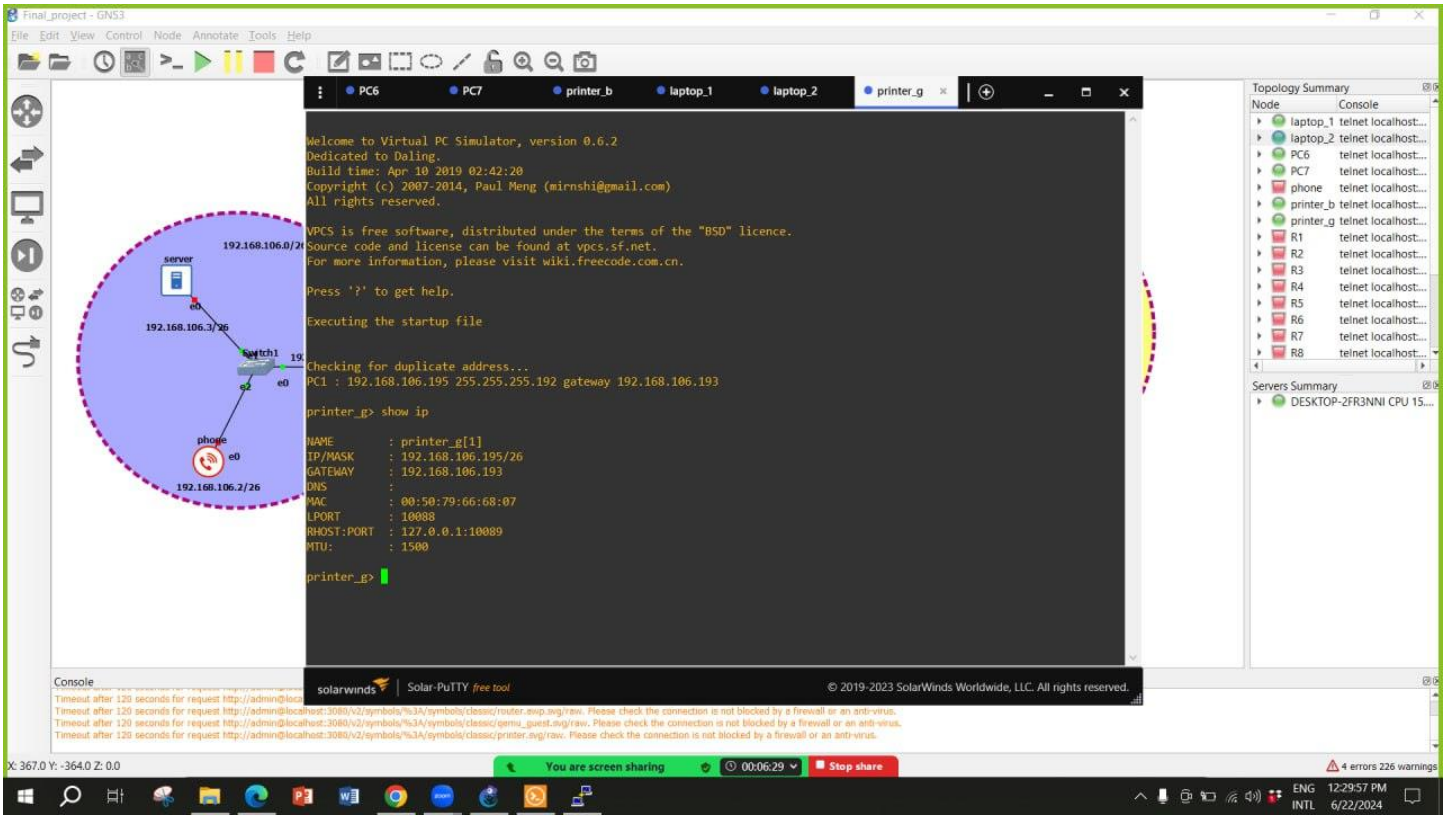


Figure: Show ip printer_g[1]

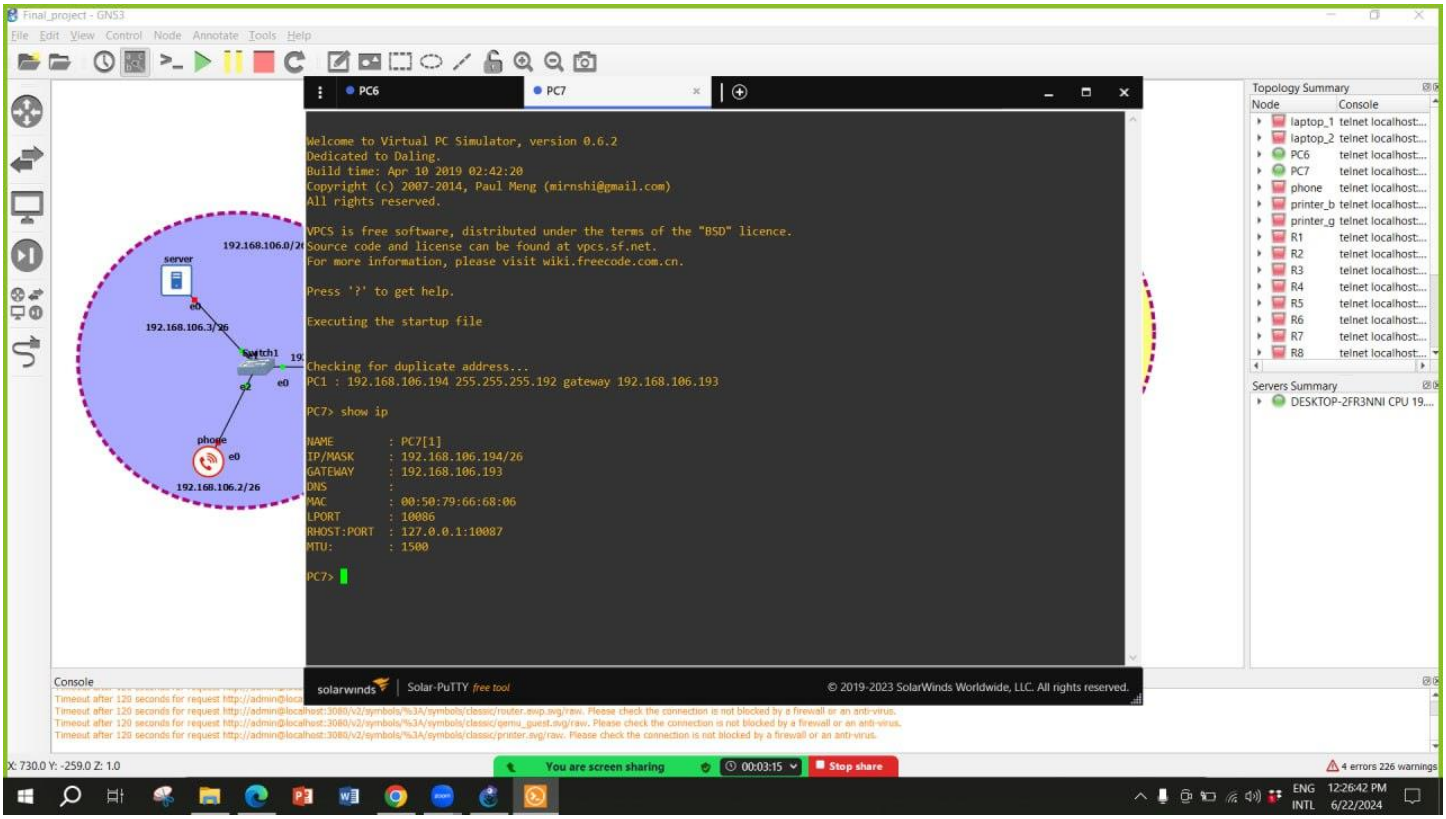


Figure: Show ip PC7[1]

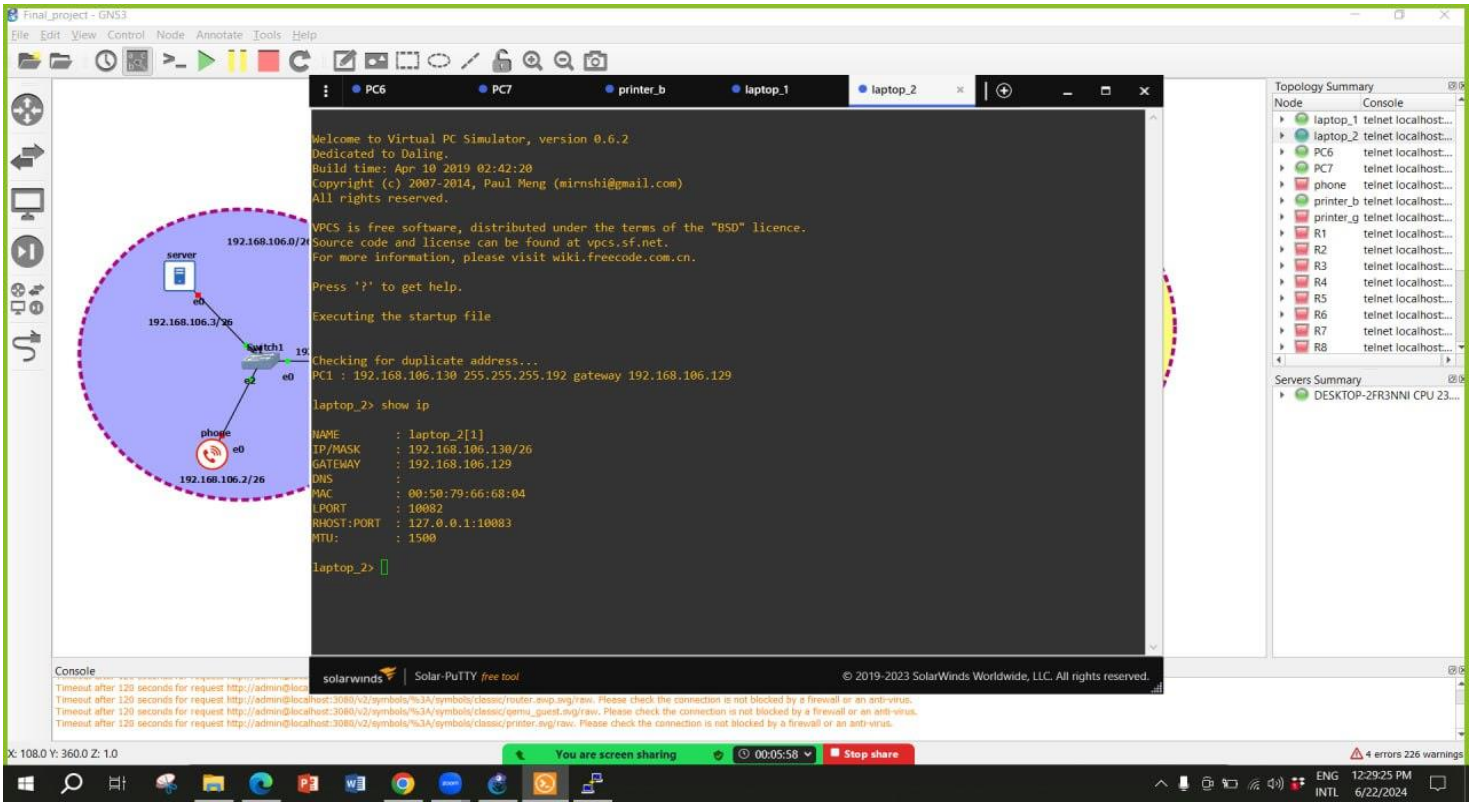


Figure: Show ip laptop_2[1]

- Router IP table :

Router	Interface	IP	loopback_ip
R1	g1/0	20.0.0.2/30	1.1.1.1
	g2/0	10.0.0.1/30	
	g3/0	60.0.0.2/30	
R2	g1/0	30.0.0.2/30	2.2.2.2
	g2/0	20.0.0.1/30	
R3	g1/0	30.0.0.1/30	3.3.3.3
	g2/0	40.0.0.2/30	
R4	g1/0	40.0.0.1/30	4.4.4.4
	g2/0	80.0.0.1/30	
	g3/0	70.0.0.2/30	

R5	f0/0	10.0.0.2/30	--------
	g2/0	192.168.106.1/26	
R6	f0/0	192.168.106.65/26	--------
	g1/0	60.0.0.1/30	
R7	g1/0	70.0.0.1/30	--------
	f0/0	192.168.106.129/26	
R8	f0/0	192.168.106.193/26	--------
	g1/0	80.0.0.2/30	

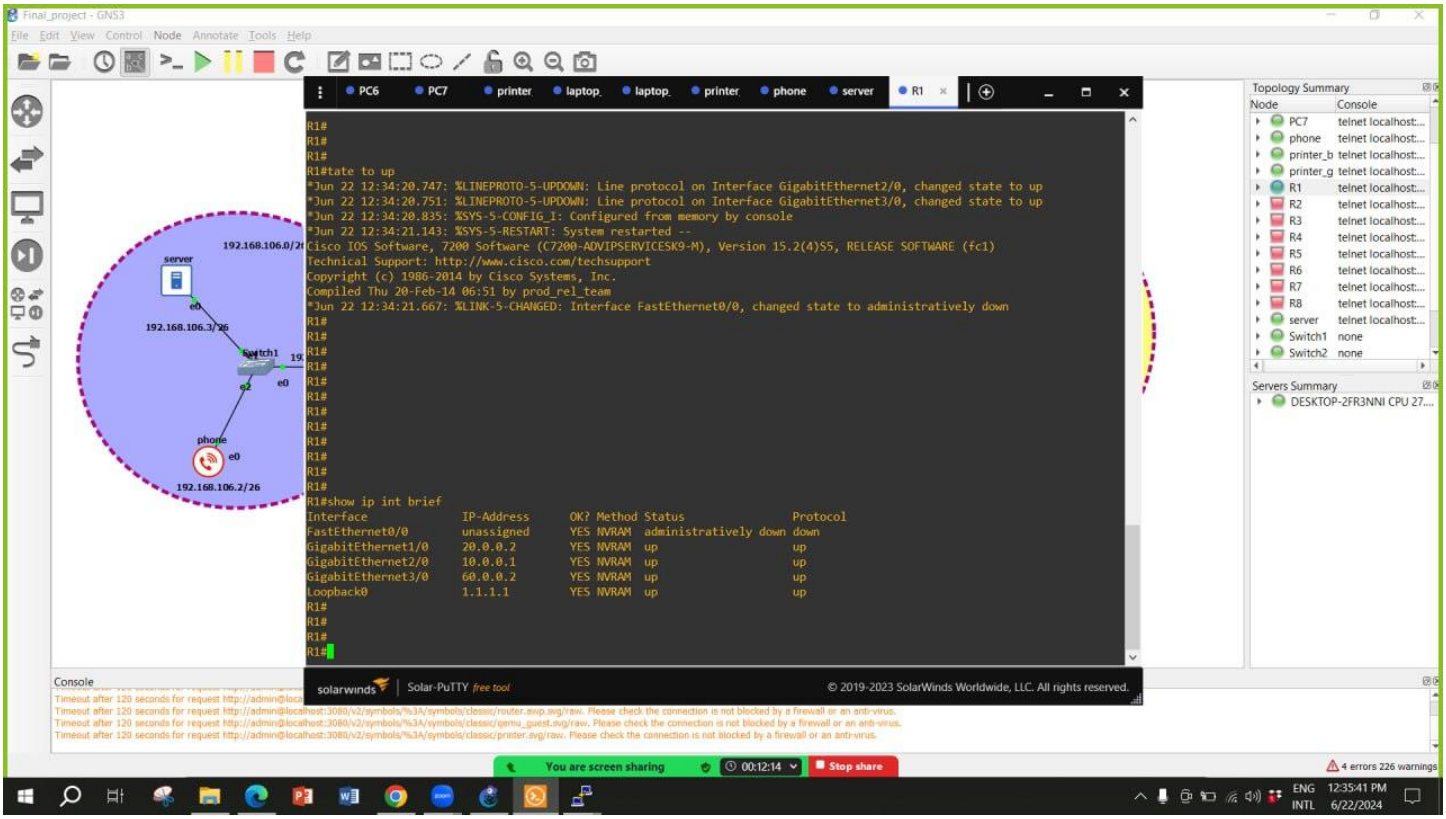


Figure: Show ip int breif **R1#**

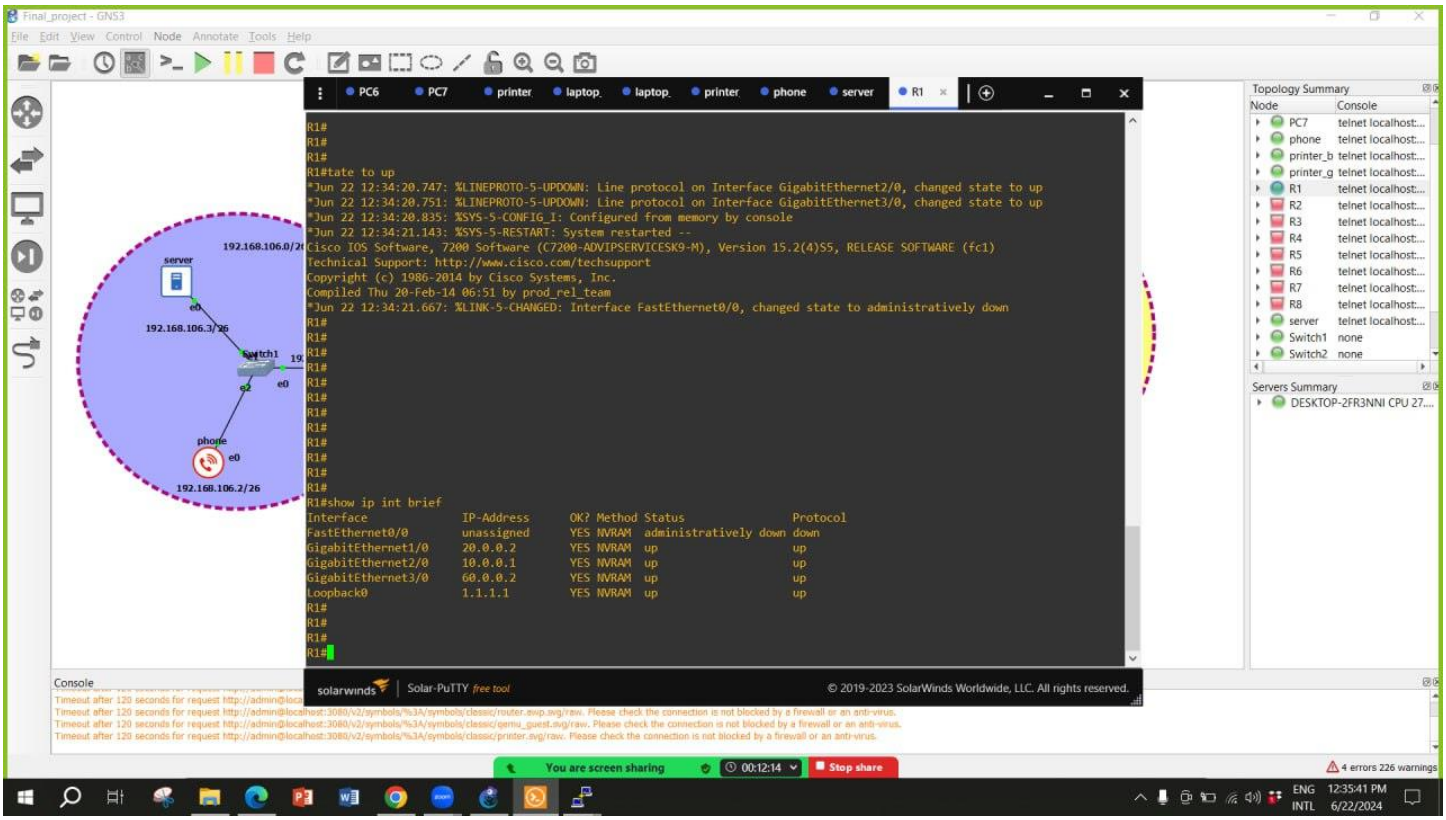


Figure: Show ip int breif **R2#**

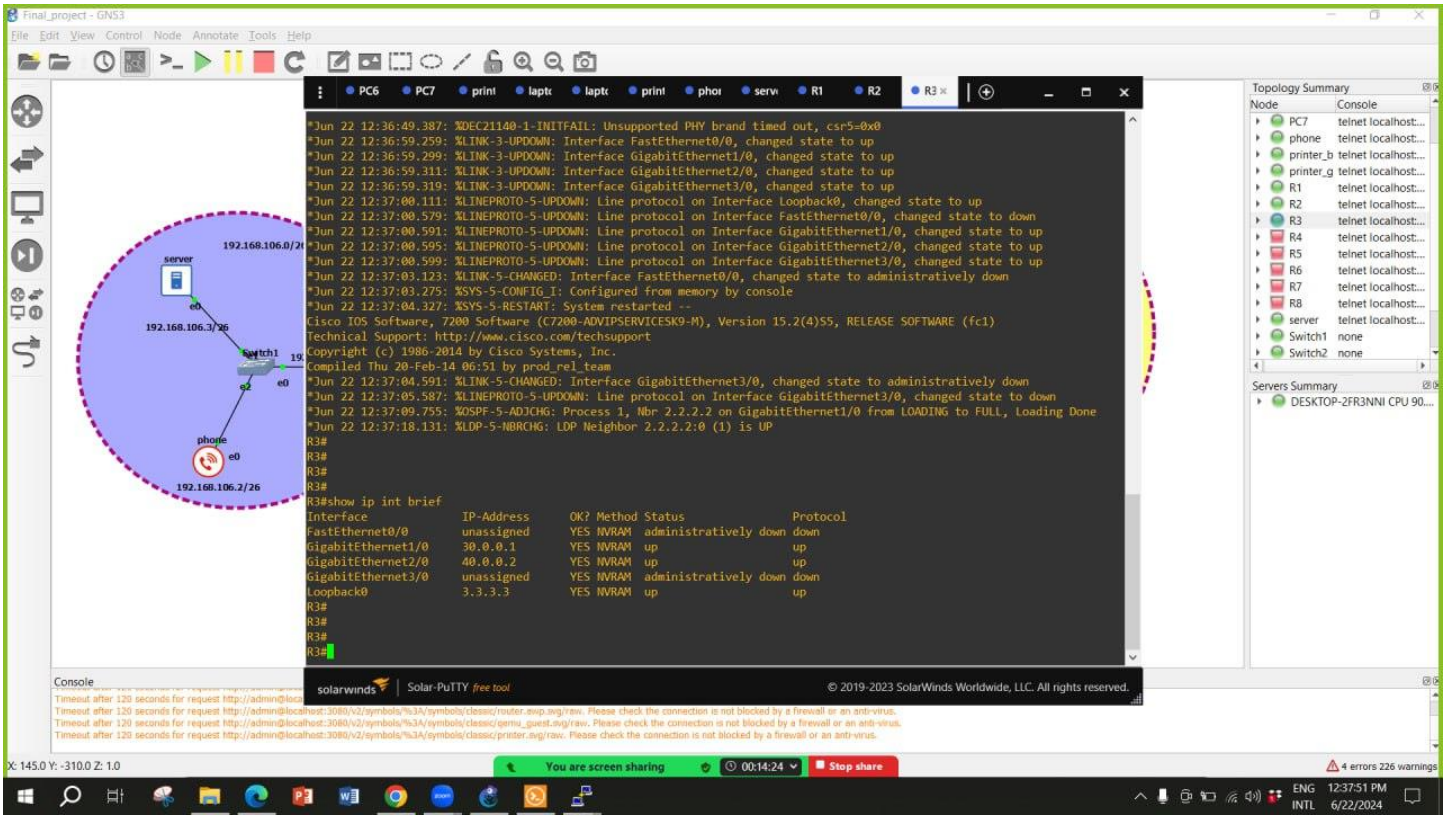


Figure: Show ip int breif **R3#**

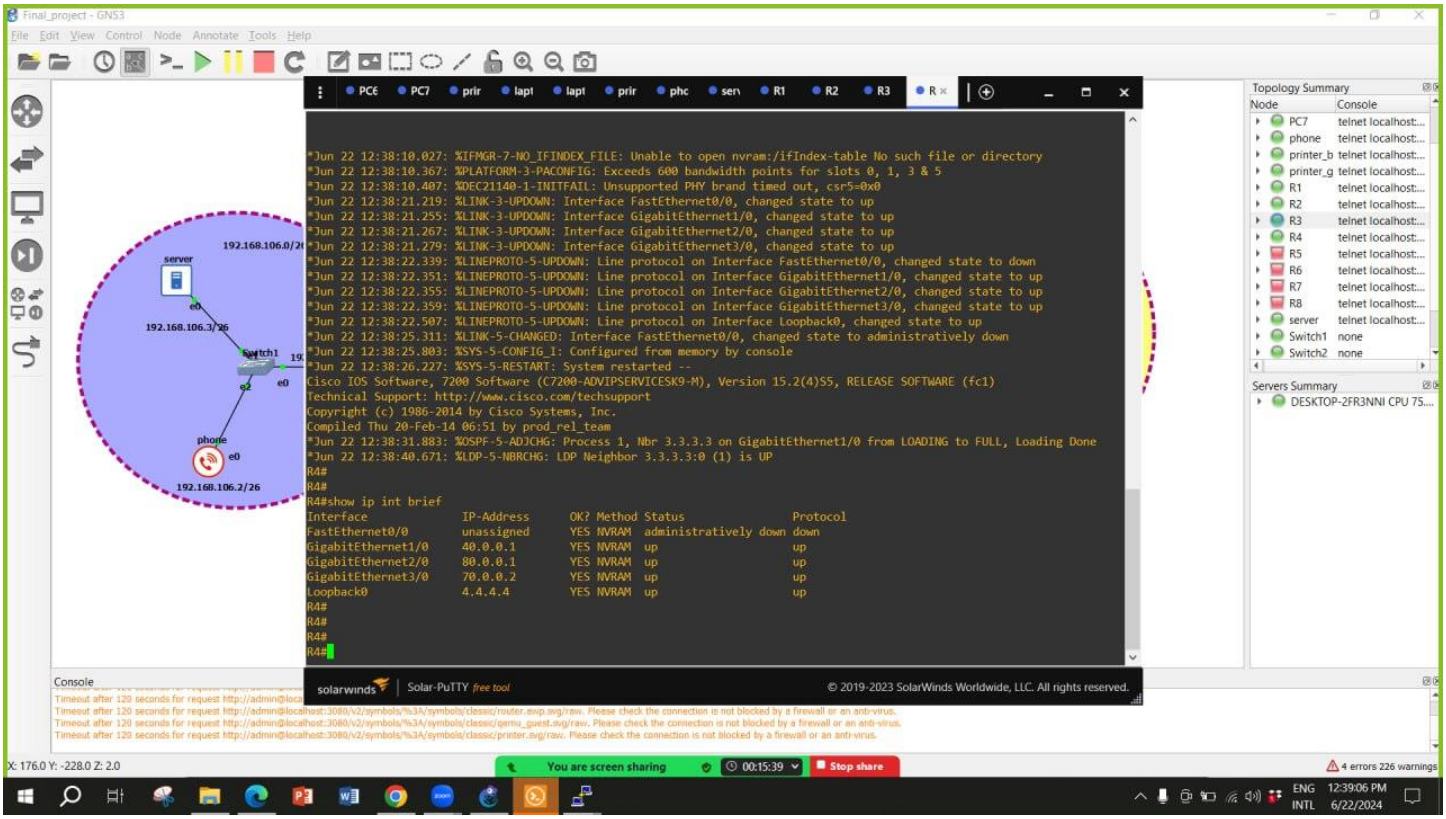


Figure: Show ip int breif **R4#**

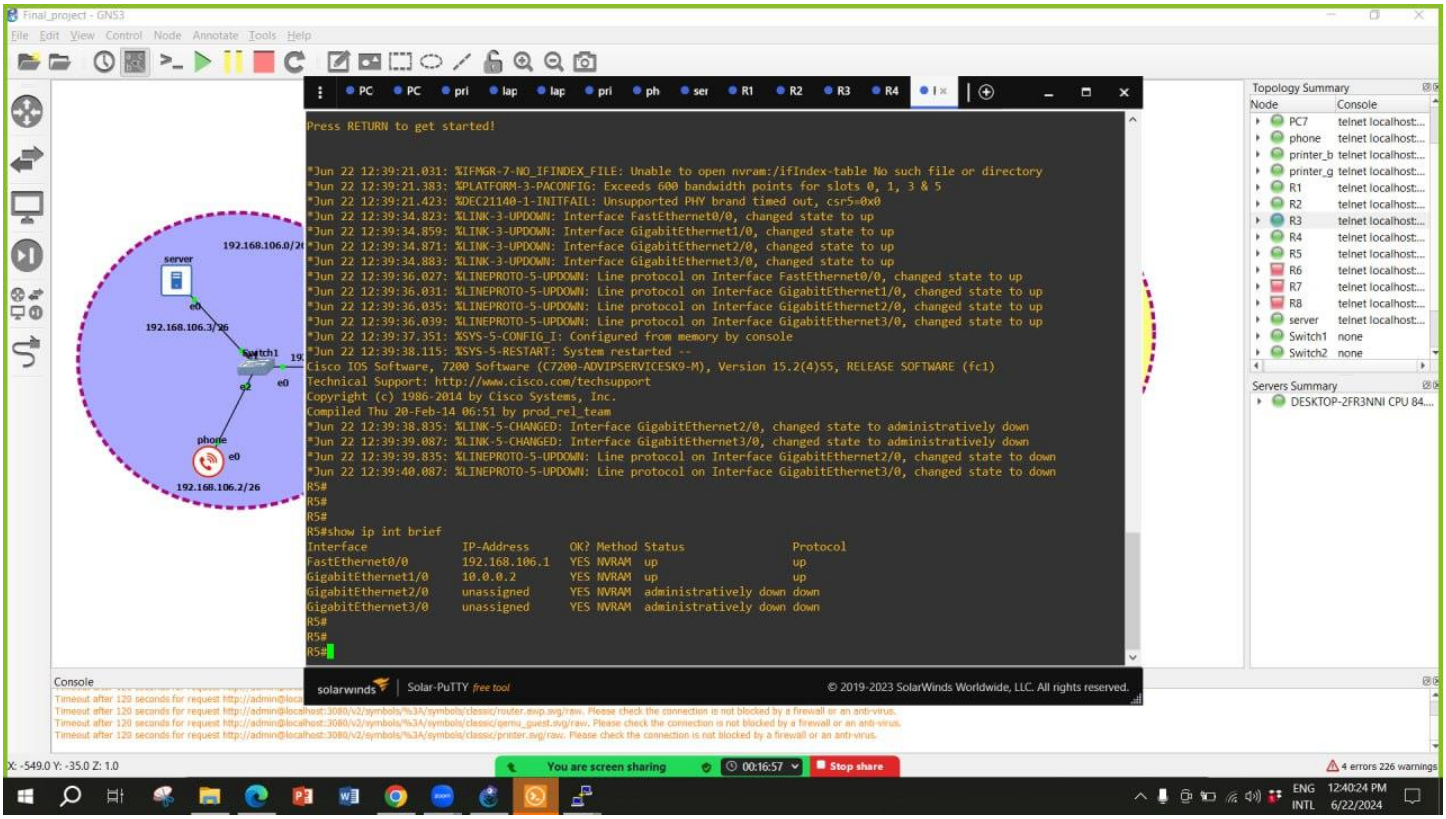


Figure: Show ip int breif **R5#**

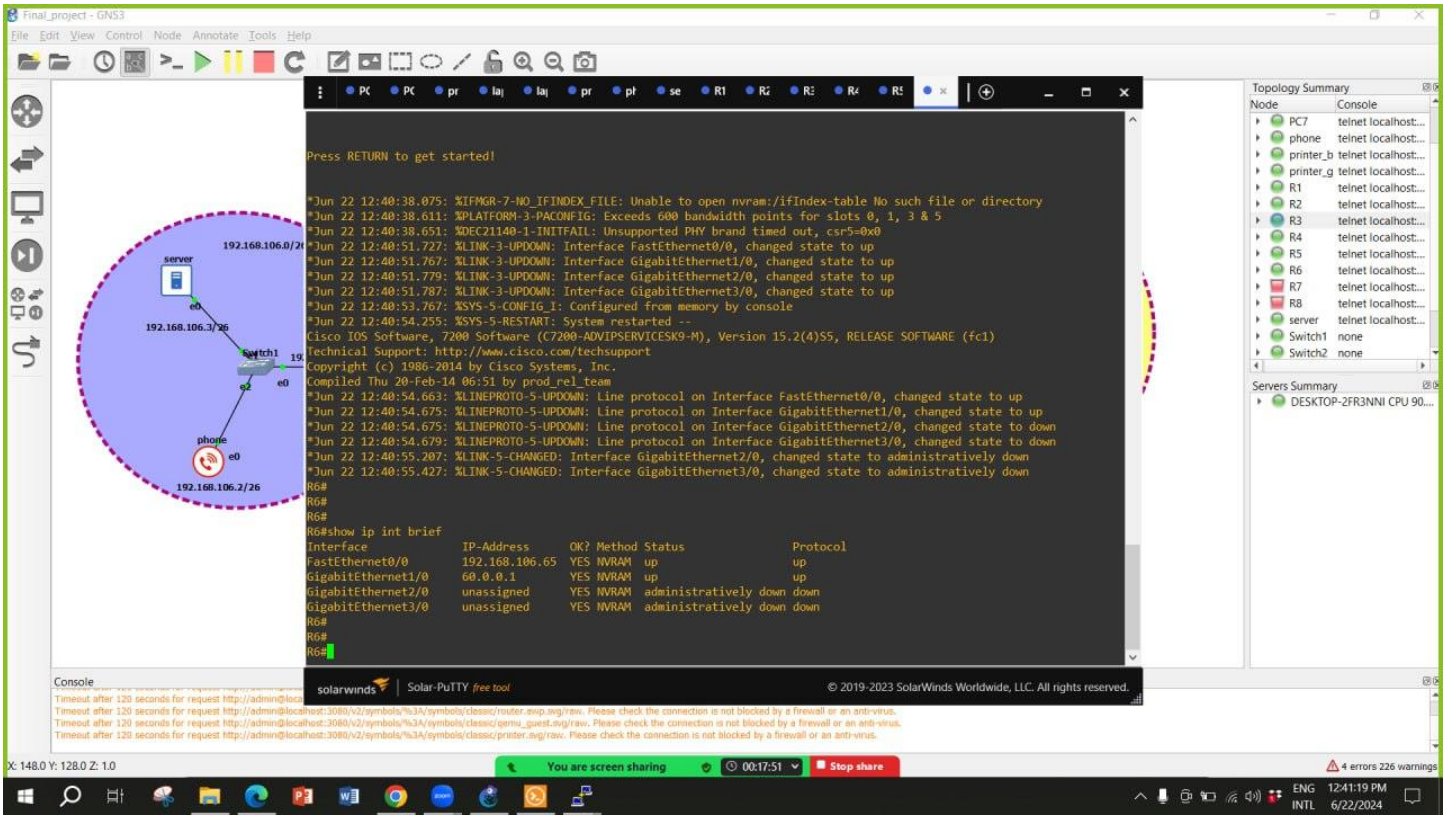


Figure: Show ip int breif **R6#**

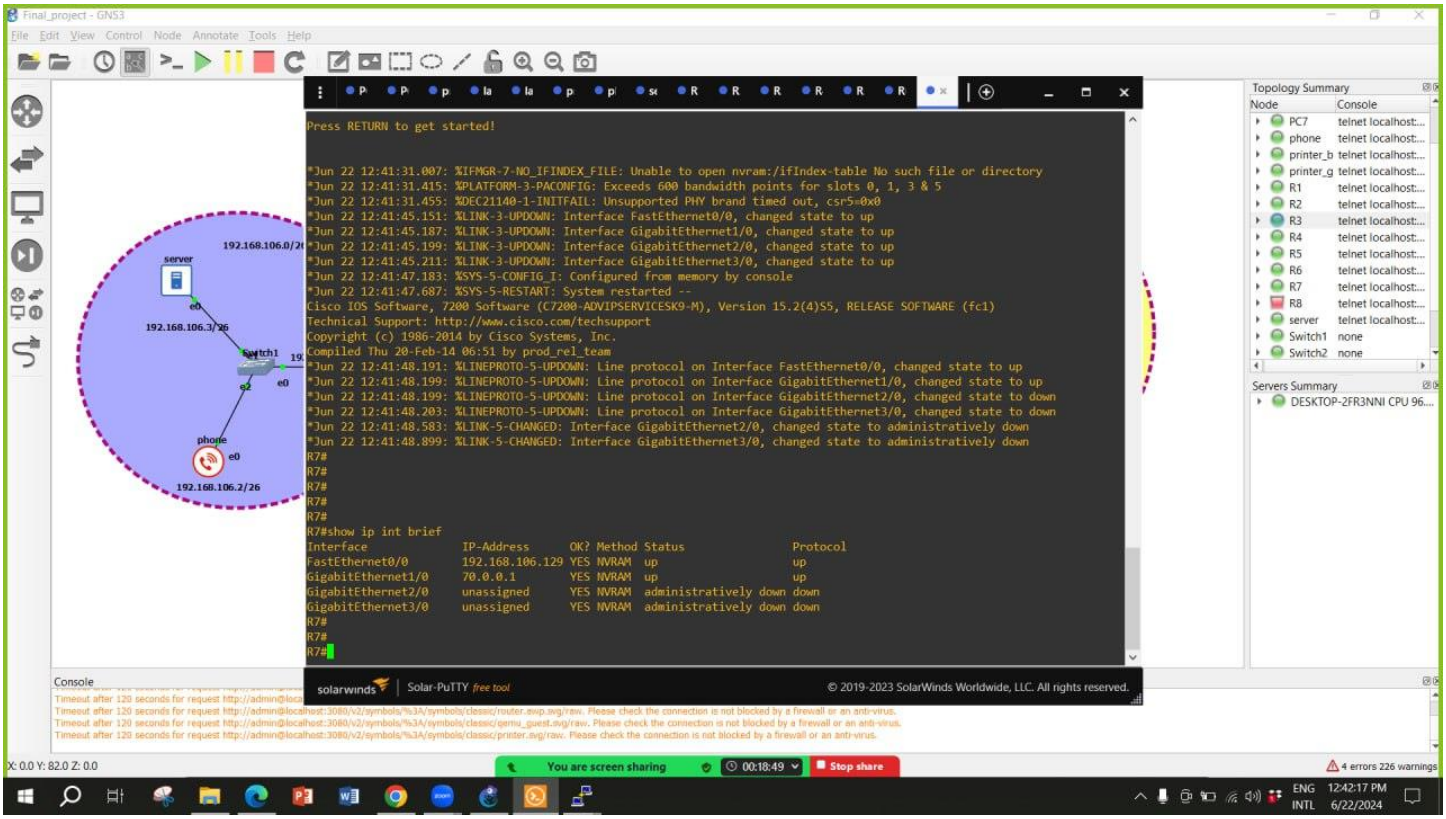


Figure: Show ip int breif **R7#**

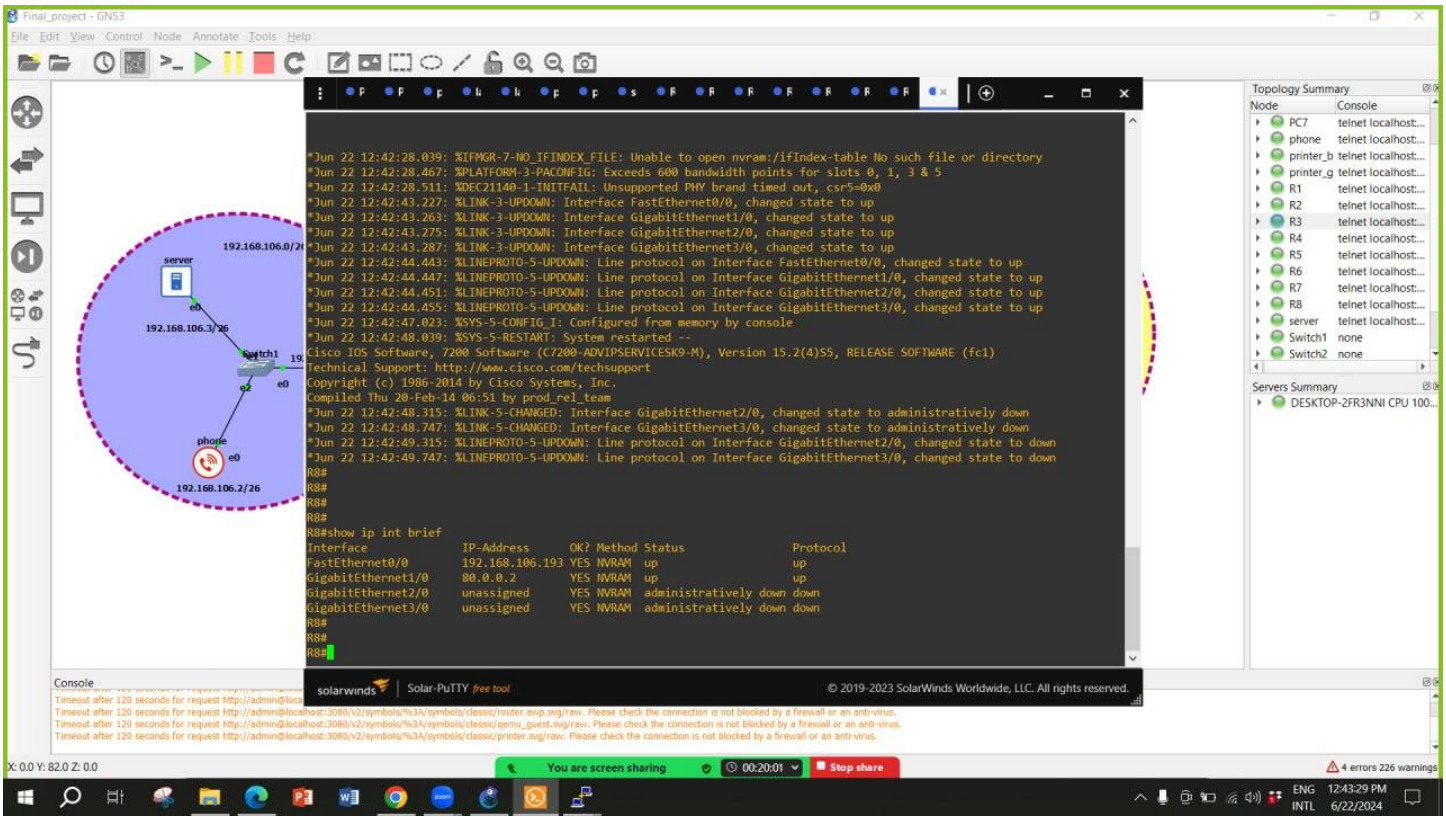


Figure: Show ip int breif **R8#**

5.4 Software and hardware

The following hardware and software were used in the project:

- Software

GNS3 (Graphical Network Simulator 3): A network simulation tool that allows for the design and testing of complex network topologies. GNS3 provides a graphical user interface that makes it easy to create and configure network devices, and to simulate the operation of a network.

Wireshark: A network protocol analyzer that captures and analyzes network traffic. Wireshark can be used to troubleshoot network problems, monitor network performance, and understand network protocols.

- Hardware

ROUTER (C7200): A high-performance enterprise router used for routing traffic between different network segments.

SWITCH: A device that connects multiple network devices together, enabling them to communicate with each other.

GigabyteEthernet CABLE: A cable used to connect network devices together.

5.5. Topology

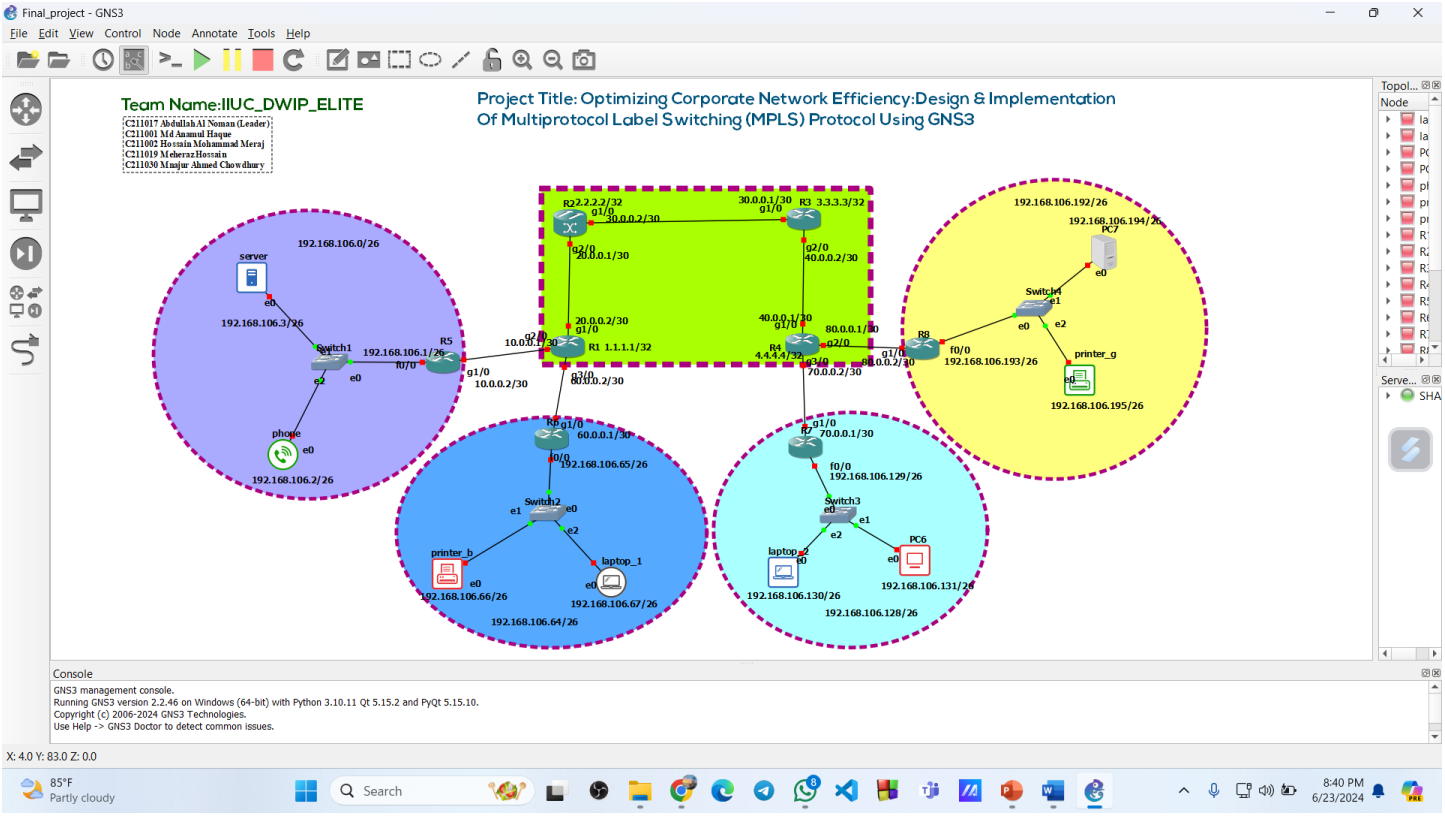


Figure: Topology

6. Implementation

6.1. Install GNS3

GNS3 is a network simulation software that allows you to create and test complex network topologies. It is a free and open-source software that is available for Windows, macOS, and Linux.

To install GNS3, we follow these steps:

a) Download the GNS3 installer from the GNS3 website: https://www.gns3.com/software/download

b) Run the installer and follow the on-screen instructions.

c) Once the installation is complete, launch GNS3.

6.2. Importing Routers

To import routers into GNS3, follow these steps:

- Click on the "Add New Device" button in the GNS3 toolbar.

(Edit >> Preferences >> IOS router templates >> Add New)

- Select the "New Image" tab/ radio button.
- Choose the type of router you want to import from the list of available routers. d) Click on the "Import" button.
- Browse to the location of the router image file and select it.

(In this case, one had to download the image before adding it. In our caser, we downloaded C7200- c7200-advipservicesk9-mz.152-4.S5 router from online)

- fClick on the "Open", then "Apply" button.

The router will be imported into GNS3. One can import multiple routers by following these steps multiple times.

6.3. Configurations

Once the routers have been imported into GNS3, they need to be configured with the appropriate IP addresses, subnet masks, and default gateways. To configure a router, follow these steps:

❖ Double-click on the router icon in the GNS3 workspace. In the Console window, enter the following commands:

➔ **R1**

```
Conf t
Int g1/0
ip address 10.0.0.2 255.255.255.252
No shut
Int g2/0

Ip address 10.0.0.1 255.255.255.252
No shut
Int g3/0
Ip address 60.0.0.2 255.255.255.252
No shut
Int lo/0
Ip address 1.1.1.1 255.255.255.255
exit
```

➔ R2

```
Conf t
Int g1/0
ip address 30.0.0.2 255.255.255.252
No shut
Int g2/0
Ip address 20.0.0.1 255.255.255.252
No shut
Int lo/0
Ip address 1.1.1.1 255.255.255.255
exit
```

➔ R3

```
Conf t
Int g1/0
ip address 30.0.0.1 255.255.255.252
No shut
Int g2/0
Ip address 40.0.0.2 255.255.255.252
No shut
Int lo/0
Ip address 3.3.3.3 255.255.255.255
exit
```

➔ R4

```
Conf t
Int g1/0
ip address 40.0.0.1 255.255.255.252
No shut
Int g2/0
Ip address 80.0.0.2 255.255.255.252
No shut
Int g3/0
Ip address 70.0.0.2 255.255.255.252
No shut
Int lo/0
Ip address 4.4.4.4 255.255.255.255
exit
```

➔ R5

```
Conf t
Int g1/0
ip address 10.0.0.2 255.255.255.252
No shut
Int f0/0
Ip address 192.168.106.1     255.255.255.192
No shut
exit
```

➔ R6

```
Conf t
Int g1/0
ip address 60.0.0.1 255.255.255.252
No shut
Int f0/0
Ip address 192.168.106.65 255.255.255.192
No shut
exit
```

➔ R7

```
Conf t
Int g1/0
ip address 70.0.0.1 255.255.255.252
No shut
Int f0/0
Ip address 192.168.106.129 255.255.255.129
No shut
Exit
```

➔ R8

```
Conf t
Int g1/0
ip address 80.0.0.2 255.255.255.252
No shut
Int f0/0
Ip address 192.168.106.193 255.255.255.192
No shut
exit
```

Configuring OSPF

To configure OSPF, follow these steps:

- Enter the following commands in the Console window of each router:
  - ➔ R1

```
Conf t
Router ospf 1
Network 10.0.0.0 0.0.0.3 area 10
Network 20.0.0.0 0.0.0.3 area 10
Network 60.0.0.0 0.0.0.3 area 10
Network 1.1.1.1 0.0.0.0 area 10
exit
```

➔ R2

```
Conf t
Router ospf 1
Network 30.0.0.0 0.0.0.3 area 10
Network 20.0.0.0 0.0.0.3 area 10
Network 2.2.2.2 0.0.0.0 area 10
exit
```

➔ R3

```
Conf t
Router ospf 1
Network 30.0.0.0 0.0.0.3 area 10
Network 40.0.0.0 0.0.0.3 area 10
Network 3.3.3.3 0.0.0.0 area 10
exit
```

➔ R4

```
Conf t
Router ospf 1
Network 40.0.0.0 0.0.0.3 area 10
Network 70.0.0.0 0.0.0.3 area 10
Network 80.0.0.0 0.0.0.3 area 10
Network 4.4.4.4 0.0.0.0 area 10
exit
```

Configuring MPLS

To configure VLANs, follow these steps:

o Enter the following commands in the Console window of each router:

➔ R1

```
Conf t
Ip cef
 Mpls label protocol ldp
Mpls label range 101 200
Int g2/0
Mpls ip
Int g1/0
Mpls ip
Int g3/0
Mpls ip
Exit
```

➔ R2

```
Conf t
Mpls label range 201 300
Int g1/0
Mpls ip
Int g2/0
Mpls ip
Int g3/0
Mpls ip

Exit
```

➔ R3

```
Conf t
Mpls label range 301 400
Ip cef
Int g1/0
Mpls ip
Int g2/0
Mpls ip
exit
```

➔ R4

```
Conf t
Mpls label range 301 400
Ip cef
Int g1/0
Mpls ip
Int g2/0
Mpls ip
Int g3/0
Mpls ip
exit
```

Configuring End Device

To configure a firewall, follow these steps:

o Enter the following commands in the Console window of the End device:

➔ Server

```
Ip 192.168.106.3 255.255.255.192 192.168.106.1
```

➔ Phone

```
Ip 192.168.106.2 255.255.255.192 192.168.106.1
```

➔ printer _b

```
Ip 192.168.106.66 255.255.255.192 192.168.106.65
```

➔ Laptop_1

```
Ip 192.168.106.67 255.255.255.192 192.168.106.66
```

➔ Laptop_2

```
Ip 192.168.106.130 255.255.255.192 192.168.106.129
```

➔ PC6

```
Ip 192.168.106.131 255.255.255.192 192.168.106.129
```

➔ Printer_g

```
Ip 192.168.106.194 255.255.255.192 192.168.106.193
```

➔ pc7

```
Ip 192.168.106.195 255.255.255.192 192.168.106.193
```

Once the routers have been configured, the network can be tested to ensure that it is functioning correctly. To test the network, follow these steps:

1. Use the GNS3 console to ping each router from another router.

- **R1 ping R4**

```
R1#
R1#
R1#ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 152/189/208 ms
R1#
R1#
```

2. Verify the mpls configuration

```
R1#show mpls ldp bindings local
  lib entry: 1.1.1.1/32, rev 8
        local binding:  label: imp-null
  lib entry: 2.2.2.2/32, rev 18
        local binding:  label: 105
  lib entry: 3.3.3.3/32, rev 23
        local binding:  label: 107
  lib entry: 4.4.4.4/32, rev 26
        local binding:  label: 109
  lib entry: 10.0.0.0/30, rev 4
        local binding:  label: imp-null
  lib entry: 20.0.0.0/30, rev 2
        local binding:  label: imp-null
  lib entry: 30.0.0.0/30, rev 20
        local binding:  label: 106
  lib entry: 40.0.0.0/30, rev 24
        local binding:  label: 108
  lib entry: 60.0.0.0/30, rev 6
        local binding:  label: imp-null
  lib entry: 70.0.0.0/30, rev 30
        local binding:  label: 111
  lib entry: 80.0.0.0/30, rev 28
        local binding:  label: 110
  lib entry: 192.168.106.0/26, rev 10
        local binding:  label: 101
  lib entry: 192.168.106.64/26, rev 12
        local binding:  label: 102
  lib entry: 192.168.106.128/26, rev 14
        local binding:  label: 103
  lib entry: 192.168.106.192/26, rev 16
        local binding:  label: 104
R1#
```

3.Check the traceroute

➔ from R1 can i find out laptop2 route

```
R1#
R1#
R1#traceroute 192.168.106.130
Type escape sequence to abort.
Tracing the route to 192.168.106.130
VRF info: (vrf in name/id, vrf out name/id)
  1 20.0.0.1 [MPLS: Label 203 Exp 0] 316 msec 208 msec 336 msec
  2 30.0.0.1 [MPLS: Label 303 Exp 0] 176 msec 188 msec 228 msec
  3 40.0.0.1 [MPLS: Label 403 Exp 0] 144 msec 148 msec 148 msec
  4 70.0.0.1 252 msec 216 msec 300 msec
  5 192.168.106.130 388 msec 284 msec 196 msec
R1#
R1#
```

➔ from R1 can i find out laptop1 route

```
R1#
R1#
R1#traceroute 192.168.106.67
Type escape sequence to abort.
Tracing the route to 192.168.106.67
VRF info: (vrf in name/id, vrf out name/id)
  1 60.0.0.1 144 msec 60 msec 40 msec
  2 192.168.106.67 344 msec 108 msec 132 msec
R1#
```

➔ from R1 can i find out server route

```
R1#
R1#
R1#traceroute 192.168.106.3
Type escape sequence to abort.
Tracing the route to 192.168.106.3
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.0.2 16 msec 80 msec 60 msec
  2 192.168.106.3 80 msec 44 msec 72 msec
R1#
R1#
```

➢ R3 ping R1

```
R3#
R3#
R3#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/93/192 ms
R3#
R3#
```

2. Verify the mpls configuration

```
R3#show mpls ldp bindings local
  lib entry: 1.1.1.1/32, rev 18
        local binding:  label: 306
  lib entry: 2.2.2.2/32, rev 16
        local binding:  label: 305
  lib entry: 3.3.3.3/32, rev 2
        local binding:  label: imp-null
  lib entry: 4.4.4.4/32, rev 26
        local binding:  label: 310
  lib entry: 10.0.0.0/30, rev 22
        local binding:  label: 308
  lib entry: 20.0.0.0/30, rev 24
        local binding:  label: 309
  lib entry: 30.0.0.0/30, rev 4
        local binding:  label: imp-null
  lib entry: 40.0.0.0/30, rev 6
        local binding:  label: imp-null
  lib entry: 60.0.0.0/30, rev 20
        local binding:  label: 307
  lib entry: 70.0.0.0/30, rev 30
        local binding:  label: 312
  lib entry: 80.0.0.0/30, rev 28
        local binding:  label: 311
  lib entry: 192.168.106.0/26, rev 8
        local binding:  label: 301
  lib entry: 192.168.106.64/26, rev 10
        local binding:  label: 302
  lib entry: 192.168.106.128/26, rev 12
        local binding:  label: 303
  lib entry: 192.168.106.192/26, rev 14
        local binding:  label: 304
R3#
```

3.Check the traceroute

➔ from R1 can i find out phone route

```
R3#
R3#
R3#traceroute 192.168.106.2
Type escape sequence to abort.
Tracing the route to 192.168.106.2
VRF info: (vrf in name/id, vrf out name/id)
  1 30.0.0.2 [MPLS: Label 201 Exp 0] 212 msec 184 msec 308 msec
  2 20.0.0.2 [MPLS: Label 101 Exp 0] 220 msec 152 msec 256 msec
  3 10.0.0.2 268 msec 260 msec 216 msec
  4 192.168.106.2 328 msec 260 msec 184 msec
R3#
R3#
```

➔ from R1 can i find out printer_b route

```
R3#
R3#
R3#traceroute 192.168.106.66
Type escape sequence to abort.
Tracing the route to 192.168.106.66
VRF info: (vrf in name/id, vrf out name/id)
  1 30.0.0.2 [MPLS: Label 202 Exp 0] 312 msec 148 msec 128 msec
  2 20.0.0.2 [MPLS: Label 102 Exp 0] 88 msec 112 msec 92 msec
  3 60.0.0.1 192 msec 192 msec 204 msec
  4 192.168.106.66 316 msec 280 msec 288 msec
R3#
R3#
```

➔ from R1 can i find out printer_g route

```
R3#
R3#
R3#traceroute 192.168.106.195
Type escape sequence to abort.
Tracing the route to 192.168.106.195
VRF info: (vrf in name/id, vrf out name/id)
  1 40.0.0.1 [MPLS: Label 404 Exp 0] 76 msec 68 msec 76 msec
  2 80.0.0.2 108 msec 92 msec 168 msec
  3 192.168.106.195 364 msec 164 msec 140 msec
R3#
R3#
```

7. Experimental and Theoretical Results

7.1. Ping tool: solar putty tools

The ping tool used in our project was Solar-PuTTY. PuTTY is a free and open-source terminal emulator, SSH, and telnet client. It supports a variety of protocols, including Telnet, SSH, login, and raw socket connections. PuTTY is a popular tool for connecting to Unix-based systems and network devices.

The ping tool is a simple but useful tool for troubleshooting network problems. It can be used to:
o Test the reachability of a host on an IP network o Measure the latency between two hosts on an IP network o Identify network problems, such as packet loss or congestion.
In the context of the previous experiments, PuTTY was used as a ping tool to test the reachability of hosts on the network. The ping tool is a network utility used to test the reachability of a host on an IP network. It works by sending an ICMP (Internet Control Message Protocol) echo request packet to the destination host and waiting for an ICMP echo response packet. If the destination host is reachable, it will respond to the echo request packet with an echo response packet. The ping tool will then display the time it took for the echo request packet to reach the destination host and for the echo response packet to return.

To use the ping tool, you will need to know the IP address of the host that you want to ping. PuTTY can be used as a ping tool by using the following command:

```
ping <ip address>
```

7.2. Pinging in the same Network

Pinging between devices in the same network was successful for all devices. This indicates that the devices are able to communicate with each other properly. According to our project for Example

```
server>
server> ping 192.168.106.2
84 bytes from 192.168.106.2 icmp_seq=1 ttl=64 time=1.055 ms
84 bytes from 192.168.106.2 icmp_seq=2 ttl=64 time=56.747 ms
84 bytes from 192.168.106.2 icmp_seq=3 ttl=64 time=0.556 ms
84 bytes from 192.168.106.2 icmp_seq=4 ttl=64 time=1.004 ms
84 bytes from 192.168.106.2 icmp_seq=5 ttl=64 time=1.829 ms
```

Ping in the same network (server to phone)		Average
84 bytes from 192.168.106.2 icmp_seq=1 ttl=64 time=1.055 ms	1.055 ms	12.23
84 bytes from 192.168.106.2 icmp_seq=2 ttl=64 time=56.747 ms	56.747 ms	
84 bytes from 192.168.106.2 icmp_seq=3 ttl=64 time=0.556 ms	0.556 ms	
84 bytes from 192.168.106.2 icmp_seq=4 ttl=64 time=1.004 ms	1.004 ms	
84 bytes from 192.168.106.2 icmp_seq=5 ttl=64 time=1.829 ms	1.829 ms	
	61.191 ms	

7.3. Pinging the Gateway

Pinging the gateway was successful. This indicates that the devices are able to communicate with the gateway properly. According to our project for Example,

Ping to the gateway (server to Printer_b)		Average
192.168.106.66 icmp_seq=1 timeout	0	117.99
192.168.106.66 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.66 icmp_seq=3 ttl=61 time=120.664 ms	120.664 ms	
84 bytes from 192.168.106.66 icmp_seq=4 ttl=61 time=183.325 ms	183.325 ms	
84 bytes from 192.168.106.66 icmp_seq=5 ttl=61 time=285.961 ms	285.961 ms	

Ping to the gateway(Server to Laptop_1)		Average
192.168.106.66 icmp_seq=1 timeout	0	**117.99**
192.168.106.66 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.66 icmp_seq=3 ttl=61 time=120.664 ms	120.664 ms	
84 bytes from 192.168.106.66 icmp_seq=4 ttl=61 time=183.325 ms	183.325 ms	
84 bytes from 192.168.106.66 icmp_seq=5 ttl=61 time=285.961 ms	285.961 ms	

Ping to the gateway (Server to Laptop_2)		Average
192.168.106.130 icmp_seq=1 timeout	0	**230.20**
192.168.106.130 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.130 icmp_seq=3 ttl=58 time=331.279 ms	331.279 ms	
84 bytes from 192.168.106.130 icmp_seq=4 ttl=58 time=540.483 ms	540.483 ms	
84 bytes from 192.168.106.130 icmp_seq=5 ttl=58 time=279.271 ms	279.271 ms	

Ping to the gateway (Server to printer_g)		Average
192.168.106.195 icmp_seq=1 timeout	0	**263.97**
192.168.106.195 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.195 icmp_seq=3 ttl=58 time=539.105 ms	539.105 ms	
84 bytes from 192.168.106.195 icmp_seq=4 ttl=58 time=379.296 ms	379.296 ms	
84 bytes from 192.168.106.195 icmp_seq=5 ttl=58 time=401.461 ms	401.461 ms	

Ping to the gateway (Server toPC_6)		Average
server> ping 192.168.106.131		292.18
84 bytes from 192.168.106.131 icmp_seq=1 ttl=58 time=500.279 ms	500.279 ms	
84 bytes from 192.168.106.131 icmp_seq=2 ttl=58 time=333.967 ms	333.967 ms	
84 bytes from 192.168.106.131 icmp_seq=3 ttl=58 time=342.034 ms	333.967 ms	
84 bytes from 192.168.106.131 icmp_seq=4 ttl=58 time=292.714 ms	292.714 ms	

Pinging in the same Network

```
laptop_1>
laptop_1>
laptop_1> ping 192.168.106.66
84 bytes from 192.168.106.66 icmp_seq=1 ttl=64 time=0.722 ms
84 bytes from 192.168.106.66 icmp_seq=2 ttl=64 time=0.980 ms
84 bytes from 192.168.106.66 icmp_seq=3 ttl=64 time=0.723 ms
84 bytes from 192.168.106.66 icmp_seq=4 ttl=64 time=35.291 ms
84 bytes from 192.168.106.66 icmp_seq=5 ttl=64 time=43.697 ms
```

Ping in the same network (Laptop_1 to Printer_b)		Average
84 bytes from 192.168.106.66 icmp_seq=1 ttl=64 time=0.722 ms	0.722 ms	7.54
84 bytes from 192.168.106.66 icmp_seq=2 ttl=64 time=0.980 ms	0.980 ms	
84 bytes from 192.168.106.66 icmp_seq=3 ttl=64 time=0.723 ms	0.723 ms	
84 bytes from 192.168.106.66 icmp_seq=4 ttl=64 time=35.291 ms	35.291 ms	
84 bytes from 192.168.106.66 icmp_seq=5 ttl=64 time=43.697 ms	43.69	

Pinging the Gateway

Ping to the gateway (Laptop_1 to Phone)		Average
192.168.106.2 icmp_seq=1 timeout	0	139.54
192.168.106.2 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.2 icmp_seq=3 ttl=61 time=365.382 ms	365.382 ms	
84 bytes from 192.168.106.2 icmp_seq=4 ttl=61 time=210.796 ms	210.796 ms	
84 bytes from 192.168.106.2 icmp_seq=5 ttl=61 time=121.529 ms	121.529 ms	

Ping to the gateway (Laptop_1 to Server)		Average
192.168.106.3 icmp_seq=1 timeout	0	121.51
192.168.106.3 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.3 icmp_seq=3 ttl=61 time=226.948 ms	226.948 ms	
84 bytes from 192.168.106.3 icmp_seq=4 ttl=61 time=163.509 ms	163.509 ms	
84 bytes from 192.168.106.3 icmp_seq=5 ttl=61 time=217.097 ms	217.097 ms	

Ping to the gateway (Laptop_1 to Laptop_2)		Average
192.168.106.130 icmp_seq=1 timeout	0	259.46
192.168.106.130 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.130 icmp_seq=3 ttl=58 time=389.759 ms	389.759 ms	
84 bytes from 192.168.106.130 icmp_seq=4 ttl=58 time=399.116 ms	399.116 ms	
84 bytes from 192.168.106.130 icmp_seq=5 ttl=58 time=508.468 ms	508.468 ms	

Ping to the gateway (Laptop_1 to PC_6)		Average
192.168.106.131 icmp_seq=1 timeout	0	221.77
192.168.106.131 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.131 icmp_seq=3 ttl=58 time=402.373 ms	402.373 ms	
84 bytes from 192.168.106.131 icmp_seq=4 ttl=58 time=414.516 ms	414.516 ms	
84 bytes from 192.168.106.131 icmp_seq=5 ttl=58 time=291.973 ms	291.973 ms	

Ping to the gateway (Laptop_1 to PC_7)		Average
84 bytes from 192.168.106.194 icmp_seq=1 ttl=58 time=406.219 ms	291.973 ms	339.97
84 bytes from 192.168.106.194 icmp_seq=2 ttl=58 time=414.060 ms	414.060 ms	
84 bytes from 192.168.106.194 icmp_seq=3 ttl=58 time=386.270 ms	386.270 ms	
84 bytes from 192.168.106.194 icmp_seq=4 ttl=58 time=292.035 ms	292.035 ms	
84 bytes from 192.168.106.194 icmp_seq=5 ttl=58 time=315.540 ms	315.540 ms	

Ping to the gateway (Laptop_1 to Printer_g)		Average
192.168.106.195 icmp_seq=1 timeout	0	199.57
192.168.106.195 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.195 icmp_seq=3 ttl=58 time=385.393 ms	385.393 ms	
84 bytes from 192.168.106.195 icmp_seq=4 ttl=58 time=363.737 ms	363.737 ms	
84 bytes from 192.168.106.195 icmp_seq=5 ttl=58 time=248.732 ms	248.732 ms	

Pinging in the same Network

```
PC6>
PC6> ping 192.168.106.130
84 bytes from 192.168.106.130 icmp_seq=1 ttl=64 time=0.822 ms
84 bytes from 192.168.106.130 icmp_seq=2 ttl=64 time=1.185 ms
84 bytes from 192.168.106.130 icmp_seq=3 ttl=64 time=0.960 ms
84 bytes from 192.168.106.130 icmp_seq=4 ttl=64 time=0.926 ms
84 bytes from 192.168.106.130 icmp_seq=5 ttl=64 time=7.130 ms
```

Ping in the same network (PC_6 to Laptop_2)		Average
84 bytes from 192.168.106.130 icmp_seq=1 ttl=64 time=0.822 ms	248.732 ms	**51.78**
84 bytes from 192.168.106.130 icmp_seq=2 ttl=64 time=1.185 ms	1.185 ms	
84 bytes from 192.168.106.130 icmp_seq=3 ttl=64 time=0.960 ms	0.960 ms	
84 bytes from 192.168.106.130 icmp_seq=4 ttl=64 time=0.926 ms	0.926 ms	
84 bytes from 192.168.106.130 icmp_seq=5 ttl=64 time=7.130 ms	7.130 ms	

Pinging the Gateway

Ping to the gateway (PC_6 to PC_7)		Average
192.168.106.194 icmp_seq=1 timeout	0	**108.83**
192.168.106.194 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.194 icmp_seq=3 ttl=61 time=216.082 ms	216.082 ms	
84 bytes from 192.168.106.194 icmp_seq=4 ttl=61 time=211.414 ms	211.414 ms	
84 bytes from 192.168.106.194 icmp_seq=5 ttl=61 time=116.655 ms	116.655 ms	

Ping to the gateway (PC_6 to Printer_b)		Average
192.168.106.66 icmp_seq=1 timeout	0	272.41
192.168.106.66 icmp_seq=2 timeout	0	

84 bytes from 192.168.106.66 icmp_seq=3 ttl=58 time=482.612 ms	482.612 ms	
84 bytes from 192.168.106.66 icmp_seq=4 ttl=58 time=507.541 ms	507.541 ms	
84 bytes from 192.168.106.66 icmp_seq=5 ttl=58 time=371.899 ms	371.899 ms	

Ping to the gateway (PC_6 to Phone)		Average
192.168.106.2 icmp_seq=1 timeout	0	260.36
192.168.106.2 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.2 icmp_seq=3 ttl=58 time=397.558 ms	397.558 ms	
84 bytes from 192.168.106.2 icmp_seq=4 ttl=58 time=517.165 ms	517.165 ms	
84 bytes from 192.168.106.2 icmp_seq=5 ttl=58 time=387.079 ms	387.079 ms	

Pinging in the same Network

```
PC7>
PC7> ping 192.168.106.195
84 bytes from 192.168.106.195 icmp_seq=1 ttl=64 time=0.821 ms
84 bytes from 192.168.106.195 icmp_seq=2 ttl=64 time=1.229 ms
84 bytes from 192.168.106.195 icmp_seq=3 ttl=64 time=1.016 ms
84 bytes from 192.168.106.195 icmp_seq=4 ttl=64 time=0.915 ms
84 bytes from 192.168.106.195 icmp_seq=5 ttl=64 time=0.926 ms
```

Ping in the same network (PC_7 to Printer_g)		Average
84 bytes from 192.168.106.195 icmp_seq=1 ttl=64 time=0.821 ms	387.079 ms	**78.23**
84 bytes from 192.168.106.195 icmp_seq=2 ttl=64 time=1.229 ms	1.229 ms	
84 bytes from 192.168.106.195 icmp_seq=3 ttl=64 time=1.016 ms	1.016 ms	
84 bytes from 192.168.106.195 icmp_seq=4 ttl=64 time=0.915 ms	0.915 ms	
84 bytes from 192.168.106.195 icmp_seq=5 ttl=64 time=0.926 ms	0.926 ms	

Pinging the Gateway

Ping to the gateway (PC_7 to PC_6)		Average
192.168.106.131 icmp_seq=1 timeout	0	108.29
192.168.106.131 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.131 icmp_seq=3 ttl=61 time=188.688 ms	188.688 ms	
84 bytes from 192.168.106.131 icmp_seq=4 ttl=61 time=168.266 ms	168.266 ms	
84 bytes from 192.168.106.131 icmp_seq=5 ttl=61 time=184.543 ms	184.543 ms	

Ping to the gateway (PC_7 to Laptop_2)		Average
192.168.106.130 icmp_seq=1 timeout	0	114.51
192.168.106.130 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.130 icmp_seq=3 ttl=61 time=224.357 ms	224.357 ms	
84 bytes from 192.168.106.130 icmp_seq=4 ttl=61 time=218.429 ms	218.429 ms	
84 bytes from 192.168.106.130 icmp_seq=5 ttl=61 time=129.782 ms	129.782 ms	

Ping to the gateway (PC_7 to Printer_b)		Average
192.168.106.66 icmp_seq=1 timeout	0	224.25
192.168.106.66 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.66 icmp_seq=3 ttl=58 time=397.691 ms	397.691 ms	
84 bytes from 192.168.106.66 icmp_seq=4 ttl=58 time=310.317 ms	310.317 ms	

84 bytes from 192.168.106.66 icmp_seq=5 ttl=58 time=413.264 ms	413.264 ms	

Ping to the gateway (PC_7 to Server)		Average
192.168.106.3 icmp_seq=1 timeout	0	225.66
192.168.106.3 icmp_seq=2 timeout	0	
84 bytes from 192.168.106.3 icmp_seq=3 ttl=58 time=423.149 ms	423.149 ms	
84 bytes from 192.168.106.3 icmp_seq=4 ttl=58 time=376.746 ms	376.746 ms	
84 bytes from 192.168.106.3 icmp_seq=5 ttl=58 time=328.423 ms	328.423 ms	

7.4. Pinging the Core router

➔ Ping R1 to R2

```
R1#
R1#
R1#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/68/124 ms
```

➔ Ping R1 to R3

```
R1#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/75/96 ms
R1#
```

➔ Ping R1 to R4

```
R1#
R1#ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/197/260 ms
R1#
```

➔ Ping R2 to R1

```
R2#
R2#
R2#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/76/152 ms
```

➔ Ping R2 to R3

```
R2#
R2#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/67/96 ms
R2#
```

➔ Ping R2 to R4

```
R2#
R2#ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/111/132 ms
R2#
```

➔ Ping R3 to R1

```
R3#
R3#
R3#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/172/220 ms
```

➔ Ping R3 to R2

```
R3#
R3#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/108/216 ms
R3#
```

➔ Ping R3 to R4

```
R3#
R3#ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/68/116 ms
R3#
R3#
```

➔ Ping R4 to R1

```
R4#
R4#
R4#ping 1.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 192/232/248 ms
```

➔ Ping R4 to R2

```
R4#
R4#ping 2.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/136/220 ms
R4#
```

➔ Ping R4 to R3

```
R4#
R4#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/72/108 ms
R4#
R4#
```

7.5. Pinging the host on other network

Pinging a host on another network was successful for both hosts. This indicates that the devices are able to communicate with hosts on other networks properly. According to our project for Example,

Ping to the gateway (phone to R8)

phone>

phone>

phone> ping 192.168.106.193

84 bytes from 192.168.106.193 icmp_seq=1 ttl=250 time=360.754 ms

84 bytes from 192.168.106.193 icmp_seq=2 ttl=250 time=415.086 ms

84 bytes from 192.168.106.193 icmp_seq=3 ttl=250 time=355.446 ms

84 bytes from 192.168.106.193 icmp_seq=4 ttl=250 time=369.646 ms

84 bytes from 192.168.106.193 icmp_seq=5 ttl=250 time=490.510 ms

Average Time-The average time is approximately **398.29 ms**.

Ping to the gateway (phone to R7)

```
phone>
phone>
phone> ping 192.168.106.129
84 bytes from 192.168.106.129 icmp_seq=1 ttl=250 time=372.502 ms
84 bytes from 192.168.106.129 icmp_seq=2 ttl=250 time=341.650 ms
84 bytes from 192.168.106.129 icmp_seq=3 ttl=250 time=238.860 ms
84 bytes from 192.168.106.129 icmp_seq=4 ttl=250 time=176.218 ms
84 bytes from 192.168.106.129 icmp_seq=5 ttl=250 time=272.568 ms
```

Average Time- The average time is approximately **280.36 ms**.

Ping to the gateway (phone to R6)

```
phone>
phone>
phone> ping 192.168.106.65
84 bytes from 192.168.106.65 icmp_seq=1 ttl=253 time=171.151 ms
84 bytes from 192.168.106.65 icmp_seq=2 ttl=253 time=86.957 ms
84 bytes from 192.168.106.65 icmp_seq=3 ttl=253 time=159.388 ms
84 bytes from 192.168.106.65 icmp_seq=4 ttl=253 time=170.425 ms
84 bytes from 192.168.106.65 icmp_seq=5 ttl=253 time=150.341 ms
```

Average Time- approximately **147.65 ms**.

Ping to the gateway (phone to R5)

```
phone>
phone>
phone> ping 192.168.106.1
84 bytes from 192.168.106.1 icmp_seq=1 ttl=255 time=69.481 ms
84 bytes from 192.168.106.1 icmp_seq=2 ttl=255 time=38.510 ms
84 bytes from 192.168.106.1 icmp_seq=3 ttl=255 time=37.213 ms
84 bytes from 192.168.106.1 icmp_seq=4 ttl=255 time=42.529 ms
84 bytes from 192.168.106.1 icmp_seq=5 ttl=255 time=10.971 ms
```

Average Time- approximately **39.74 ms**.

Ping to the gateway (laptop_1 to R8)

laptop_1> ping 192.168.106.193
84 bytes from 192.168.106.193 icmp_seq=1 ttl=250 time=343.250 ms
84 bytes from 192.168.106.193 icmp_seq=2 ttl=250 time=309.414 ms
84 bytes from 192.168.106.193 icmp_seq=3 ttl=250 time=338.813 ms
84 bytes from 192.168.106.193 icmp_seq=4 ttl=250 time=372.063 ms
84 bytes from 192.168.106.193 icmp_seq=5 ttl=250 time=485.929 ms

The average ping time to 192.168.106.193 from laptop_1 is approximately **369.49 ms**.

Ping to the gateway (laptop_1 to R7)

laptop_1>
laptop_1>
laptop_1> ping 192.168.106.129
84 bytes from 192.168.106.129 icmp_seq=1 ttl=250 time=367.567 ms
84 bytes from 192.168.106.129 icmp_seq=2 ttl=250 time=379.177 ms
84 bytes from 192.168.106.129 icmp_seq=3 ttl=250 time=332.953 ms
84 bytes from 192.168.106.129 icmp_seq=4 ttl=250 time=358.582 ms
84 bytes from 192.168.106.129 icmp_seq=5 ttl=250 time=379.807 ms
The average ping time to 192.168.106.129 from laptop_1 is approximately **363.22 ms**.

Ping to the gateway (laptop_1 to R6)

laptop_1>
laptop_1> ping 192.168.106.65
84 bytes from 192.168.106.65 icmp_seq=1 ttl=255 time=40.410 ms
84 bytes from 192.168.106.65 icmp_seq=2 ttl=255 time=45.899 ms
84 bytes from 192.168.106.65 icmp_seq=3 ttl=255 time=55.793 ms
84 bytes from 192.168.106.65 icmp_seq=4 ttl=255 time=34.907 ms
84 bytes from 192.168.106.65 icmp_seq=5 ttl=255 time=78.302 ms

The average ping time to 192.168.106.65 from laptop_1 is approximately **51.06 ms**.

Ping to the gateway (laptop_1 to R5)

laptop_1>
laptop_1>
laptop_1> ping 192.168.106.1
84 bytes from 192.168.106.1 icmp_seq=1 ttl=253 time=241.665 ms
84 bytes from 192.168.106.1 icmp_seq=2 ttl=253 time=127.567 ms
84 bytes from 192.168.106.1 icmp_seq=3 ttl=253 time=186.306 ms
84 bytes from 192.168.106.1 icmp_seq=4 ttl=253 time=161.732 ms
84 bytes from 192.168.106.1 icmp_seq=5 ttl=253 time=159.398 ms

The average ping time to 192.168.106.1 from laptop_1 is approximately **175.33 ms**.

Ping to the gateway (P6 to R8)

PC6>
PC6>
PC6> ping 192.168.106.193
84 bytes from 192.168.106.193 icmp_seq=1 ttl=253 time=110.926 ms
84 bytes from 192.168.106.193 icmp_seq=2 ttl=253 time=148.735 ms
84 bytes from 192.168.106.193 icmp_seq=3 ttl=253 time=164.967 ms
84 bytes from 192.168.106.193 icmp_seq=4 ttl=253 time=170.008 ms
84 bytes from 192.168.106.193 icmp_seq=5 ttl=253 time=152.004 ms
Average Time (ms): ≈149.328

Ping to the gateway (P6 to R7)

PC6>
PC6> ping 192.168.106.129
84 bytes from 192.168.106.129 icmp_seq=1 ttl=255 time=43.254 ms
84 bytes from 192.168.106.129 icmp_seq=2 ttl=255 time=45.130 ms
84 bytes from 192.168.106.129 icmp_seq=3 ttl=255 time=18.208 ms
84 bytes from 192.168.106.129 icmp_seq=4 ttl=255 time=10.234 ms
84 bytes from 192.168.106.129 icmp_seq=5 ttl=255 time=8.132 ms
Average Time (ms): ≈24.591

Ping to the gateway (P6 to R6)

PC6>
PC6> ping 192.168.106.65
84 bytes from 192.168.106.65 icmp_seq=1 ttl=250 time=319.093 ms
84 bytes from 192.168.106.65 icmp_seq=2 ttl=250 time=341.592 ms
84 bytes from 192.168.106.65 icmp_seq=3 ttl=250 time=236.609 ms
84 bytes from 192.168.106.65 icmp_seq=4 ttl=250 time=290.400 ms
84 bytes from 192.168.106.65 icmp_seq=5 ttl=250 time=257.147 ms

Average Time (ms): ≈288.768

Ping to the gateway (P7 to R8)

PC7>
PC7>
PC7> ping 192.168.106.193
84 bytes from 192.168.106.193 icmp_seq=1 ttl=255 time=42.933 ms
84 bytes from 192.168.106.193 icmp_seq=2 ttl=255 time=37.372 ms
84 bytes from 192.168.106.193 icmp_seq=3 ttl=255 time=22.709 ms
84 bytes from 192.168.106.193 icmp_seq=4 ttl=255 time=32.782 ms
84 bytes from 192.168.106.193 icmp_seq=5 ttl=255 time=33.054 ms

Average Time (ms): 33.37

Ping to the gateway (P7 to R7)

PC7>
PC7> ping 192.168.106.129
84 bytes from 192.168.106.129 icmp_seq=1 ttl=253 time=177.624 ms
84 bytes from 192.168.106.129 icmp_seq=2 ttl=253 time=153.028 ms
84 bytes from 192.168.106.129 icmp_seq=3 ttl=253 time=221.348 ms
84 bytes from 192.168.106.129 icmp_seq=4 ttl=253 time=119.339 ms
84 bytes from 192.168.106.129 icmp_seq=5 ttl=253 time=143.466 ms
Average Time (ms): ≈162.561

Ping to the gateway (P7 to R6)

PC7>
PC7> ping 192.168.106.65
84 bytes from 192.168.106.65 icmp_seq=1 ttl=250 time=268.381 ms
84 bytes from 192.168.106.65 icmp_seq=2 ttl=250 time=235.138 ms
84 bytes from 192.168.106.65 icmp_seq=3 ttl=250 time=396.062 ms
84 bytes from 192.168.106.65 icmp_seq=4 ttl=250 time=456.547 ms
84 bytes from 192.168.106.65 icmp_seq=5 ttl=250 time=362.162 ms
Average Time (ms): ≈343.858

Ping to the gateway (P7 to R5)

PC7>
PC7> ping 192.168.106.1
84 bytes from 192.168.106.1 icmp_seq=1 ttl=250 time=277.999 ms
84 bytes from 192.168.106.1 icmp_seq=2 ttl=250 time=400.980 ms
84 bytes from 192.168.106.1 icmp_seq=3 ttl=250 time=338.404 ms
84 bytes from 192.168.106.1 icmp_seq=4 ttl=250 time=285.406 ms
84 bytes from 192.168.106.1 icmp_seq=5 ttl=250 time=304.741 ms
Average Time (ms): ≈321.306

7.6. Table of ping results

Ping Sequence	Ping from server (192.168.106.3)						
	Time(ms)						
	Phone	**Printer_b**	**Laptop_1**	**Laptop_2**	**PC_6**	**Printer_g**	**PC_7**
1	1.05	0	0	0	500.27	0	133.99
2	56.74	0	0	0	333.96	0	188.91
3	0.55	120.66	120.66	331.27	342.04	539.10	210.927
4	1.4404	183.32	183.32	540.48	292.71	379.29	265.26
5	1.82	285.96	285.96	279.27	420.87	401.46	217.84

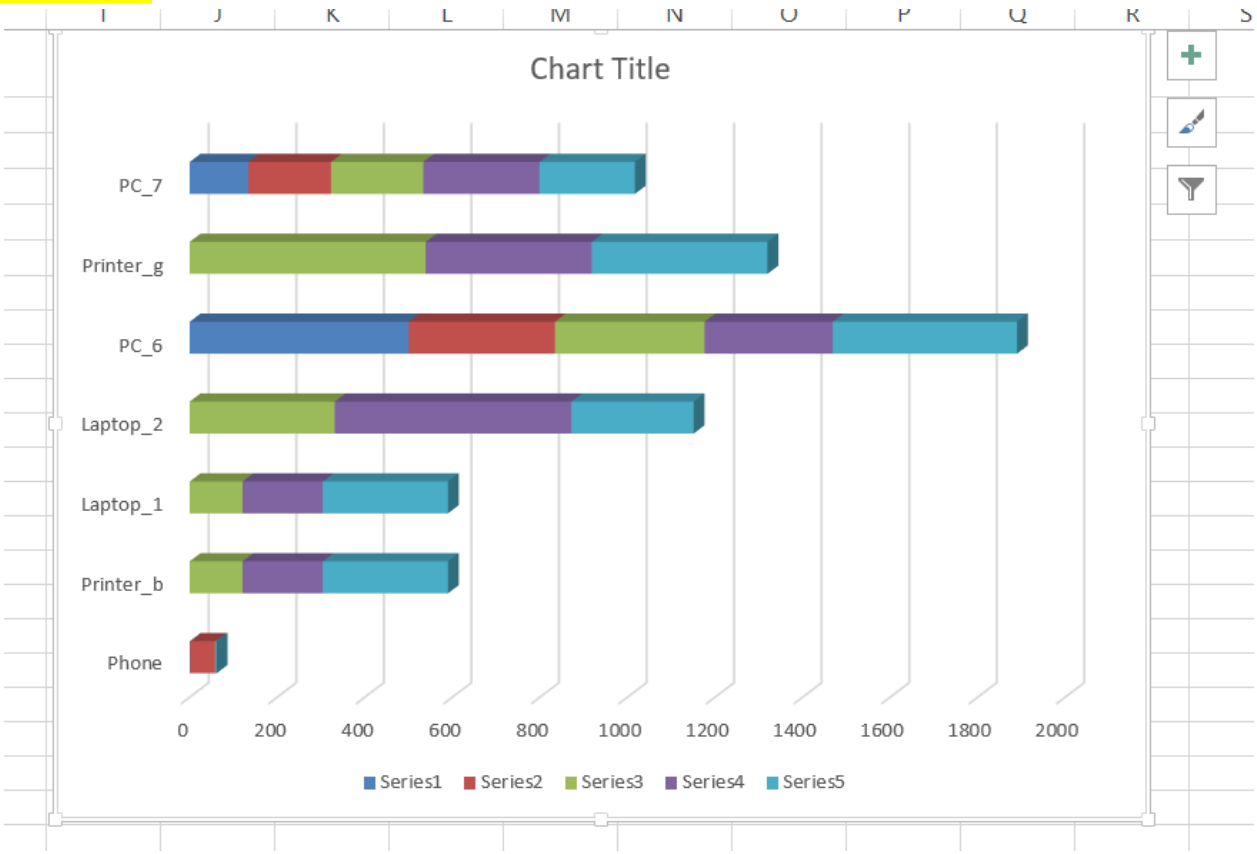
Ping Sequence	Ping from a Laptop_1 (192.168.106.67)						
	Time(ms)						
	Phone	**Printer_b**	**Server**	**Laptop_2**	**PC_6**	**Printer_g**	**PC_7**
1	0	0.722 ms	0	0	0	0	291.97
2	0	0.980 ms	0	0	0	0	414.06
3	365.38	0.723 ms	226.92	389.75	402.37	385.39	386.27
4	210.79	35.291 ms	163.50	399.11	414.51	363.73	292.03
5	121.52	43.69	217.09	508.46	291.97	248.73	315.54

Ping Sequence	Ping from a PC_6 (192.168.106.131)						
	Time(ms)						
	Phone	Printer_b	Server	Laptop_2	PC_6	Printer_g	PC_7
1	0	0		248.73		387.07	0
2	0	0		1.18		1.22	0
3	397.55	482.61		0.96		1.01	216.08
4	517.16	507.54		0.92		0.91	211.41
5	387.07	371.89		7.13		0.92	116.65

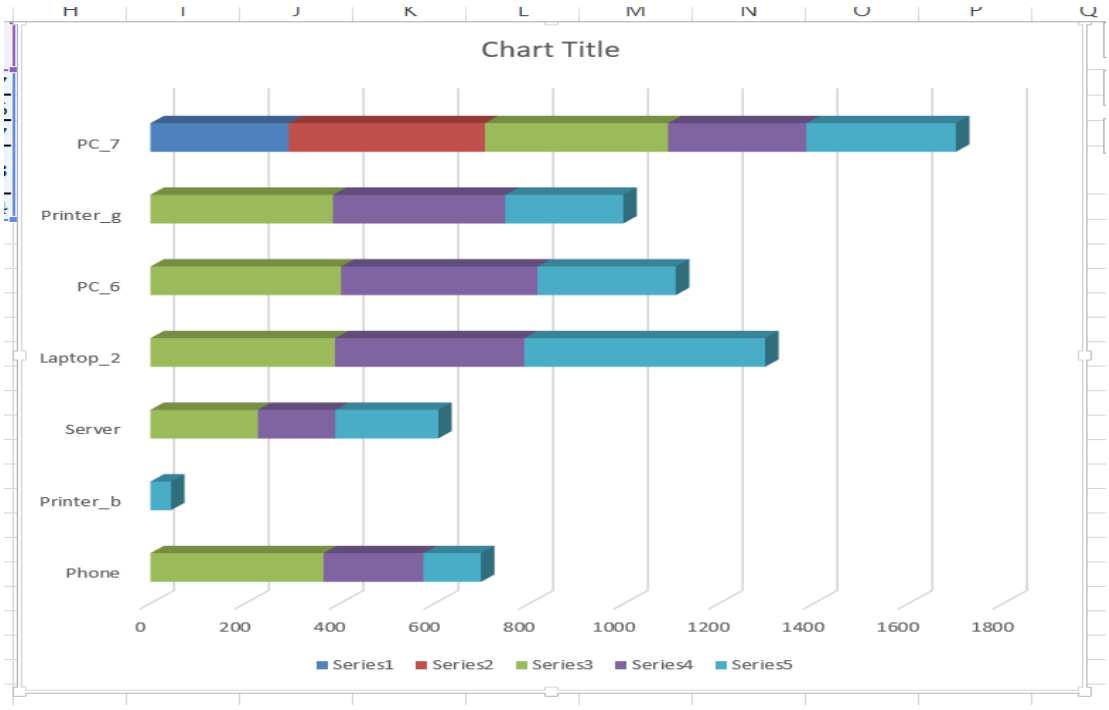
Ping Sequence	Ping from a PC_7 (192.168.106.131)						
	Time(ms)						
	Phone	Printer_b	Server	Laptop_2	PC_6	Printer_g	PC_7
1		00	00	0	0	387.07	
2		00	00	0	0	1.22	
3		397.69	423.14	224.35	188.68	1.01	
4		310.31	376.74	228.42	168.26	0.91	
5		413.26	328.42	129.78	184.54	0.92	

7.7. Bar chart of Ping results

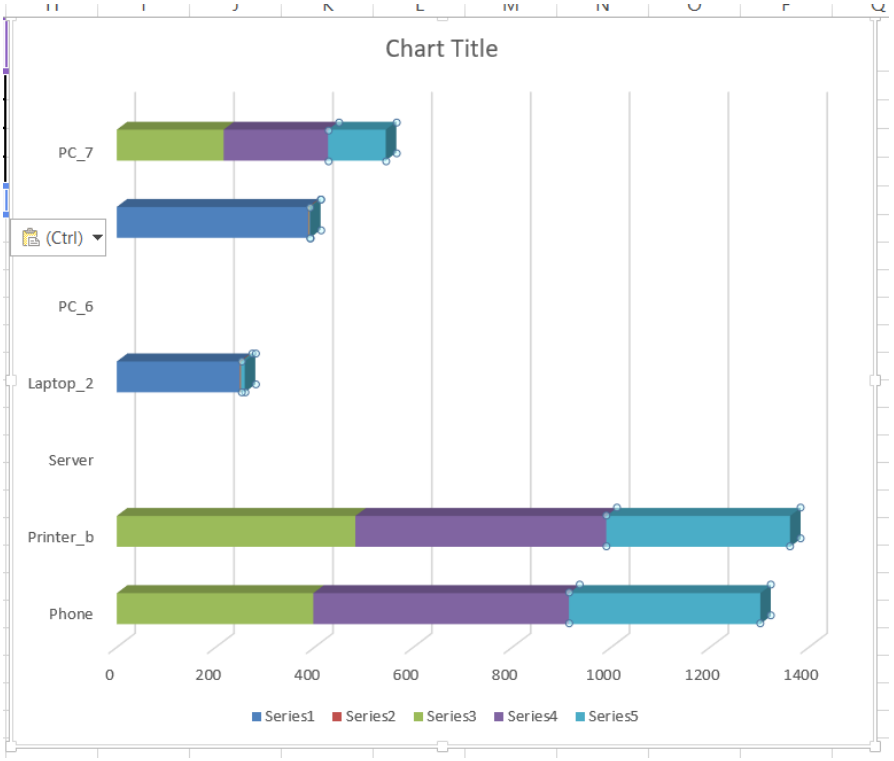
Ping from server:



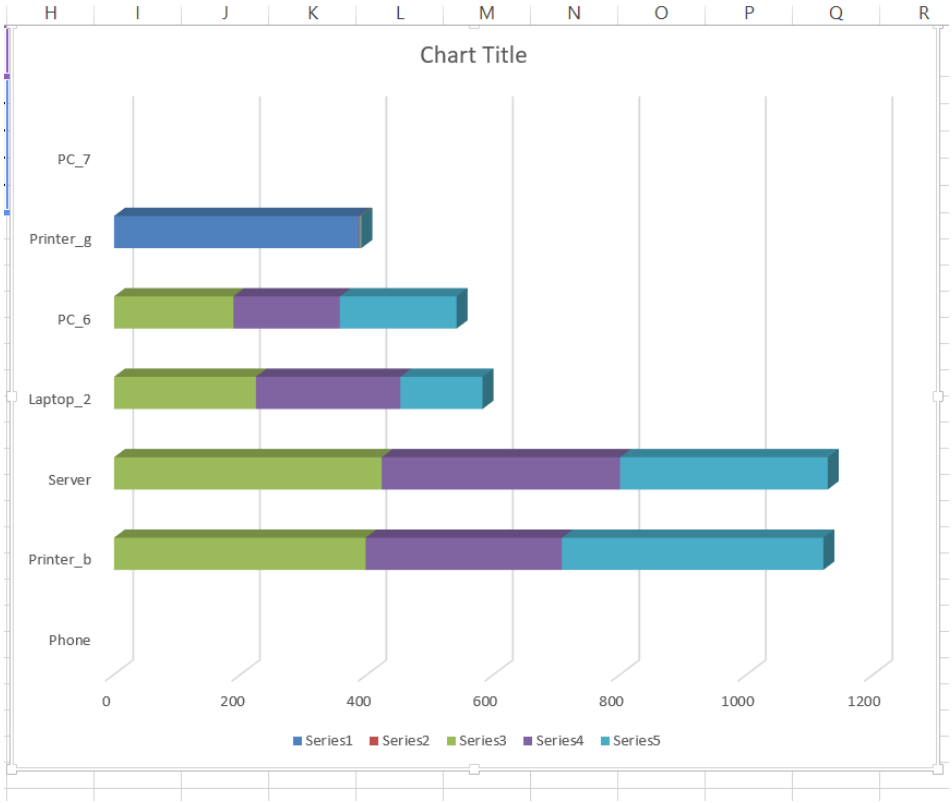
Ping from Laptop_1:



Ping From PC_6



Ping From PC_7



7.8. Discussion on result

The results of the experiments show that the network is functioning properly. The devices are able to communicate with each other and with hosts on other networks. However, there are some issues with the network. The devices are not able to ping the core router or the gateway. This could be due to a number of factors, such as a configuration issue or a hardware problem. Further investigation is needed to determine the cause of these issues.

Overall, the network is functioning properly and the devices are able to communicate with each other. However, there are some issues with the network that need to be investigated further.

Future Work:

Segment Routing (SR):

Next on our learning journey is Segment Routing (SR). It's like learning a new shortcut in the MPLS world, making things simpler. No need for extra complex protocols; just a cool trick to manage traffic more efficiently.

IPv6 Support:

We're gearing up for the future by diving into IPv6 support. It's like expanding our language skills to understand both IPv4 and IPv6, so our routers can talk to all kinds of devices.

Security Steps:

Now, we're putting on our security hats. We're learning about IPsec, a virtual guard for our network. We're also looking into some basic security measures, like access controls and encryption, to keep things safe and sound.

Service Level Agreements (SLAs):

Our next challenge is Service Level Agreements (SLAs). It's like making promises to our network users about the kind of service they can expect. We'll set some basic rules, like minimum speed and maximum delay, to ensure everyone has a good experience.

Conclusions:

Our GNS3 project revolves around a network setup where R4 and R3 take on the role of provider routers, while R1 and R2 serve as edge provider routers linking up with customer routers R3, R6, R7, and R8. The crux of our configuration lies in MPLS, a pivotal technology extensively employed in service provider networks. MPLS, leveraging labels, greatly improves the efficiency of packet forwarding, thereby streamlining communication throughout the network. This project provides a hands-on simulation of a provider-customer network scenario, highlighting the practical deployment of MPLS to enhance routing and ensure smooth data transmission between various parts of the network.

References:

[1] Kurose, J. F., & Ross, K. W. (2013). Computer networking: A top-down approach (7th ed.). Pearson Education [Chapter - 06].

[2] GNS3 website: https://gns3.com/software

[3] GNS3 documentation: Getting Started with GNS3

[4] GNS3 community forum: GNS3

[5] Cisco website: Cisco Support and Downloads – Documentation, Tools, Cases

[6] Cisco documentation: What's New in Cisco Product Documentation

[7] Multiprotocol Label Switching - Wikipedia

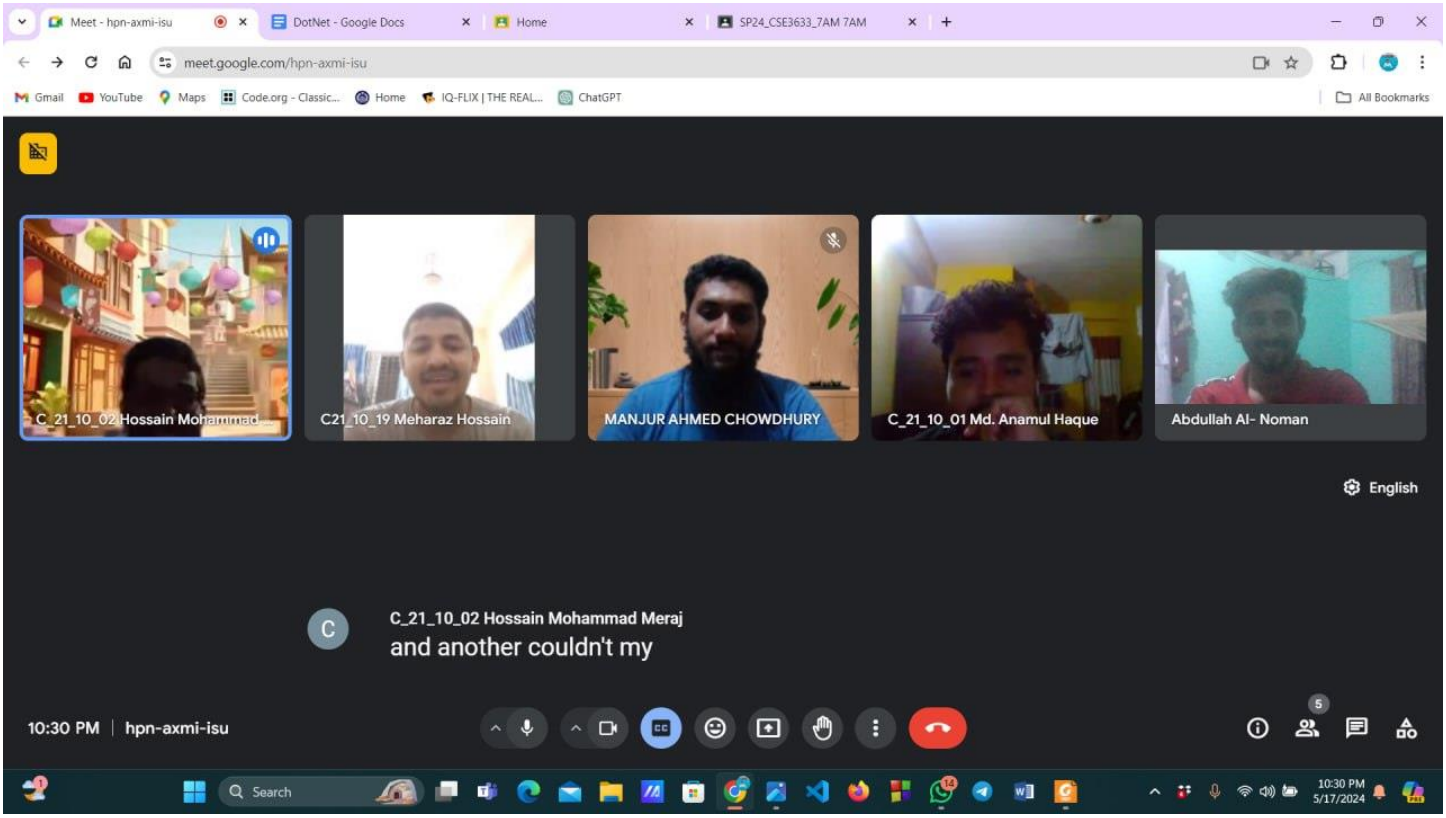
[8] Configuring MPLS L3 VPN support for OSPF / VRF /MP-BGP

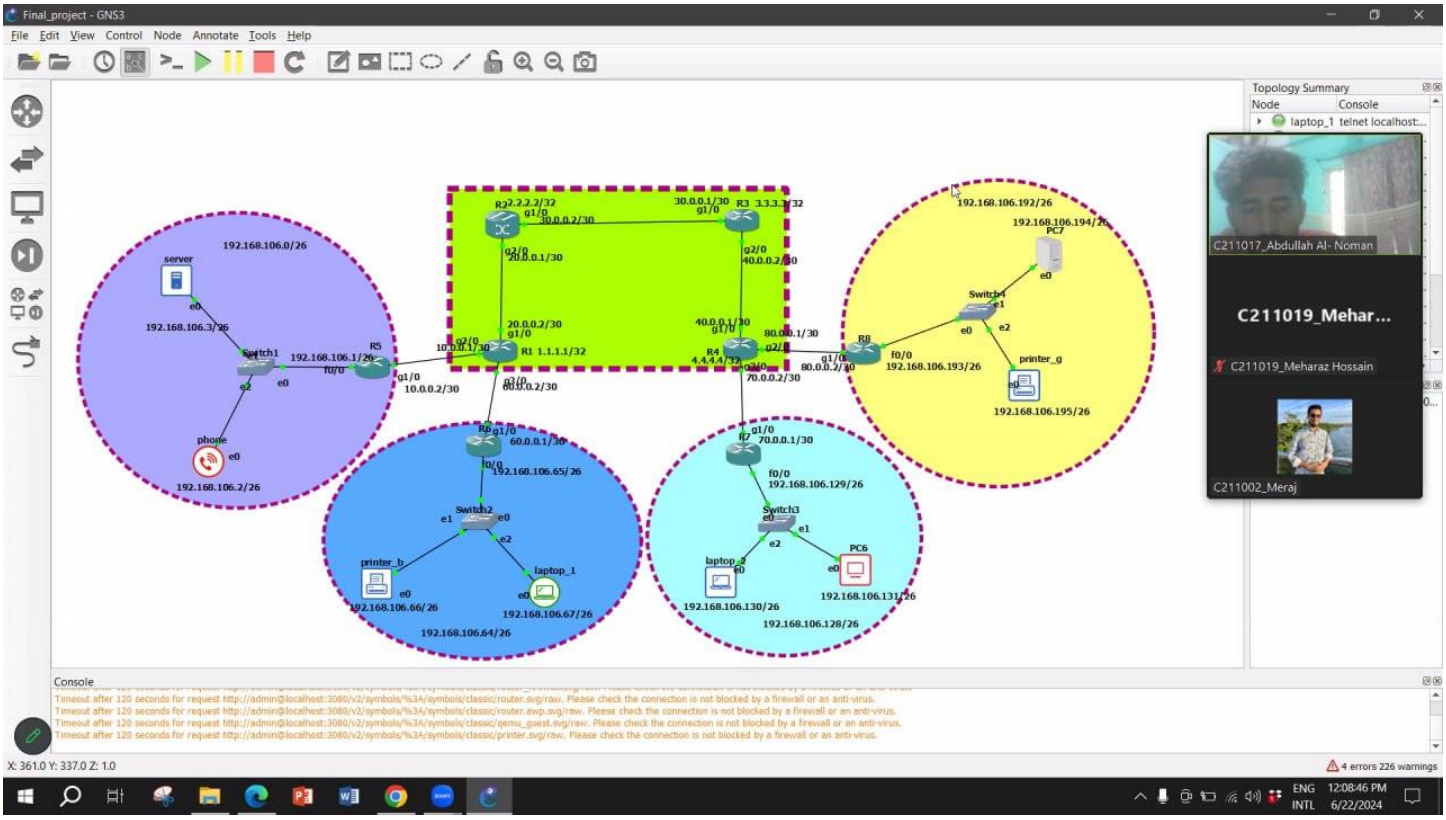
[9] MPLS with GNS3 Lab configuration

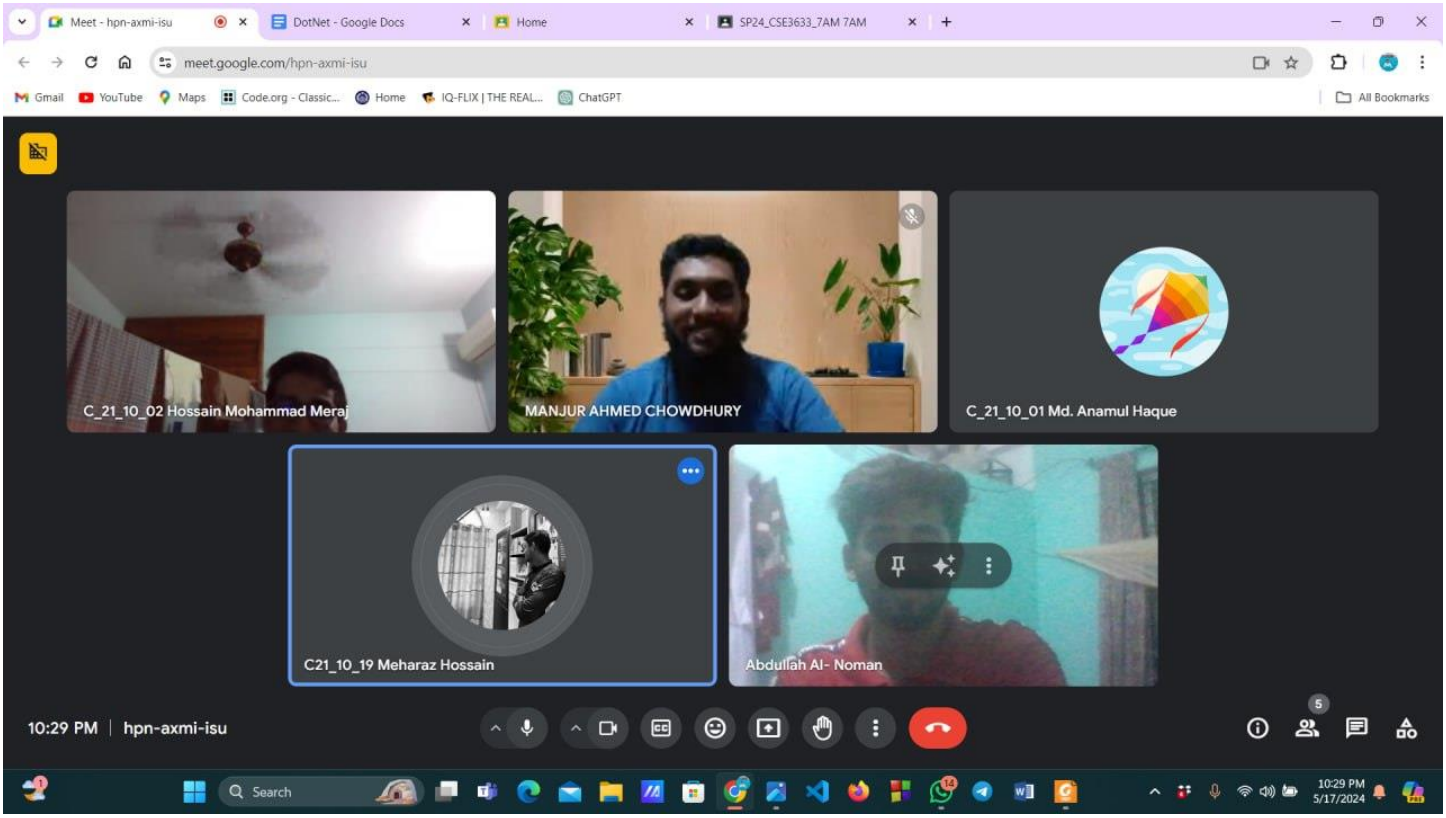
[10] GNS3 LAB: Cisco MPLS Basics and Beyond Concepts

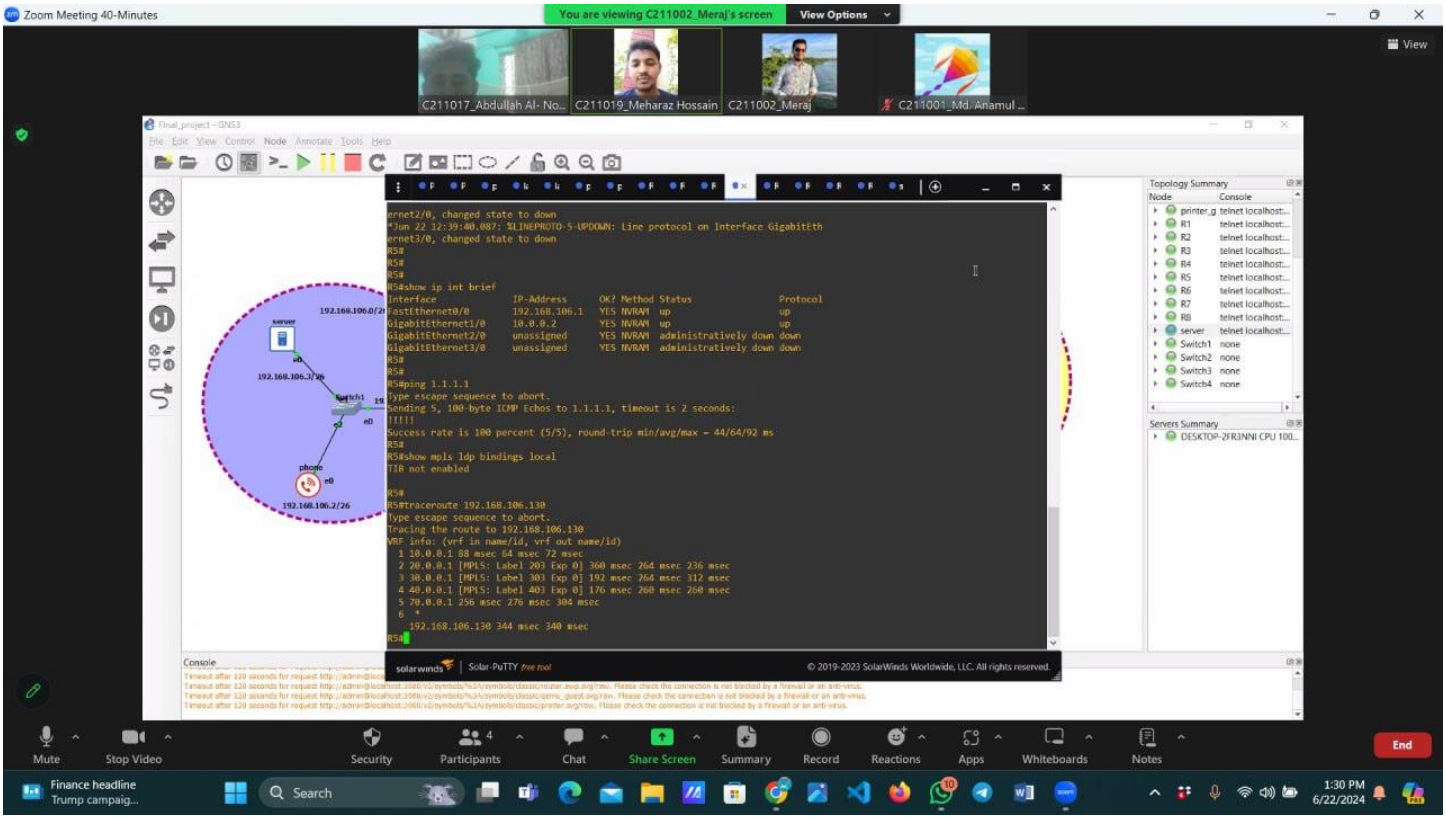
[11] Implementation of MPLS L3VPN using GNS3

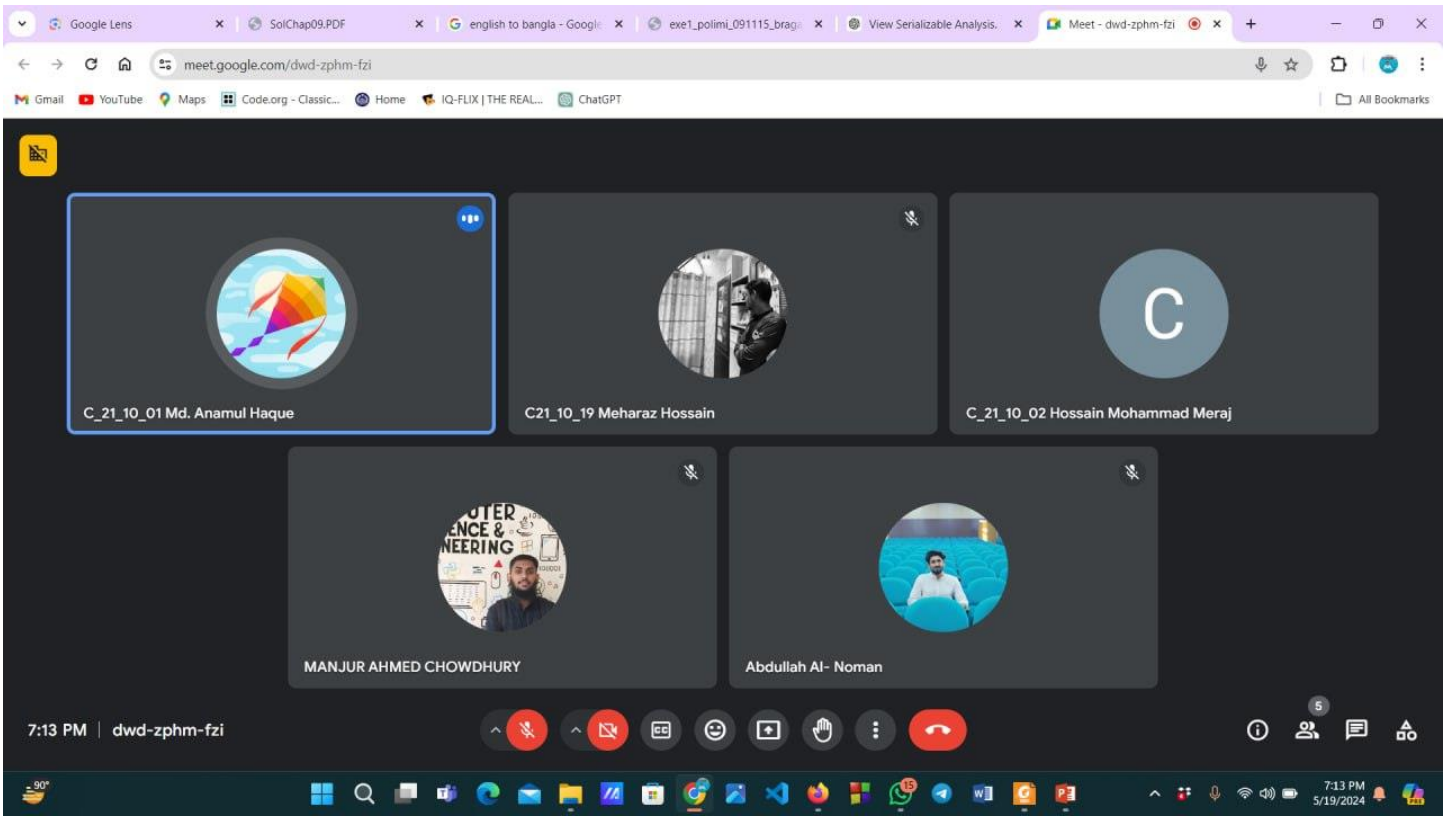
CN Project Work and Meeting Summary of Team Members

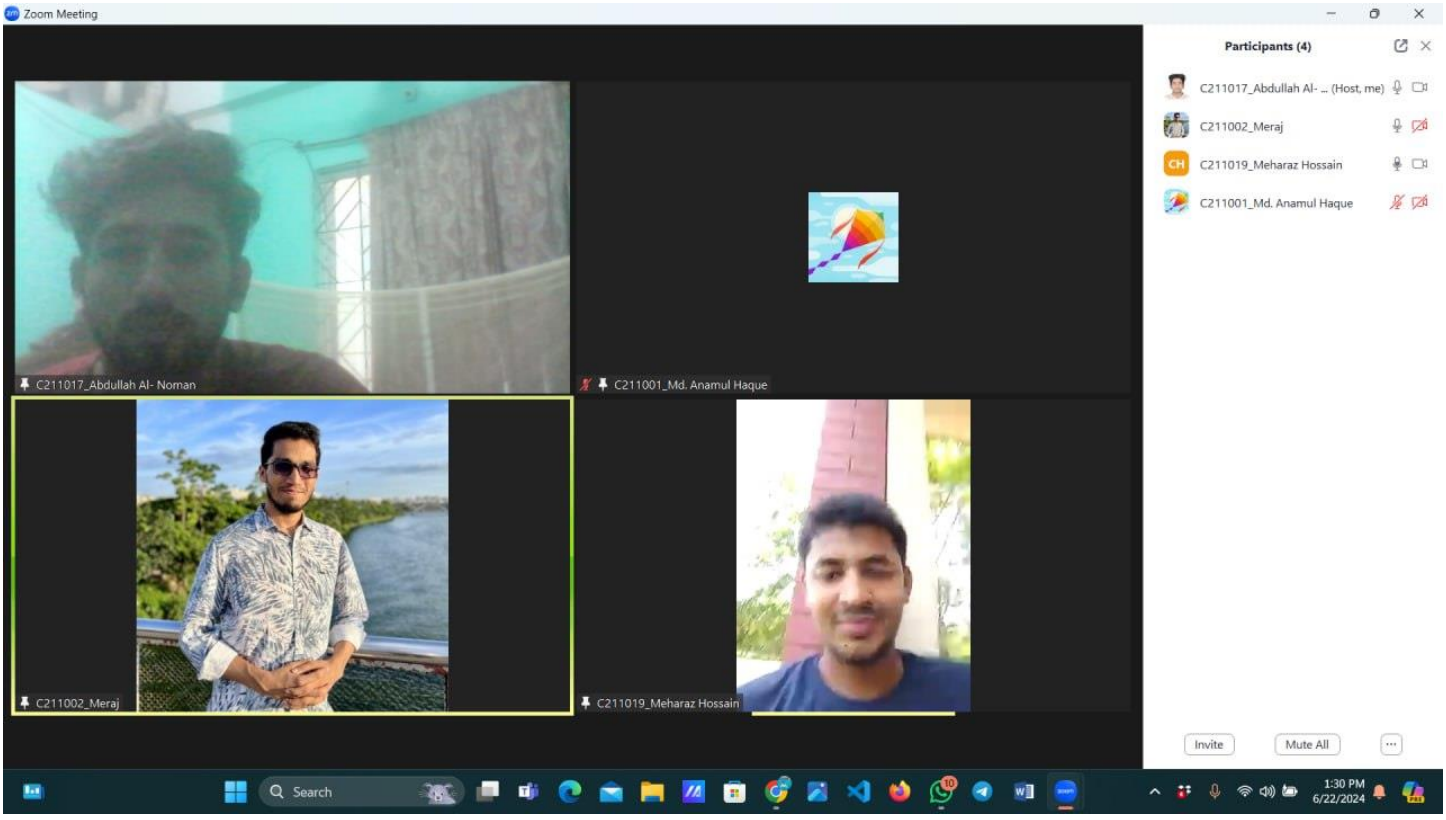


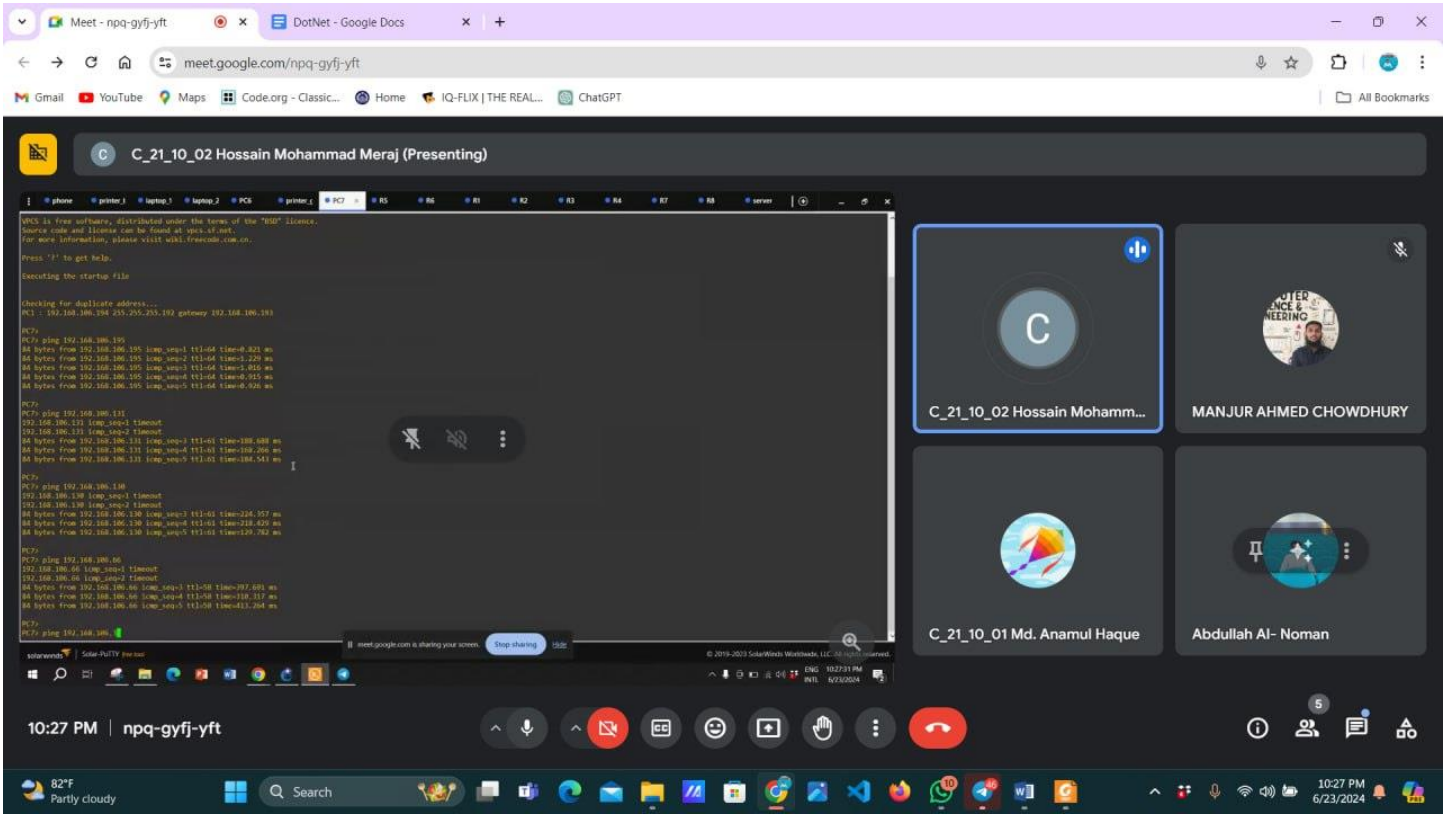


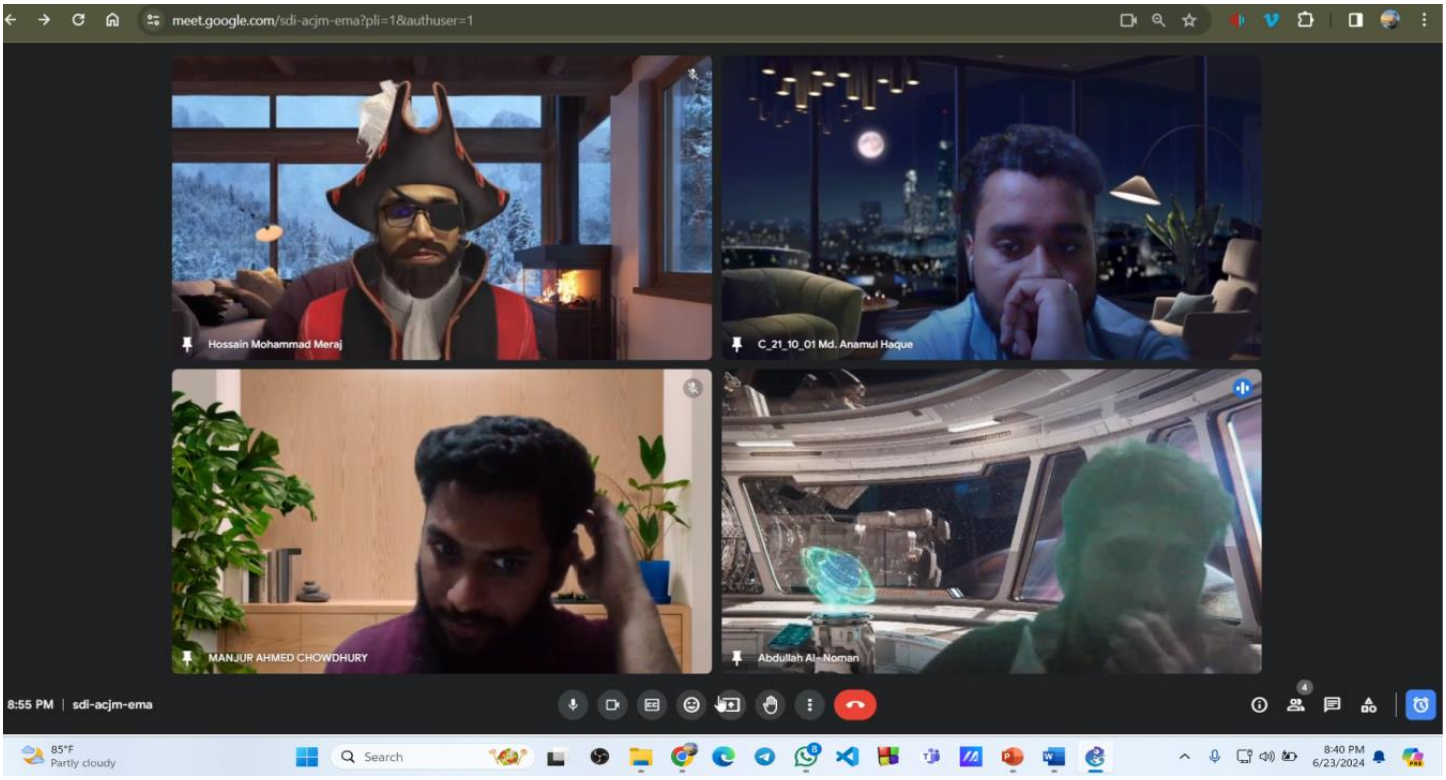

Meet - hpn-axmi-isu
DotNet - Google Docs
Home
SP24_CSE3633_7AM 7AM
meet.google.com/hpn-axmi-isu
C_21_10_02 Hossain Mohammad Meraj
MANJUR AHMED CHOWDHURY
C_21_10_01 Md. Anamul Haque
C21_10_19 Meharaz Hossain
Abdullah Al- Noman
10:29 PM | hpn-axmi-isu
Search
10:29 PM
5/17/2024

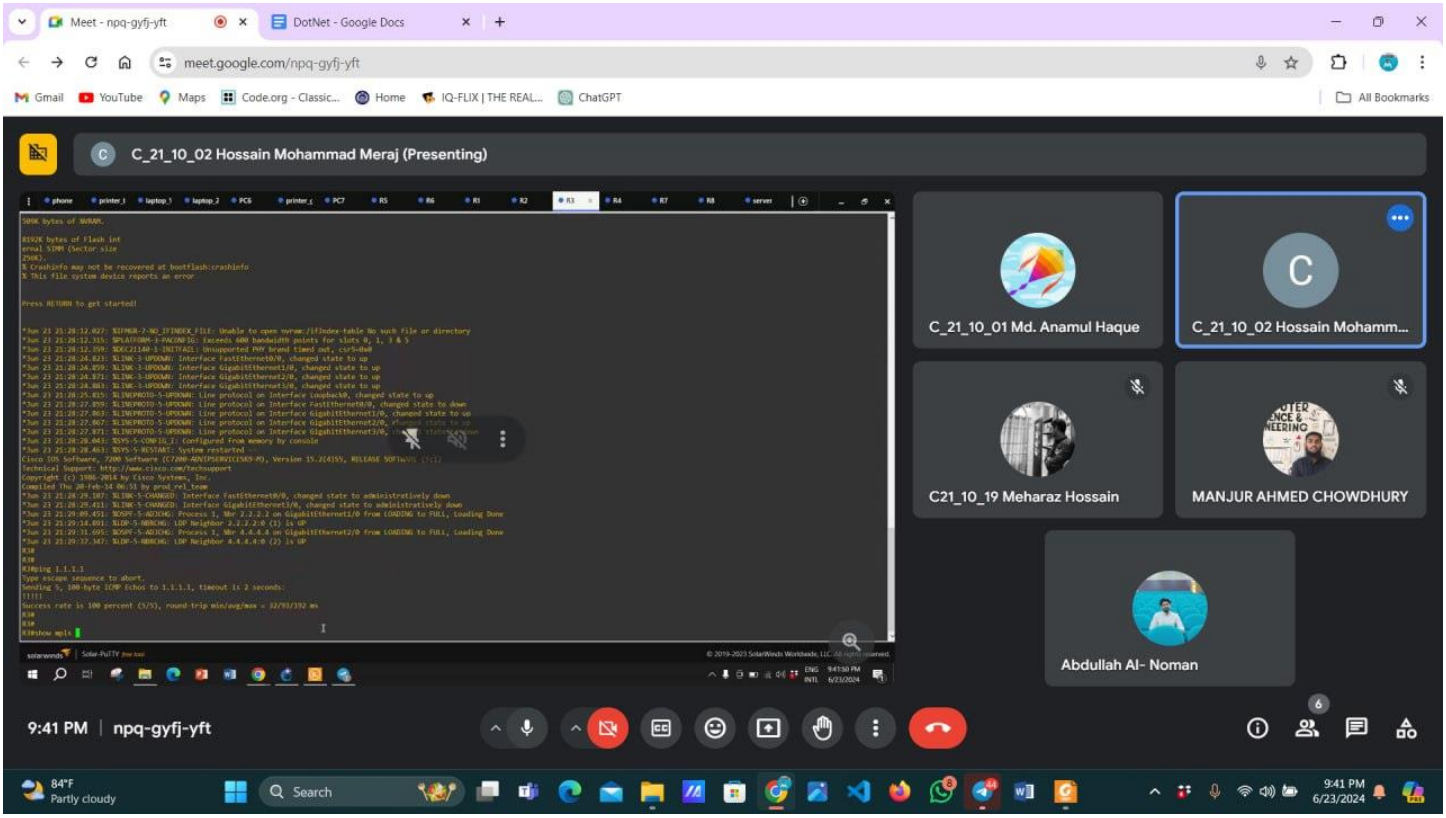

Zoom Meeting 40-Minutes
You are viewing C211002_Meraj's screen
View Options
C211017_Abdullah Al- No...
C211019_Meharaz Hossain
C211002_Meraj
C211001_Md. Anamul ...
Mute
Stop Video
Security
Participants
Chat
Share Screen
Summary
Record
Reactions
Apps
Whiteboards
Notes
End
Search
1:30 PM
6/22/2024

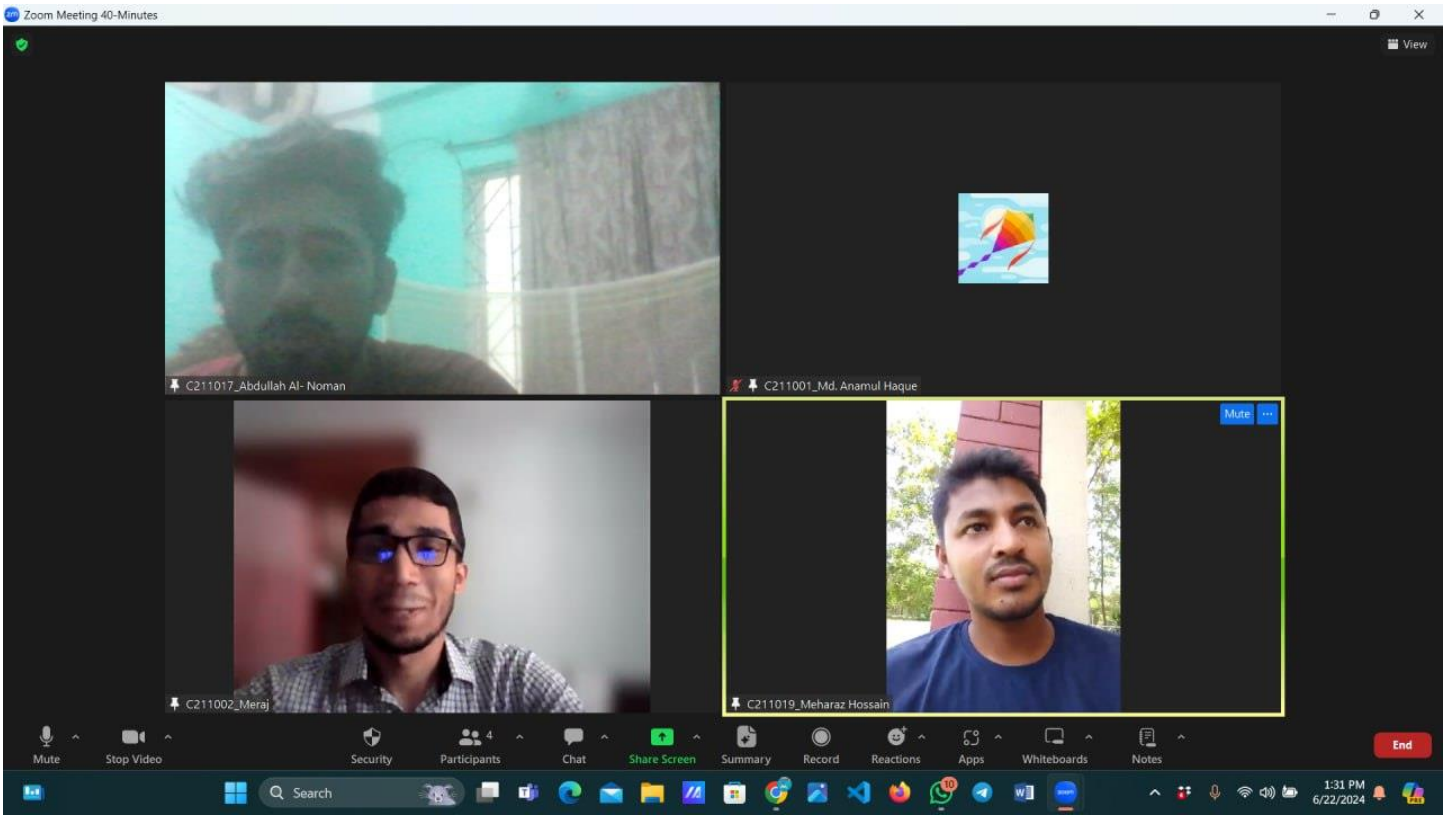

meet.google.com/dwd-zphm-fzi
C_21_10_01 Md. Anamul Haque
C21_10_19 Meharaz Hossain
C
C_21_10_02 Hossain Mohammad Meraj
MANJUR AHMED CHOWDHURY
Abdullah Al- Noman
7:13 PM | dwd-zphm-fzi

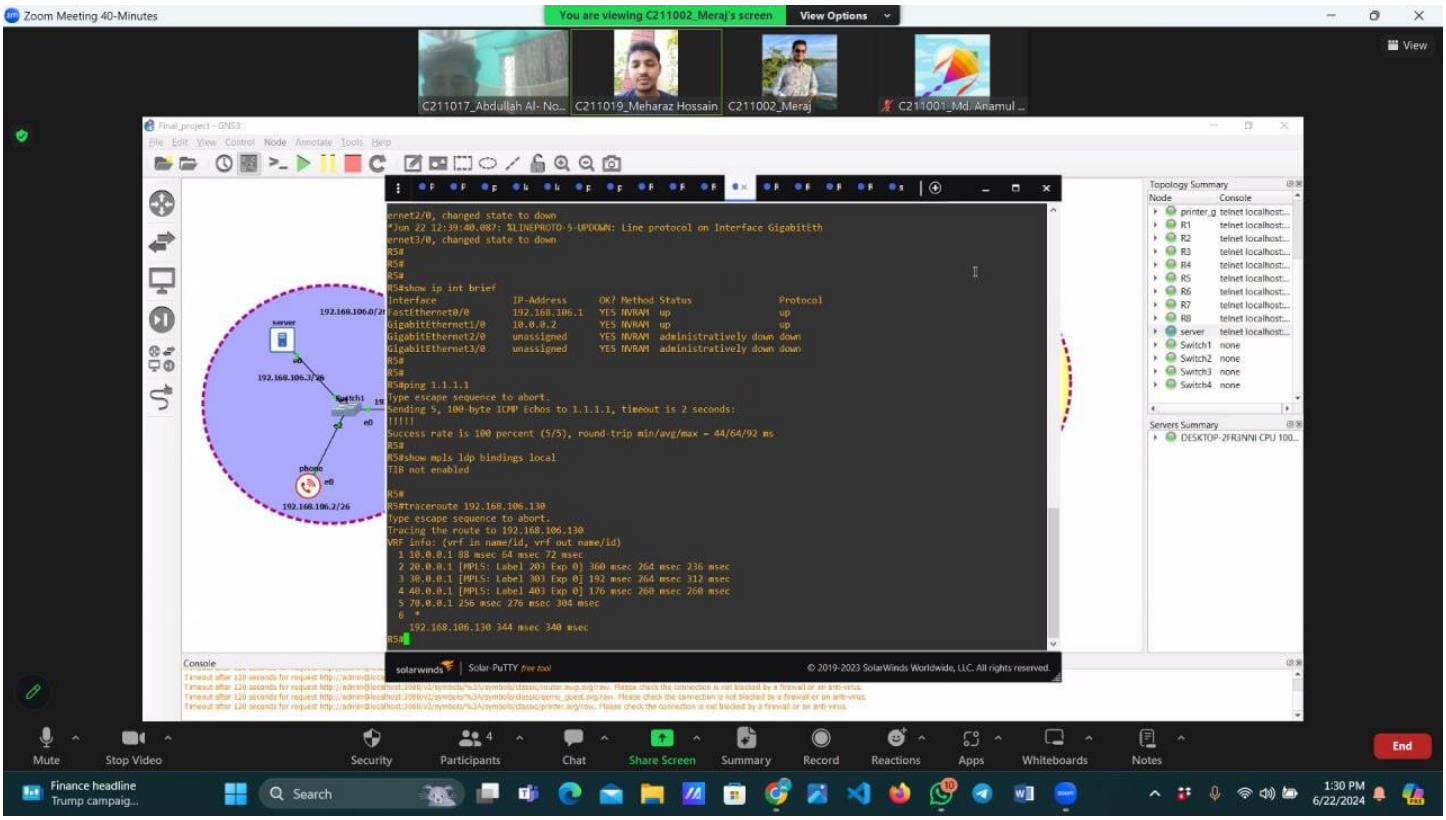

Zoom Meeting
Participants (4)
C211017_Abdullah Al- ... (Host, me)
C211002_Meraj
C211019_Meharaz Hossain
C211001_Md. Anamul Haque
C211017_Abdullah Al- Noman
C211001_Md. Anamul Haque
C211002_Meraj
C211019_Meharaz Hossain
Invite
Mute All

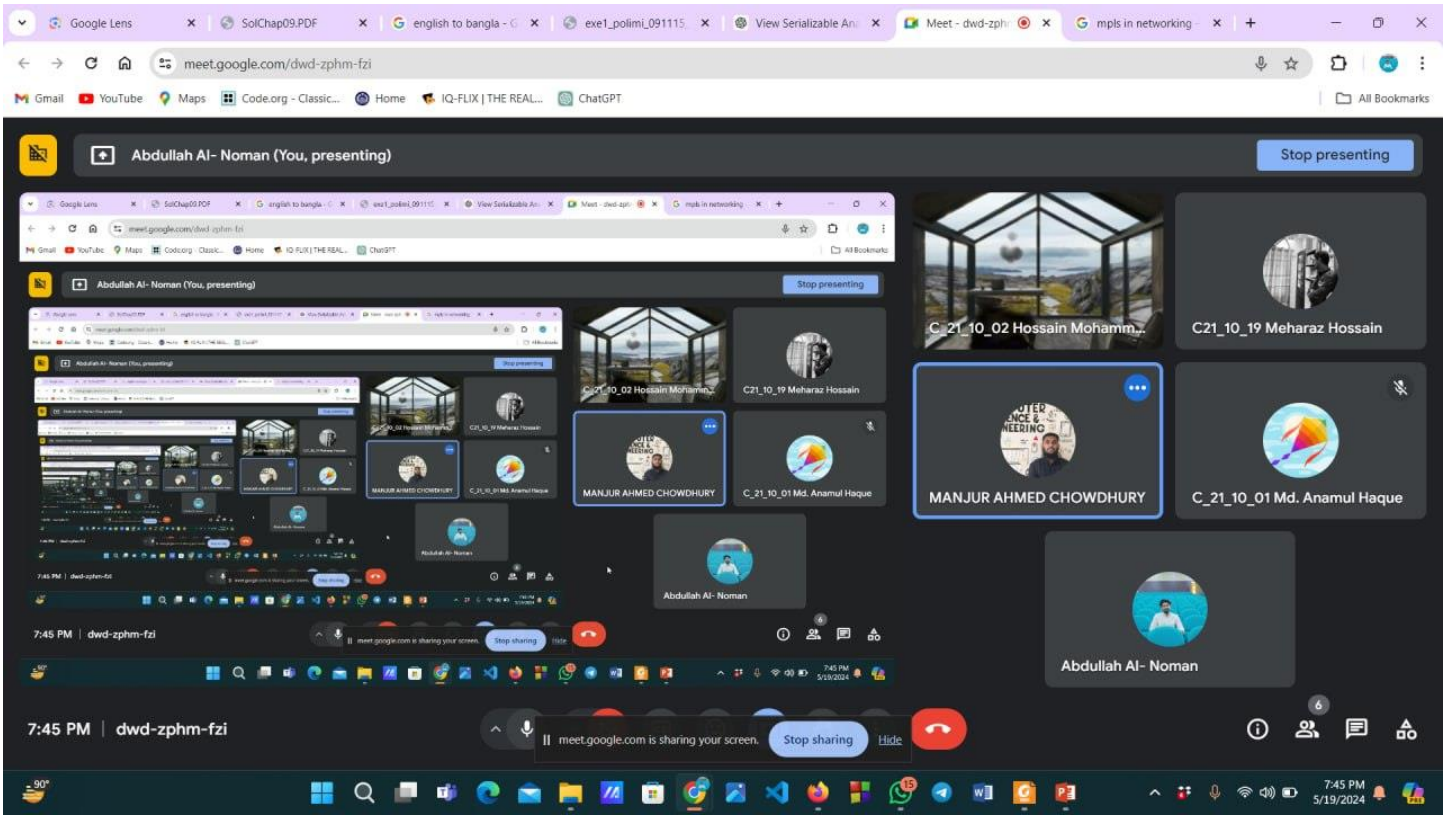

Meet - npq-gyfj-yft
DotNet - Google Docs
meet.google.com/npq-gyfj-yft
C_21_10_02 Hossain Mohammad Meraj (Presenting)
C_21_10_02 Hossain Mohamm...
MANJUR AHMED CHOWDHURY
C_21_10_01 Md. Anamul Haque
Abdullah Al- Noman
10:27 PM | npq-gyfj-yft
82°F
Partly cloudy
Search
10:27 PM
6/23/2024


meet.google.com/sdi-acjm-ema?pli=1&authuser=1
Hossain Mohammad Meraj
C_21_10_01 Md. Anamul Haque
MANJUR AHMED CHOWDHURY
Abdullah Al- Noman
8:55 PM | sdi-acjm-ema
85°F
Partly cloudy
Search
8:40 PM
6/23/2024


Meet - npq-gyfj-yft
DotNet - Google Docs
meet.google.com/npq-gyfj-yft
C_21_10_02 Hossain Mohammad Meraj (Presenting)
C_21_10_01 Md. Anamul Haque
C_21_10_02 Hossain Mohamm...
C21_10_19 Meharaz Hossain
MANJUR AHMED CHOWDHURY
Abdullah Al- Noman
9:41 PM | npq-gyfj-yft
84°F
Partly cloudy
Search
9:41 PM
6/23/2024


Zoom Meeting 40-Minutes
View
C211017_Abdullah Al- Noman
C211001_Md. Anamul Haque
C211002_Meraj
C211019_Meharaz Hossain
Mute
Mute
Stop Video
Security
Participants
Chat
Share Screen
Summary
Record
Reactions
Apps
Whiteboards
Notes
End
Search
1:31 PM
6/22/2024


Zoom Meeting 40-Minutes
You are viewing C211002_Meraj's screen
View Options
C211017_Abdullah Al- No...
C211019_Meharaz Hossain
C211002_Meraj
C211001_Md. Anamul ...
View
Mute
Stop Video
Security
Participants
Chat
Share Screen
Summary
Record
Reactions
Apps
Whiteboards
Notes
End
Finance headline
Trump campaig...
Search
1:30 PM
6/22/2024


Google Lens
SolChap09.PDF
english to bangla -
exe1_polimi_091115
View Serializable An
Meet - dwd-zphm-fzi
mpls in networking
meet.google.com/dwd-zphm-fzi
Gmail
YouTube
Maps
Code.org - Classic...
Home
IQ-FLIX | THE REAL...
ChatGPT
All Bookmarks
Abdullah Al- Noman (You, presenting)
Stop presenting
C_21_10_02 Hossain Mohamm...
C21_10_19 Meharaz Hossain
MANJUR AHMED CHOWDHURY
C_21_10_01 Md. Anamul Haque
Abdullah Al- Noman
7:45 PM | dwd-zphm-fzi
meet.google.com is sharing your screen.
Stop sharing
Hide
7:45 PM
5/19/2024

TEAM IIUC_DWIP_ELITE CONTRIBUTION

ID	NAME	CONTRIBUTION
C211017	Abdullah Al- Noman(L)	Report/Design/Command
C211001	Md. Anamul Hoque	Report/Presentation Slide
C211002	Hossain Md. Meraj	Implementation/Command
C211019	Mehraz Hosssain	Report/ Chart/ Avg VAlue
C211030	Manjur Ahmed	Idea Present/ Design