NETW191
SOHO Network

Prepared by Hector Acosta

Introduction

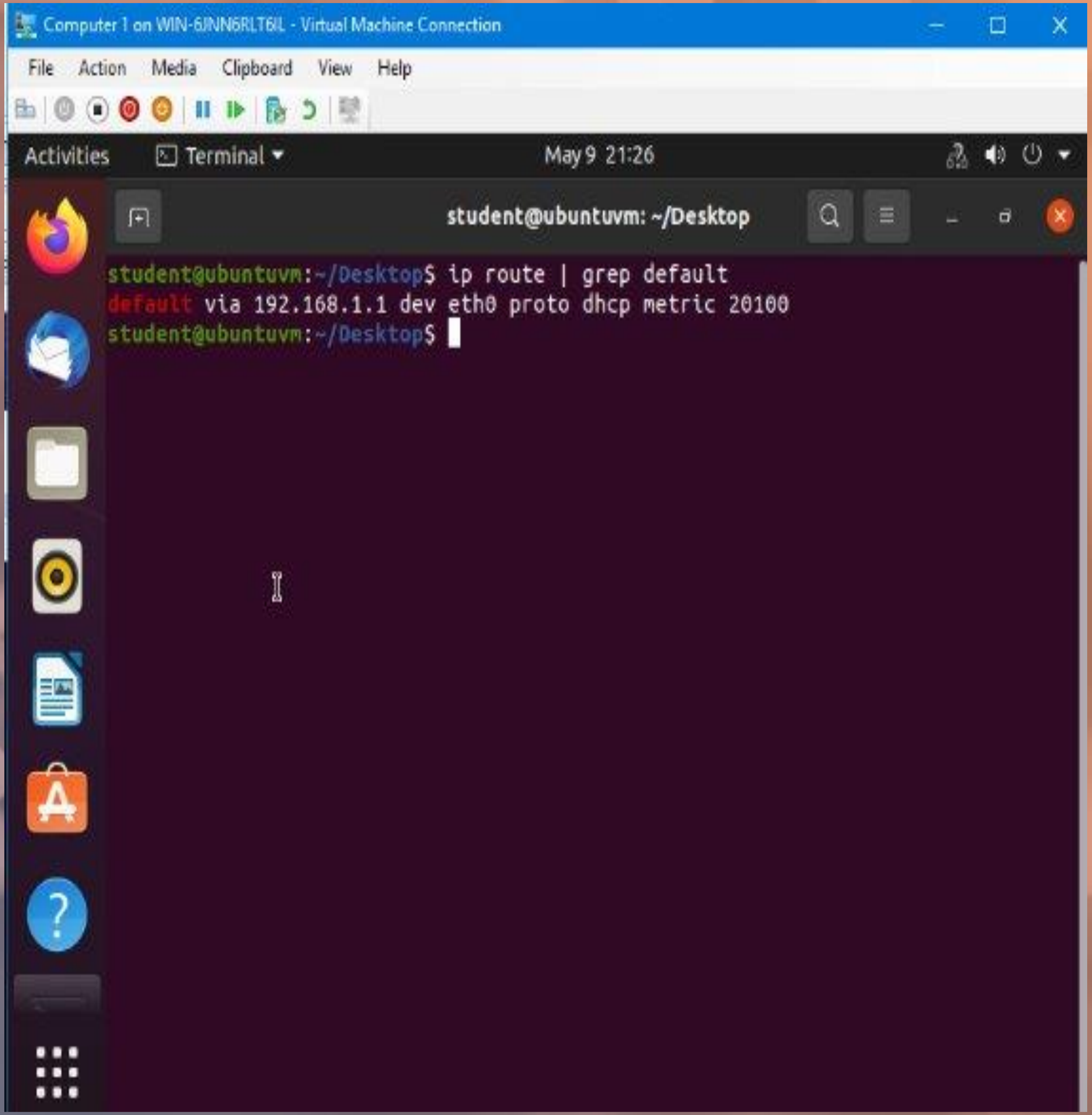
This project delves into the fundamentals of networking, which are crucial in the rapidly evolving world of the Internet of Things (IoT). It encompasses the design and development of a network, focusing on key aspects such as SOHO (Small Office/Home Office) router configurations, subnetting, connectivity testing, network documentation, and SOHO wireless network security. Each module builds on this foundation: implementing an IPv4 addressing scheme for the SOHO Router, testing connectivity among network devices, subnetting a class C network and configuring loopback interfaces, creating a detailed network diagram using Microsoft Visio, and enhancing the security of an SOHO wireless network. Through these modules, the project not only facilitates an understanding of current networking technologies but also prepares for future advancements in Information Technology, particularly in the realm of IoT.

Introduction to IPv4 Addressing

In this part of my NETW191 project, I focus on implementing an IPv4 addressing scheme to support a robust network infrastructure. The primary objective is to assign an IPv4 address to the SOHO Router virtual machine. This process includes discovering the default gateway, accessing the router's management interface, and configuring the IPv4 address on the LAN interface of the SOHO Router.

Preparation

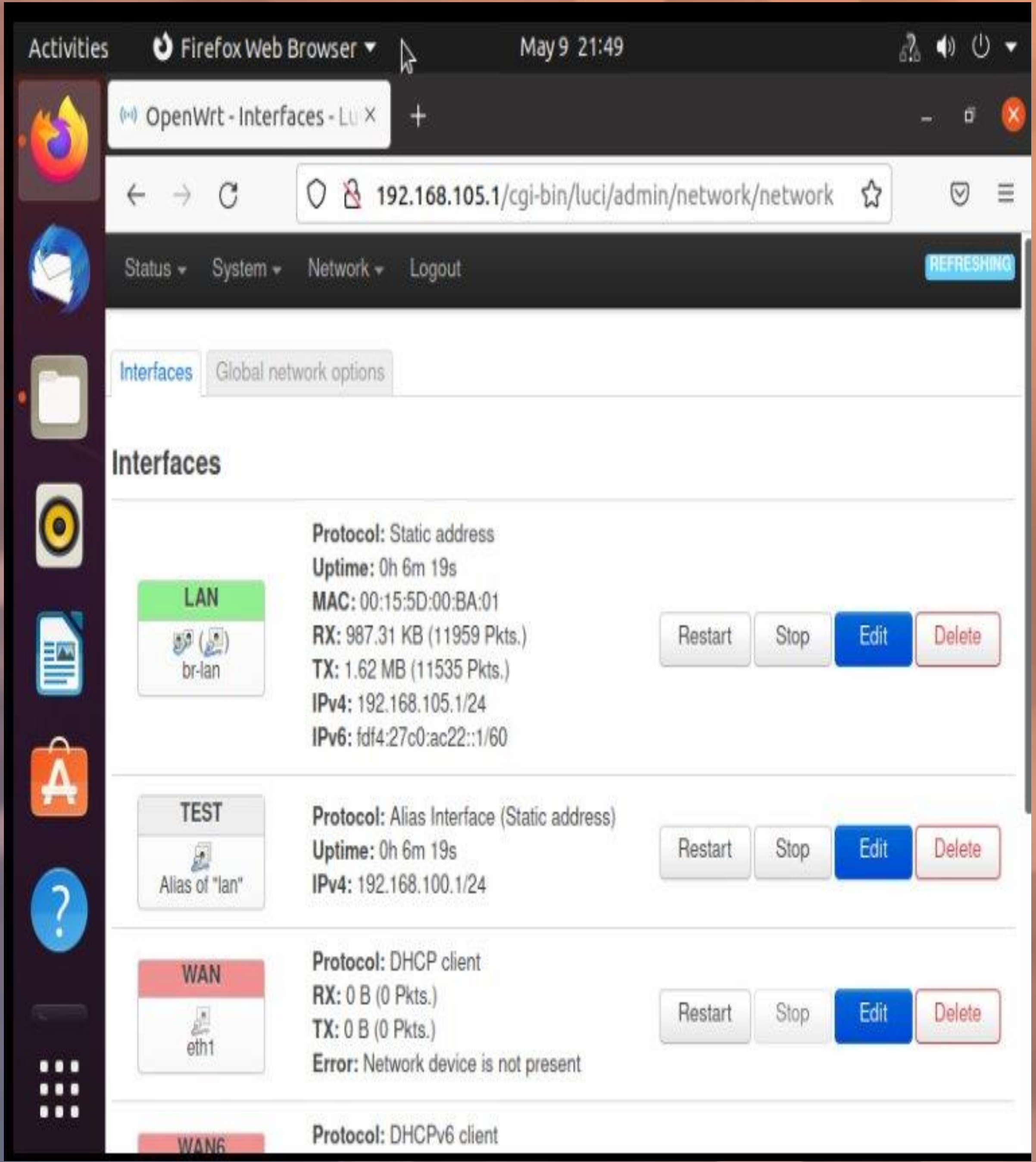
- **Discover the Default Gateway:** Open a terminal window and run the appropriate command to display network information, including the default gateway IP address.
- **Capture Date/Time Information:** Ensure the terminal window shows the date and time at the top for documentation purposes.
- **Access Router's Management Interface:** Use the default gateway IP address to log in to the router's management interface.


Computer 1 on WIN-6JNN6RLT6IL - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Activities
Terminal
May 9 21:26
student@ubuntuvm: ~/Desktop

```
student@ubuntuvm:~/Desktop$ ip route | grep default
default via 192.168.1.1 dev eth0 proto dhcp metric 20100
student@ubuntuvm:~/Desktop$ 
```

IPv4 Address Assignment

- **Access Interfaces Page:** Navigate to the interfaces page on the router's management interface.
- **Assign New IPv4 Address:** Configure the IPv4 address for the LAN interface.
- **Capture Date/Time Information:** Ensure the date and time are visible next to the Firefox Web Browser tab for accurate documentation.



192.168.105.1/cgi-bin/luci/admin/network/network

Interfaces

LAN
br-lan

Protocol: Static address
Uptime: 0h 6m 19s
MAC: 00:15:5D:00:BA:01
RX: 987.31 KB (11959 Pkts.)
TX: 1.62 MB (11535 Pkts.)
IPv4: 192.168.105.1/24
IPv6: fdf4:27c0:ac22::1/60

TEST
Alias of "lan"

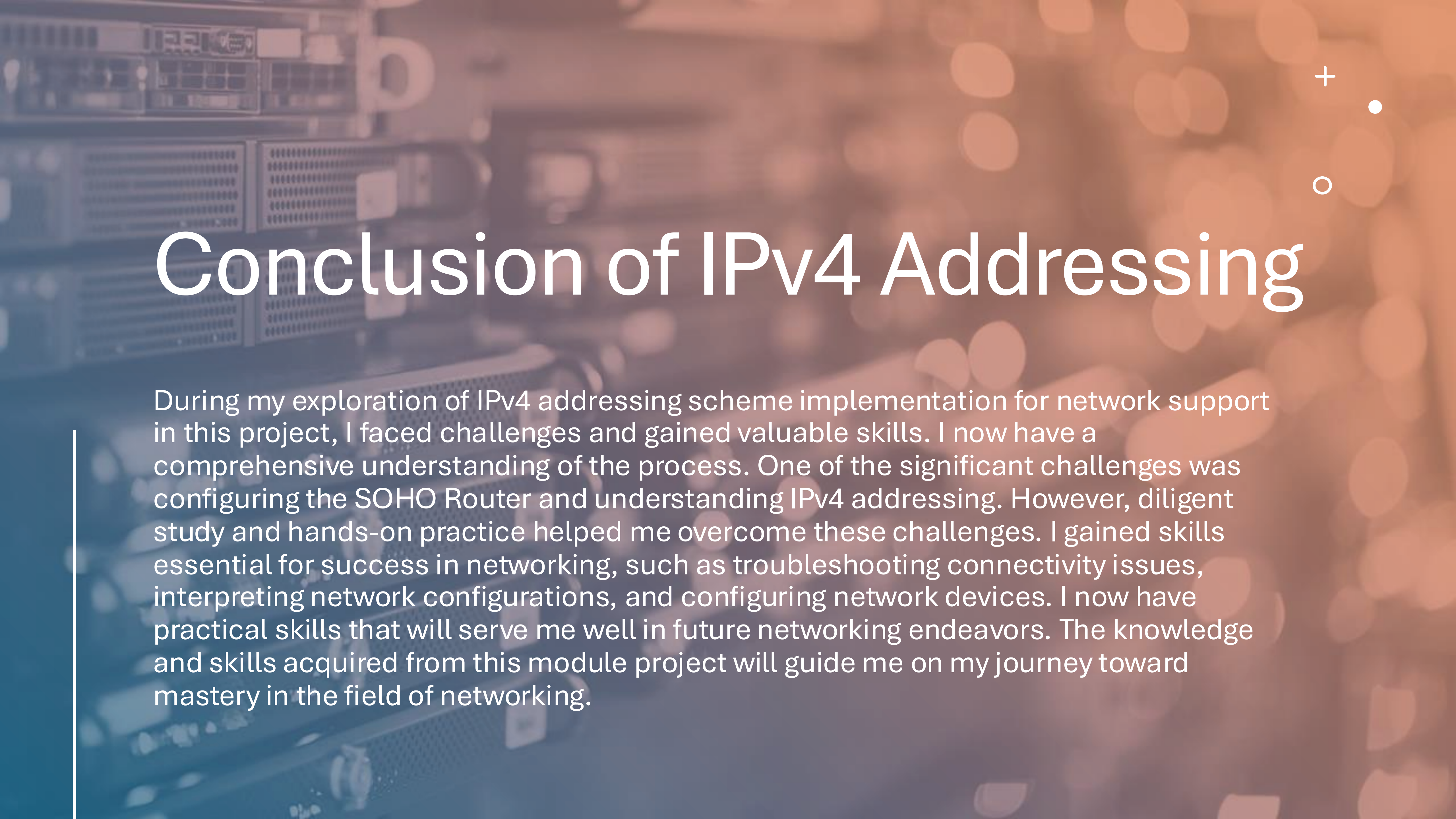
Protocol: Alias Interface (Static address)
Uptime: 0h 6m 19s
IPv4: 192.168.100.1/24

WAN
eth1

Protocol: DHCP client
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
Error: Network device is not present

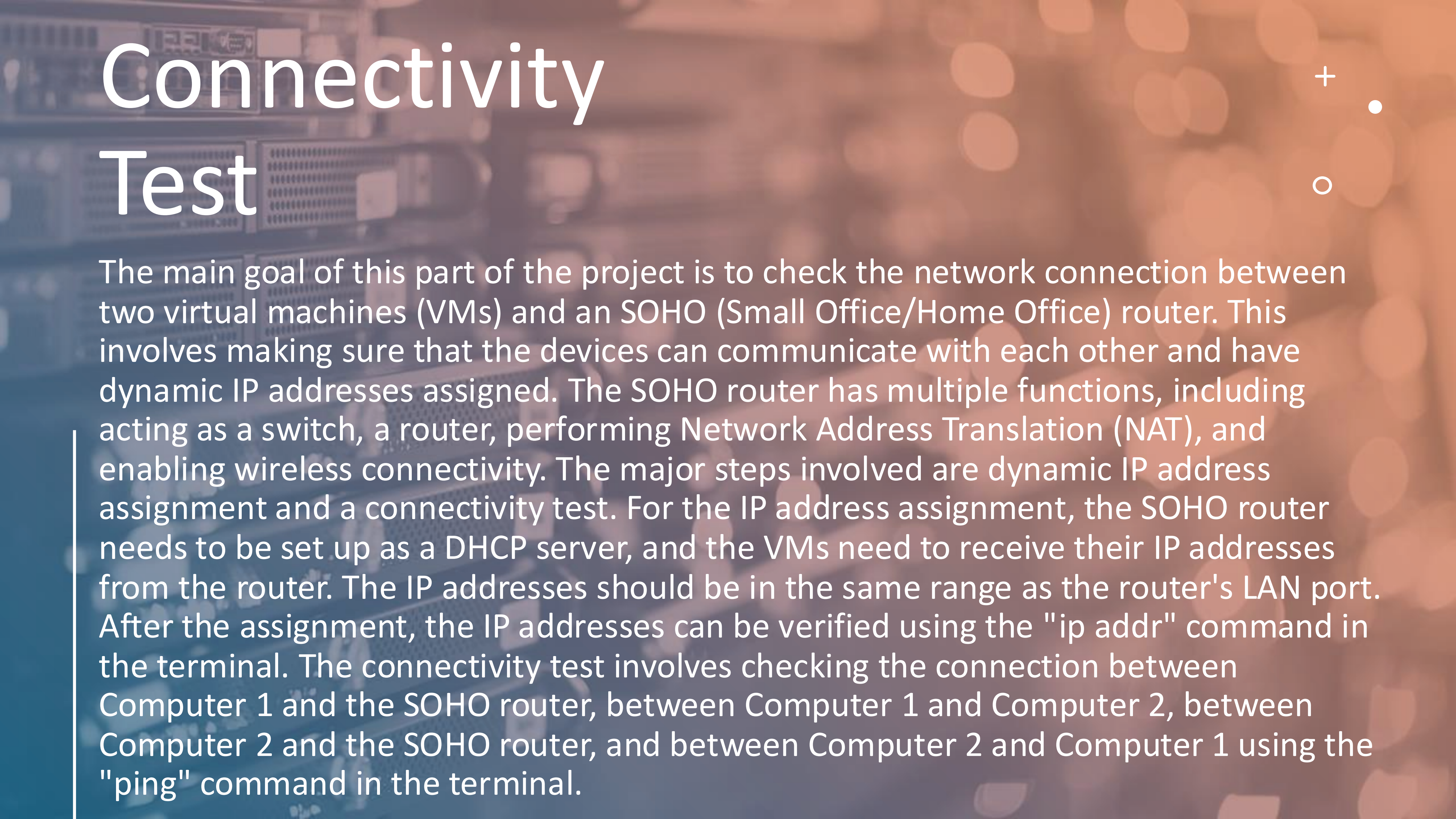
WAN6

Protocol: DHCPv6 client



Conclusion of IPv4 Addressing

During my exploration of IPv4 addressing scheme implementation for network support in this project, I faced challenges and gained valuable skills. I now have a comprehensive understanding of the process. One of the significant challenges was configuring the SOHO Router and understanding IPv4 addressing. However, diligent study and hands-on practice helped me overcome these challenges. I gained skills essential for success in networking, such as troubleshooting connectivity issues, interpreting network configurations, and configuring network devices. I now have practical skills that will serve me well in future networking endeavors. The knowledge and skills acquired from this module project will guide me on my journey toward mastery in the field of networking.

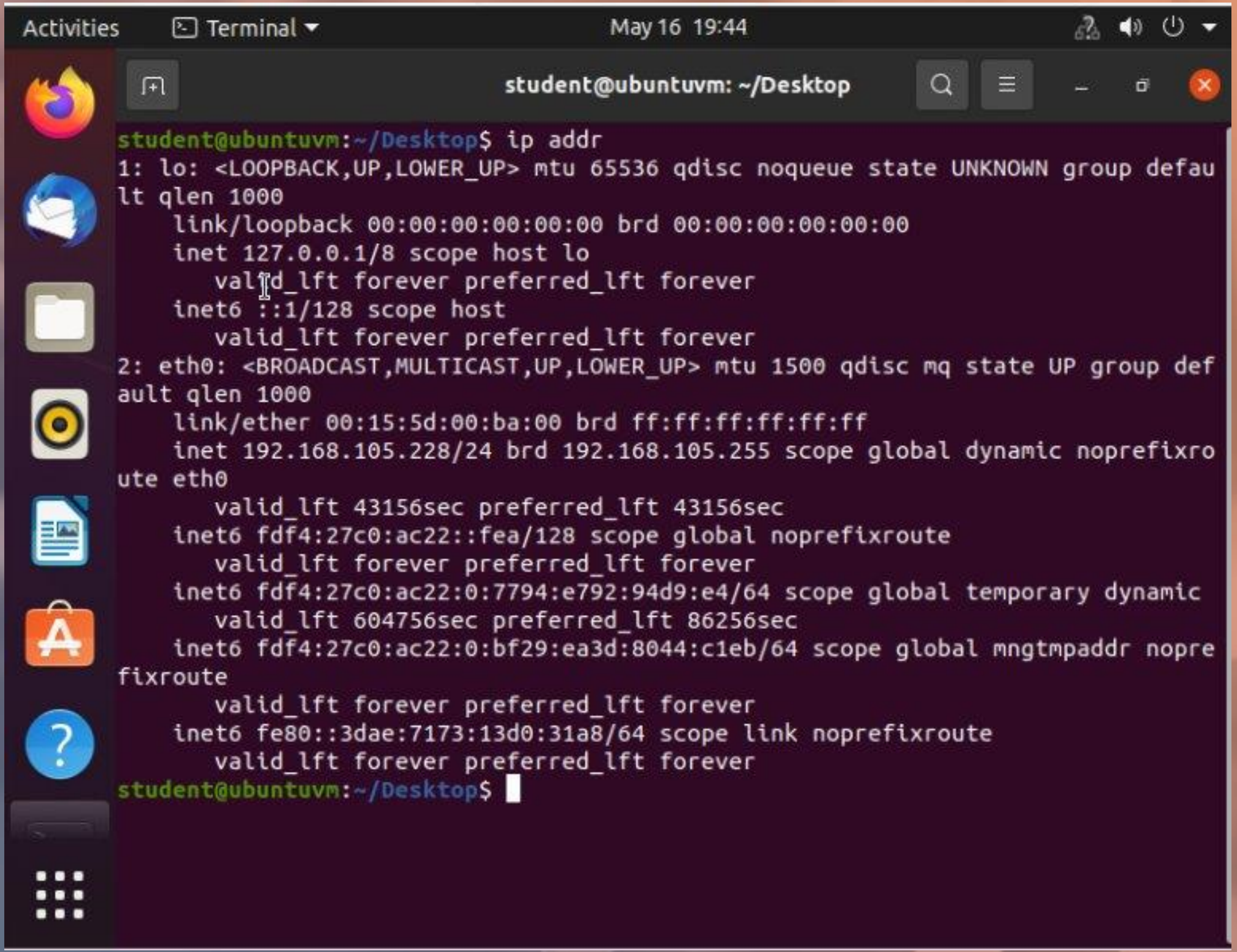


Connectivity Test

The main goal of this part of the project is to check the network connection between two virtual machines (VMs) and an SOHO (Small Office/Home Office) router. This involves making sure that the devices can communicate with each other and have dynamic IP addresses assigned. The SOHO router has multiple functions, including acting as a switch, a router, performing Network Address Translation (NAT), and enabling wireless connectivity. The major steps involved are dynamic IP address assignment and a connectivity test. For the IP address assignment, the SOHO router needs to be set up as a DHCP server, and the VMs need to receive their IP addresses from the router. The IP addresses should be in the same range as the router's LAN port. After the assignment, the IP addresses can be verified using the "ip addr" command in the terminal. The connectivity test involves checking the connection between Computer 1 and the SOHO router, between Computer 1 and Computer 2, between Computer 2 and the SOHO router, and between Computer 2 and Computer 1 using the "ping" command in the terminal.

Dynamic IP Address Assignment for Computer 1 VM

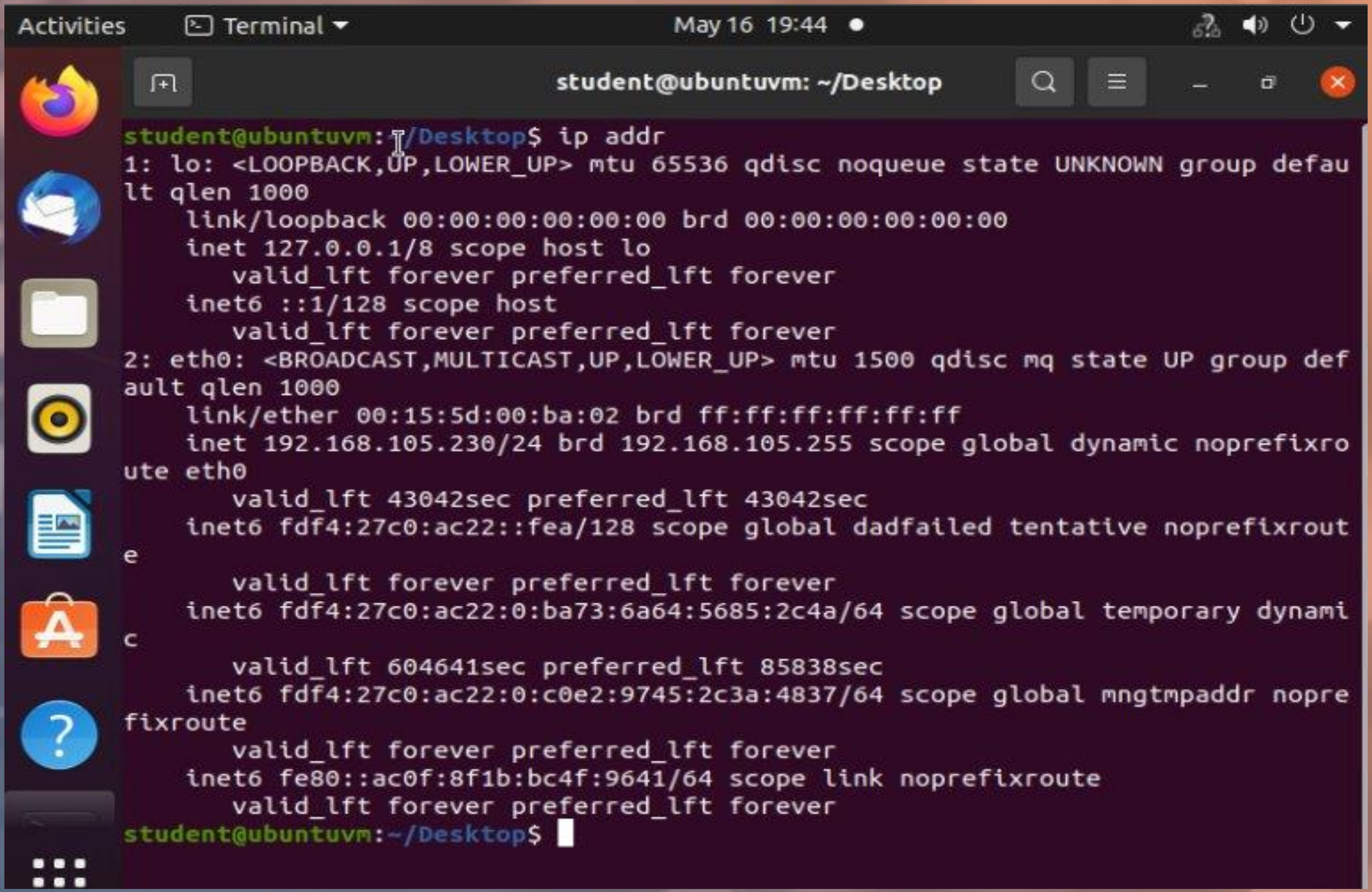
- Took a screenshot of the Terminal window displaying the IPv4 address of the Computer 1 VM.
- This step was crucial to verify that the Computer 1 VM received a dynamic IP address from the SOHO router's DHCP server.
- Captured the date/time information on top of the Terminal window to provide context and ensure documentation accuracy.



```
student@ubuntuvm:~/Desktop$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group def
ault qlen 1000
    link/ether 00:15:5d:00:ba:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.105.228/24 brd 192.168.105.255 scope global dynamic noprefixro
ute eth0
       valid_lft 43156sec preferred_lft 43156sec
    inet6 fdf4:27c0:ac22::fea/128 scope global noprefixroute
       valid_lft forever preferred_lft forever
    inet6 fdf4:27c0:ac22:0:7794:e792:94d9:e4/64 scope global temporary dynamic
       valid_lft 604756sec preferred_lft 86256sec
    inet6 fdf4:27c0:ac22:0:bf29:ea3d:8044:c1eb/64 scope global mngtmpaddr nopre
fixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::3dae:7173:13d0:31a8/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
student@ubuntuvm:~/Desktop$
```

Dynamic IP Address Assignment for Computer 2 VM

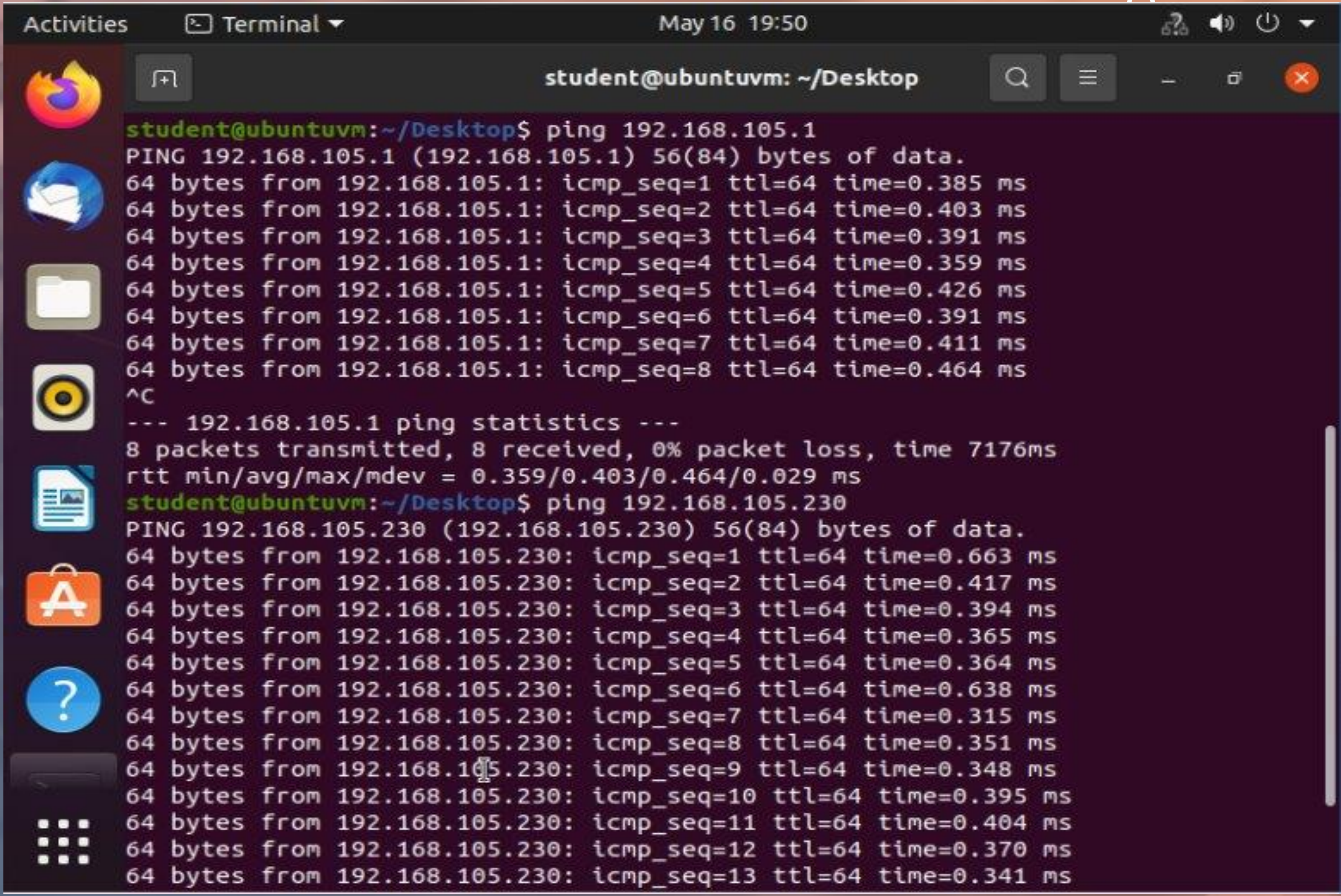
- Took a screenshot of the Terminal window displaying the IPv4 address of the Computer 2 VM.
- This step was crucial to verify that the Computer 2 VM received a dynamic IP address from the SOHO router's DHCP server.
- Captured the date/time information on top of the Terminal window to provide context and ensure documentation accuracy.



```
student@ubuntuvm:~/Desktop$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defau
lt qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group def
ault qlen 1000
    link/ether 00:15:5d:00:ba:02 brd ff:ff:ff:ff:ff:ff
    inet 192.168.105.230/24 brd 192.168.105.255 scope global dynamic noprefixro
ute eth0
       valid_lft 43042sec preferred_lft 43042sec
    inet6 fdf4:27c0:ac22::fea/128 scope global dadfailed tentative noprefixrout
e
       valid_lft forever preferred_lft forever
    inet6 fdf4:27c0:ac22:0:ba73:6a64:5685:2c4a/64 scope global temporary dynami
c
       valid_lft 604641sec preferred_lft 85838sec
    inet6 fdf4:27c0:ac22:0:c0e2:9745:2c3a:4837/64 scope global mngtmpaddr nopre
fixroute
       valid_lft forever preferred_lft forever
    inet6 fe80::ac0f:8f1b:bc4f:9641/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
student@ubuntuvm:~/Desktop$ 
```

Connectivity Test from Computer 1 VM

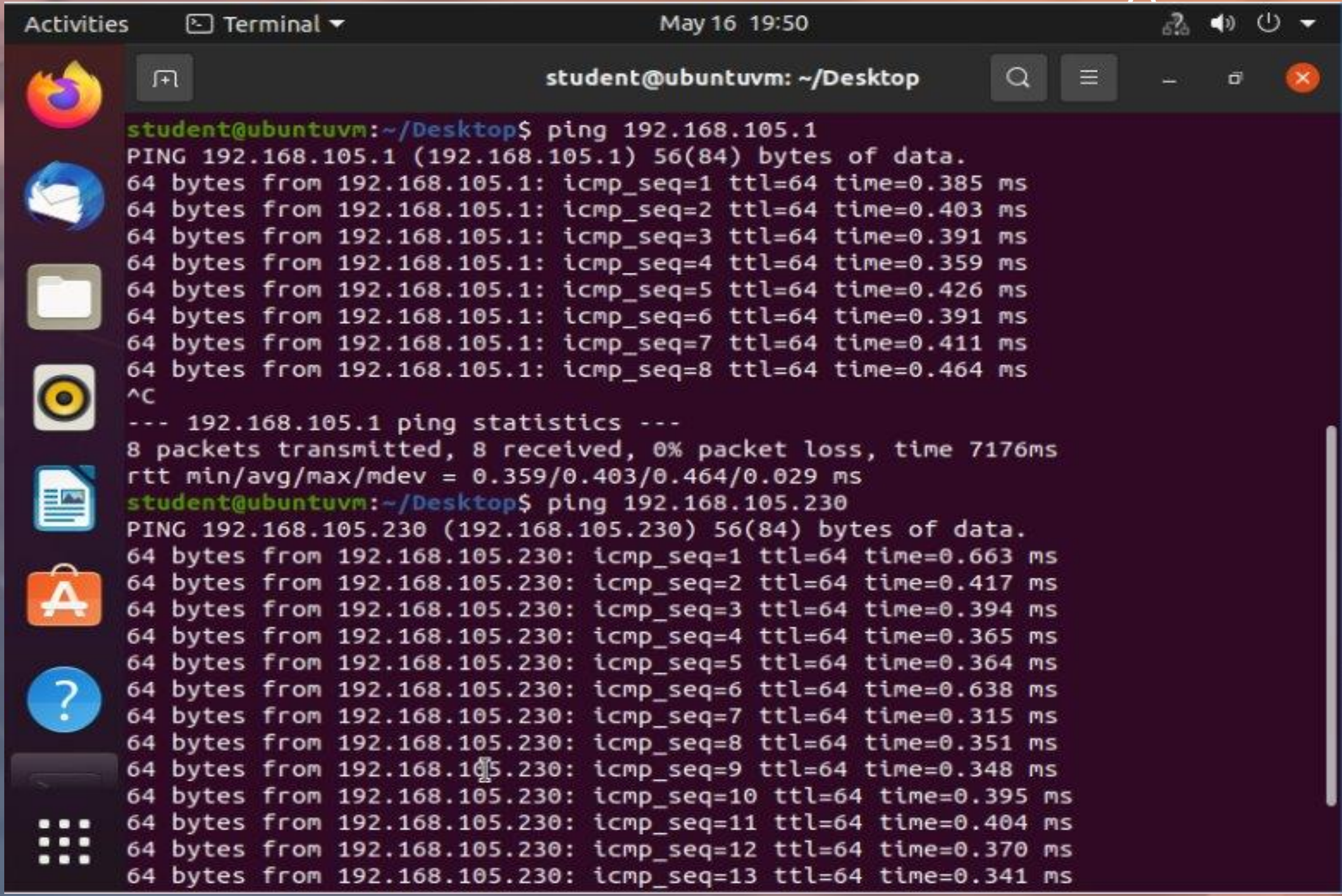
- Documented the connectivity test FROM the Computer 1 VM TO the SOHO Router VM and FROM the Computer 1 VM TO the Computer 2 VM through a Terminal window screenshot.
- Conducted to ensure seamless communication between devices within the network.
- Incorporated the date/time information on top of the Terminal window to maintain a chronological record of the testing process.



```
student@ubuntuvm:~/Desktop$ ping 192.168.105.1
PING 192.168.105.1 (192.168.105.1) 56(84) bytes of data.
64 bytes from 192.168.105.1: icmp_seq=1 ttl=64 time=0.385 ms
64 bytes from 192.168.105.1: icmp_seq=2 ttl=64 time=0.403 ms
64 bytes from 192.168.105.1: icmp_seq=3 ttl=64 time=0.391 ms
64 bytes from 192.168.105.1: icmp_seq=4 ttl=64 time=0.359 ms
64 bytes from 192.168.105.1: icmp_seq=5 ttl=64 time=0.426 ms
64 bytes from 192.168.105.1: icmp_seq=6 ttl=64 time=0.391 ms
64 bytes from 192.168.105.1: icmp_seq=7 ttl=64 time=0.411 ms
64 bytes from 192.168.105.1: icmp_seq=8 ttl=64 time=0.464 ms
^C
--- 192.168.105.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7176ms
rtt min/avg/max/mdev = 0.359/0.403/0.464/0.029 ms
student@ubuntuvm:~/Desktop$ ping 192.168.105.230
PING 192.168.105.230 (192.168.105.230) 56(84) bytes of data.
64 bytes from 192.168.105.230: icmp_seq=1 ttl=64 time=0.663 ms
64 bytes from 192.168.105.230: icmp_seq=2 ttl=64 time=0.417 ms
64 bytes from 192.168.105.230: icmp_seq=3 ttl=64 time=0.394 ms
64 bytes from 192.168.105.230: icmp_seq=4 ttl=64 time=0.365 ms
64 bytes from 192.168.105.230: icmp_seq=5 ttl=64 time=0.364 ms
64 bytes from 192.168.105.230: icmp_seq=6 ttl=64 time=0.638 ms
64 bytes from 192.168.105.230: icmp_seq=7 ttl=64 time=0.315 ms
64 bytes from 192.168.105.230: icmp_seq=8 ttl=64 time=0.351 ms
64 bytes from 192.168.105.230: icmp_seq=9 ttl=64 time=0.348 ms
64 bytes from 192.168.105.230: icmp_seq=10 ttl=64 time=0.395 ms
64 bytes from 192.168.105.230: icmp_seq=11 ttl=64 time=0.404 ms
64 bytes from 192.168.105.230: icmp_seq=12 ttl=64 time=0.370 ms
64 bytes from 192.168.105.230: icmp_seq=13 ttl=64 time=0.341 ms
```

Connectivity Test from Computer 2 VM

- •Captured a screenshot of the Terminal window displaying the connectivity test FROM the Computer 2 VM TO the SOHO Router VM and FROM the Computer 2 VM TO the Computer 1 VM.
- •Executed to verify bidirectional communication within the network setup.
- •Included the date/time information on top of the Terminal window for comprehensive documentation and chronological context.



```
student@ubuntuvm:~/Desktop$ ping 192.168.105.1
PING 192.168.105.1 (192.168.105.1) 56(84) bytes of data.
64 bytes from 192.168.105.1: icmp_seq=1 ttl=64 time=0.385 ms
64 bytes from 192.168.105.1: icmp_seq=2 ttl=64 time=0.403 ms
64 bytes from 192.168.105.1: icmp_seq=3 ttl=64 time=0.391 ms
64 bytes from 192.168.105.1: icmp_seq=4 ttl=64 time=0.359 ms
64 bytes from 192.168.105.1: icmp_seq=5 ttl=64 time=0.426 ms
64 bytes from 192.168.105.1: icmp_seq=6 ttl=64 time=0.391 ms
64 bytes from 192.168.105.1: icmp_seq=7 ttl=64 time=0.411 ms
64 bytes from 192.168.105.1: icmp_seq=8 ttl=64 time=0.464 ms
^C
--- 192.168.105.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7176ms
rtt min/avg/max/mdev = 0.359/0.403/0.464/0.029 ms
student@ubuntuvm:~/Desktop$ ping 192.168.105.230
PING 192.168.105.230 (192.168.105.230) 56(84) bytes of data.
64 bytes from 192.168.105.230: icmp_seq=1 ttl=64 time=0.663 ms
64 bytes from 192.168.105.230: icmp_seq=2 ttl=64 time=0.417 ms
64 bytes from 192.168.105.230: icmp_seq=3 ttl=64 time=0.394 ms
64 bytes from 192.168.105.230: icmp_seq=4 ttl=64 time=0.365 ms
64 bytes from 192.168.105.230: icmp_seq=5 ttl=64 time=0.364 ms
64 bytes from 192.168.105.230: icmp_seq=6 ttl=64 time=0.638 ms
64 bytes from 192.168.105.230: icmp_seq=7 ttl=64 time=0.315 ms
64 bytes from 192.168.105.230: icmp_seq=8 ttl=64 time=0.351 ms
64 bytes from 192.168.105.230: icmp_seq=9 ttl=64 time=0.348 ms
64 bytes from 192.168.105.230: icmp_seq=10 ttl=64 time=0.395 ms
64 bytes from 192.168.105.230: icmp_seq=11 ttl=64 time=0.404 ms
64 bytes from 192.168.105.230: icmp_seq=12 ttl=64 time=0.370 ms
64 bytes from 192.168.105.230: icmp_seq=13 ttl=64 time=0.341 ms
```

Conclusion of Connectivity Test

Through the comprehensive examination of dynamic IP address assignment and connectivity testing, this project has successfully validated the network connection between two virtual machines (VMs) and a SOHO (Small Office/Home Office) router. By configuring the SOHO router as a DHCP server, dynamic IP addresses were efficiently assigned to the VMs, facilitating seamless communication within the network.

The connectivity tests conducted between the VMs and the SOHO router, as well as between the VMs themselves, demonstrated the robustness and reliability of the network setup. These tests confirmed that data packets could traverse the network efficiently, ensuring effective communication between devices.

IP Subnetting and Loopback Interfaces

This part of the project involves IP subnetting and configuring loopback interfaces on an SOHO router to simulate network environments. The process includes subnetting an IP address block, configuring virtual interfaces, and testing network connectivity. This section is divided into three parts: IP Subnetting, Loopback Interfaces, and Connectivity Tests.

Part 1: IP Subnetting

- Dividing IP address block into two subnets with /25 prefix.

Part 2: Loopback Interfaces

- Access SOHO Router Management Interface.

- Create Loopback Interfaces: Loopback1 and Loopback2.

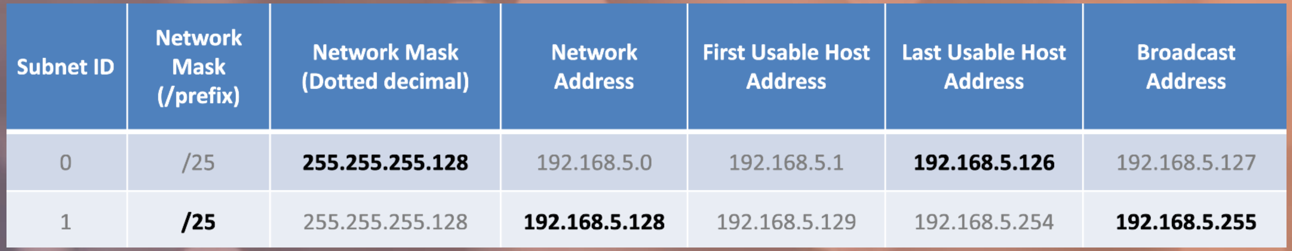
Part 3: Connectivity Tests

- Verify connectivity to Loopback interfaces.

These steps complete the process of subnetting an IP address block, configuring loopback interfaces on the SOHO router, and verifying network connectivity.

IP Subnetting

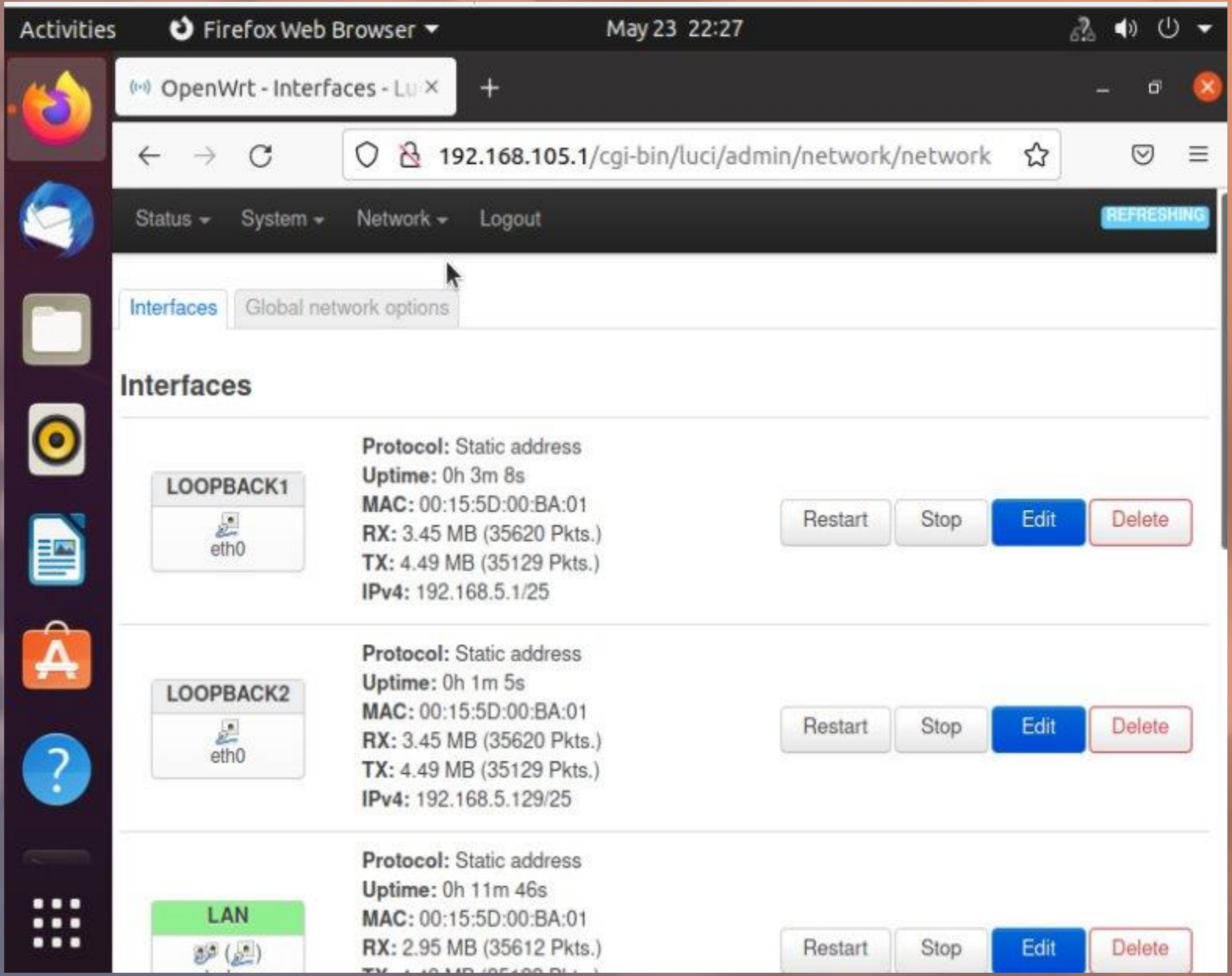
- This table with two /25 subnets:
- This step demonstrates the division of an IP address block into smaller, manageable subnets for efficient network organization.
- List the following for each subnet:
- Subnet notation:
- Clearly identifies the subnet structure.
- Network address:
- Specifies the starting point of the subnet.
- First usable host address:
- Indicates the first IP address that can be assigned to a device.
- Last usable host address:
- Indicates the last IP address that can be assigned to a device.
- Broadcast address:
- Used for sending data to all hosts within the subnet.



Subnet ID	Network Mask (/prefix)	Network Mask (Dotted decimal)	Network Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0	/25	**255.255.255.128**	192.168.5.0	192.168.5.1	**192.168.5.126**	192.168.5.127
1	**/25**	255.255.255.128	**192.168.5.128**	192.168.5.129	192.168.5.254	**192.168.5.255**

Loopback Interfaces

- Screenshot showing both Loopback1 and Loopback2 interfaces:
- Demonstrates the creation of virtual interfaces for testing and management purposes.
- Ensure the screenshot displays the correct IPv4 addresses for both interfaces:
- Verifies that the loopback interfaces have been correctly configured with the assigned IP addresses.
- Include the date/time information on top of the desktop window for context:
- Provides a time-stamped record of the configuration process, ensuring accurate documentation.
- subnet.



Interfaces

LOOPBACK1
eth0

Protocol: Static address
Uptime: 0h 3m 8s
MAC: 00:15:5D:00:BA:01
RX: 3.45 MB (35620 Pkts.)
TX: 4.49 MB (35129 Pkts.)
IPv4: 192.168.5.1/25

LOOPBACK2
eth0

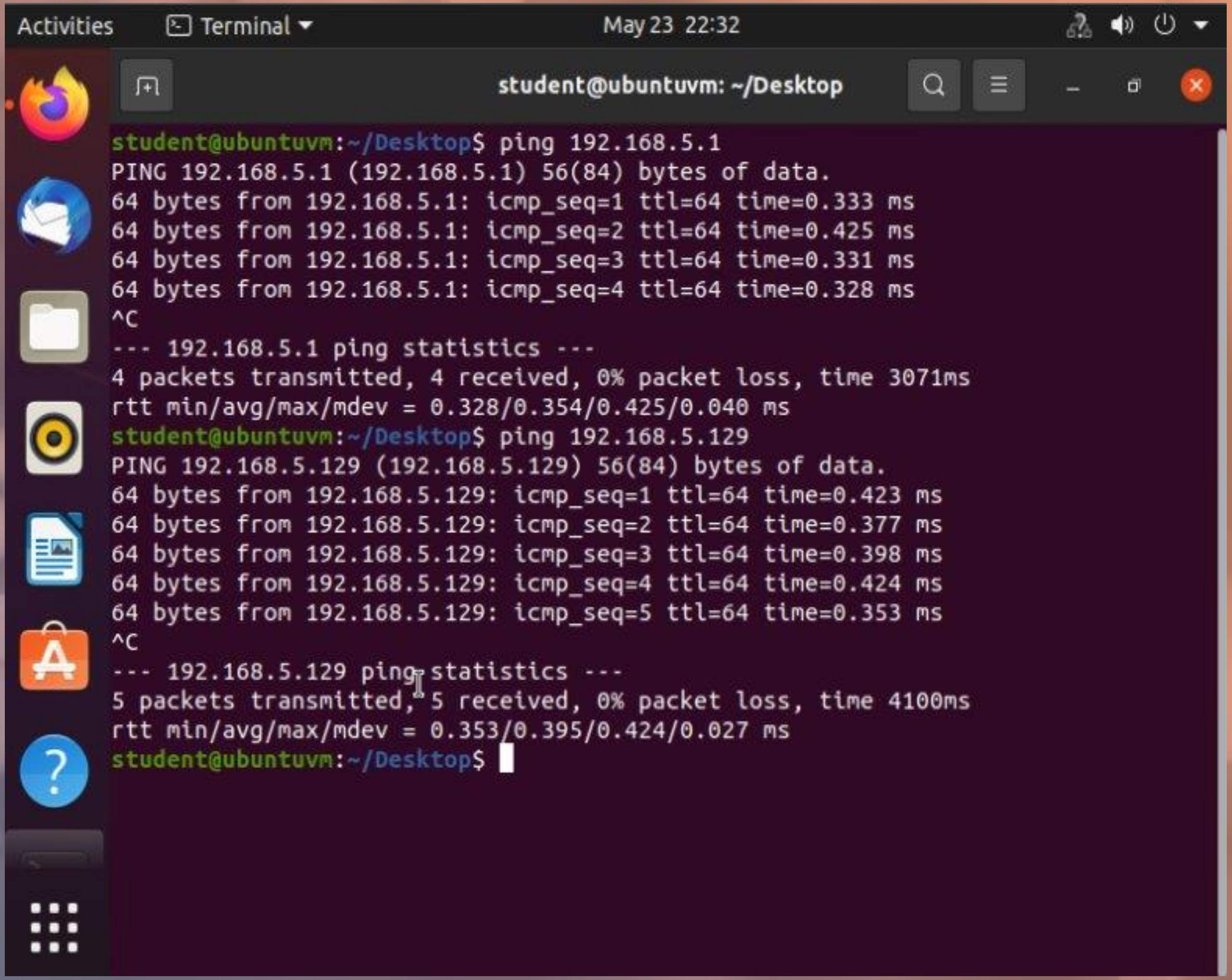
Protocol: Static address
Uptime: 0h 1m 5s
MAC: 00:15:5D:00:BA:01
RX: 3.45 MB (35620 Pkts.)
TX: 4.49 MB (35129 Pkts.)
IPv4: 192.168.5.129/25

LAN

Protocol: Static address
Uptime: 0h 11m 46s
MAC: 00:15:5D:00:BA:01
RX: 2.95 MB (35612 Pkts.)

Connectivity Tests

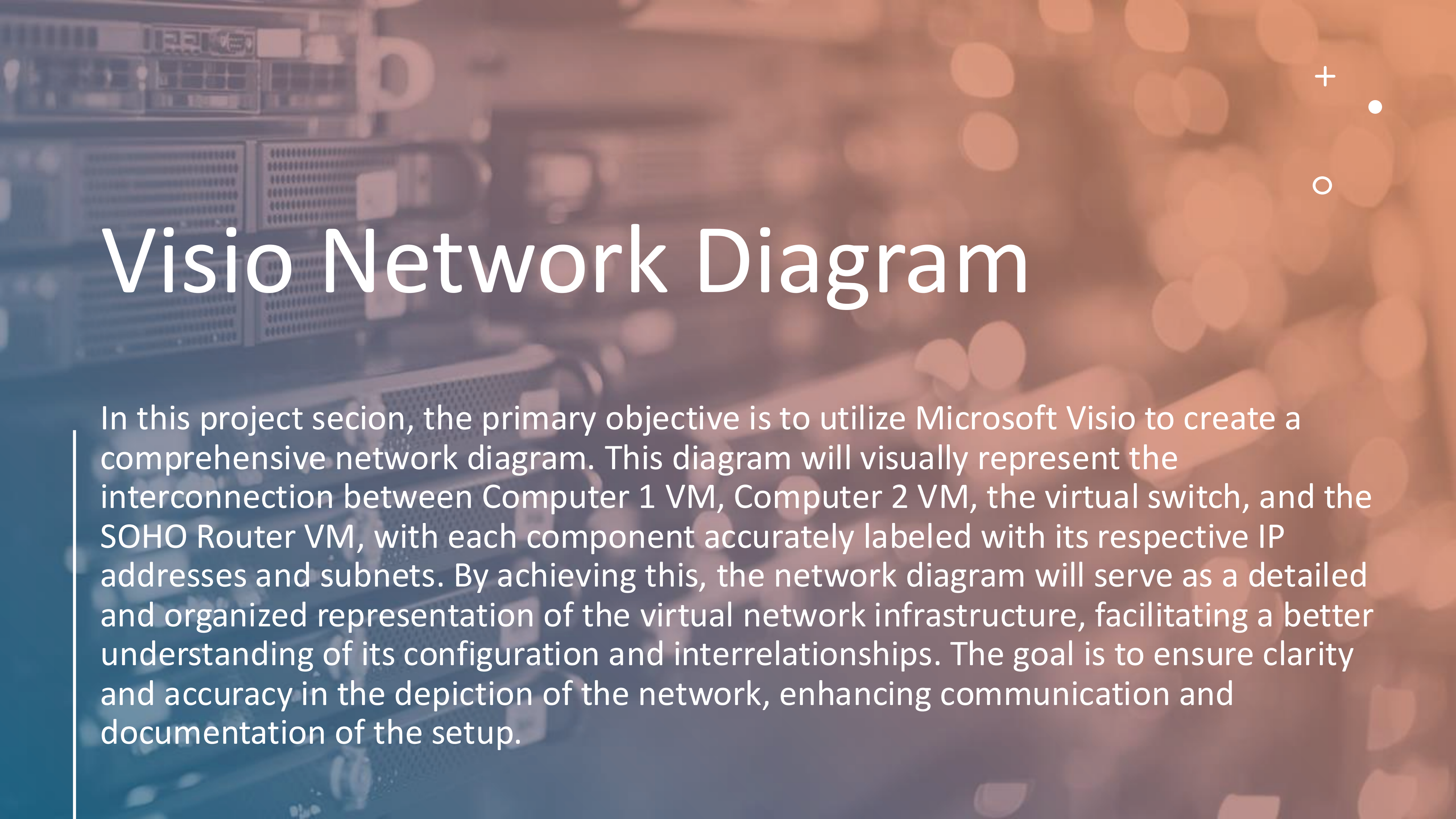
- Screenshot displaying successful ping tests from Computer 1 VM:
- Confirms that the network setup allows communication with the loopback interfaces.
- To the Loopback1 interface:
- Verifies connectivity to the first loopback interface, ensuring its accessibility.
- To the Loopback2 interface:
- Verifies connectivity to the second loopback interface, ensuring its accessibility.
- Ensure the screenshot shows the date/time information on top of the desktop window for documentation purposes:
- Provides a time-stamped record of the connectivity tests, ensuring accurate documentation and verification of successful configuration.



```
student@ubuntuvm:~/Desktop$ ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1) 56(84) bytes of data.
64 bytes from 192.168.5.1: icmp_seq=1 ttl=64 time=0.333 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=64 time=0.425 ms
64 bytes from 192.168.5.1: icmp_seq=3 ttl=64 time=0.331 ms
64 bytes from 192.168.5.1: icmp_seq=4 ttl=64 time=0.328 ms
^C
--- 192.168.5.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3071ms
rtt min/avg/max/mdev = 0.328/0.354/0.425/0.040 ms
student@ubuntuvm:~/Desktop$ ping 192.168.5.129
PING 192.168.5.129 (192.168.5.129) 56(84) bytes of data.
64 bytes from 192.168.5.129: icmp_seq=1 ttl=64 time=0.423 ms
64 bytes from 192.168.5.129: icmp_seq=2 ttl=64 time=0.377 ms
64 bytes from 192.168.5.129: icmp_seq=3 ttl=64 time=0.398 ms
64 bytes from 192.168.5.129: icmp_seq=4 ttl=64 time=0.424 ms
64 bytes from 192.168.5.129: icmp_seq=5 ttl=64 time=0.353 ms
^C
--- 192.168.5.129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4100ms
rtt min/avg/max/mdev = 0.353/0.395/0.424/0.027 ms
student@ubuntuvm:~/Desktop$
```

Conclusion of IP Subnetting and Loopback Interfaces

This section of the project successfully demonstrated practical applications of IP subnetting and loopback interface configuration on an SOHO router to simulate network environments. By dividing an IP address block into two /25 subnets, we optimized IP address allocation and enhanced network organization. Configuring Loopback1 and Loopback2 interfaces provided essential tools for testing and troubleshooting. Connectivity tests from the Computer 1 VM to both loopback interfaces confirmed successful communication and correct network configuration. This project provided valuable hands-on experience in subnetting, configuring virtual interfaces, and verifying network connectivity—crucial skills for effective network design and management.

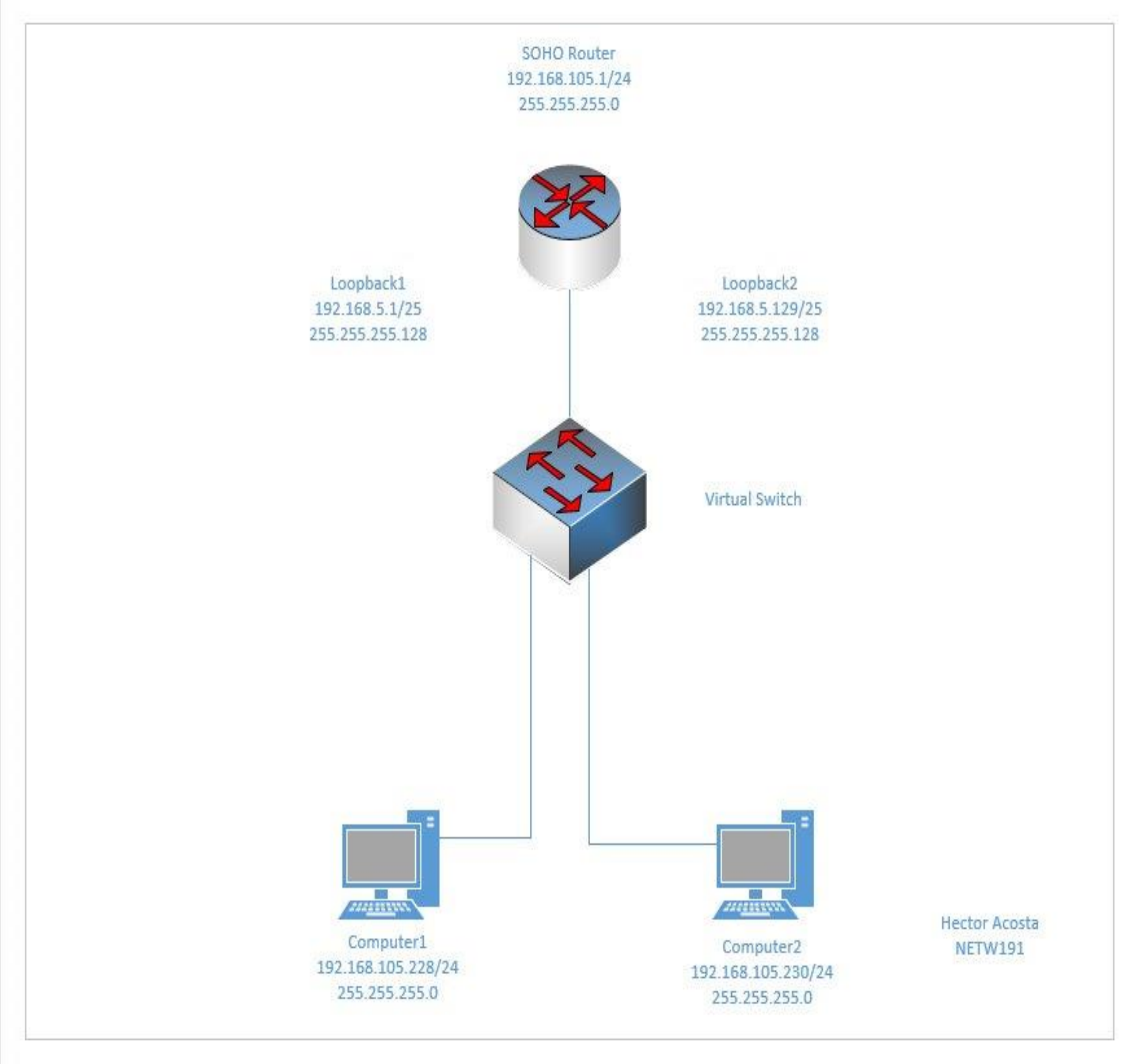


Visio Network Diagram

In this project secion, the primary objective is to utilize Microsoft Visio to create a comprehensive network diagram. This diagram will visually represent the interconnection between Computer 1 VM, Computer 2 VM, the virtual switch, and the SOHO Router VM, with each component accurately labeled with its respective IP addresses and subnets. By achieving this, the network diagram will serve as a detailed and organized representation of the virtual network infrastructure, facilitating a better understanding of its configuration and interrelationships. The goal is to ensure clarity and accuracy in the depiction of the network, enhancing communication and documentation of the setup.

Microsoft Visio Network Diagram

- Diagram Illustration:
- Describe that the diagram will illustrate the interconnection between Computer 1 VM, Computer 2 VM, the virtual switch, and the SOHO Router VM.
- Ensure that all components are shown with proper IP addresses and labeling.
- Accuracy and Detail:
- Explain the importance of accurately depicting each component to reflect the real network setup.
- Mention that detailed labeling helps in identifying each network element and its role.
- Initials Inclusion:
- State that your initials will be included in the bottom right corner of the diagram.
- This helps in personalizing the work and attributing the diagram to the creator.



Conclusion of Visio Network Diagram

This section of the project successfully demonstrated the use of Microsoft Visio to create a detailed network diagram that accurately represents the virtual network infrastructure. By illustrating the interconnections between Computer 1 VM, Computer 2 VM, the virtual switch, and the SOHO Router VM, and including precise IP addresses and labels, the diagram provides a clear and organized view of the network configuration. This visual documentation is essential for better understanding, planning, troubleshooting, and managing network environments. The project underscored the importance of accurate and detailed diagrams in network design and highlighted the practical skills gained in creating and interpreting network diagrams.

SOHO Wireless Network Security

In Module 6 of the course NETW191 Project, we learned about enhancing the security of a Small Office Home Office (SOHO) wireless network using the TP-Link TL-WR902AC router emulator. The module started with preparation steps, such as accessing the TP-Link emulator, identifying the default username and password, and emphasizing the importance of changing these defaults to improve security. We then discussed address management methods, comparing the benefits of configuring device IP addresses manually (static IP) versus using a DHCP server (dynamic IP) to control network access. Additionally, we explored MAC filtering, which allows or denies network access based on MAC addresses, and provided guidelines on using deny and allow filtering rules effectively. The module also covered wireless security protocols available on the router, recommending WPA/WPA2 - Personal for its strong security and ease of implementation. Finally, we reflect on the true security functions and practical steps to safeguard a home wireless network, emphasizing the importance of strong passwords, firmware updates, and network monitoring to protect against cyber threats and unauthorized access.

SOHO Wireless Network Security

1. What are the factory default username and password of a TP-Link router? Why is it important to change the default username and password of a SOHO router?

Answer: The default username and password is admin/admin. Leaving the default credentials unchanged makes your network vulnerable to unauthorized access because they are well-known and easily found on the internet, allowing anyone to gain access, change settings, monitor traffic, and potentially compromise your devices, which can also expose sensitive information that could be used maliciously.

2. To protect a SOHO wireless network with a small number of devices, which address management method provides more control, configuring the device IP addresses manually (static IP) or using a DHCP server (dynamic IP)? Why?

Answer: Static IP addresses provide more control and stability. Because each device will have a fixed IP address, which can simplify troubleshooting and network management.

SOHO Wireless Network Security

3. What does MAC filtering do? If needed, when would you use deny filtering rules and when would you use allow filtering rules? What happens to devices that want to connect, if the “Allow the stations specified by any enabled entries in the list to access” function is enabled but there are no entries in the list?

Answer: MAC filtering is a security feature that allows or denies devices access to a network based on their unique MAC addresses. Deny filtering rules should be used when you want to block specific devices from accessing the network, such as known unauthorized devices or intruders. Allow filtering rules should be used when you want to restrict network access only to approved devices, which is beneficial in highly secure environments. If the "Allow the stations specified by any enabled entries in the list to access" function is enabled but there are no entries in the list, no devices will be able to connect to the network, effectively blocking all devices until specific MAC addresses are added to the list.

4. What wireless security settings are displayed on the Wireless Security page? Which one is recommended by the vendor? Why?

Answer: The wireless security settings displayed on the Wireless Security page include Disable Wireless Security, WPA/WPA2 - Personal (based on a pre-shared passphrase), WPA/WPA2 - Enterprise (based on a Radius Server), and WEP, with vendors recommending WPA/WPA2 - Personal for its balance of strong security, ease of use, offers strong security through encryption and ease of setup using a pre-shared passphrase.

SOHO Wireless Network Security

5. Among the configurations you explored in this module, which one is a true security function? Why?

Answer: Among the configurations explored in this module, MAC filtering is a true security function because it allows or denies devices access to the network based on their unique MAC addresses, thereby providing an additional layer of control over which devices can connect to the network.

6. What would you do to protect your wireless network at home? Why?

Answer: To protect my wireless network at home, I would change the default router credentials to something strong and unique, enable WPA3 encryption (or WPA2 if WPA3 is unavailable), set a strong Wi-Fi password, and configure MAC filtering to allow only recognized devices to connect. I would also disable Wi-Fi Protected Setup (WPS), keep the router firmware updated, disable remote management, enable the router's firewall, set up a separate guest network for visitors, and regularly monitor the list of connected devices for unauthorized access. Doing these measures will ensure robust security against various cyber threats and unauthorized access.

Conclusion of SOHO Wireless Network Security

In Module 6 of the course NETW191 project, the focus was on improving the security of a Small Office Home Office (SOHO) wireless network using the TP-Link TL-WR902AC router emulator. The module started by highlighting the importance of changing default credentials to secure the network. It then compared static IP and DHCP for managing device addresses. MAC filtering, as a security measure to control network access based on MAC addresses, was also introduced. Additionally, the module covered different wireless security protocols and recommended WPA/WPA2 - Personal for its strong security features. Technical challenges included understanding and configuring router settings such as MAC filtering and DHCP, which required using the router emulator and interpreting technical documentation. This module helped develop career skills such as proficiency in router configuration, understanding network security principles, and practical application of cybersecurity measures to protect wireless networks. Overall, the module provided valuable insights into SOHO network security and practical skills relevant to careers in network administration and cybersecurity.

Challenges

Challenges in this network project, such as creating a comprehensive network diagram using Microsoft Visio, include understanding complex network components and their interconnections. Accurately configuring and labeling IP addresses and subnets requires a solid grasp of networking concepts. Mastery of tools like Microsoft Visio for creating detailed diagrams can be daunting, as it demands technical knowledge and familiarity with the software. Ensuring accuracy in documentation and effectively communicating network configurations are crucial, yet challenging tasks. Overcoming these hurdles demands a steep learning curve and ample practice.

Skills Gained

Participating in network projects, such as enhancing the security of a Small Office/Home Office (SOHO) wireless network, equips individuals with valuable skills for cybersecurity. These include:

Understanding security protocols: Learning about wireless security protocols like WPA/WPA2 - Personal enhances knowledge of encryption methods and authentication mechanisms.

Implementing access controls: Exploring address management methods such as static IP configuration and DHCP server setup improves skills in controlling network access and managing device connections.

Deploying security measures: Practicing MAC filtering to control network access based on MAC addresses hones skills in deploying access control lists and implementing deny and allow filtering rules.

Strengthening network defenses: Emphasizing the importance of strong passwords, firmware updates, and network monitoring enhances skills in safeguarding network environments against cyber threats and unauthorized access. These skills are essential for individuals pursuing careers in cybersecurity, as they provide a solid foundation for securing network infrastructures and protecting against evolving cyber threats.

References

The guidance and resources provided by ACI Learning, which have been pivotal in expanding our understanding of networking fundamentals.

The immersive learning experiences offered by the InfoSec Environment labs, which have allowed us to apply theoretical knowledge to practical scenarios.

The insightful lectures and mentorship of Professor Peter Bieniek from DeVry University, whose expertise has guided me through the complexities of network implementation.