Fundamentals of Information Technology and Networking (NETW191)

Final Project

Jonathan Waugh

Oct. 2024

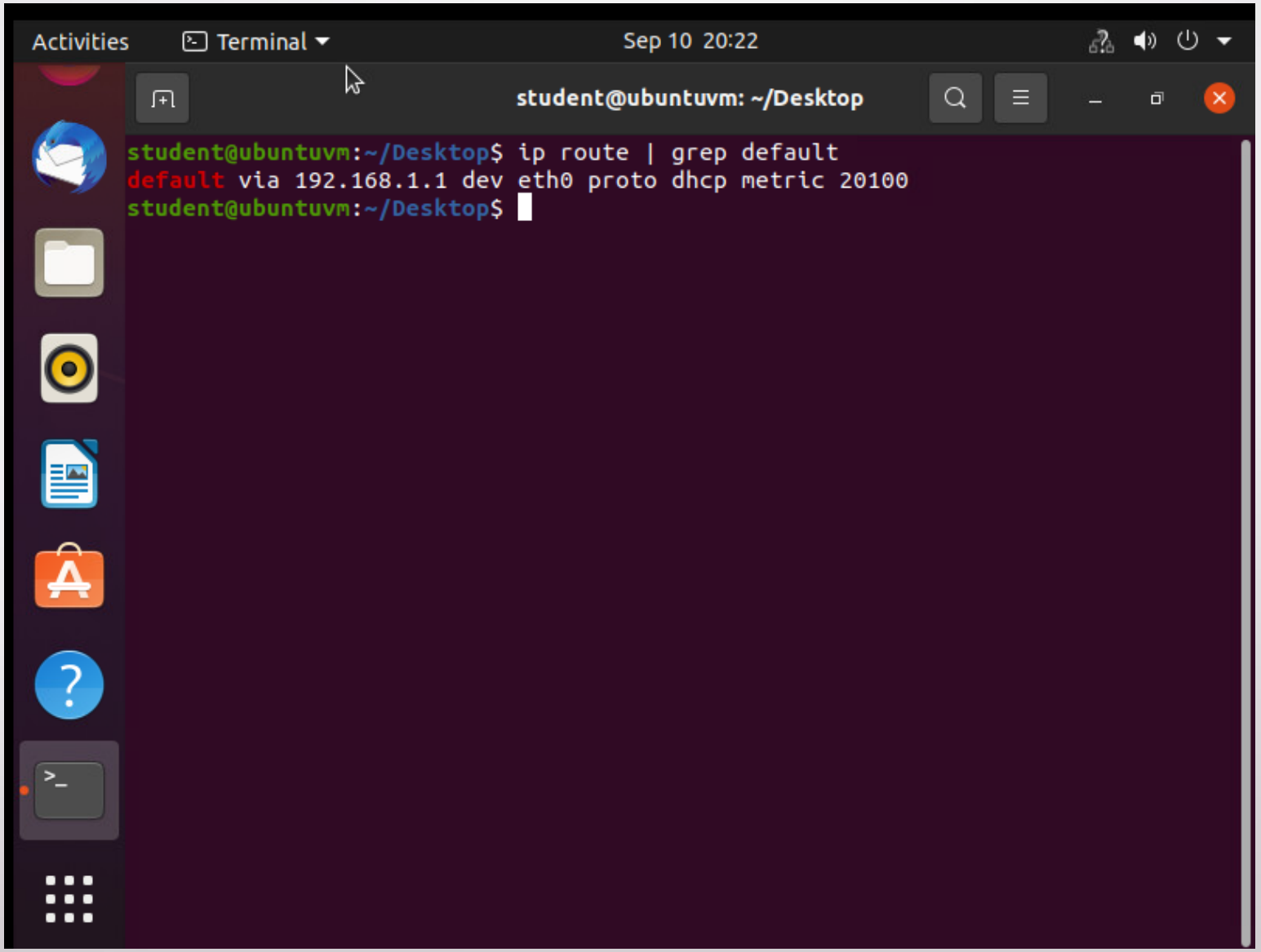
Introduction

- This presentation covers my five-part project completed while taking Fundamentals of Information Technology and Networking (NETW191)
- It includes examples of IPv4 Addressing, Connectivity Testing, IP Subnetting and Loopback Interfaces, VISIO Network Diagram, and SOHO Wireless Network Security
- The objective of this presentation is to give the viewers a better understanding of network design, function, and security

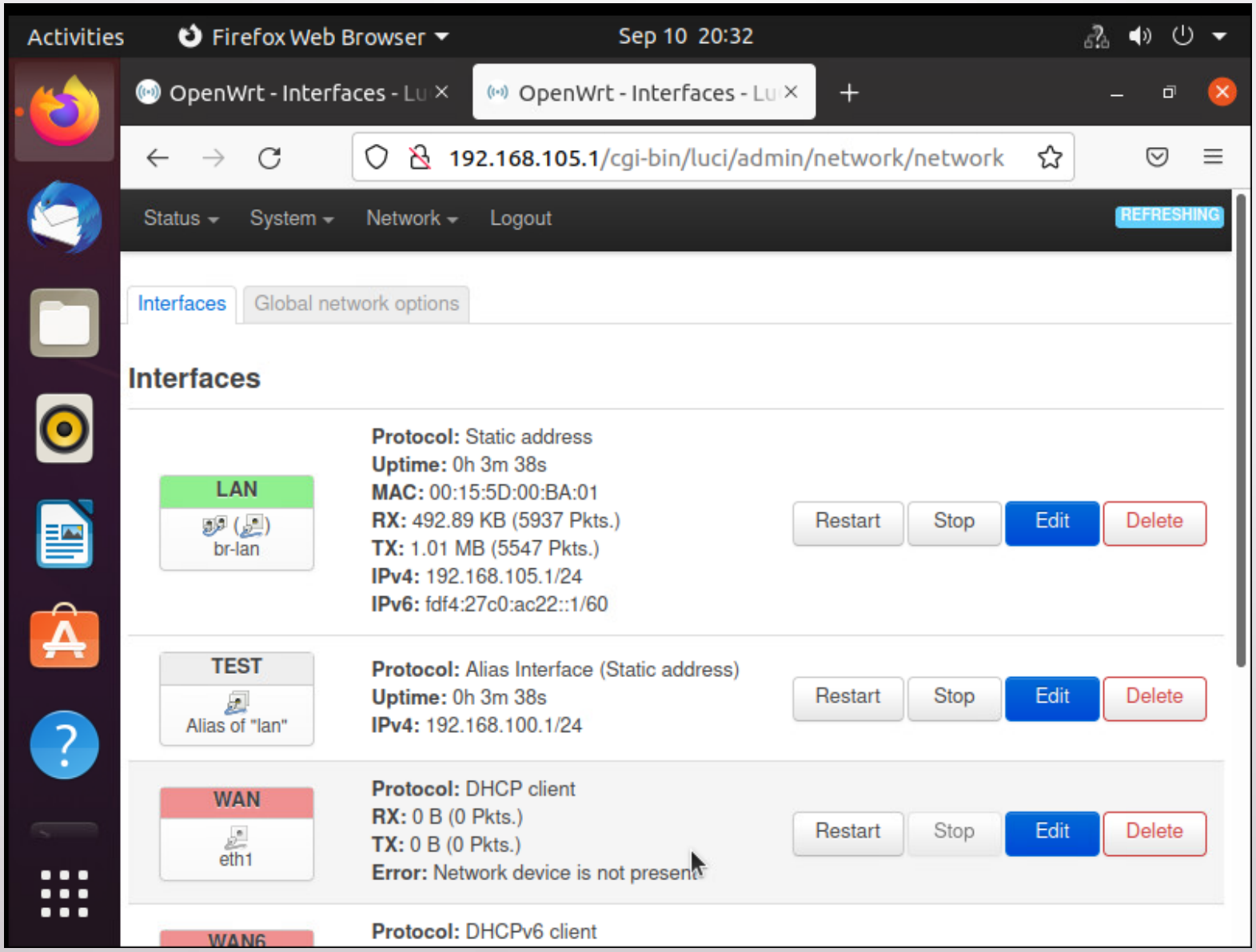
IPv4 Addressing

- In this project I will use a SOHO router virtual machine to change the root password
- Use of a browser to access SOHO router virtual machine management interface to change the IPV4 address

Preparation



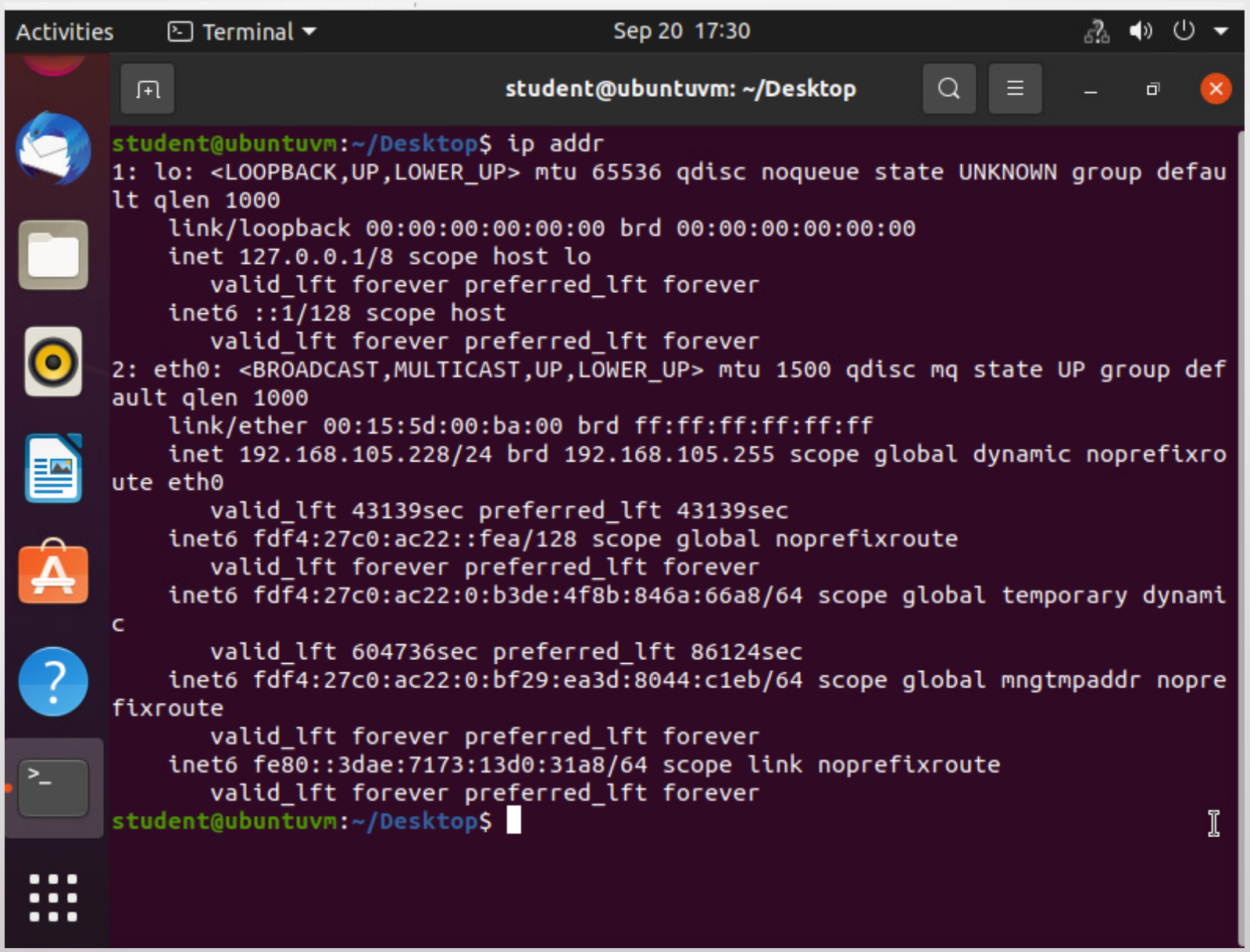
IPv4 Address Assignment



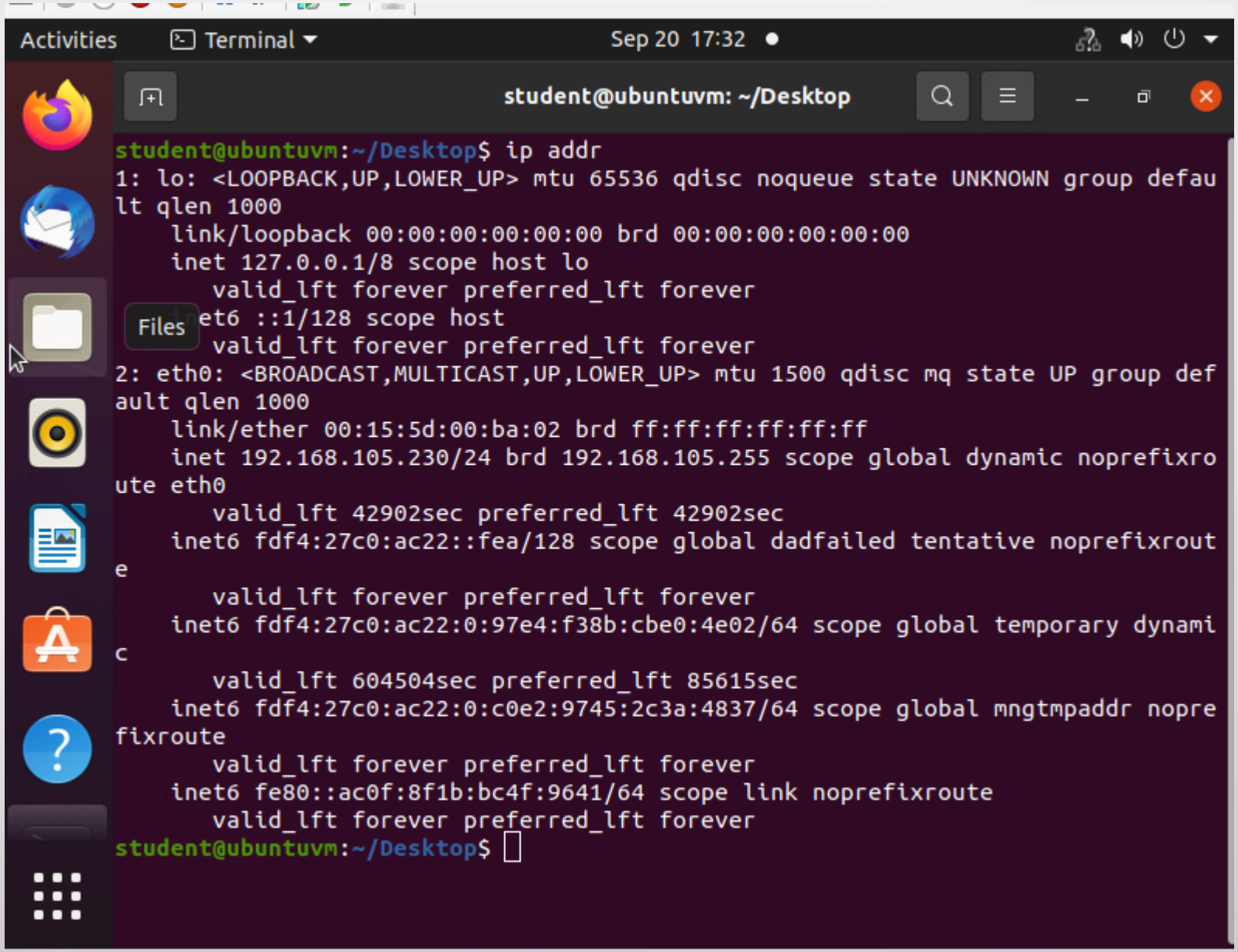
Connectivity Testing

- In this project we check the connection between two computers and a router

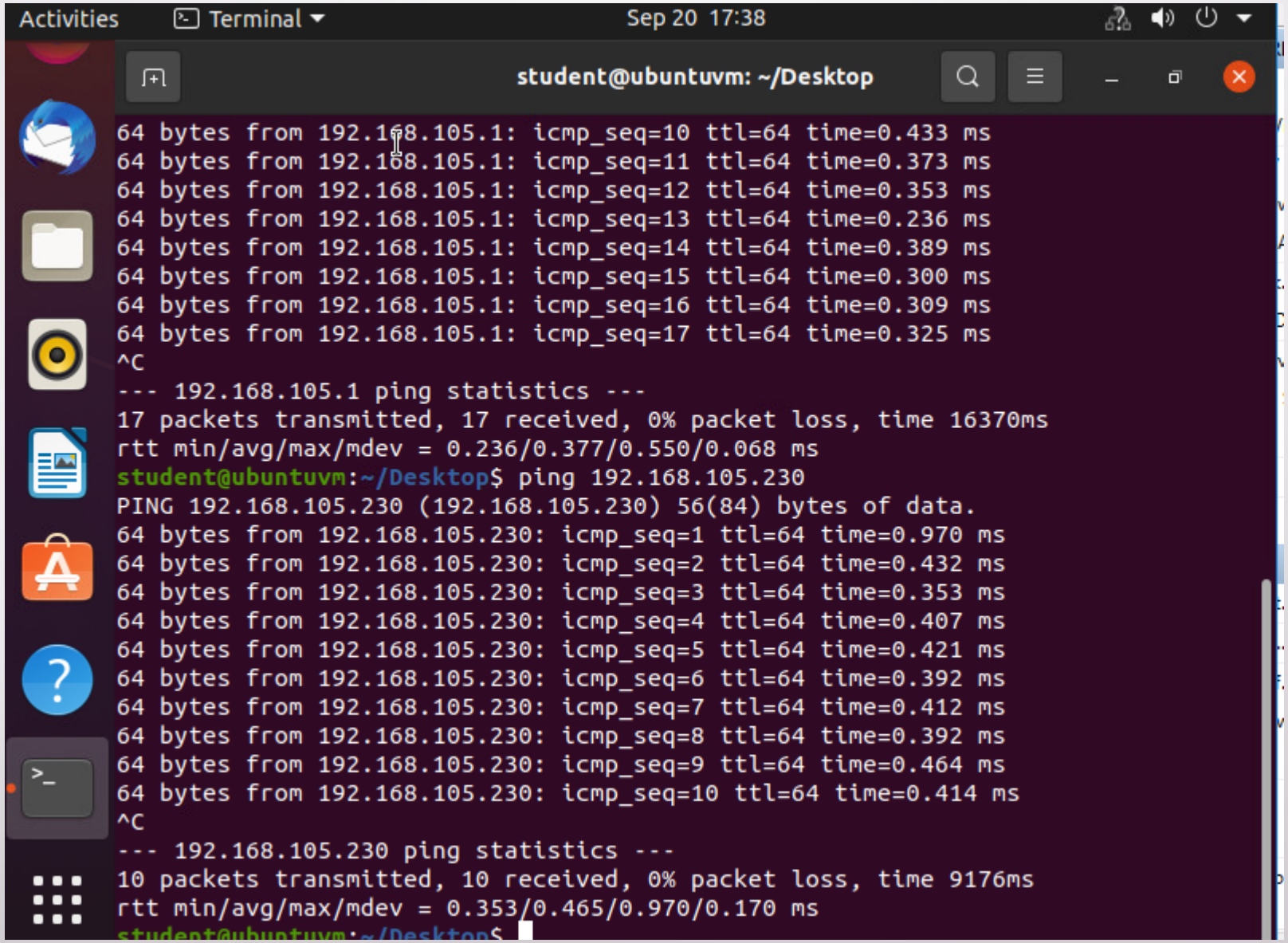
Dynamic IP Address Assignment 1



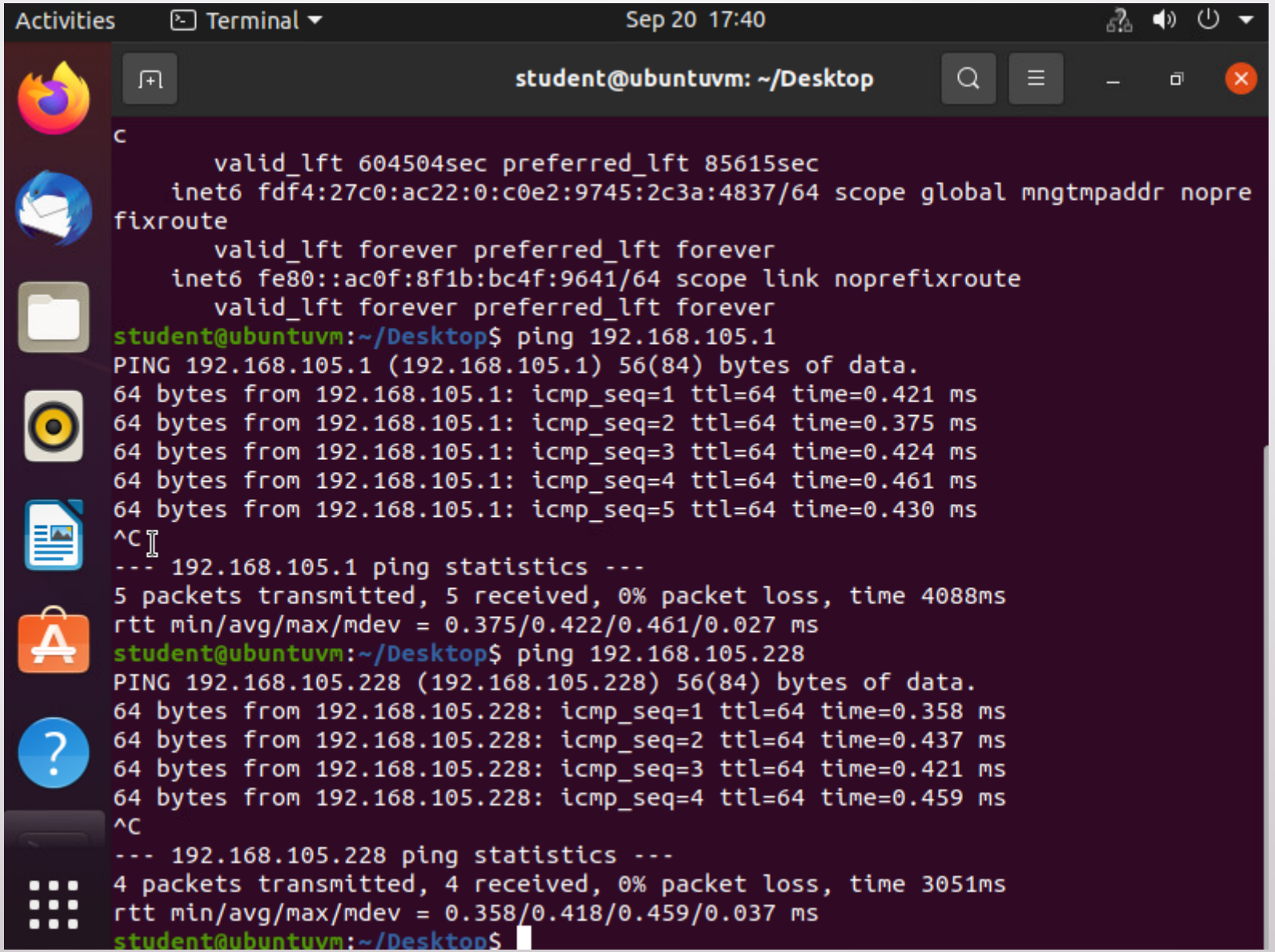
Dynamic IP Address Assignment 2



Connectivity Test 1



Connectivity Test 2



IP Subnetting Loopback Interfaces

In this project we will be IP subnetting and creating 2 new loopback interfaces called Loopback1 and Loopback2 as well as testing the connection to them.

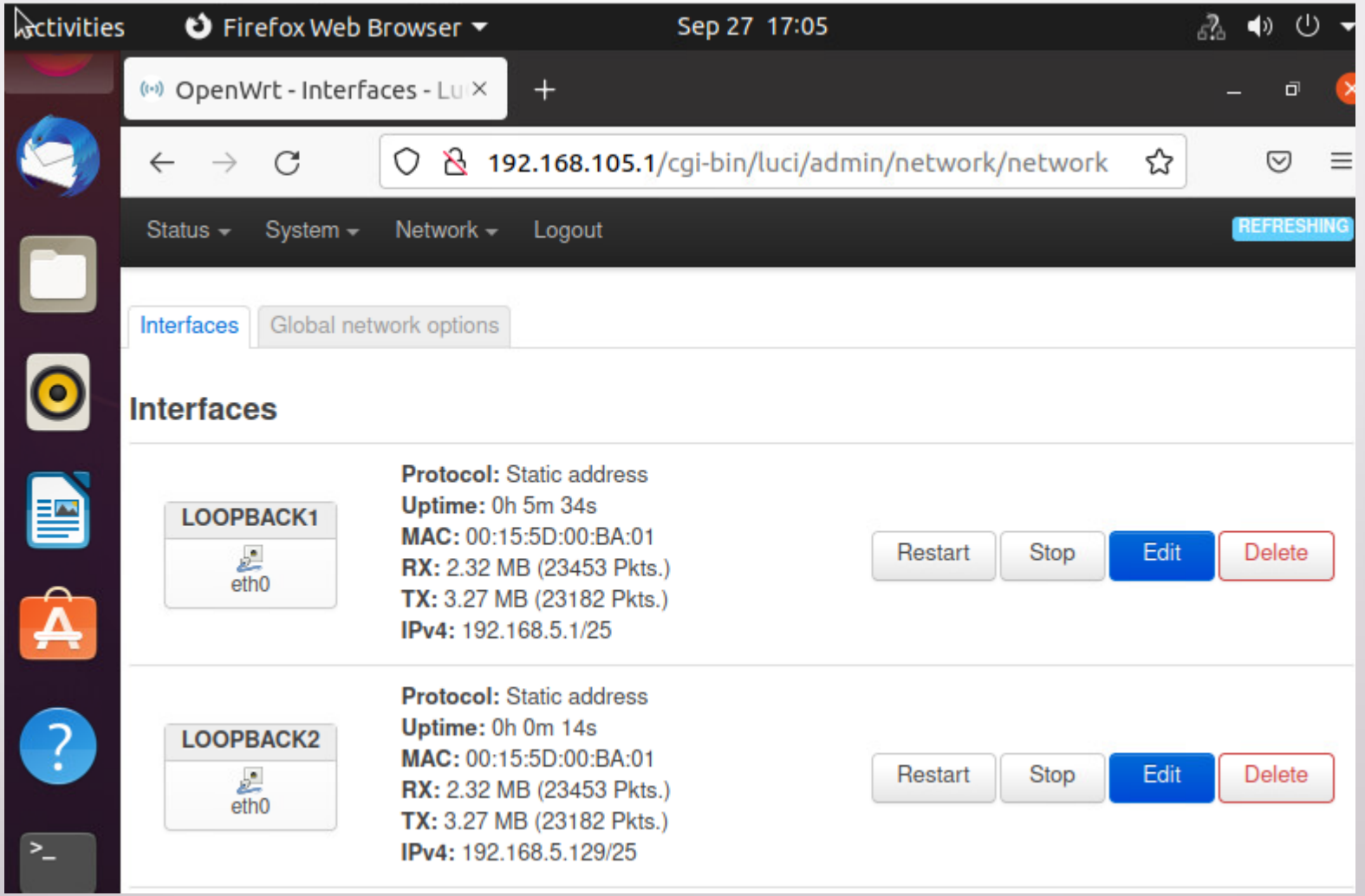
IP Subnetting

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	**196.168.5.128**	192.168.5.129	192.168.5.254	**192.168.5.255**

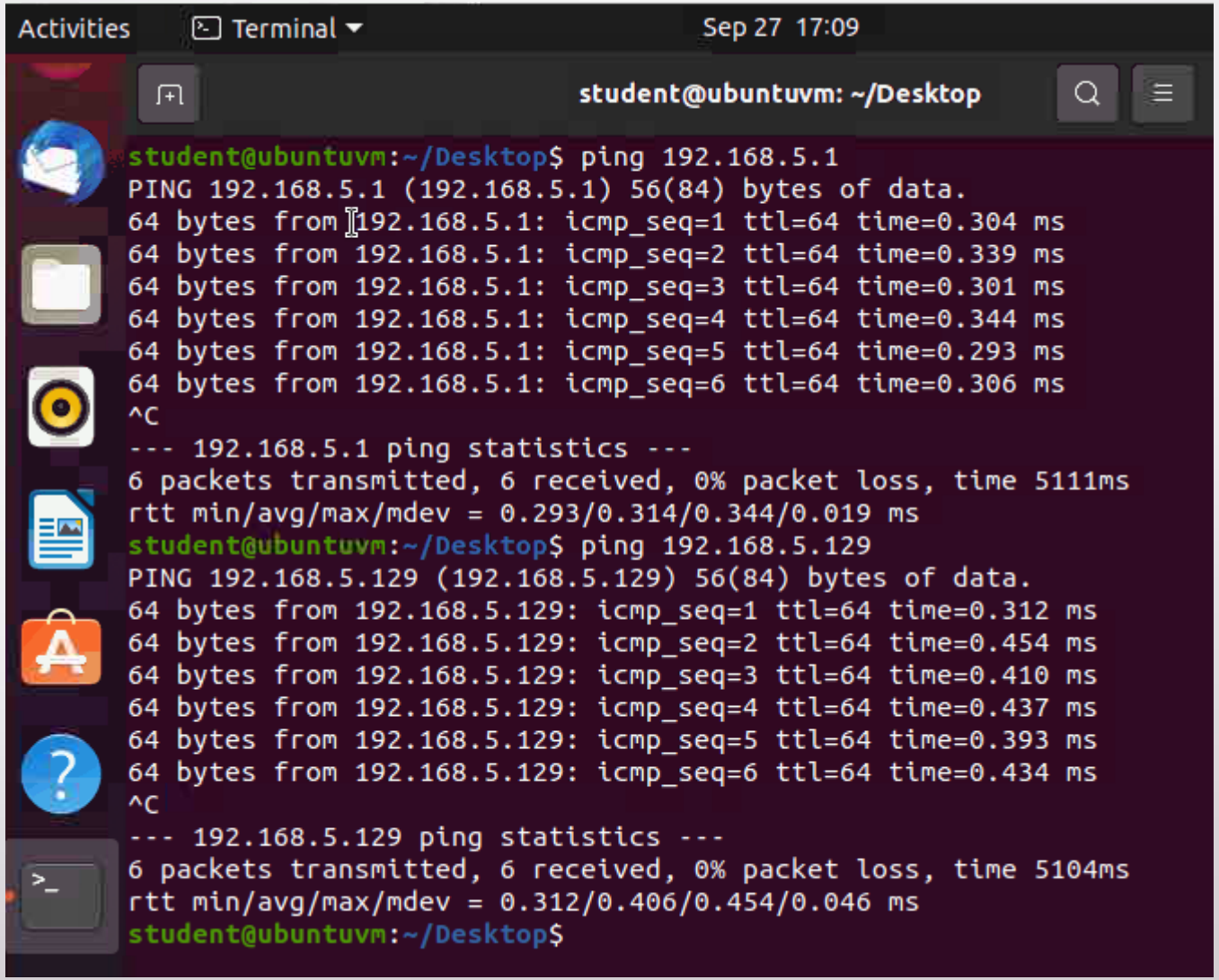
This table should include **two /25 subnets**, listing

- Subnet notation
- Network address
- First usable host address
- Last usable host address
- Broadcast address

Loopback Interfaces



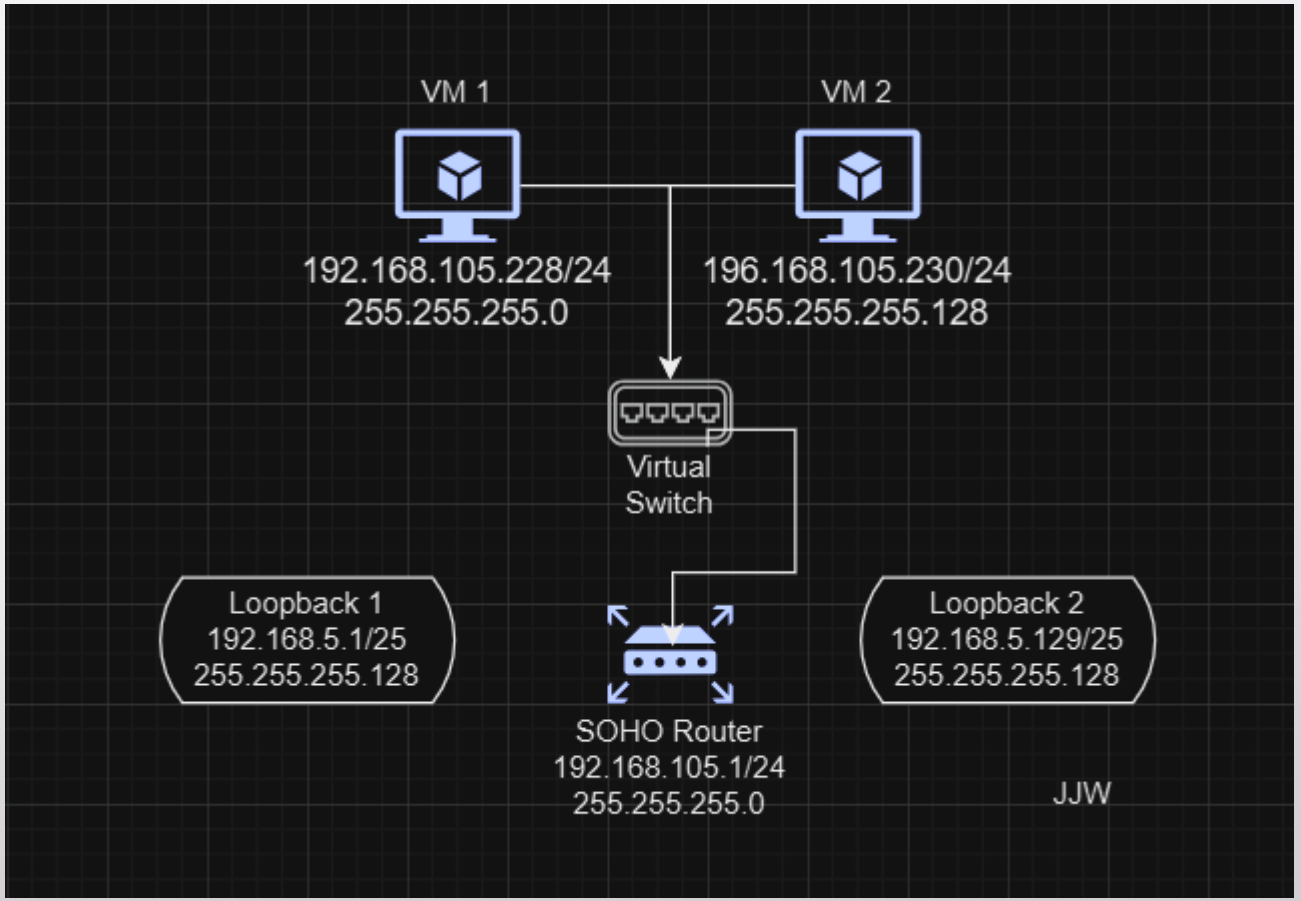
Connectivity Tests



Visio Network Diagram

In this project I used Visio to design and visually show the connections between the SOHO Router, Virtual Switch, Virtual Machine 1, Virtual Machine 2, and Loopback connections.

Microsoft Visio Network Diagram



SOHO Wireless Network Security

In this project we will discuss SOHO wireless network security and the importance of securing your network.

SOHO Wireless Network Security 1 of 3

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:

default username/password – admin/admin

It is important to change this, because if you don't anyone can easily access your router and then get into your computers from there.

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, because it uses the same IP address for each device allowing consisten access to printers, servers, or NAS. This also allows IT professionals to easily troubleshoot devices and it provides the option of limiting the number of devices, which makes everything easier to monitor and control.

SOHO Wireless Network Security 2 of 3

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 uses the unique MAC addresses of devices to control their access to the network. Deny Filtering would be used when you want to block a device from accessing the network while allow filtering grants network access permission to the specified devices. If you do not submit any entries to the “Allow the stations specified by any enabled entries in the list to access” function then no devices will be able to access the network.

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

Answer:

The security settings displayed are Disable Wireless Security, WPA/WPA2 – Personal, WPA/WPA2 – Enterprise, and WEP. The vendor recommends to enable wireless security and select WPA2-PSK AES encryption, because of stronger encryption, better security then older protocols, it’s compatible with almost all modern wireless devices, and AES provides better performance while maintaining security.

SOHO Wireless Network Security 3 of 3

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

Answer:

WPA2-PSK AES encryption is a true security function, because it ensures data sent over the network in encrypted, prevents unauthorized devices from connecting by requiring a PSK (Pre-Shared Key), checks for tampering during transmission, and meets industry standards and regulatory requirements for data security.

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

Answer:

I personally try to use a very unguessable password, always change your default network name and password, disable SSID broadcasting, enable MAC filtering, make sure to stay updated, disable remote management, and enable firewalls. I also recommend using a guest network for visitors and regularly check connected devices.

Challenges

- Challenges I faced while doing these projects was mainly navigation. I had to learn to navigate multiple interfaces and websites as well as learning to locate different information.
- I easily overcame these challenges by taking the time to re-read all of my lessons as well as reading everything written on the different interfaces and websites.

Career Skills

- Understand the concept of network addressing and network protocols
- Explain data transmission concepts and characteristics of different transmission media
- Segment a network into multiple LANs or multiple VLANs
- Understand networking fundamentals, including network types, hardware devices, topologies, the OSI model, structured cabling, and documentation
- Implement security into the design of a network
- Produce a network to a specification

Conclusion

This class provided a great teaching on the fundamentals of information technology and networking. With these teachings I can now design, setup, troubleshoot, manage, and secure a network. I also achieved the skills to monitor network performance, manage projects, identify security threats and secure them. I am excited to continue learning more about network security and hone my skills to advance me in my career path. Learning the basics of network security will allow me to better understand advanced security techniques providing a better service to future customers.

References

- Live Lessons. Professor Marzouk, Hassan and Khan Nabeel, Ronald Darnell, Rexford Okrah, Kevin Greshock, Peter Bieniek, Alex Leung, Burton Piper, Farooq Afzal. NETW191, 2024
- West, Jill. *CompTIA Network+ Guide to Networks*. 2021.
- *Network+ Guide to Networks, Loose-Leaf Version*. Cengage Learning, 2018.
- Project Guides