JEANINE CARHART

NETW 191 FINAL PROJECT AUGUST 2022

INTRODUCTION

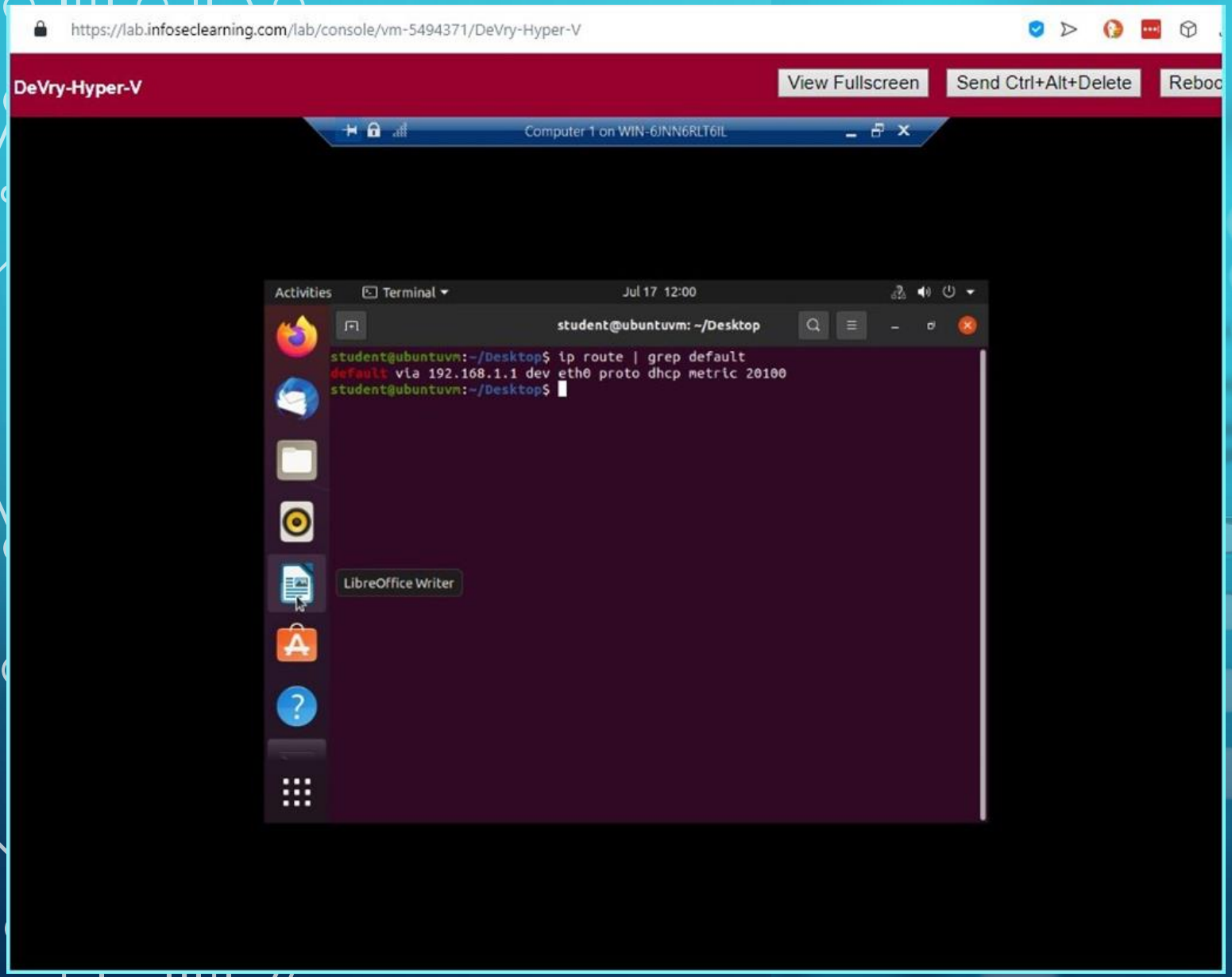
PROJECT SCOPE

- IPv4 Addressing
- Connectivity Test
- IP Subnetting and Loopback Interfaces
- Visio Network Diagram
- SOHO Wireless Network Security
- Final Project

MODULE 2

IPv4 Addressing

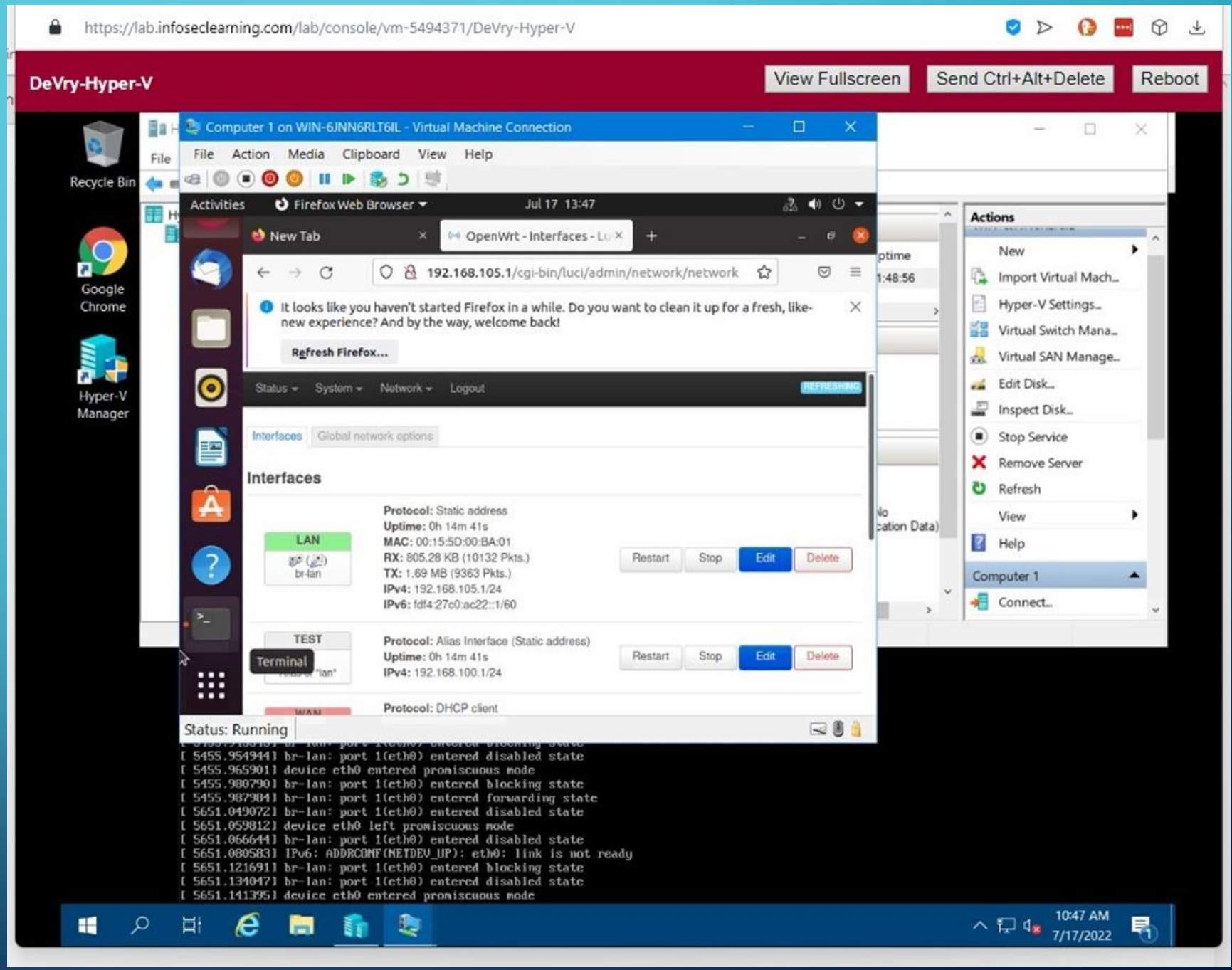
PREPARATION



This screenshot should include the terminal window that shows the default gateway IP address.

IPV4 ADDRESS ASSIGNMENT

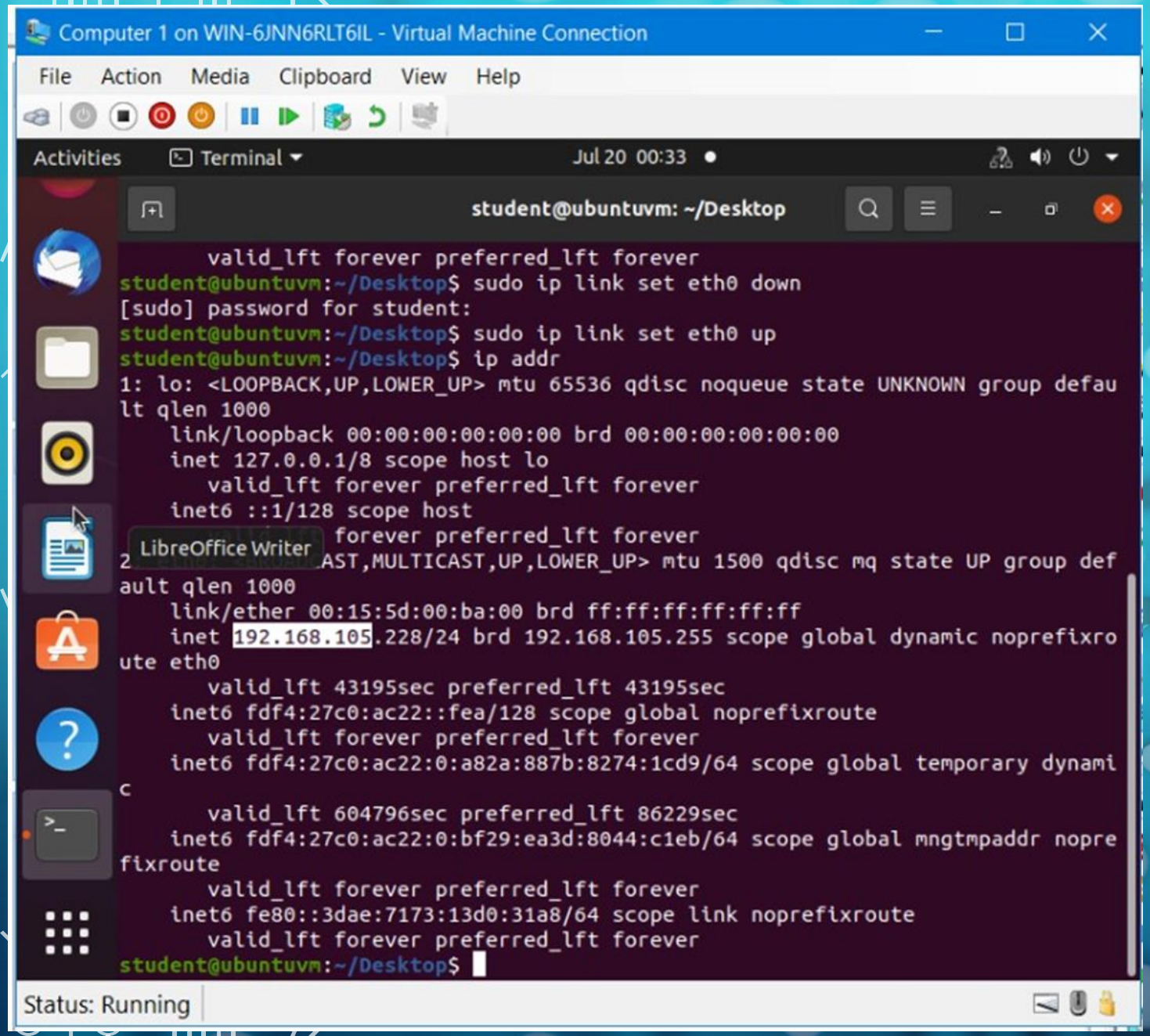
This screenshot should include the *Interfaces* page that shows the new IPv4 address on the LAN interface.



MODULE 3

Connectivity Test

DYNAMIC IP ADDRESS ASSIGNMENT



- This screenshot should show the IPv4 address of the *Computer 1* VM.

Computer 1

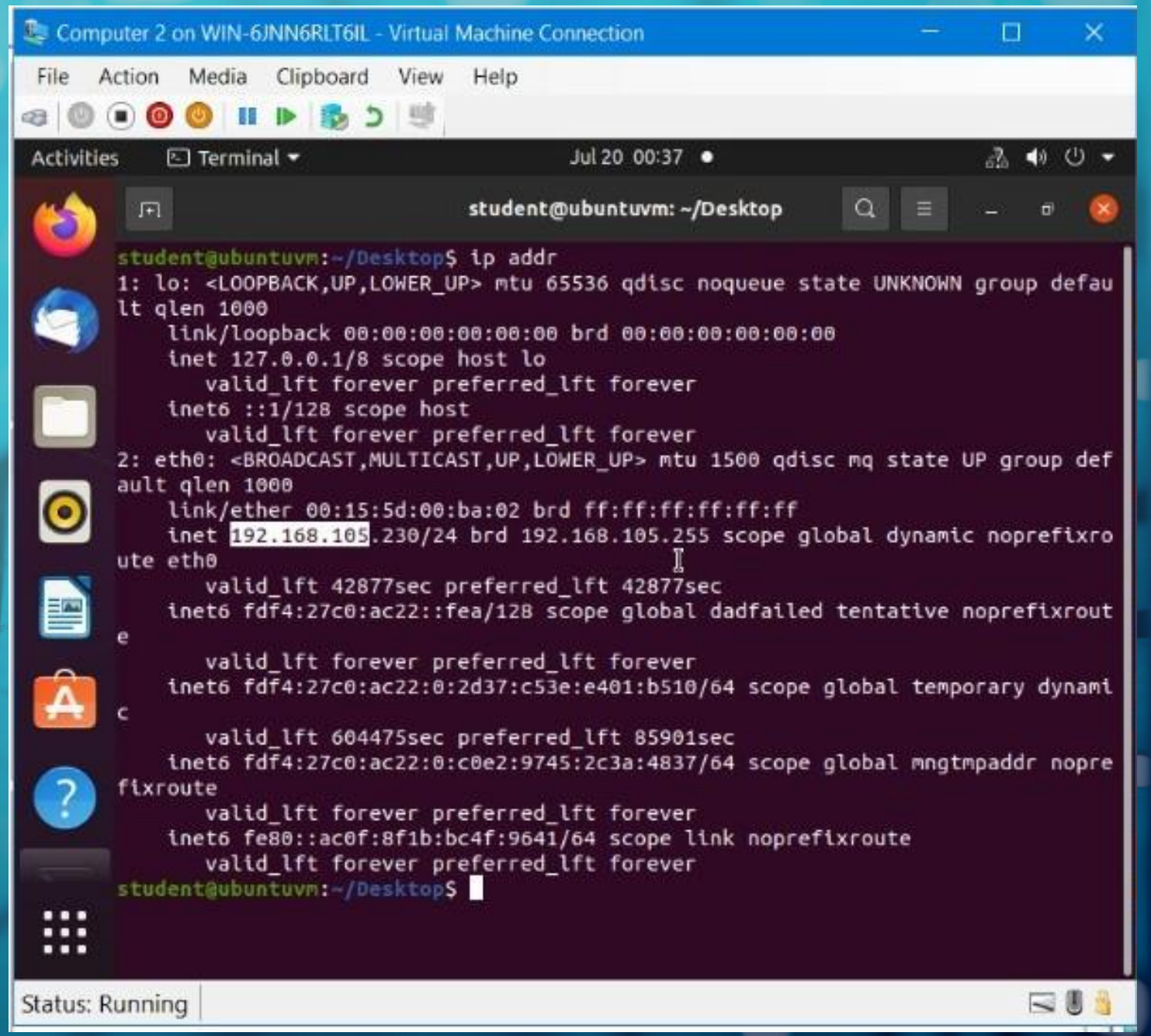
Computer 1	192.168.105.228

DYNAMIC IP ADDRESS ASSIGNMENT

This screenshot should show the IPv4 address of the *Computer 2* VM.

Computer 2

Computer 2	192.168.105.230

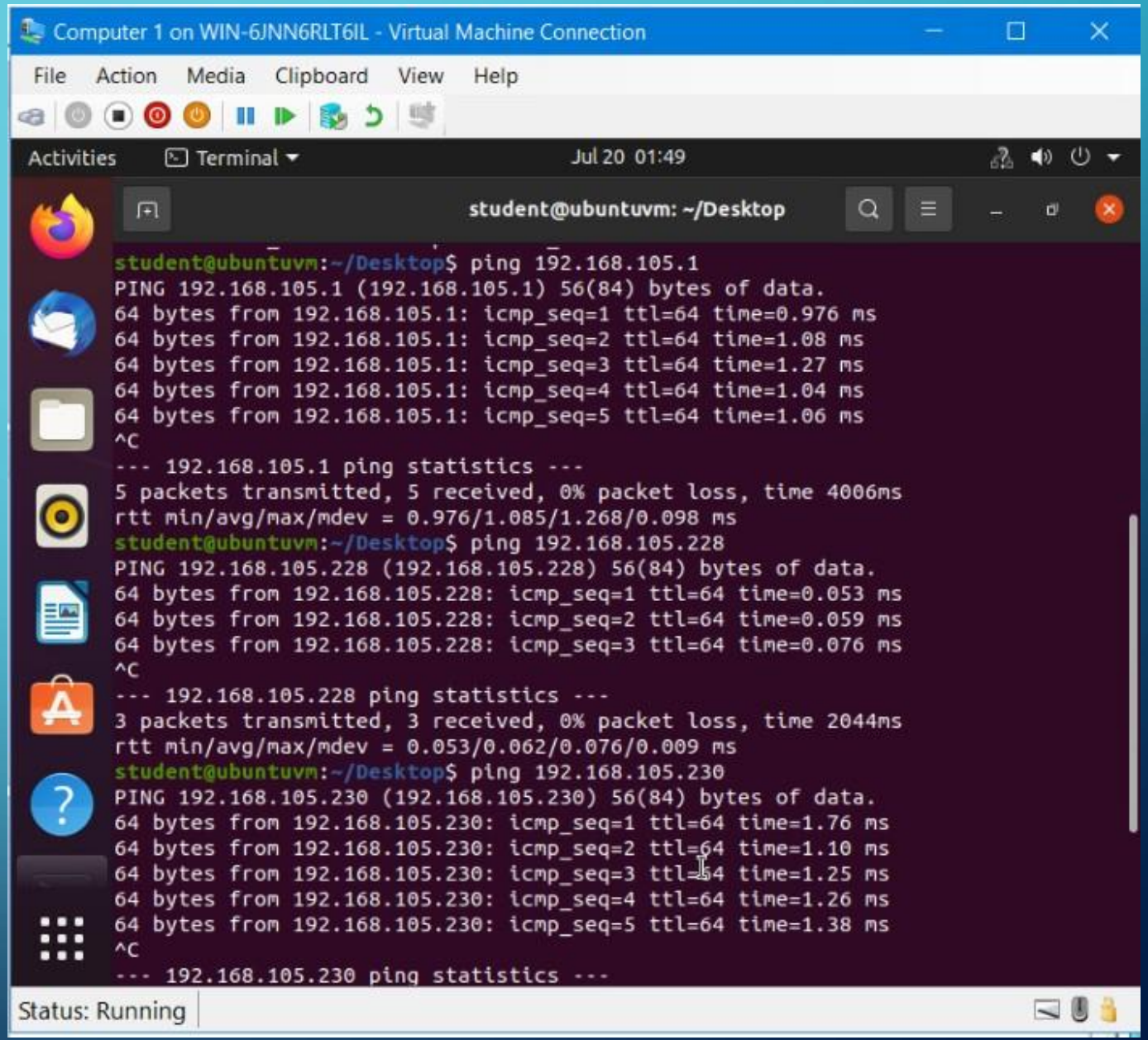


CONNECTIVITY TEST

This screenshot should show the connectivity tests between the *Computer 1* VM and the other two devices (i.e., the *SOHO Router* VM and *Computer 2* VM).

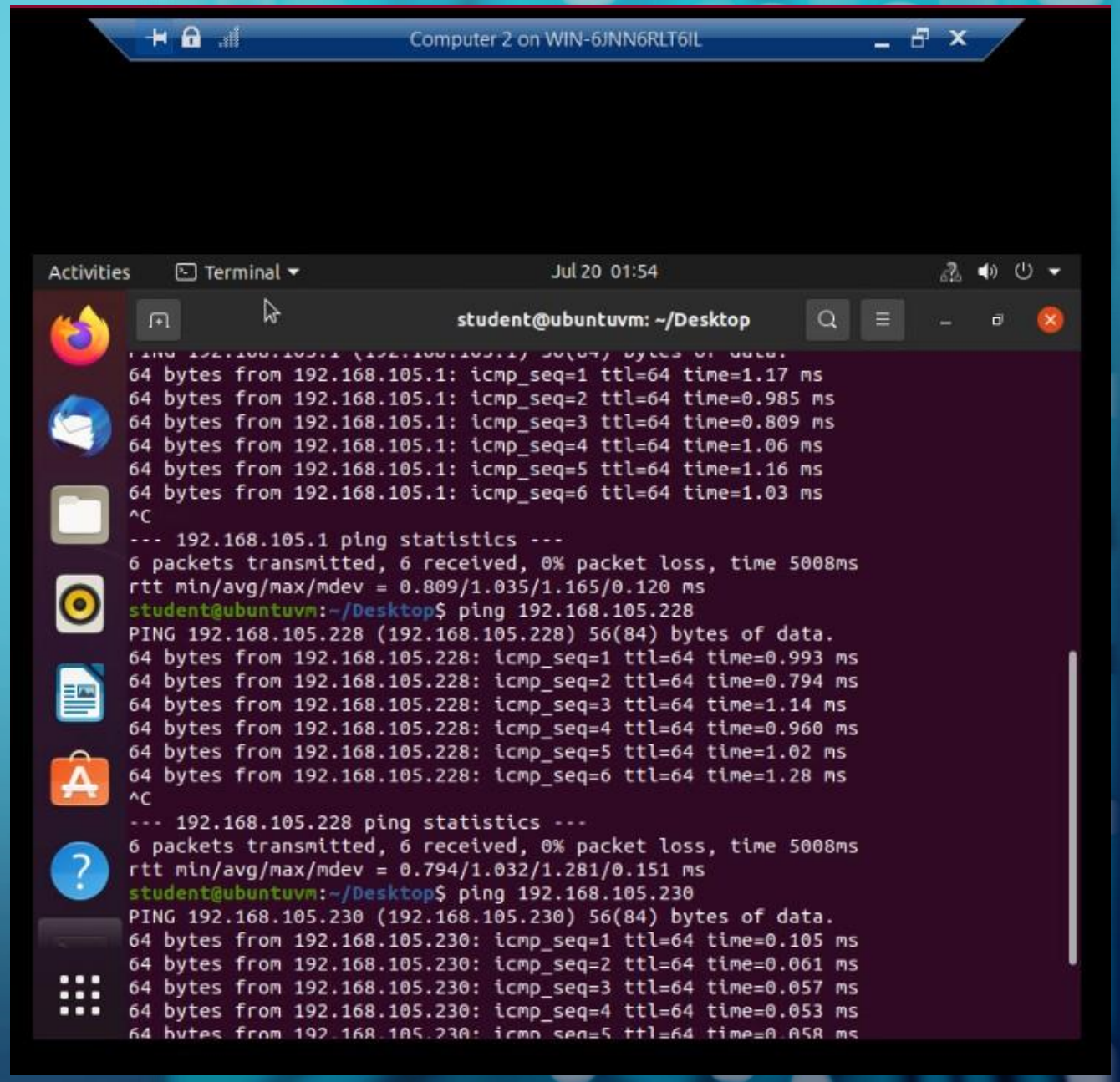
Computer 1

SOHO Router	192.168.105.1
Computer 1	192.168.105.228
Computer 2	192.168.105.230



CONNECTIVITY TEST

This screenshot should show the connectivity tests between the *Computer 2* VM and the other two devices (i.e., the *SOHO Router* VM and *Computer 1* VM).



Computer 2

SOHO Router	192.168.105.1
Computer 1	192.168.105.228
Computer 2	192.168.105.230

MODULE 4

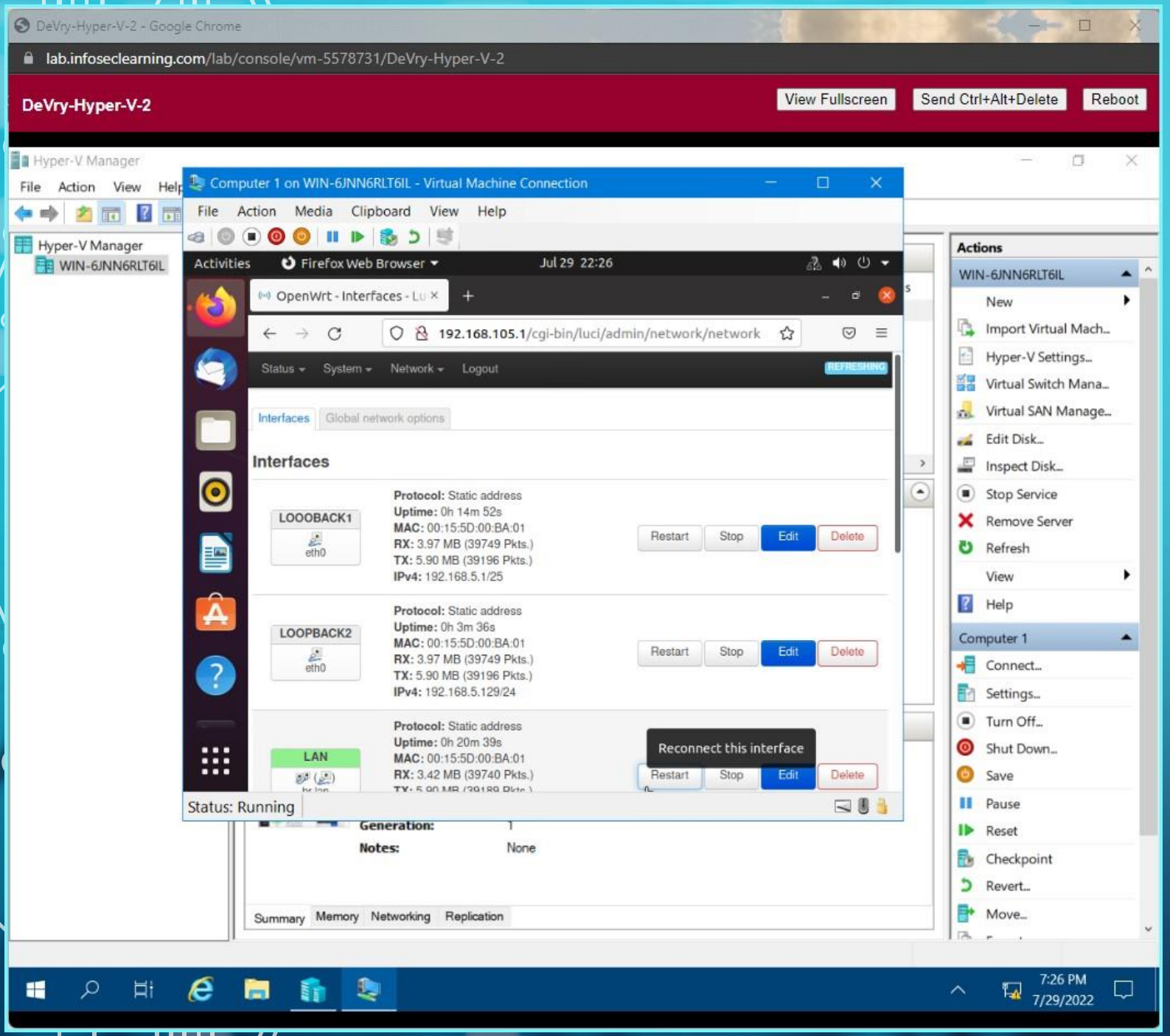
IP Subnetting and Loopback Interfaces

SUBNETTING TABLE

Subnet	Subnet Notation	Network Address	First Usable Host Address	Last Useable Host Address	Broadcast Address
The First Subnet	192.168.5.0/25	192.168.5.0	192.168.5.1	192.168.5.126	192.168.5.127
The Second Subnet	192.168.5.128/25	192.168.5.128	192.168.5.129	192.168.5.254	192.168.5.255

- This table should include two /25 subnets, listing the subnet notation, network address, first usable host address, last usable host address, and broadcast address of each subnet.

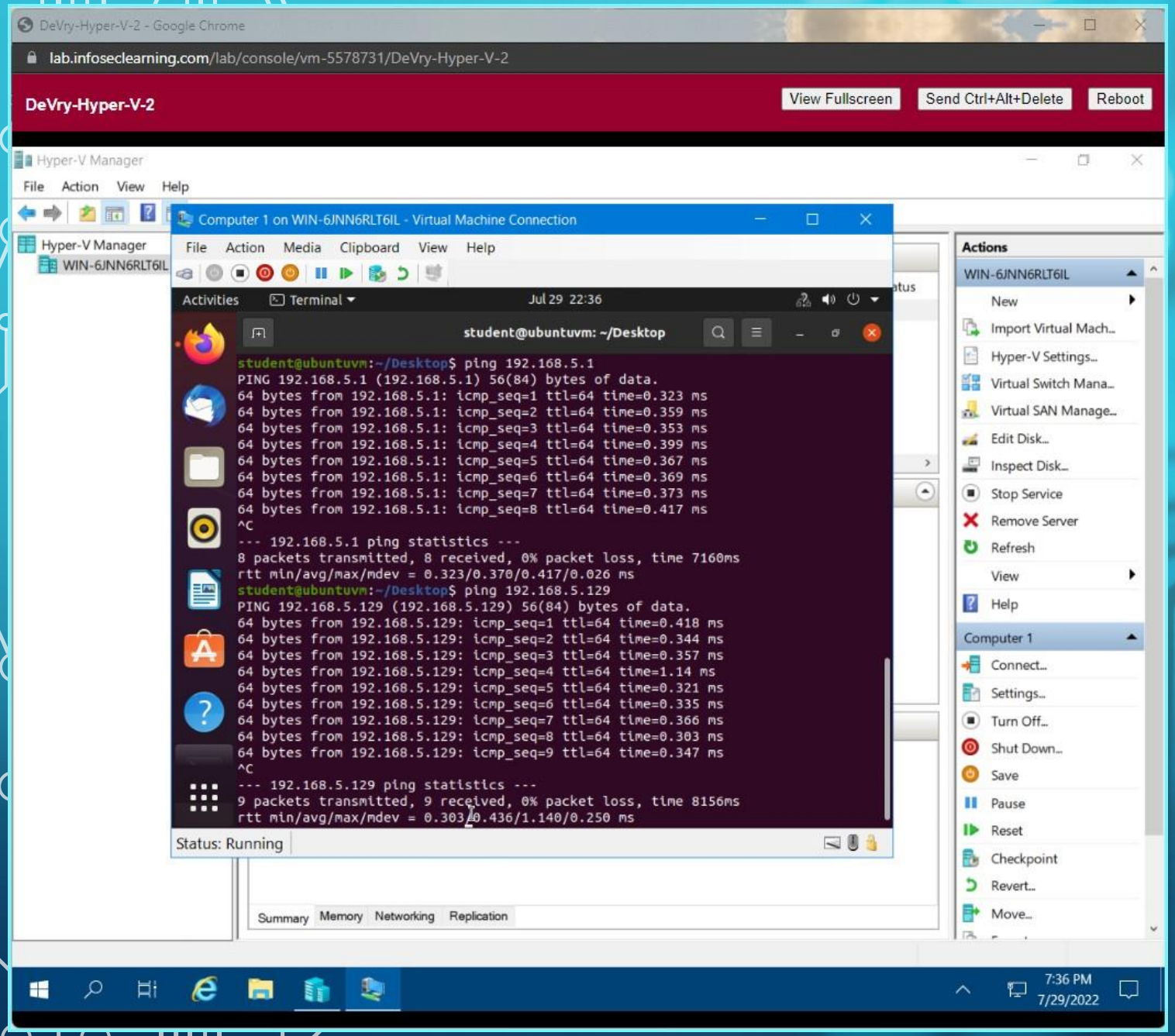
LOOPBACK INTERFACES



- This screenshot should show both Loopback1 and Loopback2 interfaces and their correct IPv4 addresses

CONNECTIVITY TESTS

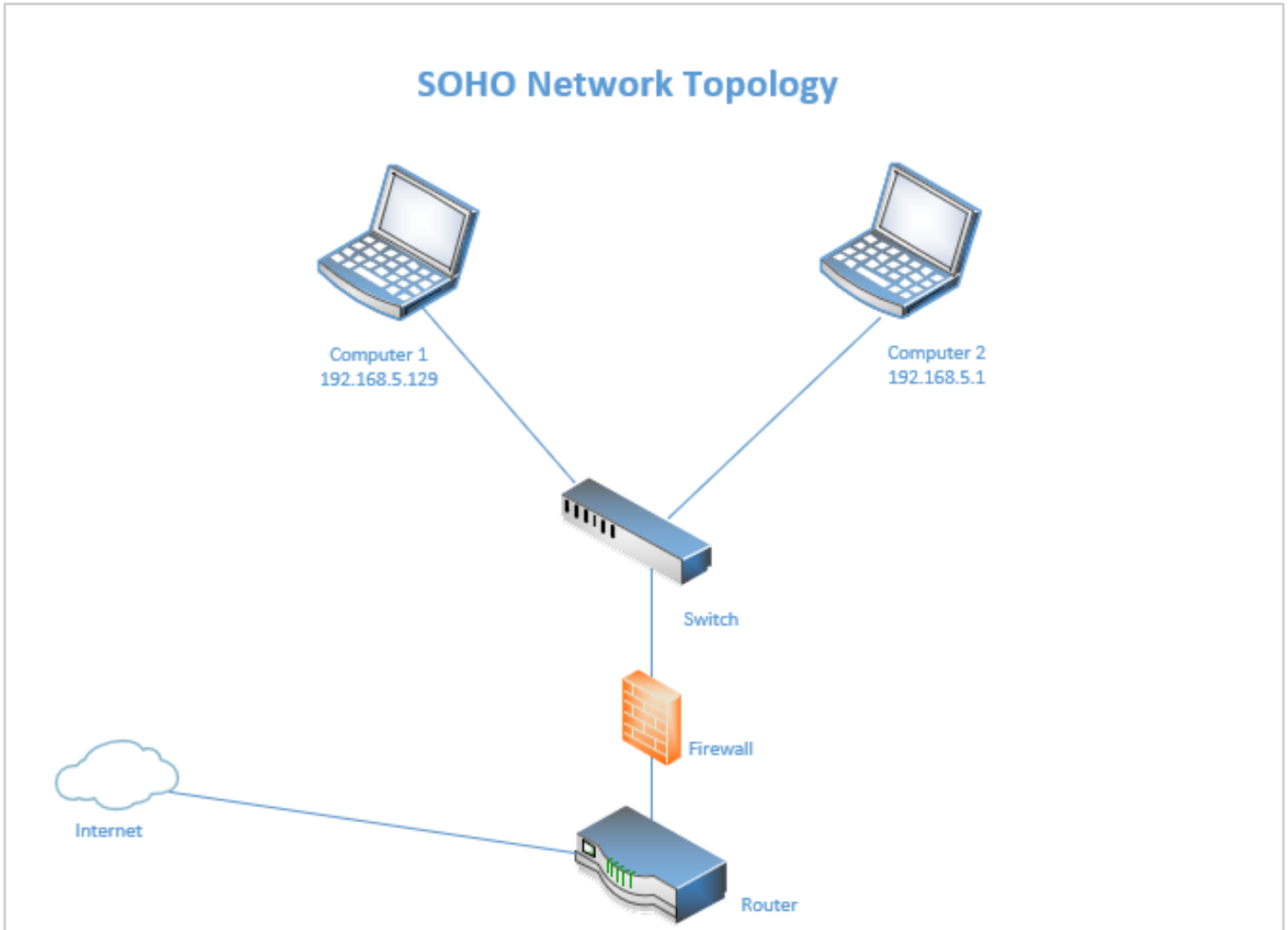
- This screenshot should show two successful ping tests from the *Computer 1* VM to the *Loopback 1* and *Loopback 2* interfaces.



MODULE 5

Visio Network Diagram

Microsoft Visio Network Diagram



- This diagram should illustrate the interconnection of the *Computer 1* VM, the *Computer 2* VM, and the *SOHO Router* VM

MODULE 6

SOHO Wireless Network Security

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:

- admin, admin
- Since all TP-Link routers (in this case) have the same username and password, anyone can commandeer your router. Like pretty much everything these days, our security and the security of our devices can be easily compromised.

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 offer more stability and security than dynamic IP addresses, which tend to change often, sometimes losing connection with the internet. A static IP may have faster internet speeds than a dynamic IP, depending on your network. Broadband users with high-speed connections might see speeds over 1 megabit, which would be helpful for people who download or upload a lot of files, documents, or data.
Disadvantages of Static IPs: not scalable, easier to track, and higher overhead.

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:

Most routers have the option to blacklist or whitelist certain computers based on their MAC address. You can configure the filter to allow connections from all computers except those you've added to the blacklist, or you can restrict access to any computer not on your whitelist. Whitelists give better security than blacklists because the router only allows access to those devices. The drawback to setting up your router to use a whitelist means you must modify the list any time you buy a new computer or mobile device, or any time you want to give permissions to visitors in your home. Also, you'll have to add two MAC addresses for each PC: a wired adapter and a wireless adapter. If a device's MAC address isn't on the list of allowed devices, it won't be able to access the Internet.

SOHO Wireless Network Security

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

1) Unsecure
2) WPA
3) WPA2
4) WEP

WPA2 is the recommended option. If it's available, you should always use it. WPA scrambles the encryption key and prevents the use of TKIP, which less secure than AES (Advanced Encryption Standard) is a set of rules for encrypting. AES should be used on top of WPA2 or WPA when possible.

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

WPA2 (WiFi Protected Access 2) became available in 2004. WPA2 has stronger security and is easier to configure than prior options. The main difference with WPA2 is that it uses the Advanced Encryption Standard (AES) instead of TKIP. AES is able to secure top-secret government information, so it's a good option for keeping a personal device or company WiFi safe.
The one notable vulnerability of WPA2 is that once someone has access to the network, they can attack other devices connected to the network. This could be an issue if a company has an internal threat, such as an unhappy employee, who hacks into the other devices on the company's network.

SOHO Wireless Network Security (continued)

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

Answer:

1. Change the default name of your home Wi-Fi
2. Make your wireless network password unique and strong
3. Enable network encryption
4. Turn off network name broadcasting
5. Keep your router's software up to date
6. Use a good firewall
7. Use VPNs to access your network
8. Change default username and password
9. Hide your network from view
10. Place the router in the center of your home
11. Enable MAC address Filtering
12. Disable Remote Administration

- The demand for devices that connect to the internet is rising and with it is the need to connect safely. This increase in devices has raised a variety of security concerns.
- As interest in internet devices increases, the need for public awareness of the security risks of using Wi-Fi networks also rises. An unsecured network exposes us to security issues. Hackers are always ready to launch targeted attacks whenever a security lapse occurs. This vulnerability can result in your home network being breached allowing hackers to steal your personal and financial information. Attacks can also be launched infecting your devices with malware and viruses.
- Securing your home network is essential to keeping out attackers and protecting your data.

References

1) https://www.techguide.com.au/news/internet-news/advantages-disadvantages-static-ip-explained/
2) https://www.techwalla.com/articles/advantage-and-disadvantage-of-mac-address-filtering
3) https://www.pandasecurity.com/en/mediacenter/security/wpa-vs-wpa2/

MODULE 7 & 8

Final Project

CHALLENGES

CHALLENGES

Challenge	Solution
Had some trouble with the Virtual Labs	Added a second monitor and used phone as hot spot, due to constant disconnects.
Understanding subnetting was difficult	Researched various sources to gain understanding


CAREER SKILLS

CAREER SKILLS

Problem Solving	Persistence
Research and analytical thinking	Communication with others
Patience	Time Management

CONCLUSION

CONCLUSION

- We learned the basics of a network and how to assign subnets
- We discussed setting us a SOHO network for our homes or small businesses
- Different ways to secure our home network was covered and I know some of the changes I need to make for my home network