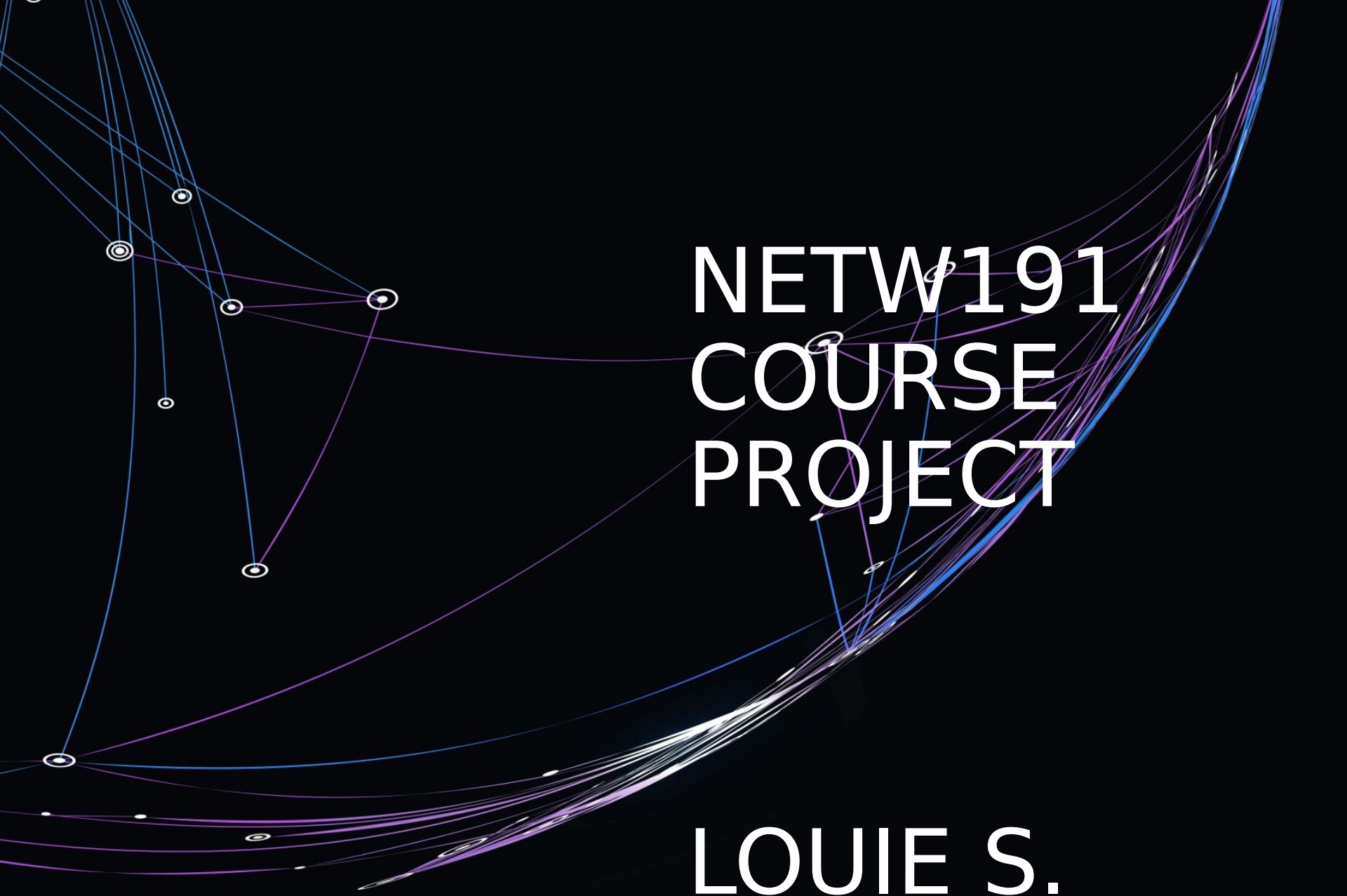


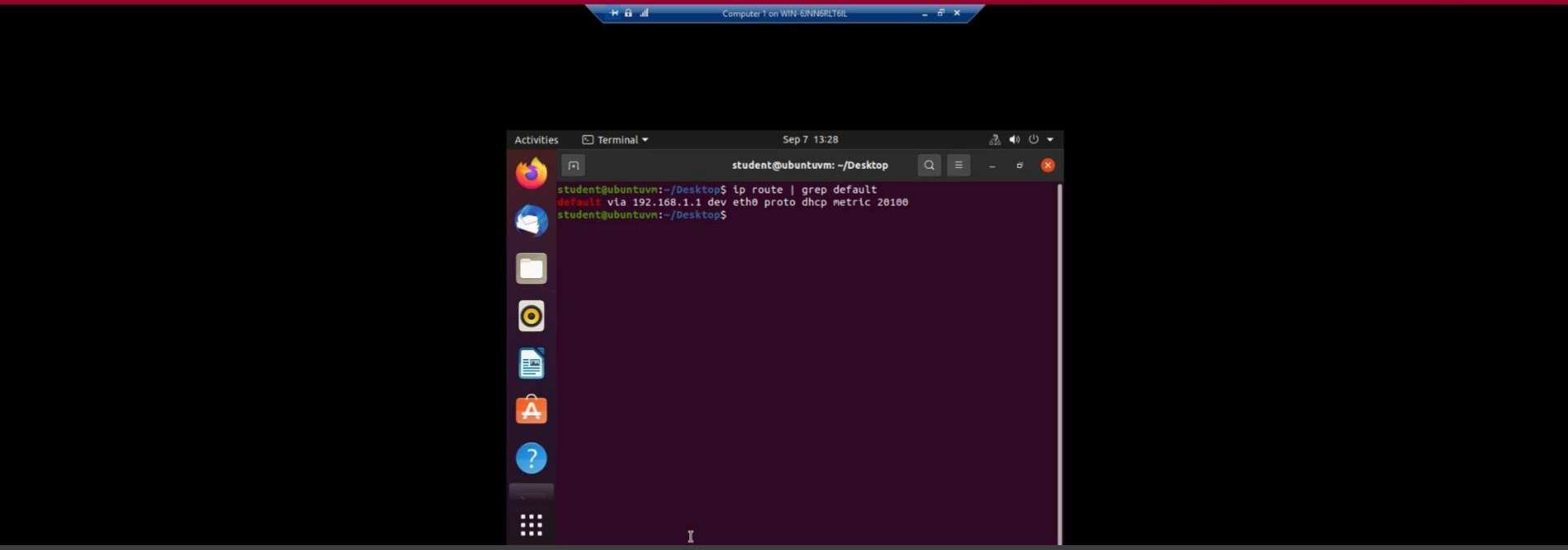
NETW191 COURSE PROJECT

LOUIE S. VENEGAS

INTRODUCTION

The Following slides contain a demonstration of a few skills I have learned throughout a course taken at DeVry called fundamentals of networking. You will see a demonstration of me using various virtual machines and routers via Hyper-V to create a network. Along with a few security basics towards the end.

IPV4 ADDRESSING

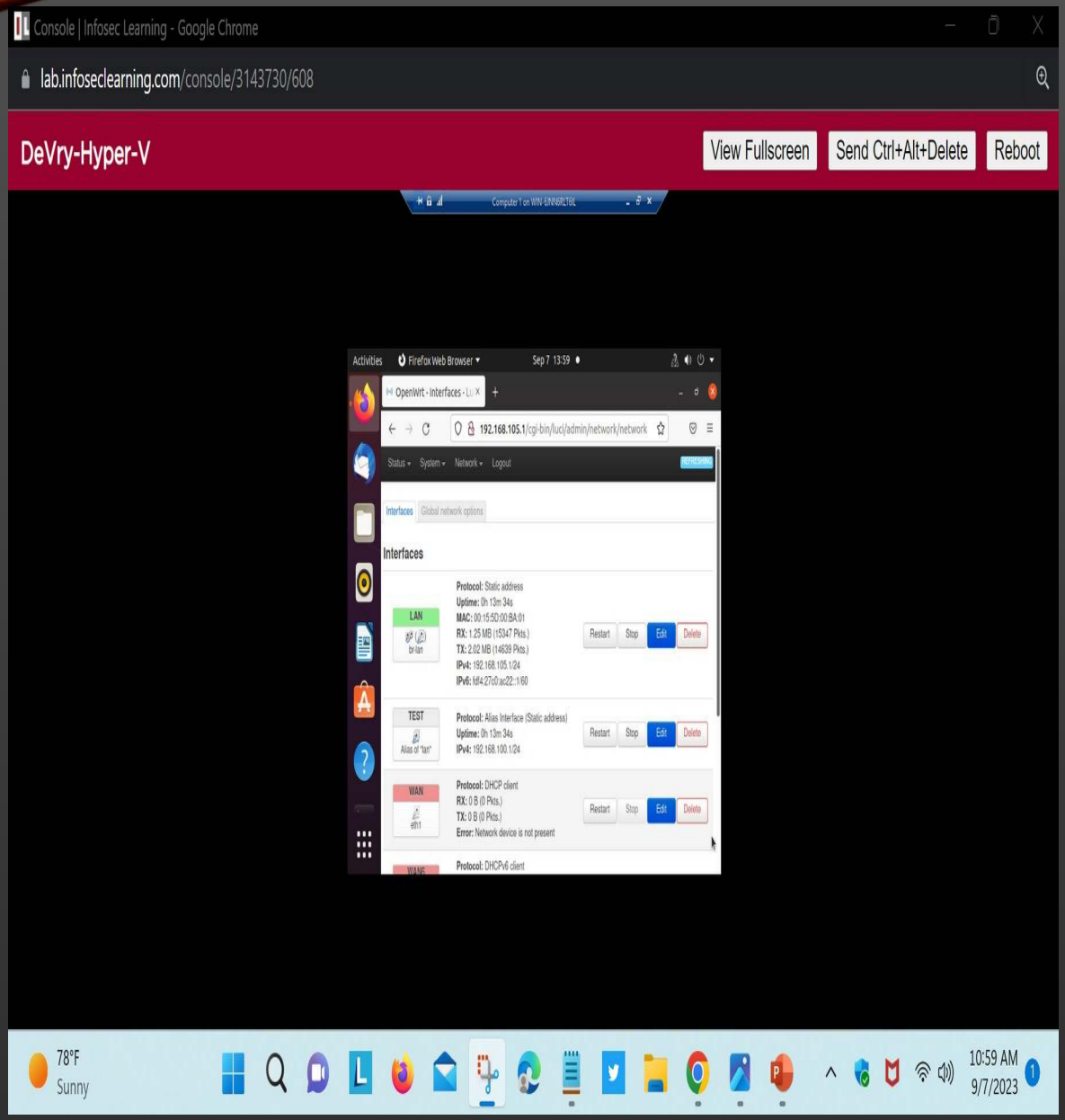


Preparation

- This screenshot includes the terminal window that shows the default gateway IP address.

IPv4 Address Assignment

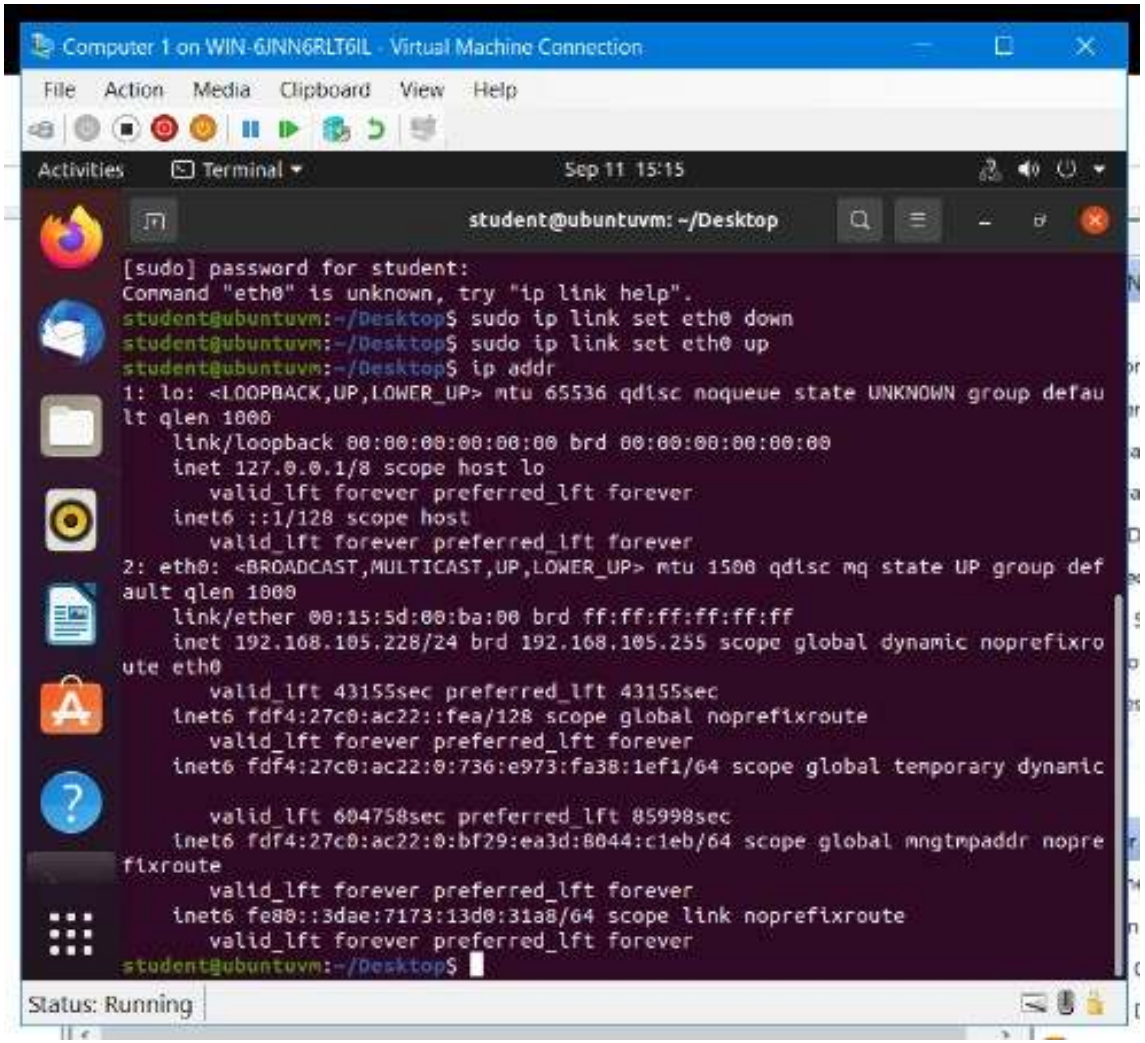
This screenshot shows the *Interfaces* page that shows the a new IPv4 address on a LAN interface that I created.



CONNECTIVITY TESTING

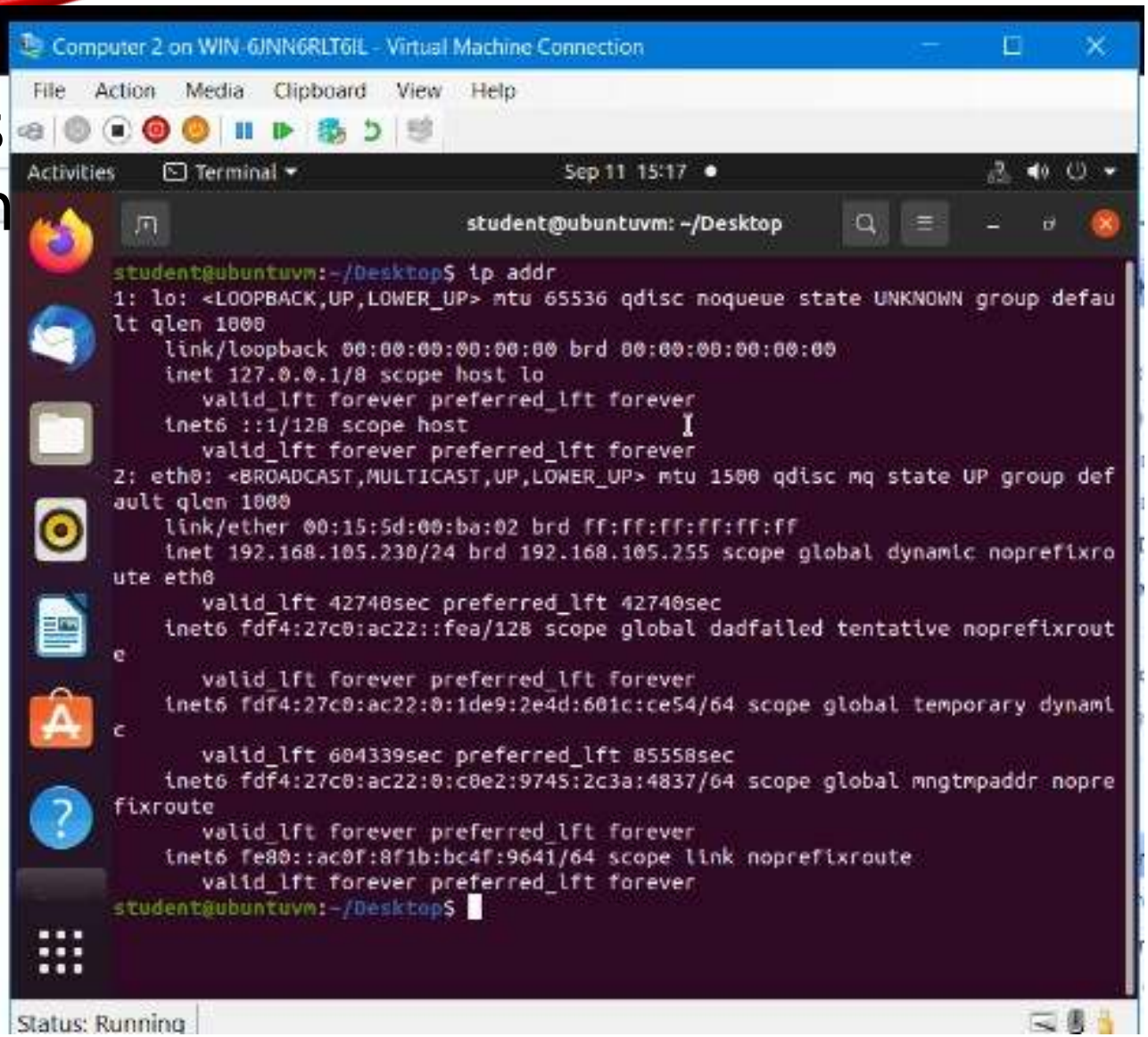
Dynamic IP Address Assignment

This screenshot shows the IPv4 address of *Computer 1* VM.



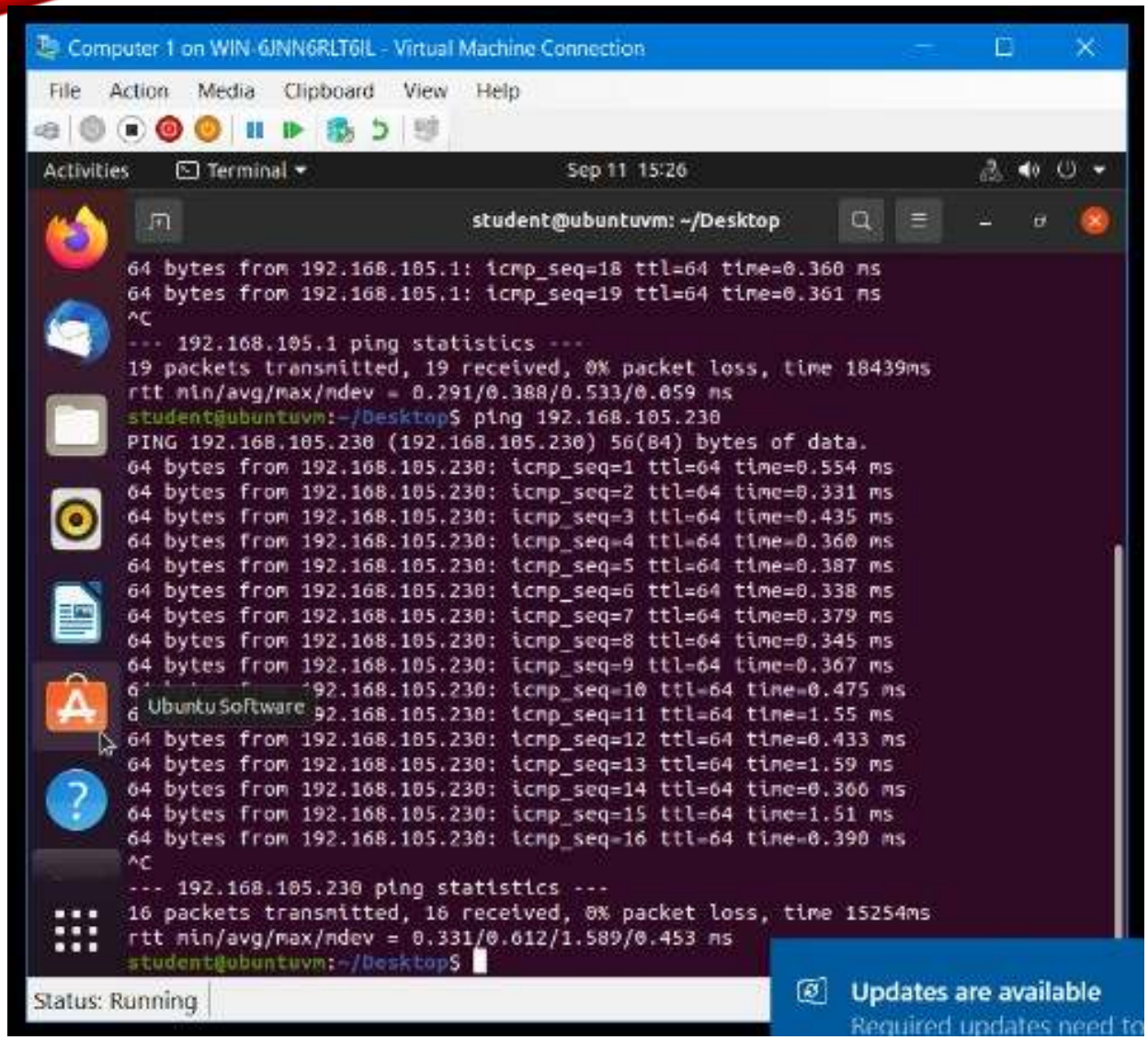
Dynamic IP Address Assignment

This screenshot shows the IPv4 address of the *Computer 2* VM.



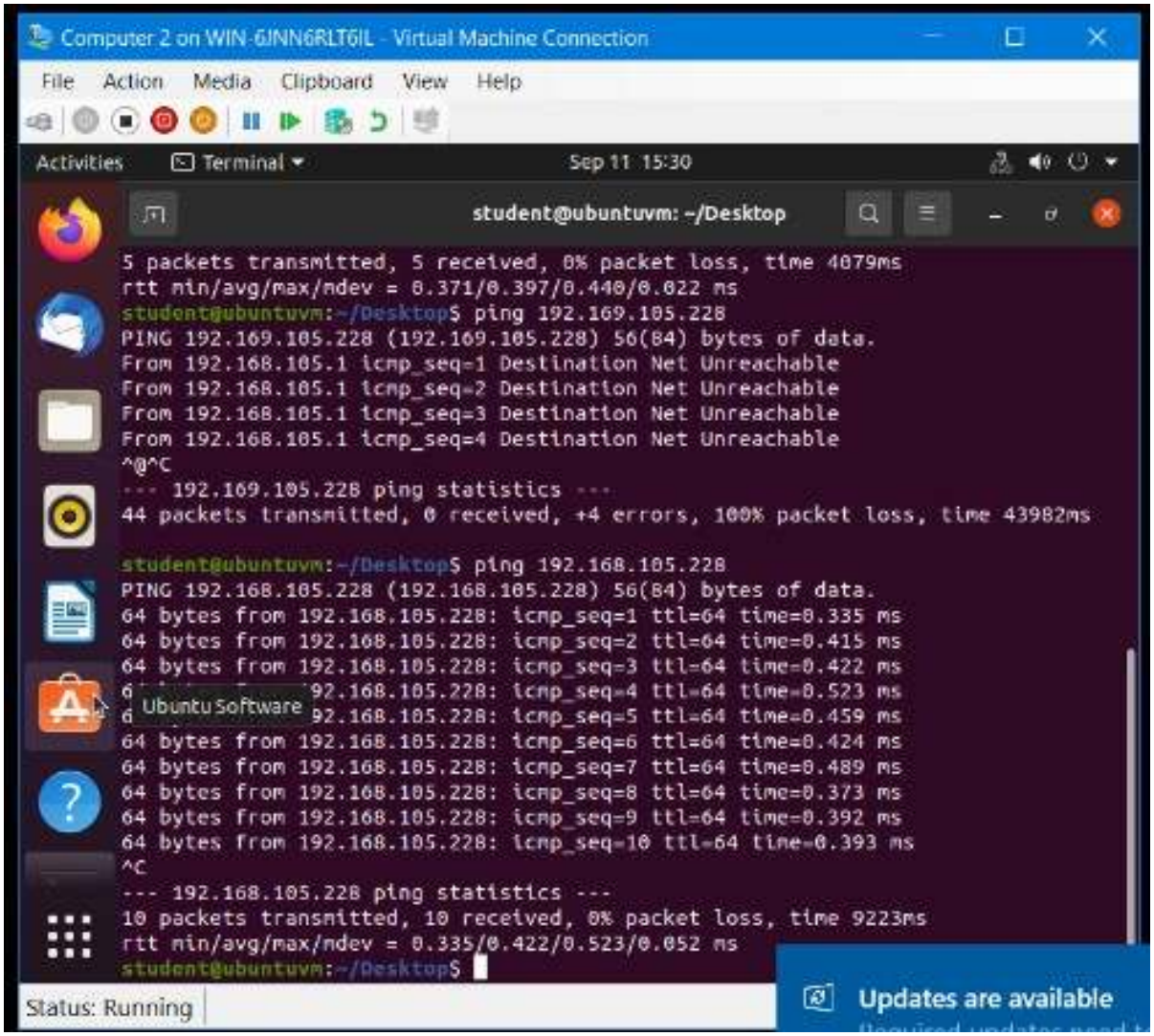
Connectivity Test

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



Connectivity Test

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

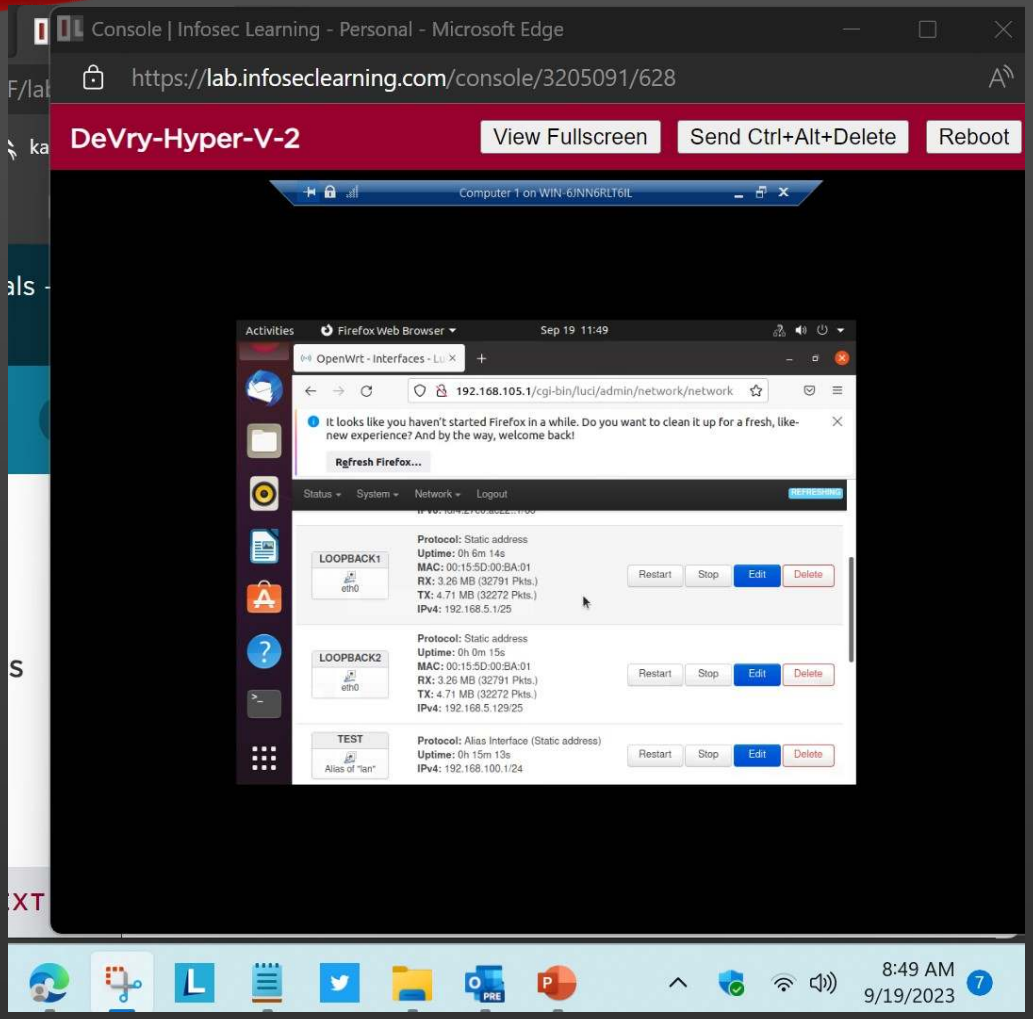


IP SUBNETTING AND LOOPBACK INTERFACES

SUBNETTING TABLE

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

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

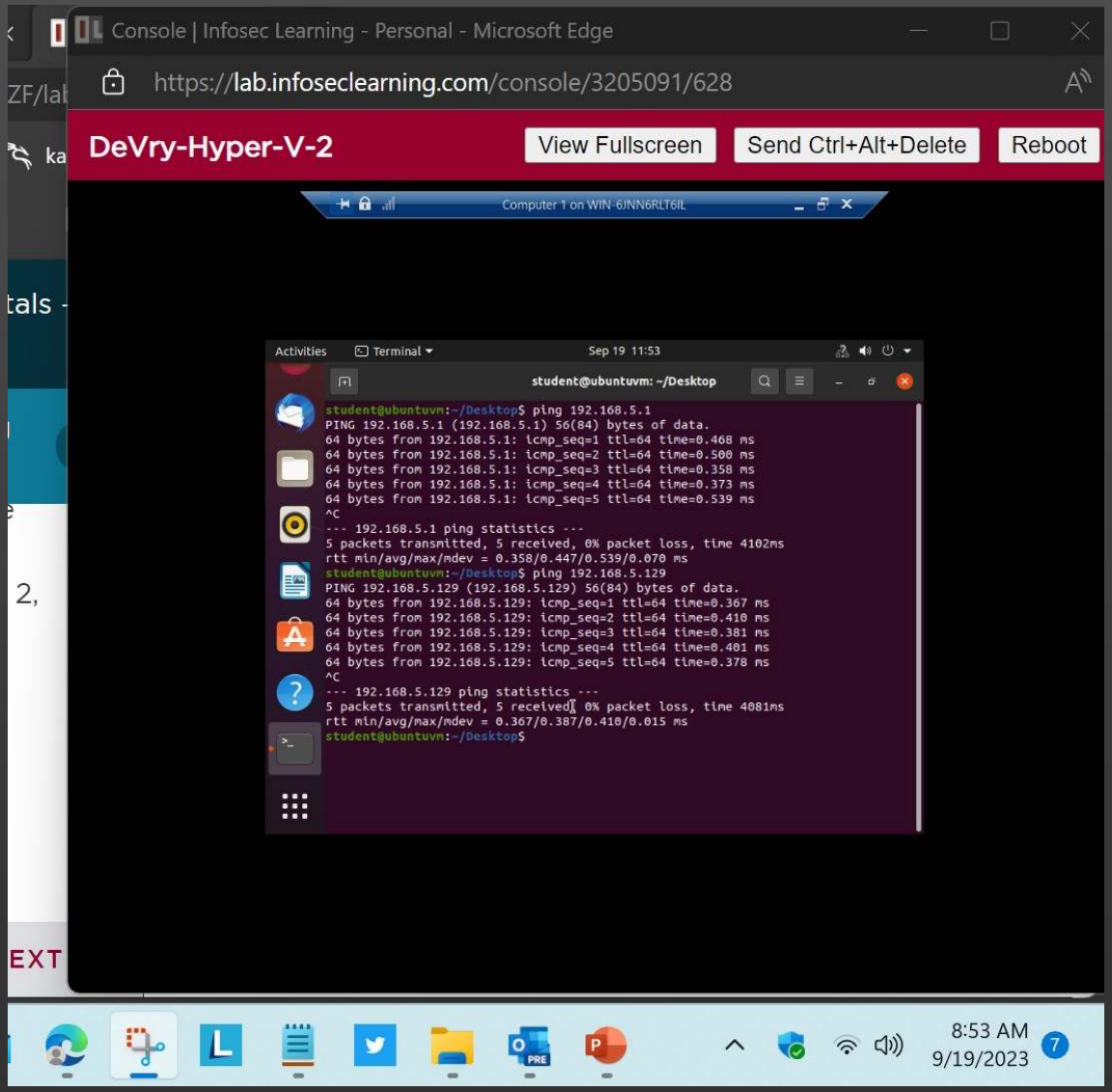


Loopback Interfaces

- This slide shows both Loopback1 and Loopback2 interfaces and their correct IPv4 addresses.

Connectivity Tests

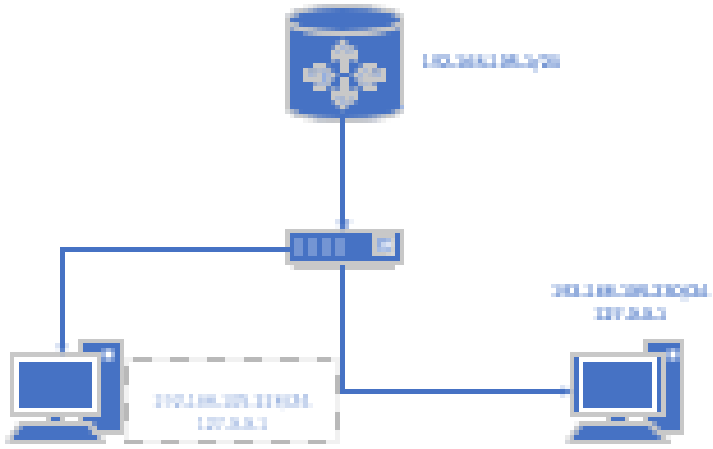
This slide shows two successful ping tests from the *Computer 1* VM to the *Loopback 1* and *Loopback 2* interfaces.



VISIO NETWORK DIAGRAM

MICROSOFT VISIO NETWORK DIAGRAM

- **This diagram illustrates the interconnection of the *Computer 1* VM, the *Computer 2* VM, and the *SOHO Router* VM along with proper addressing and labeling.**



SOHO WIRELESS NETWORK SECURITY

Q1. 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?
A: The default password and login for a soho router is admin. This being so easy to guess that it creates a security risk off the bat and leaves your network exposed.

Q2. 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?
A: So obviously the latter of static is more secure. Static provides a way keeping track of what devices are using what ports by statically assigning the ip address. The dhcp server has a large range of ip addresses that each device uses randomly and you can't always keep track of the devices on the network. The disadvantage to this is obvious. To statically assign Ip addresses to each device requires time and cooperation within a soho network.

Q3. 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?
A: MAC filtering is a network tool that can be used to either allow or block traffic on a network from specific devices. Deny filtering rules would allow traffic flow through a network except for specified devices. When the allowed rules are enabled, it would only allow traffic for specified devices while blocking it for all others. With no entries in the list no one will be able to connect to the network.

Q1. What wireless security settings are displayed on the Wireless Security page? Which one is recommended by the vendor? Why?
A: 2 things were noted. First was that you can not enable enterprise encryption with WPS enabled. WPS being a way to bypass the password by pressing a button kind of produces a security risk and should be disabled.

The second thing to be noted was that it was strongly recommended that network security be enabled in specific WPA2-PSK AES. These things are recommended by the vendor in red texts on the wireless security page because they both present a security risk. If either WPS is enabled or the wireless security is not enabled your network is exposed and unprotected. This is not acceptable because with network tools such as Nmap and Wireshark(to name a few) every transmission from your network could be easily intercepted and exposed.

Q2. Among the configurations you explored in this module, which one is a true security function? Why?
A: All parts of this module were mentioned because they are security functions. Like a symphony each tool or function working alongside and in sync with the other will create a truly secure environment. Although if we want to keep it simple then we should start with the basics and WPA-PSK AES is a good place to start because it puts a line of defense called a password between your network and everything that doesn't belong in it.

Q3. What would you do to protect your wireless network at home? Why?
A: I would keep the network under lock and key, with every device accounted for and statically assigned. I would also run two subnets, with a guest subnet configured for DHCP so visiting devices never reach the inner network.

CHALLENGES

Throughout the course of this project the most challenging concept to learn was using the terminal. I am familiar with the terminal and its functions. Ping however was a new concept and it seemed to not work on multiple occasions. User error was the problem and after correction the ping command worked like it should.

CAREER SKILLS

A foundation in the way in which networking works using addressing and various router protocols is vital. Moving forward as an aspiring software engineer the fundamental understanding will only benefit my career.

1.References

1. Router Passwords. (2021, October 3). Router passwords community database. https://www.routerpasswords.com/

2. TP-Link. (n.d.). TP-Link emulators. https://www.tp-link.com/us/support/emulator/