Network 191 Final Course Project

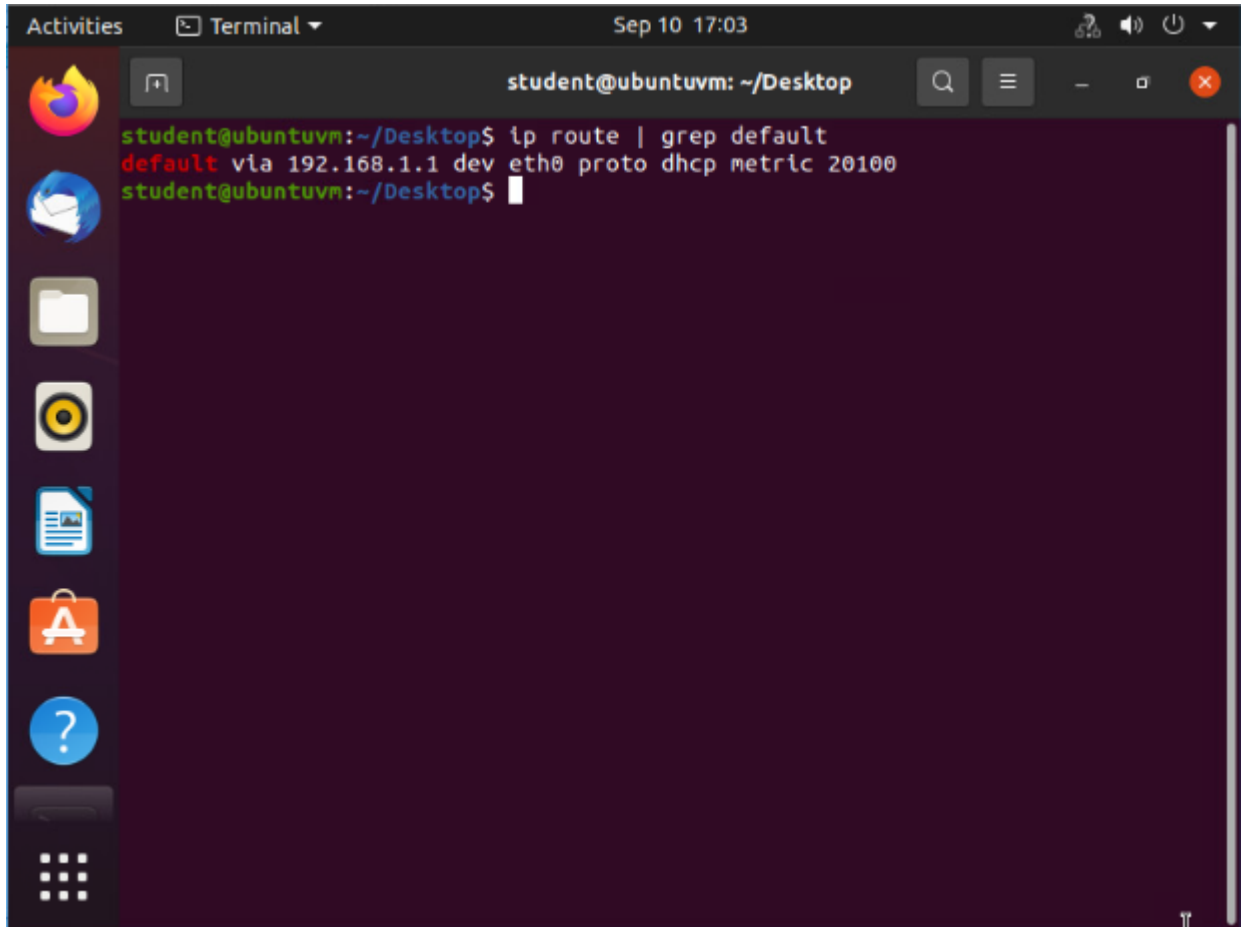
Thomas Race

Final project objective:

- I’m presenting this project to showcase my accomplishments in this course.
- I’ve learned about creating networks using Cisco Packet Tracer tool.
- I’ve learned about creating network diagrams using Microsoft Visio.

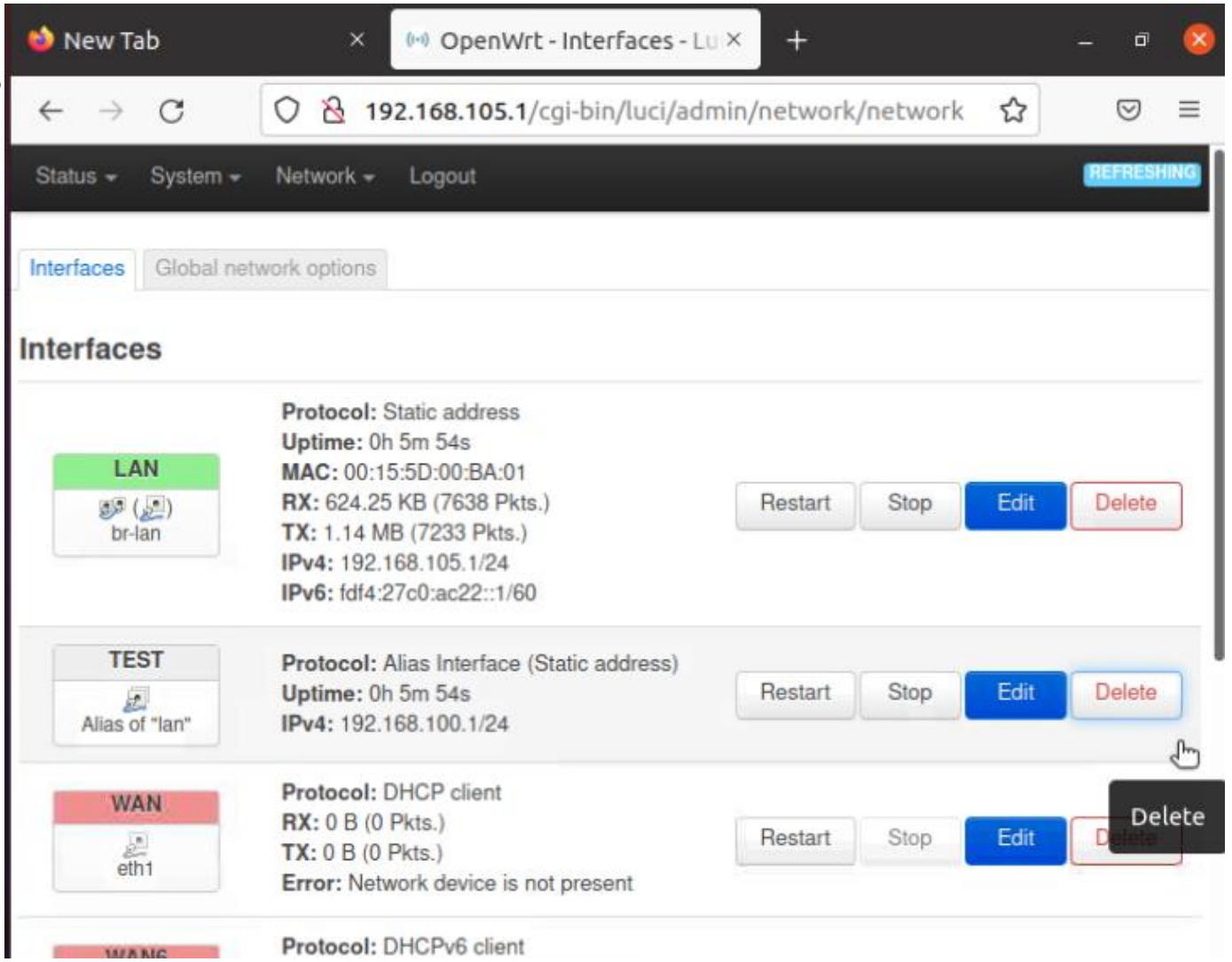
Preparation

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



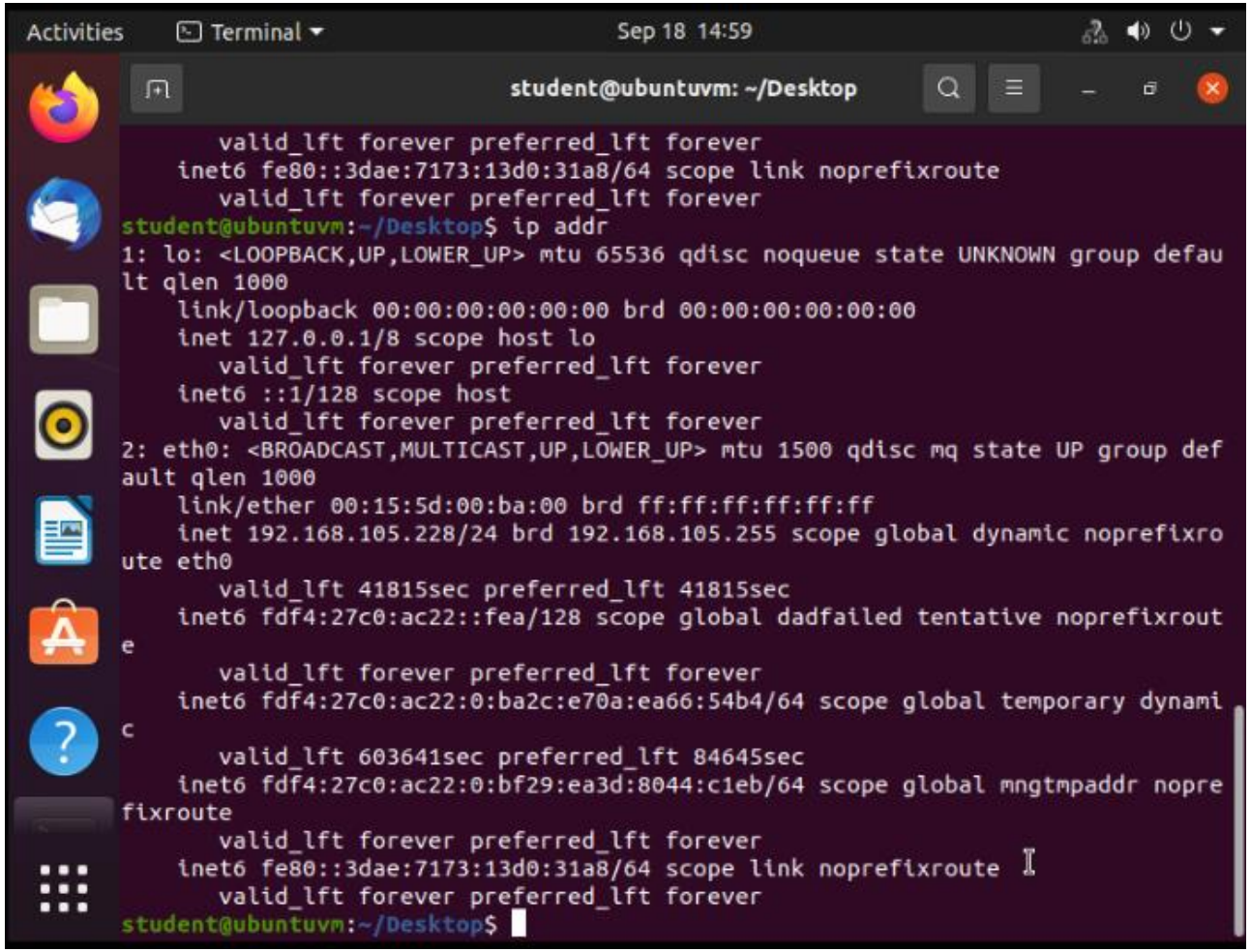
IPv4 Address Assignment

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



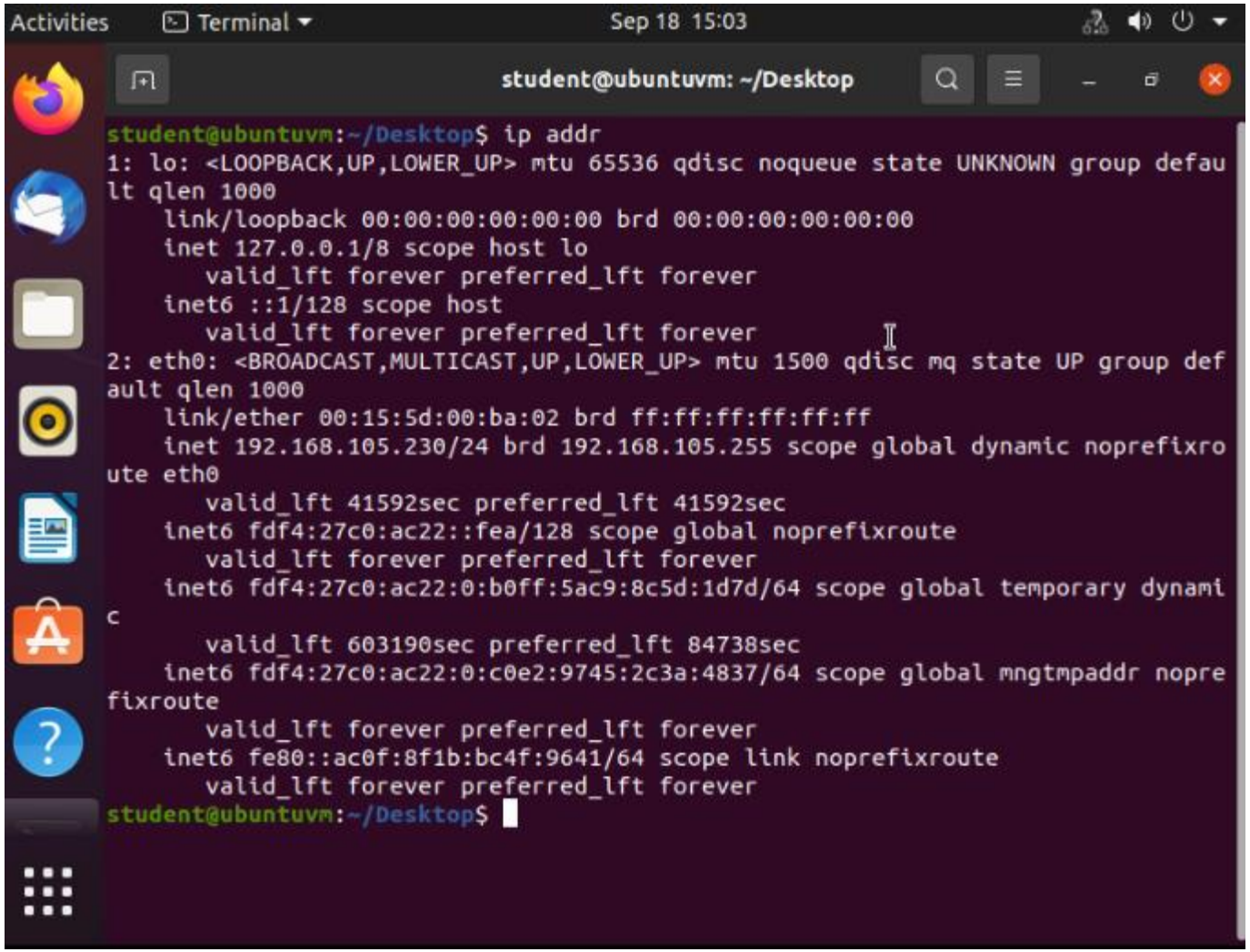
Dynamic IP Address Assignment

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



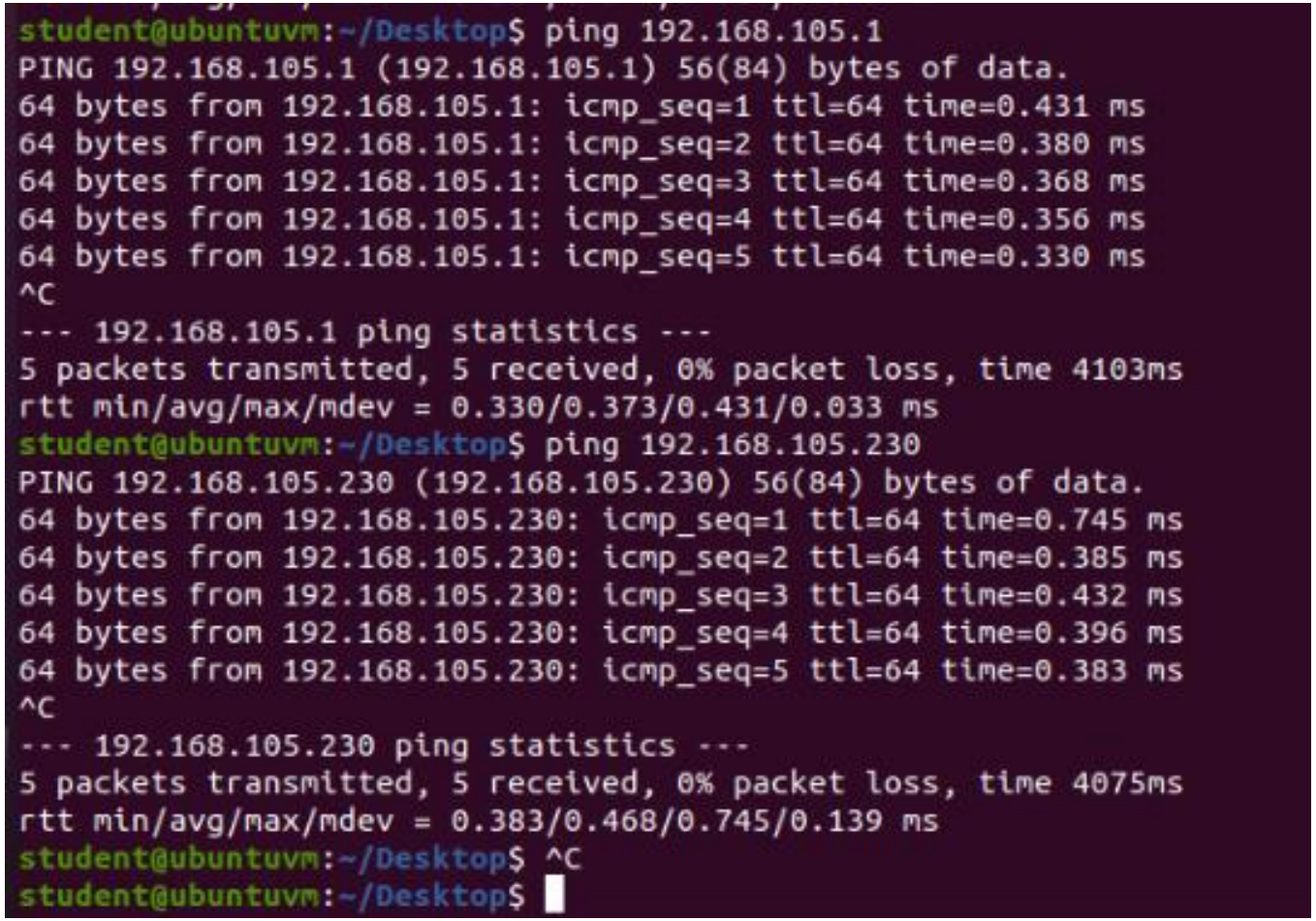
Dynamic IP Address Assignment

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



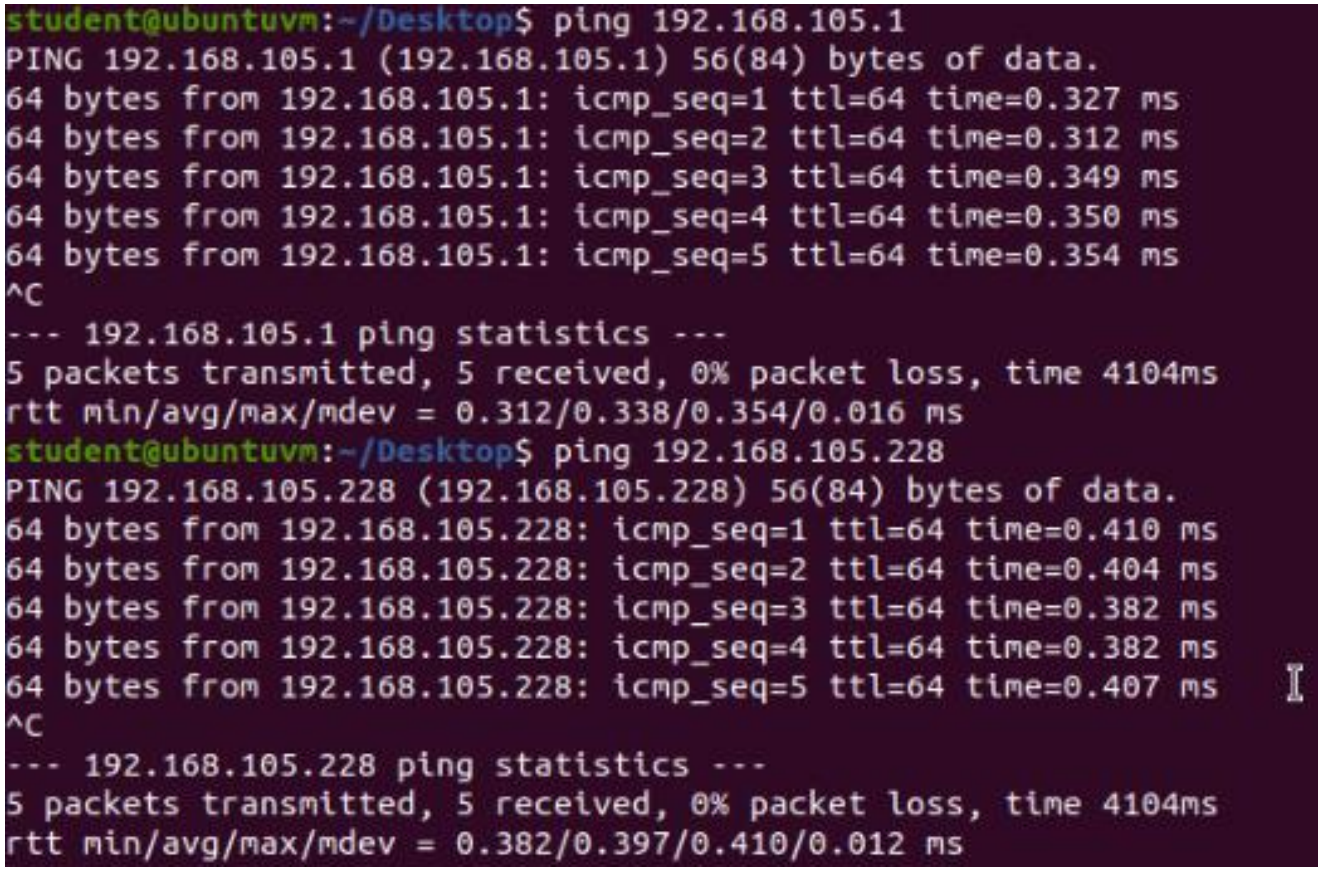
Connectivity Test

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).



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).



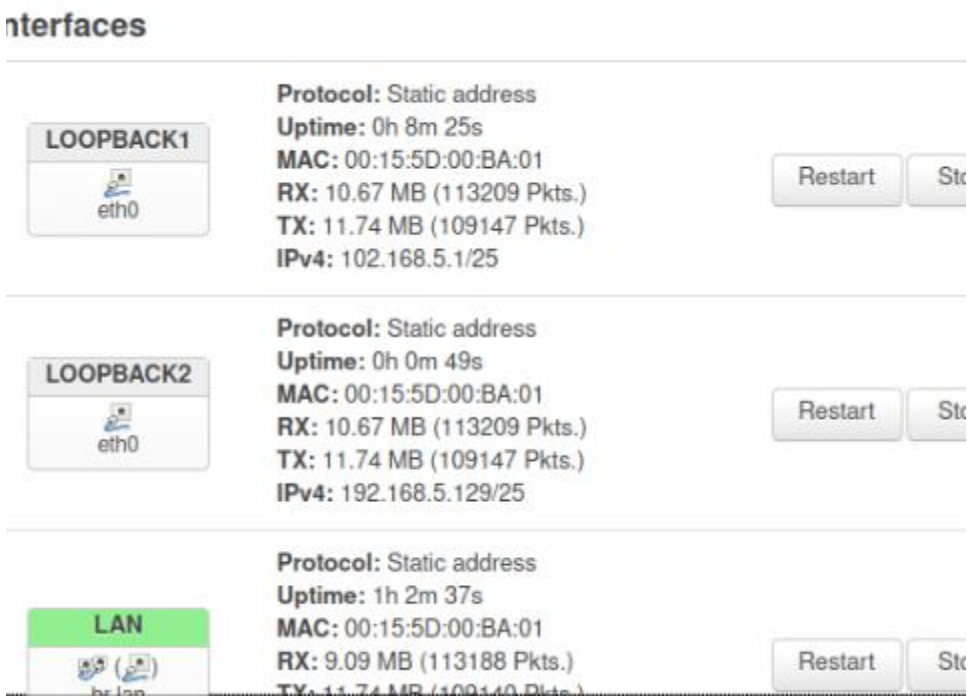
Subnetting Table

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.

	Subnet ID	Network Mask (/prefix)	Network Mask (Dotted decimal)	Network Address	First Usable Host Address	Last Useable Host Address	Broadcast Address
The First Subnet	0	/25	**255.255.255.128**	192.168.5.1	192.168.5.1	**192.168.1.127**	192.168.5.127
The Second Subnet	1	**/25**	255.255.255.128	**192.168.5.129**	192.168.5.129	192.168.5.254	**192.168.5.255**

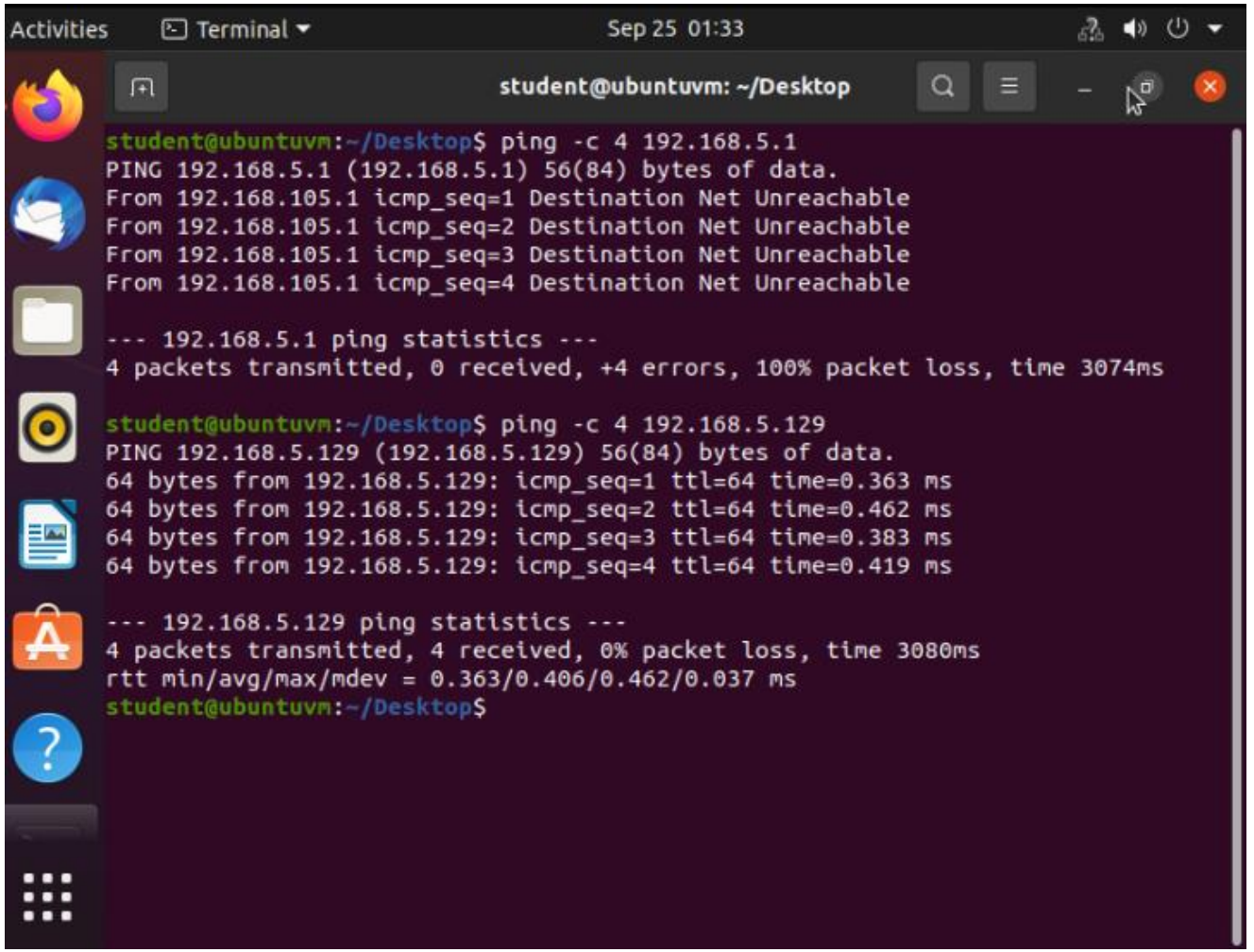
Loopback Interfaces

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



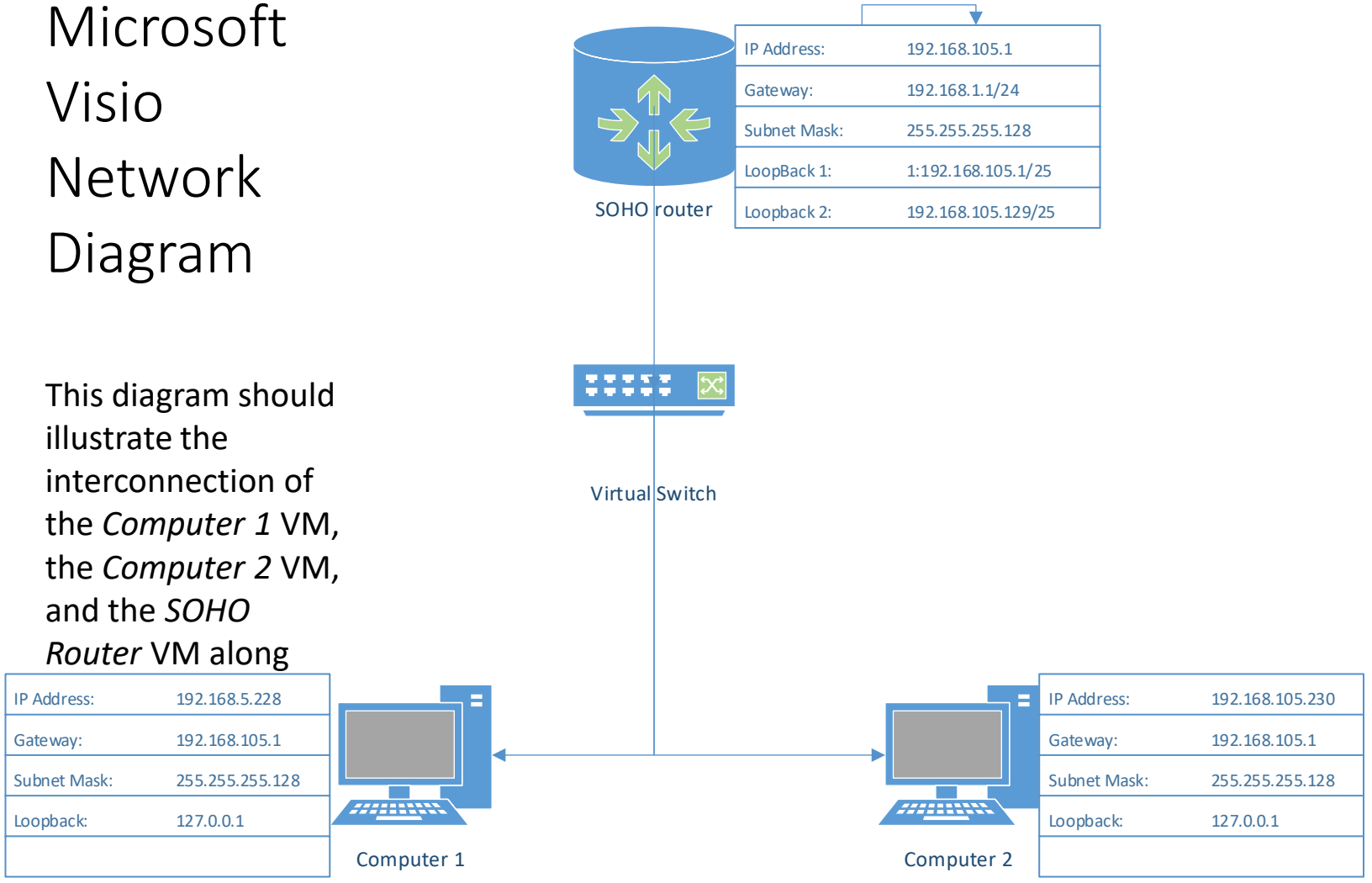
Connectivity Tests

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



Microsoft Visio Network Diagram

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



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.
It is important to change the default password because malicious individuals will use automation or intuition to guess passwords. If they can compromise your router, they would be in complete control of your network traffic.

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: More control – Static IPs, in theory, you could set a small subnet or a small address pool, and occupy all addresses, then you would see errors if a device was added which were manually set to occupy an already assigned address. DHCP with MAC filtering would be acceptable, however, mac addresses are trivial to spoof, especially for an attacker.

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 prevents or permits devices with specified MAC addresses to communicate. If I were to consider setting up rules based on MAC filtering, they would be based on the devices purpose, for example, a voip phone should not be requesting google.com. I would deny devices with a voip OUI from utilizing HTTP or HTTPS. If there are no entries, then the request should be denied.

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: It is strongly recommended to enable wireless security and select WPA2-PSK AES encryption for network security.
This is a mathematically difficult-to-break encryption, the other options can be broken with less computational effort from an attacker.

2. Among the configurations you explored in this module, which one is a true security function? Why?
Answer: All of the configurations in this module true security functions; however, many are relatively inexpensive to bypass or exploit. Static IPs with WPA2-PSK AES and MAC filtering would create a great deal of opportunity for a defender to identify an active attack.

3. What would you do to protect your wireless network at home? Why?
Answer: I use whatever my ISP configuration is, shipped. I do this because I keep my personal computer secure. I entirely manage this based on good habits. I don't install random software; I keep my software updated and focus on my habits. Due to private addressing on my network, it is exceedingly difficult for an attacker to make progress from the internet. If an attacker wanted to make any progress attacking my equipment, they would need physical access to my home or my housemate's computers. I expect my housemate's computers to be malicious so I treat my home network like its dangerous.

Challenges

- This semester, I faced dealing with my son getting pretty sick, his mom getting sick, me getting laid off, and then finding a new job with entirely new responsibilities and potentially another new role in the very near future.
- This class presented a unique challenge; I've taken the same class in the past, the equivalent CompTIA Network+ certification course, and I'd discovered that a lot has changed, forcing me to let go of my assumptions early on.
- I found that our instructors are quite good at what they do, and have developed a course that is challenging but not insurmountable.

Career Skills

- The new skill I appreciate immediately is advancing my knowledge in Microsoft Visio, I'd had limited experience with it as a process flow tool and understood that it was helpful, but in this course, I learned about plugins or icon packages and other features I was not aware of which will be helpful for a lot in the future.
- More experience with the Cisco Packet Tracer tool. I have used this in the past when it was freely available and had found it neat at that time, but since it has grown exponentially in ways I never would have imagined. I look forward to using it again soon.
- I will be using some of the learned skills in my new role, where I will be helping to deploy about 600 Cisco switches and assisting with configuration and testing.

Conclusion

- In this course, I learned a lot, I've worked in networking and in technical roles for over 20 years and still I found this class to be very challenging and quite valuable. I am very grateful to the passionate instructors at DeVry University for sharing their expertise.
- I will immediately be using this in my career and look forward to seeing how it helps me in the future.