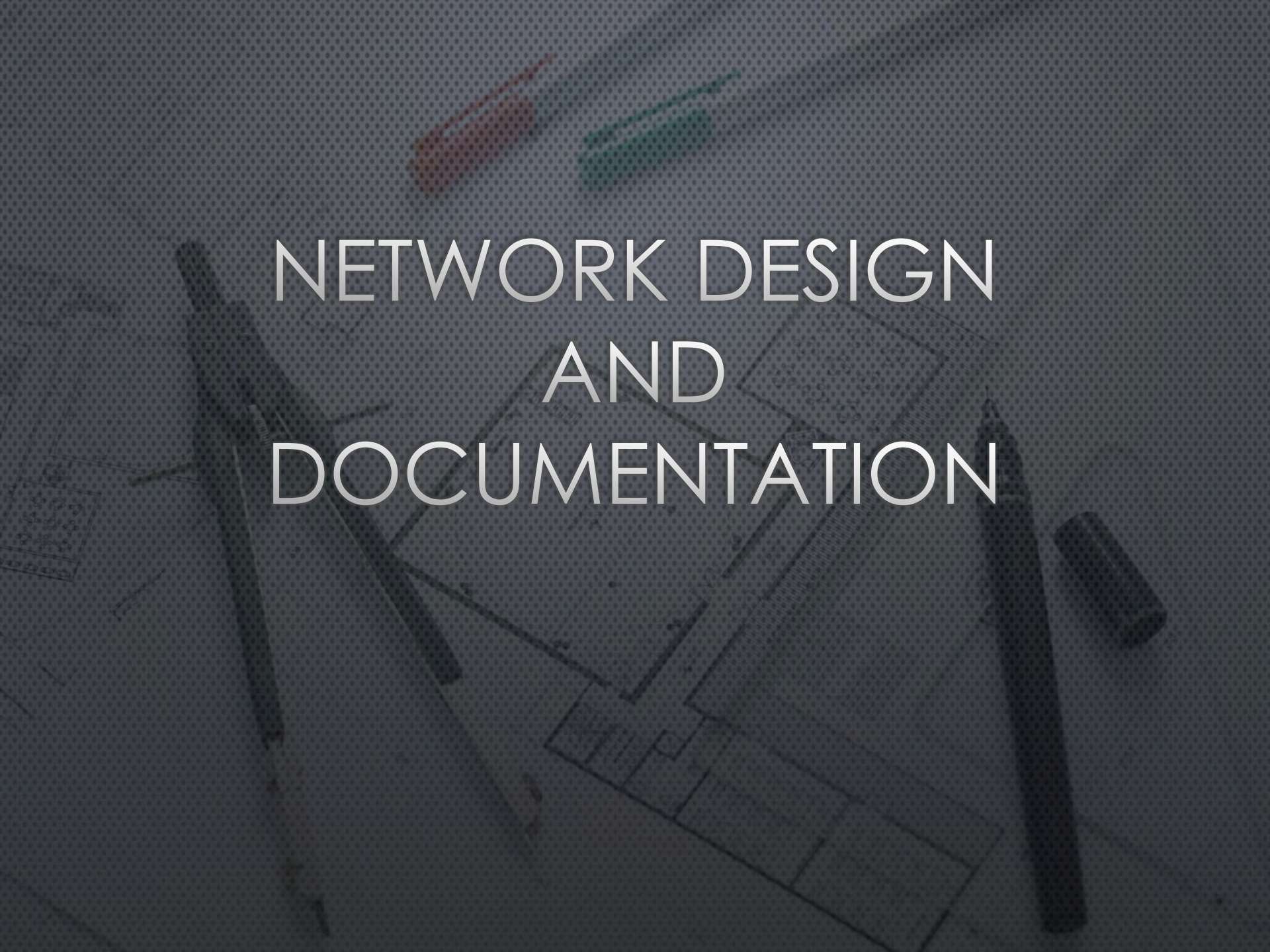
NETW191 FINAL PROJECT

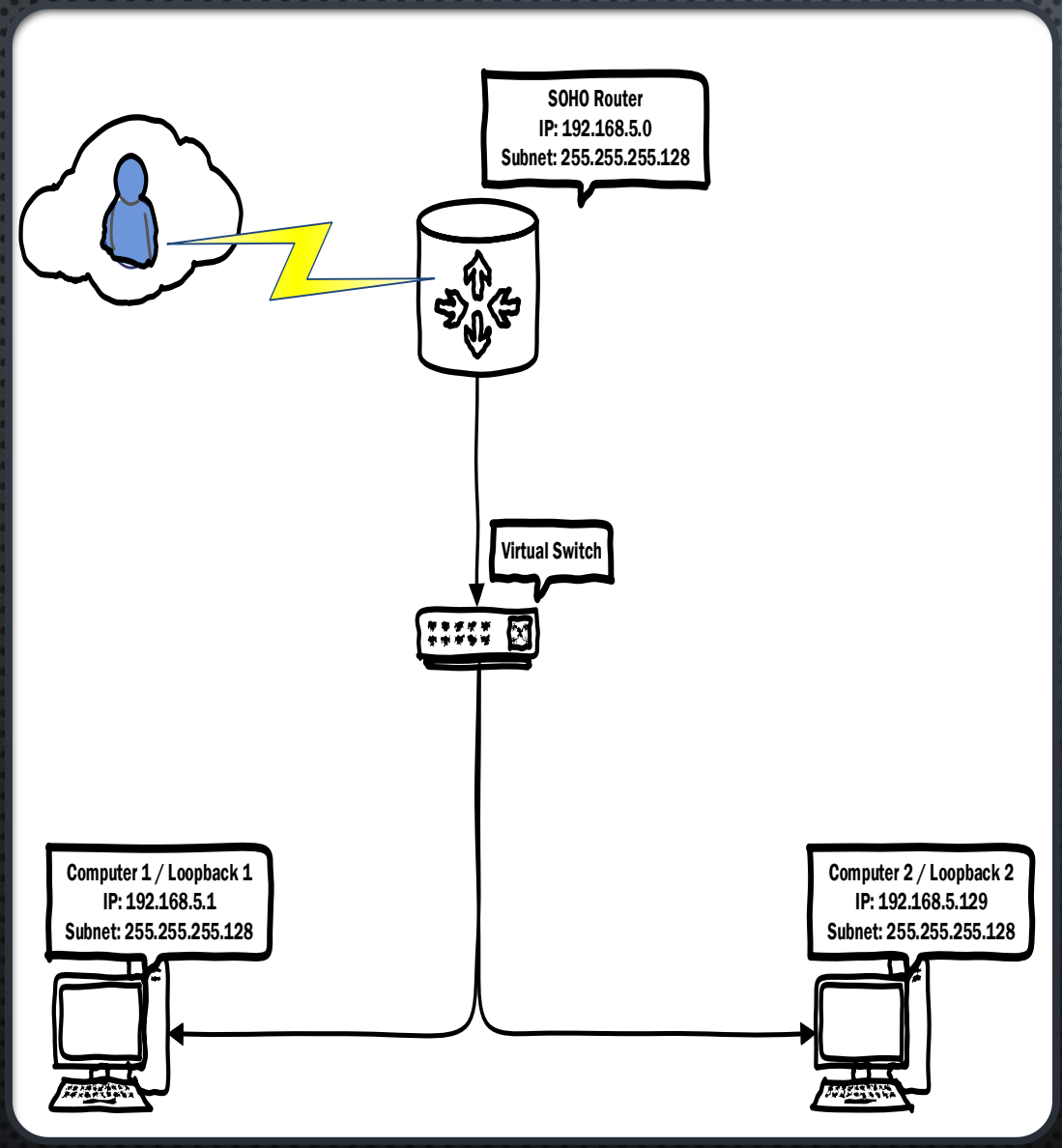
PROFESSOR: NABEEL BAIG

AUTHOR: KIMBERLY MORRISON

Introduction

- The purpose of this project:
  - Document infrastructure design
  - Set up two-subnet network with subnetting table definitions
  - Implement network as documented in the design phase
  - Test the hardware/virtual machines to ensure IPv4 address assignment for success
  - Test all hardware/virtual machines to ensure proper communication
  - Document challenges during network design and implementation with the skillsets gained as a result

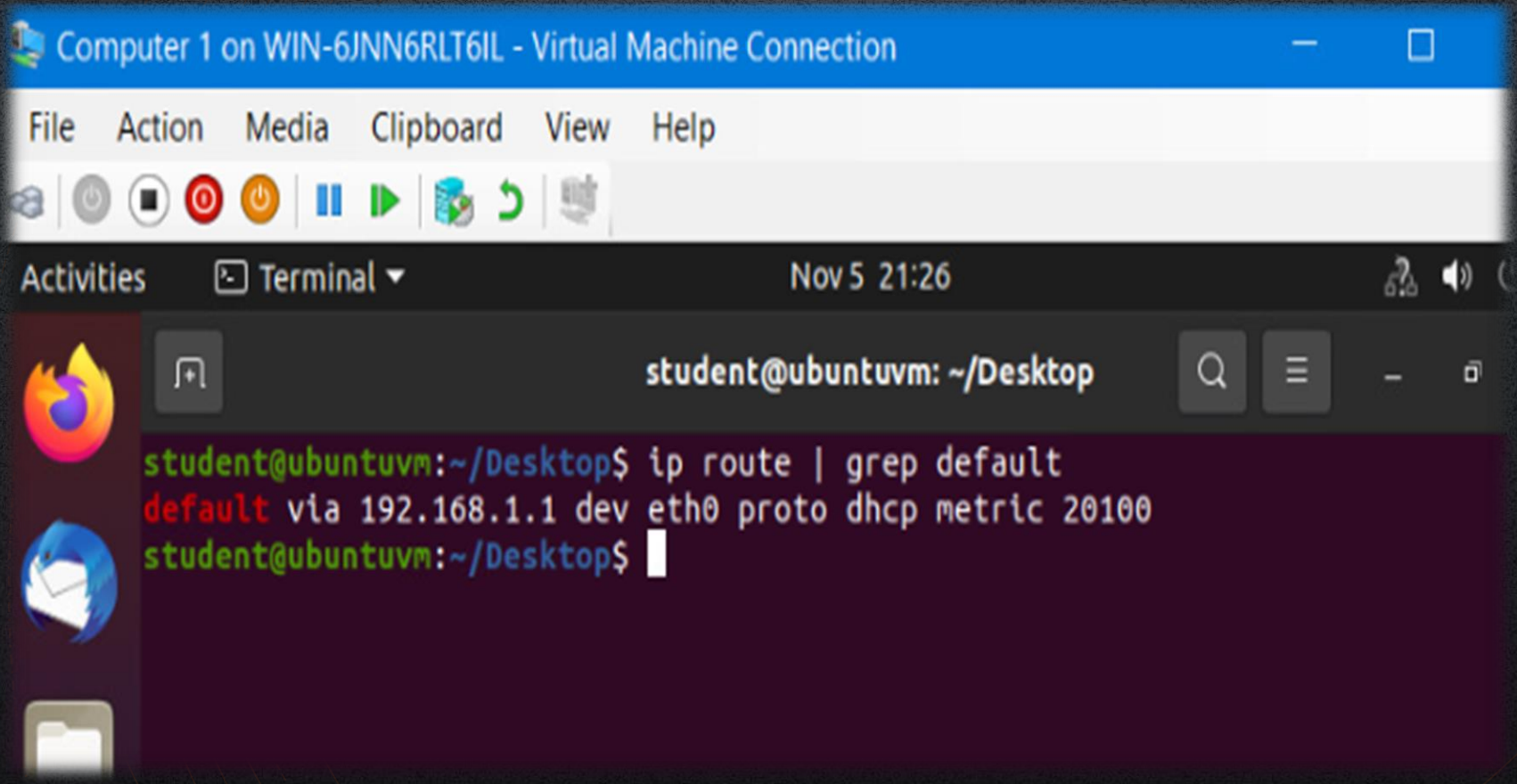

NETWORK DESIGN
AND
DOCUMENTATION



MICROSOFT VISIO NETWORK DIAGRAM

Documenting default network IP for default gateway

Screenshot of Computer 1 terminal window showing default gateway IP address.



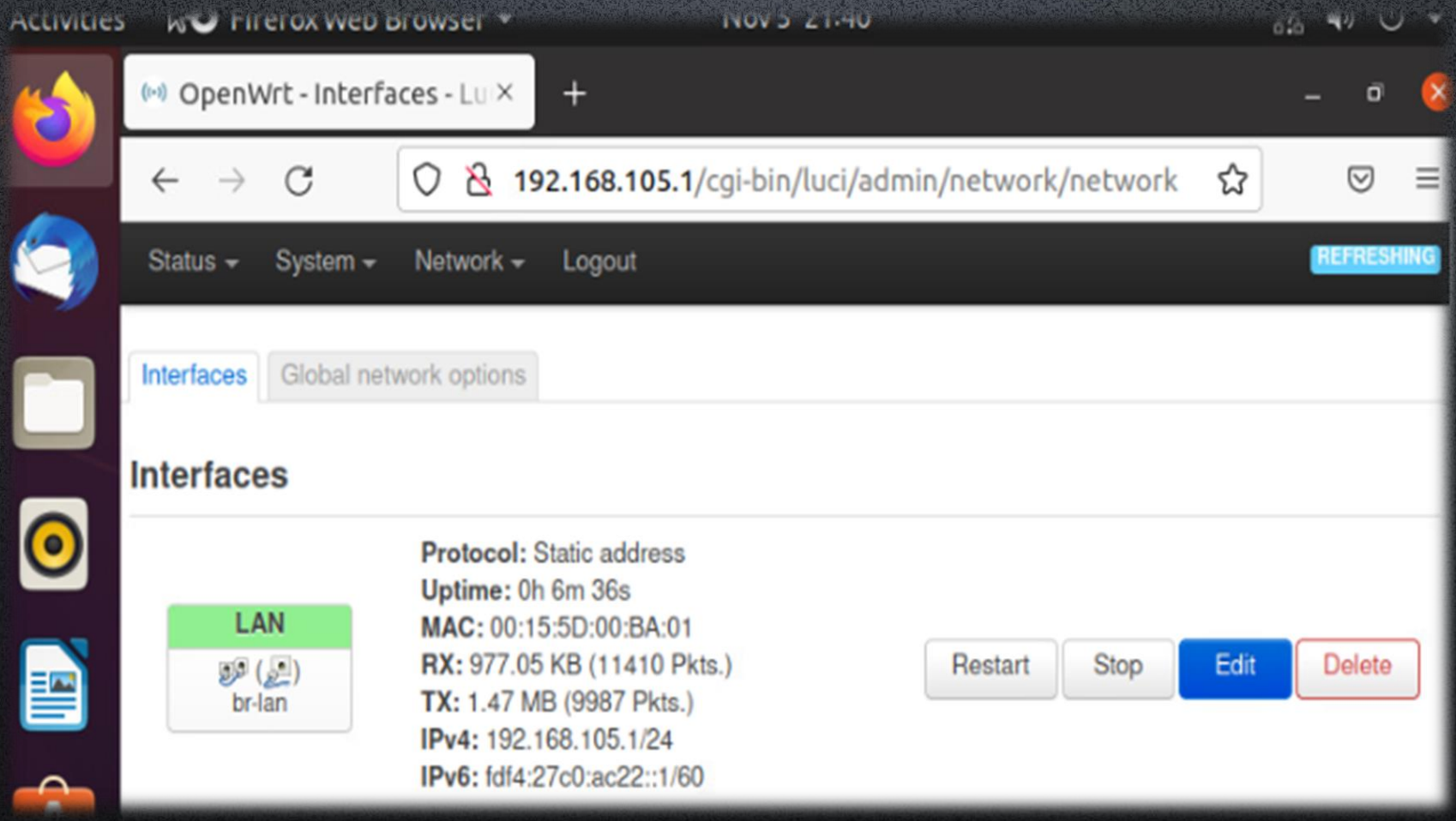
Subnetting Table

Subnet	Subnet Notation	Network Address	First Usable Host Address	Last Useable Host Address	Broadcast Address
Subnet 1	255.255.255.128/25	192.168.5.0	192.168.5.1	192.168.5.126	192.168.5.127
Subnet 2	192.168.5.128/25	192.168.5.128	192.168.5.129	192.168.5.254	192.168.5.255

NETWORK IMPLEMENTATION

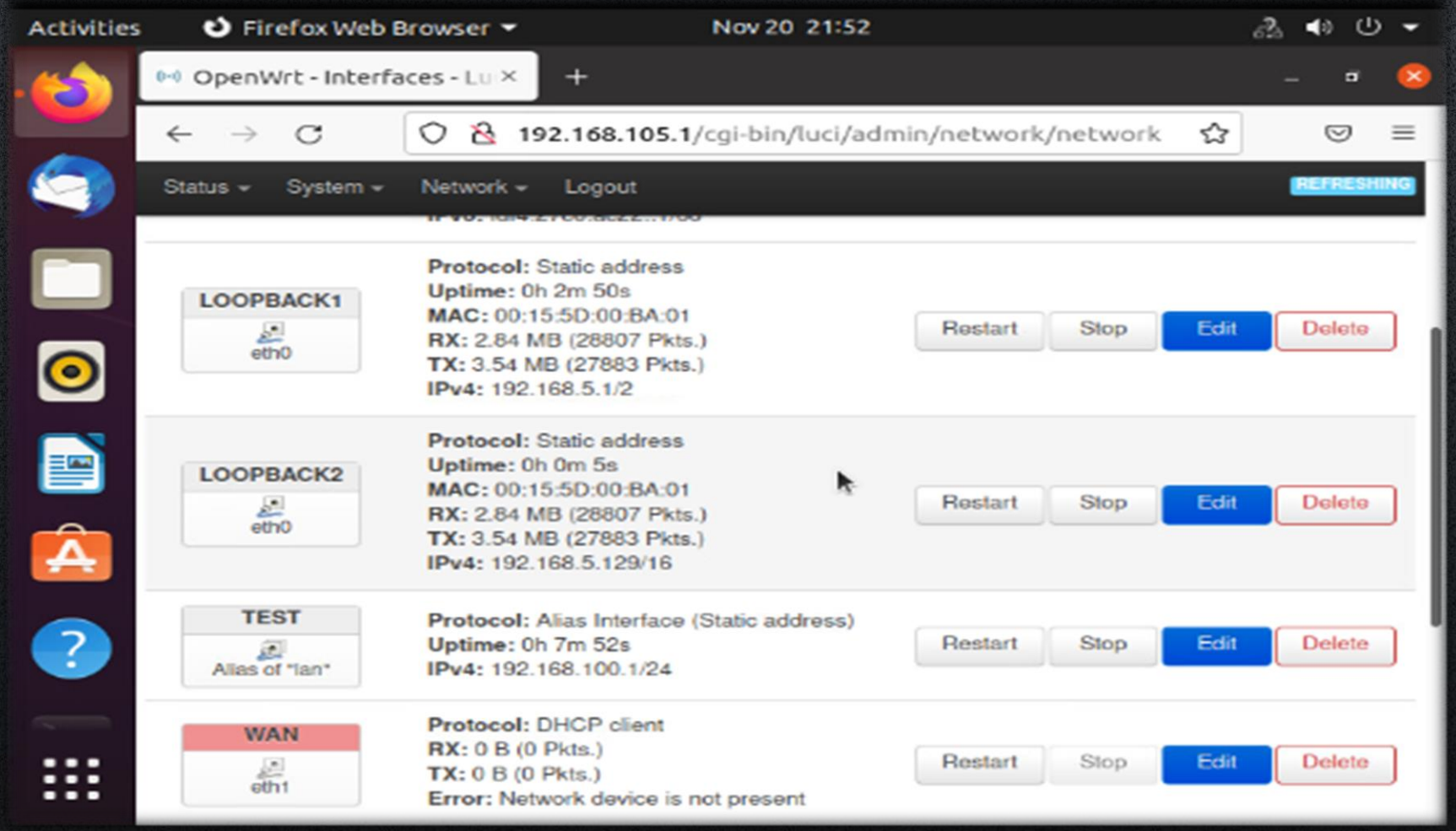
IPv4 Address Assignment for SOHO Router

Screenshot shows the *Interfaces* page with the new IPv4 address on the LAN interface.



Loopback Interfaces

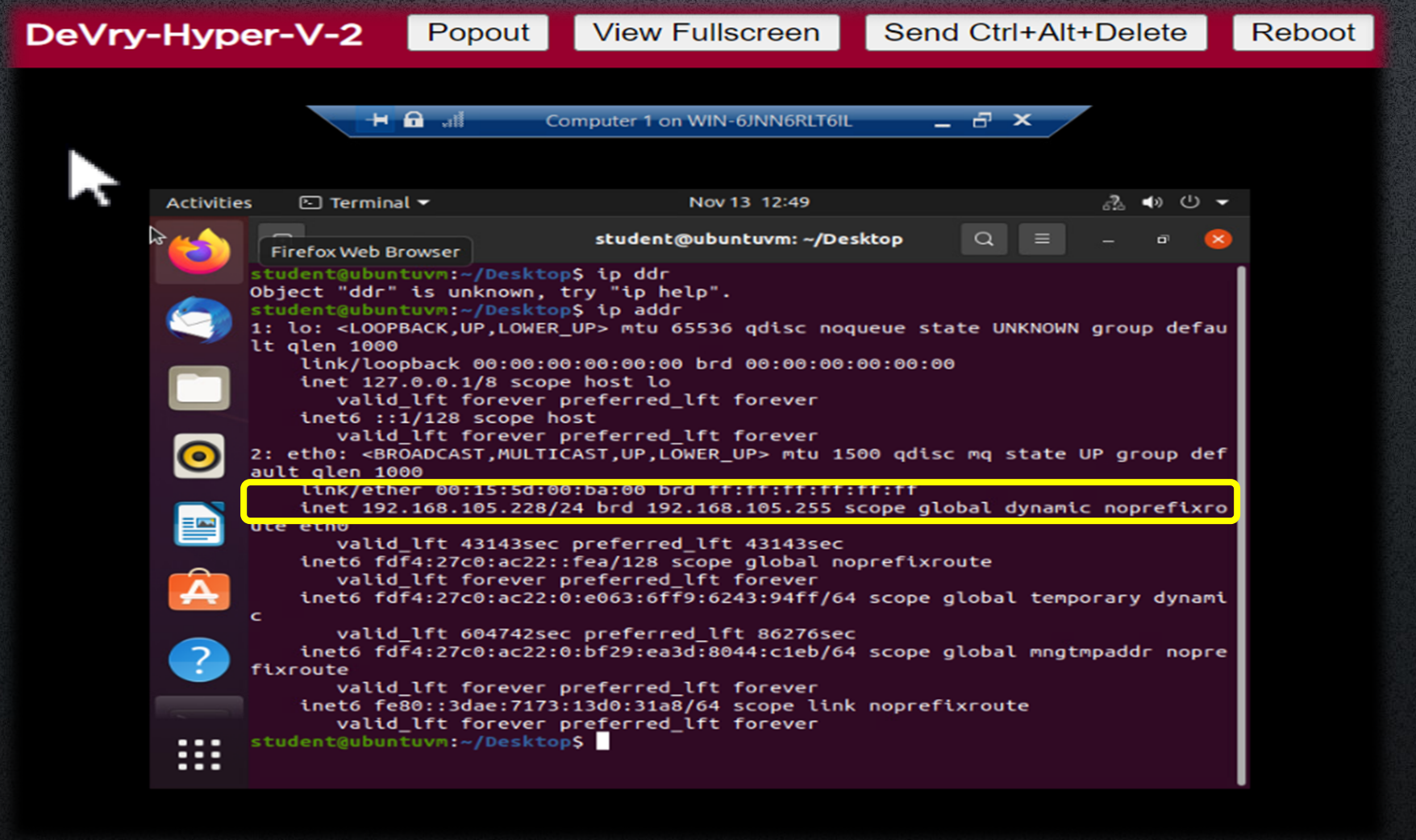
Screenshot shows IPv4 address of Loopback1 and Loopback 2



TESTING: NEW IPV4 ASSIGNMENT

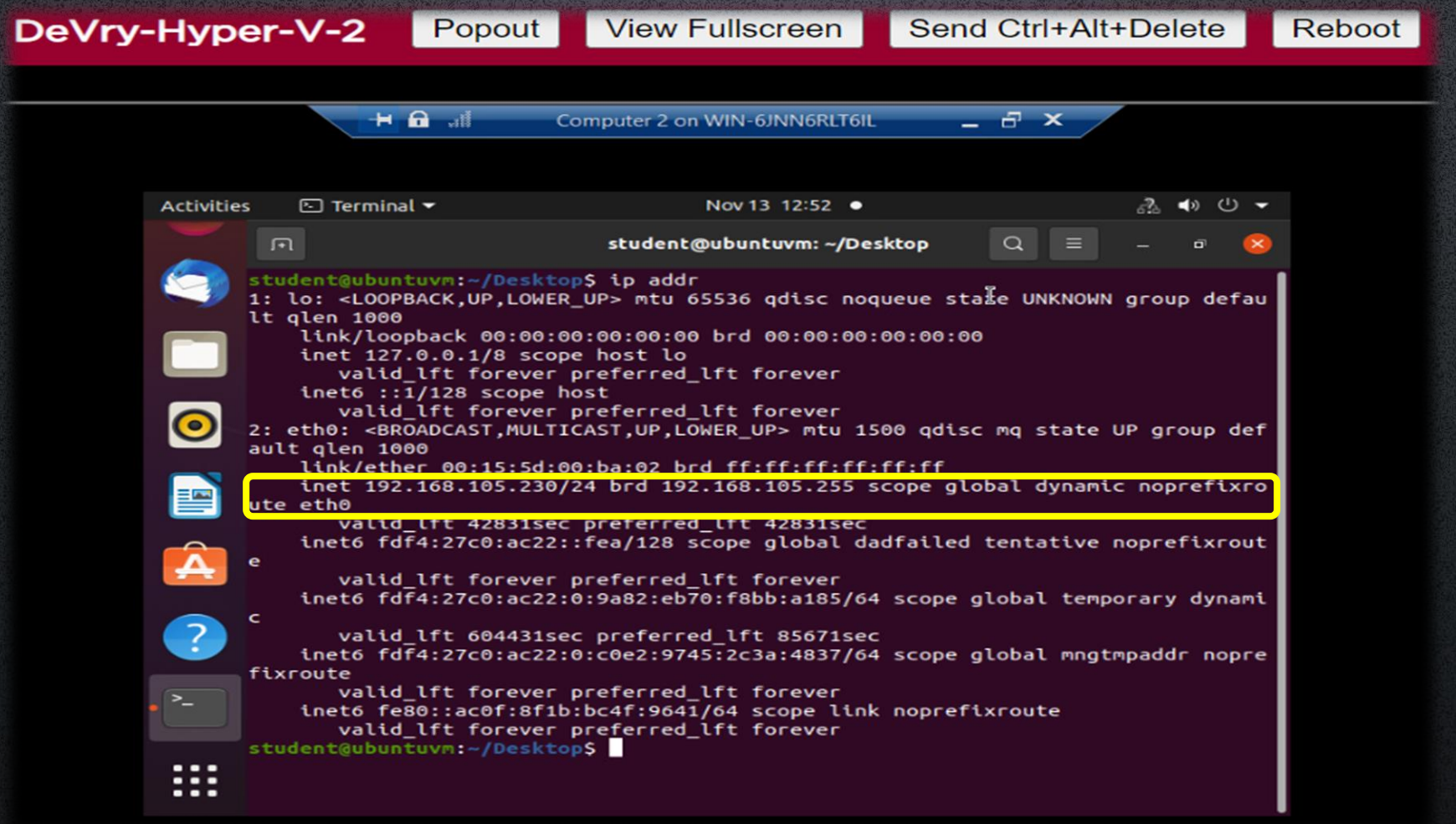
Dynamic IP Address - Computer 1 VM

Screenshot shows IPv4 address of Computer 1 VM after IP address change



Dynamic IP Address - Computer 2 VM

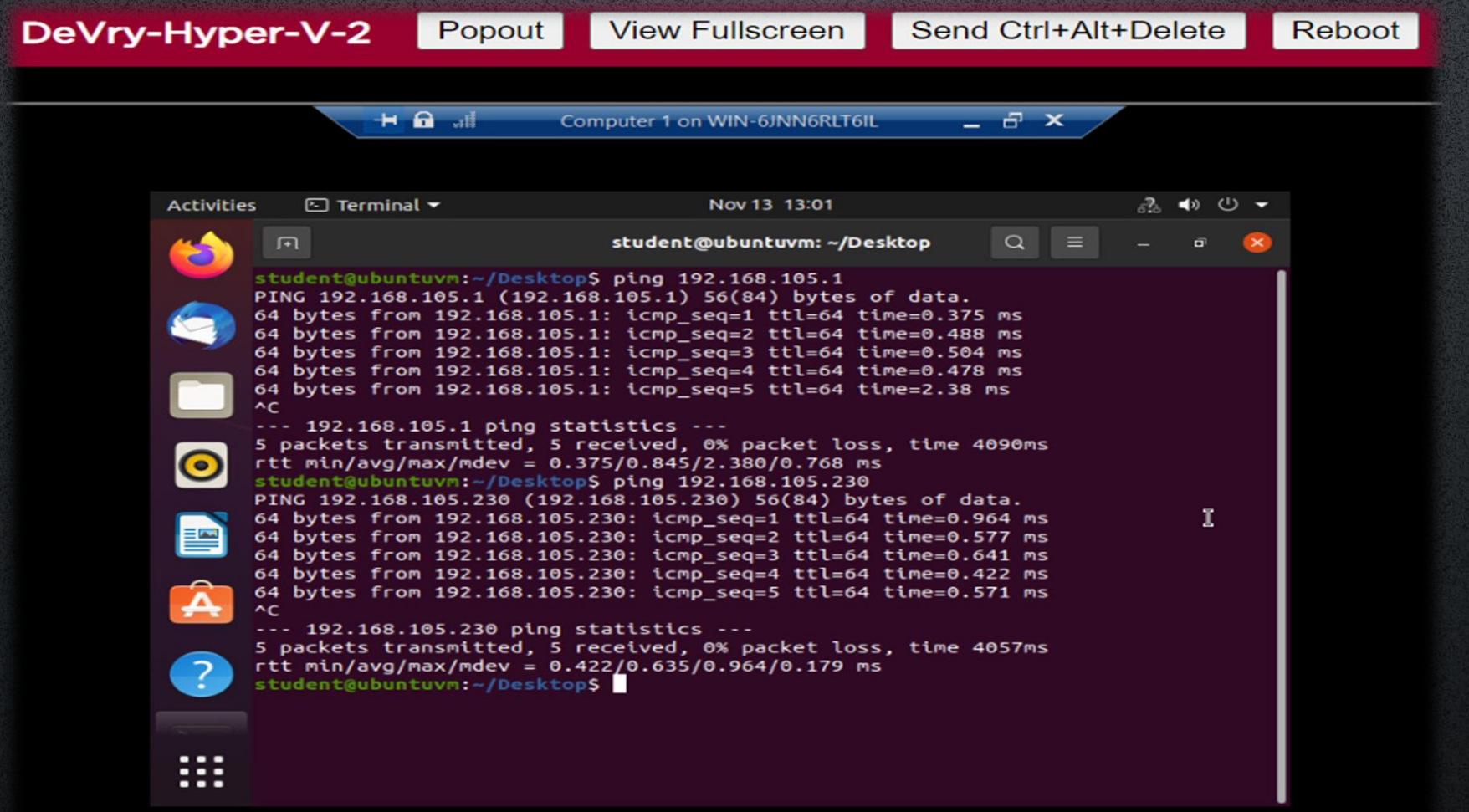
Screenshot shows IPv4 address of Computer 2 VM after IP address change



TESTING: CONNECTIVITY

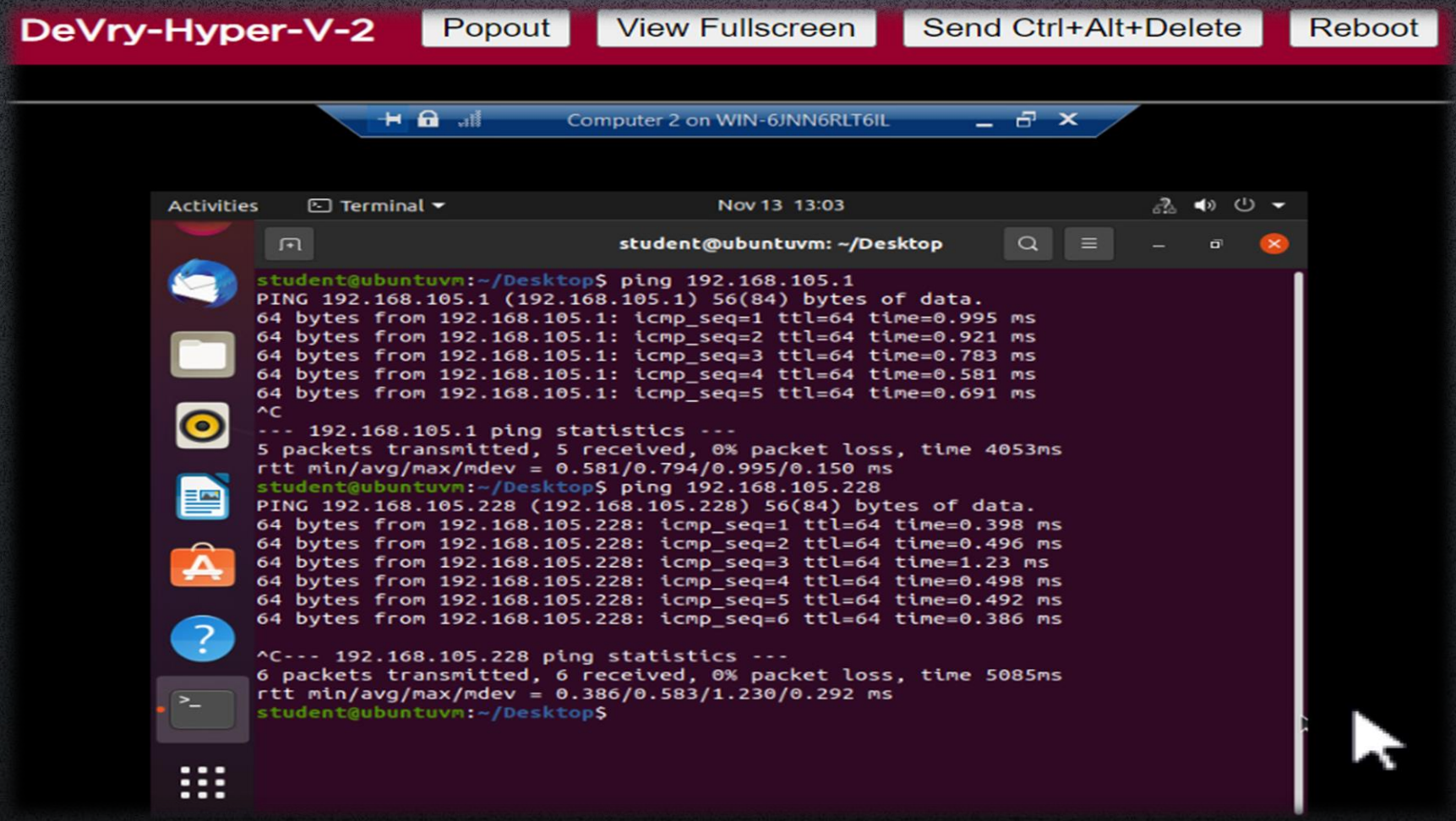
Connectivity Test – Computer 1 VM

Screenshot shows Computer 1 VM can communicate with Computer 2 and the SOHO Router.



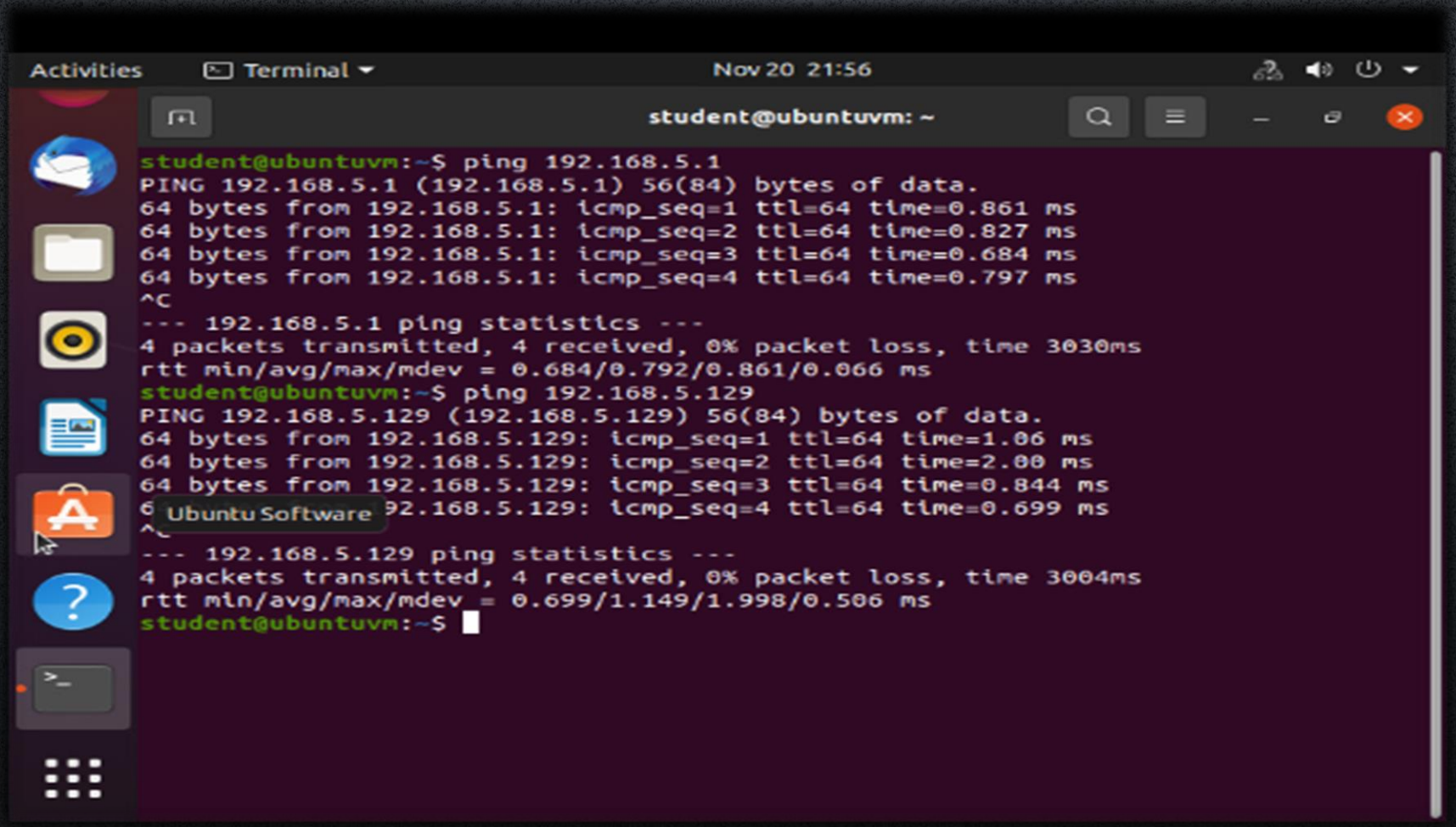
Connectivity Test – Computer 2 VM

Screenshot shows Computer 2 VM can communicate with Computer 1 and the SOHO Router.



Connectivity Test - Loopback

Screenshot shows Computer 1 VM can communicate with Loopback 1 and 2 interfaces.



SECURITY CONSIDERATIONS

SOHO WIRELESS NETWORK SECURITY

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?

- TP link username 'admin' and the password is 'admin' all lower case. If you do not change the username and password from the default settings, you leave your entire home network open to anyone to access, update and exploit.

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?

- It is easier to allow DHCP to assign IP addresses. Static IPs require manual intervention for every new device that is added to the network

SOHO WIRELESS NETWORK SECURITY

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?

- MAC filtering allows the network administrator to restrict access to the network based on the MAC address of the devices' NIC card. You would deny access to all devices that are not part of the explicit approved list. If you have no entries, no device will be able to connect to your network

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

- WPA/WPA2 - Enterprise, WEP, WPA/WPA2 - Personal(Recommended). The personal version is recommended because it uses one passkey that all can use to access the network.

SOHO WIRELESS NETWORK SECURITY

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

- WPA2 is the true security function. It requires that users enter a passkey to connect to the network. If you do not have the passkey, you are unable to access the network or devices on the network.

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

- The first thing I would do is alter the main IP address of the router from 192.168.1.0 to 192.168.XXX.0. I would ensure the admin username and password are changed to a strong password and a different username. I would then enable WPA/WPA2 Personal and create a unique and long passkey that is hard to guess. I would do this to make sure that my personal data is protected from unauthorized users.

LESSONS LEARNED

Challenges

- Creating the subnetting table was the largest challenge faced during the project setup

- I used the following websites when attempting to create the table:
  - https://www.site24x7.com/tools/ipv4-subnetcalculator.html
  - https://CIDR.xyz
  - https://www.aelius.com/njh/subnet_sheet.html

Career Skills

- Understanding how to segment networks
- Demonstrating the ability to find information that is not already known and applying to current situations

Conclusion

- This project helped me to understand:
  - how to create a network from start to finish
  - How to properly document a network
  - Understanding how to set up security and why security for a network is of the highest importance

REFERENCES

- https://www.tp-link.com/us/support/faq/426/#:~:text=The%20default%20IP%20address%20is,admin%20(all%20lower%20case)
- https://emulator.tp-link.com/902AC_US_Emulator/Emulator_Router/index.htm
- https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa
- https://www.site24x7.com/tools/ipv4-subnetcalculator.html
- https://CIDR.xyz
- https://www.aelius.com/njh/subnet_sheet.html