Fundamentals of Information NETW191

TECHNOLOGY AND NETWORKING

Presentation by Yaneth Gonzalez

TABLE OF CONTENT

INTRODUCTION

IPV4 ADDRESSING

CONNECTIVITY TEST

IP SUBNETTING AND LOOPBACK INTERFACES

VISIO NETWORK DIAGRAM

SOHO WIRELESS NETWORK SECURITY

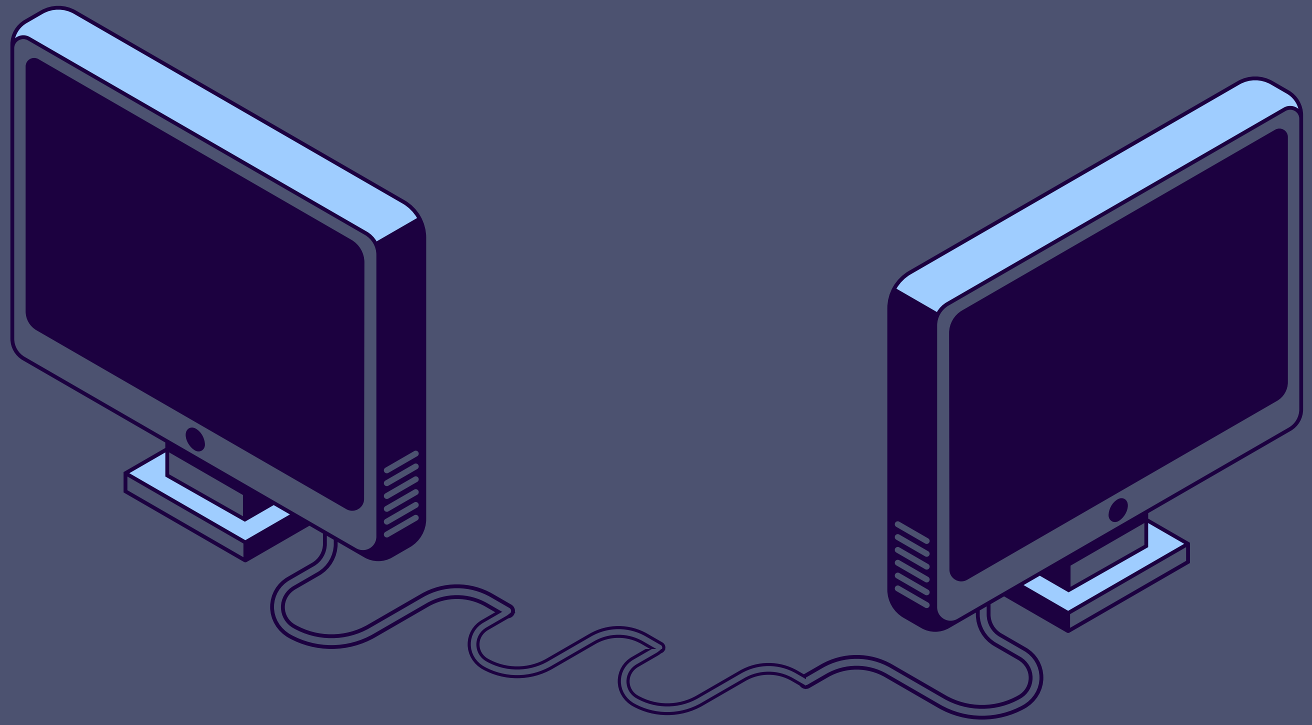
Challenges

Career Skills

Conclusion

Reference

INTRODUCTION TO FUNDAMENTALS OF IT AND NETWORKING (NETW191)



IN MY FUNDAMENTALS OF IT AND NETWORKING COURSE, I'VE GAINED VALUABLE INSIGHTS INTO THE ESSENTIAL COMPONENTS OF NETWORK SETUP AND MANAGEMENT.

THIS PRESENTATION WILL PROVIDE AN OVERVIEW OF THE KEY CONCEPTS AND HANDS-ON EXPERIENCES I'VE ENCOUNTERED, WITH A PARTICULAR FOCUS ON IPV4 ADDRESSING—A FOUNDATIONAL ASPECT OF NETWORK CONFIGURATION.

ONE OF THE PRIMARY PROJECTS IN THIS COURSE INVOLVED CONFIGURING AND VERIFYING IPV4 ADDRESSES ON NETWORK DEVICES USING LINUX. THIS PRACTICAL EXPERIENCE ALLOWED ME TO DIRECTLY APPLY THEORETICAL KNOWLEDGE IN REAL-WORLD SCENARIOS, ENHANCING MY UNDERSTANDING OF NETWORK OPERATIONS.

THROUGHOUT THE COURSE, I ENGAGED IN VARIOUS TASKS SUCH AS SETTING UP VIRTUAL NETWORKS, CONDUCTING CONNECTIVITY TESTS, AND ENSURING SECURE COMMUNICATION BETWEEN DEVICES. THESE PROJECTS NOT ONLY DEVELOPED MY TECHNICAL SKILLS BUT ALSO EMPHASIZED THE IMPORTANCE OF DOCUMENTATION AND TROUBLESHOOTING IN NETWORK MANAGEMENT.

IN THE FOLLOWING SLIDES, I'LL PRESENT THE CORE LESSONS LEARNED, FROM IP ADDRESS CONFIGURATION TO NETWORK SECURITY, ILLUSTRATING HOW THESE ELEMENTS CONTRIBUTE TO EFFECTIVE AND RELIABLE NETWORK INFRASTRUCTURE.

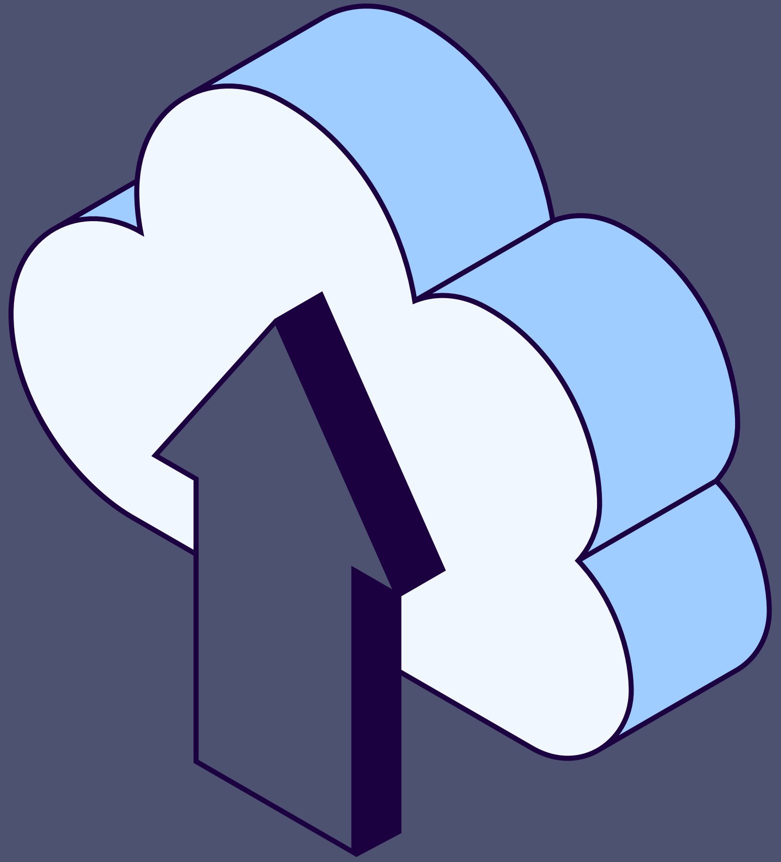
NETW191 COURSE PROJECT

MODULE 2

IPV4 ADDRESSING

THIS PROJECT MODULE FOCUSED ON IPV4 ADDRESSING

A FUNDAMENTAL ASPECT OF NETWORK CONFIGURATION AND MANAGEMENT. THE PRIMARY OBJECTIVE WAS TO CONFIGURE AND VERIFY IPV4 ADDRESSES ON NETWORK DEVICES USING LINUX. THIS HANDS-ON PROJECT PROVIDED PRACTICAL EXPERIENCE IN SETTING UP AND MANAGING IP ADDRESSES, REINFORCING THEORETICAL KNOWLEDGE THROUGH REAL-WORLD APPLICATION.



INITIAL CONFIGURATION

OPEN THE LINUX TERMINAL AND VERIFY THE DEFAULT GATEWAY IP ADDRESS, TYPICALLY 192.168.1.1.

CAPTURE A SCREENSHOT OF THE TERMINAL WINDOW SHOWING THE DEFAULT GATEWAY.

RECONFIGURATION OF DEFAULT GATEWAY

ACCESS THE ROUTER INTERFACE USING A WEB BROWSER.

CHANGE THE DEFAULT GATEWAY IP ADDRESS FROM 192.168.1.1 TO 192.168.105.

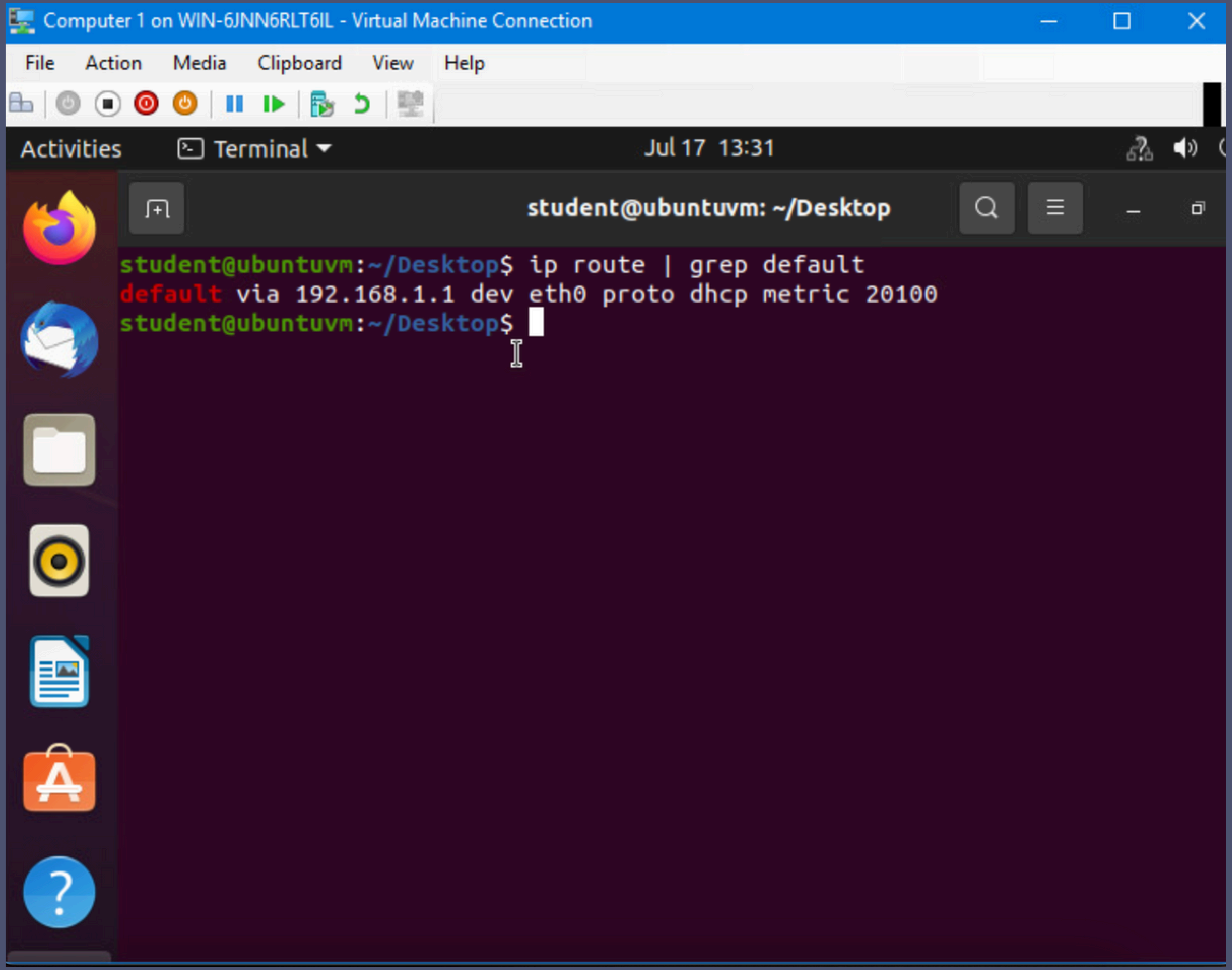
CAPTURE A SCREENSHOT OF THE UPDATED CONFIGURATION.

VERIFICATION:

ENSURE THE NEW IP ADDRESS CONFIGURATION IS CORRECTLY APPLIED.

TROUBLESHOOT ANY CONNECTIVITY ISSUES THAT ARISE FROM THE RECONFIGURATION

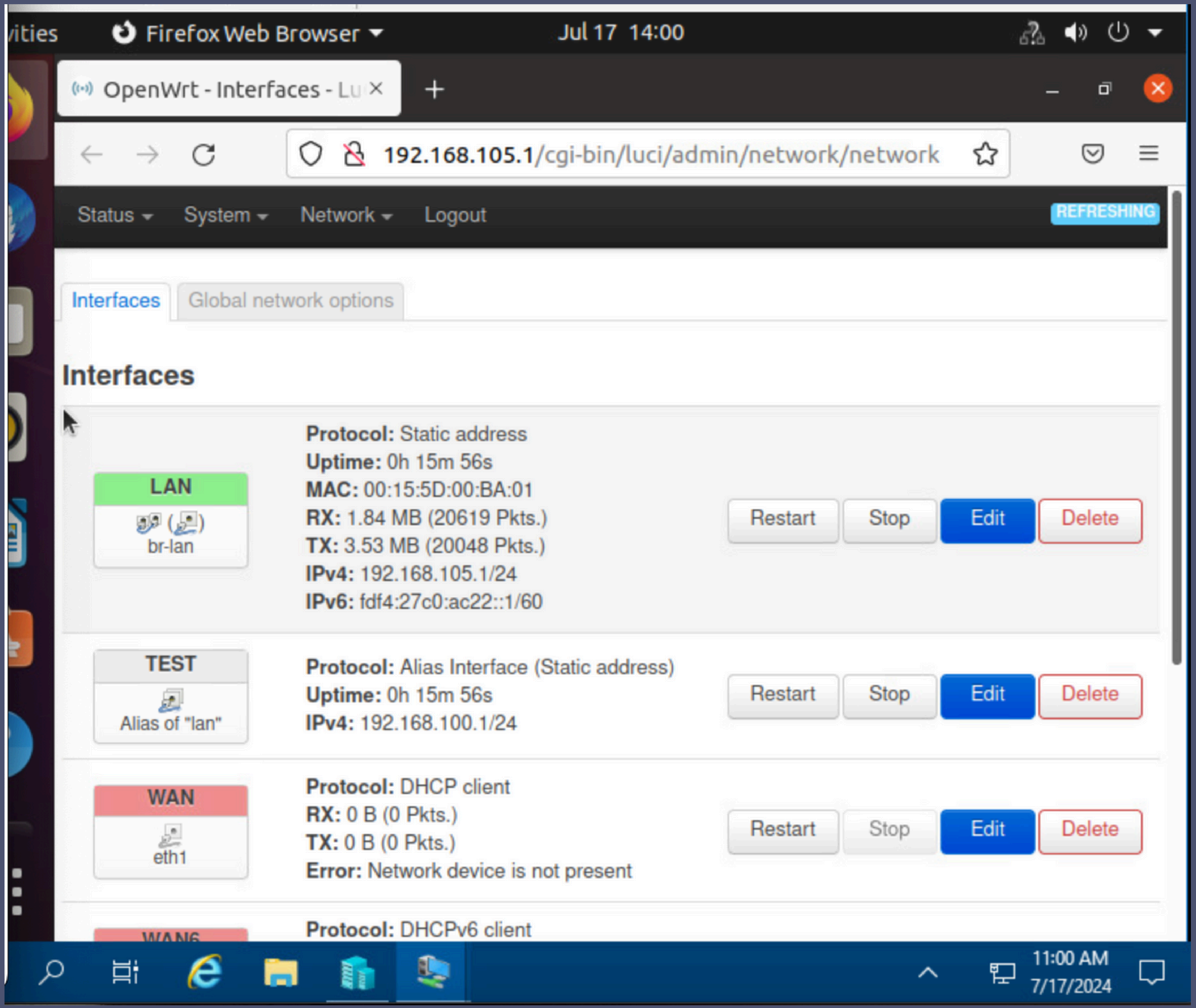
Terminal window that shows the default gateway IP address.



Computer 1 on WIN-6JNN6RLT6IL - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Activities
Terminal
Jul 17 13:31
student@ubuntuvm: ~/Desktop

```
student@ubuntuvm:~/Desktop$ ip route | grep default
default via 192.168.1.1 dev eth0 proto dhcp metric 20100
student@ubuntuvm:~/Desktop$ 
```

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



192.168.105.1/cgi-bin/luci/admin/network/network

Interfaces

LAN
br-lan

Protocol: Static address
Uptime: 0h 15m 56s
MAC: 00:15:5D:00:BA:01
RX: 1.84 MB (20619 Pkts.)
TX: 3.53 MB (20048 Pkts.)
IPv4: 192.168.105.1/24
IPv6: fdf4:27c0:ac22::1/60

TEST
Alias of "lan"

Protocol: Alias Interface (Static address)
Uptime: 0h 15m 56s
IPv4: 192.168.100.1/24

WAN
eth1

Protocol: DHCP client
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
Error: Network device is not present

WAN6

Protocol: DHCPv6 client

NETW191 COURSE PROJECT

MODULE 3

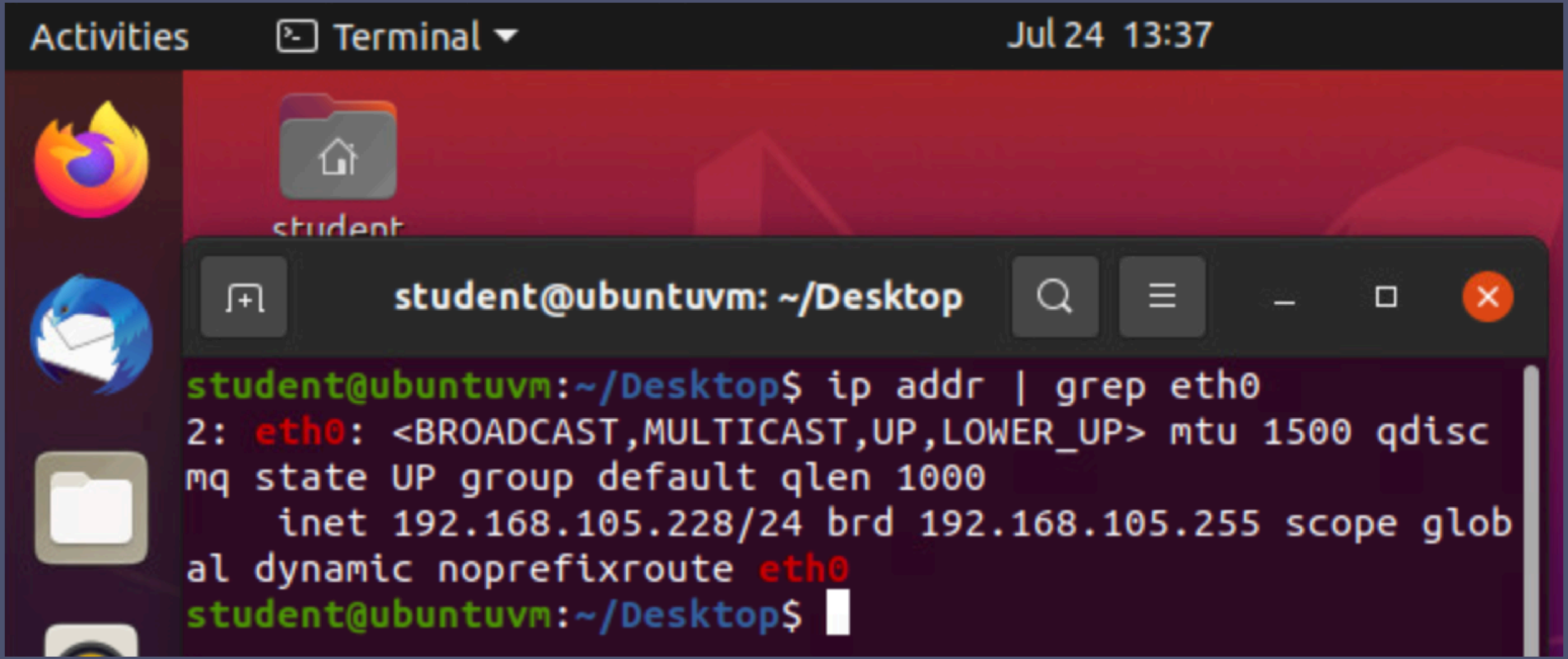
CONNECTIVITY TEST

IN THIS PROJECT, WE TESTED IF TWO VIRTUAL COMPUTERS COULD CONNECT TO A VIRTUAL ROUTER.

WE SET UP A VIRTUAL NETWORK USING HYPER-V MANAGER, CONFIGURED IP ADDRESSES, AND RAN SIMPLE NETWORK TESTS.

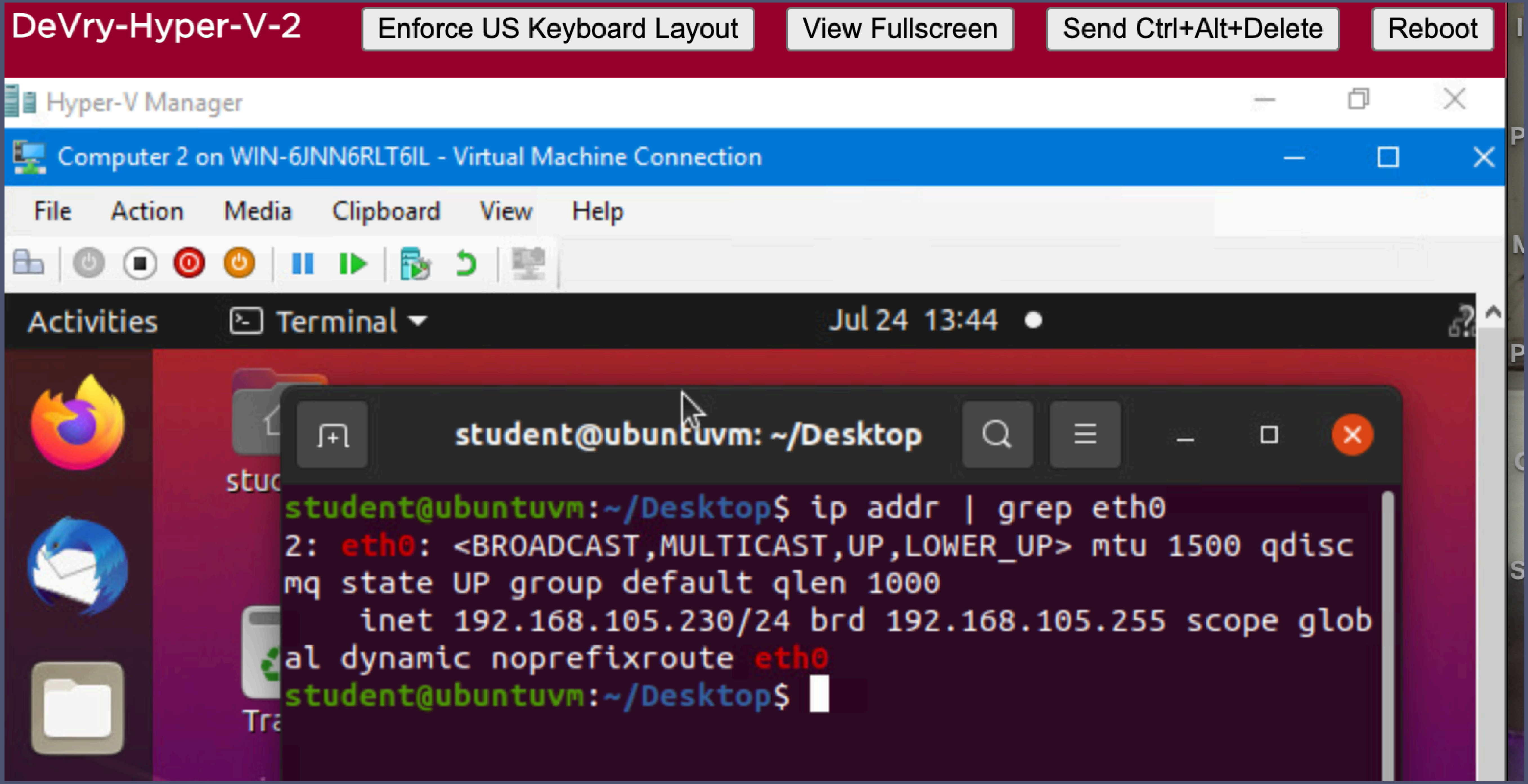
OUR GOAL WAS TO MAKE SURE THE COMPUTERS COULD COMMUNICATE WITH EACH OTHER AND THE ROUTER. THIS PROJECT HELPED US LEARN THE BASICS OF NETWORK SETUP AND TROUBLESHOOTING.

WE USED IMPORTANT NETWORK COMMANDS AND LEARNED HOW TO DOCUMENT OUR WORK.



```
student@ubuntuvm:~/Desktop$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
mq state UP group default qlen 1000
    inet 192.168.105.228/24 brd 192.168.105.255 scope glob
al dynamic noprefixroute eth0
student@ubuntuvm:~/Desktop$ 
```

This screenshot shows the terminal window and the IPv4 address of the Computer 1 VM.



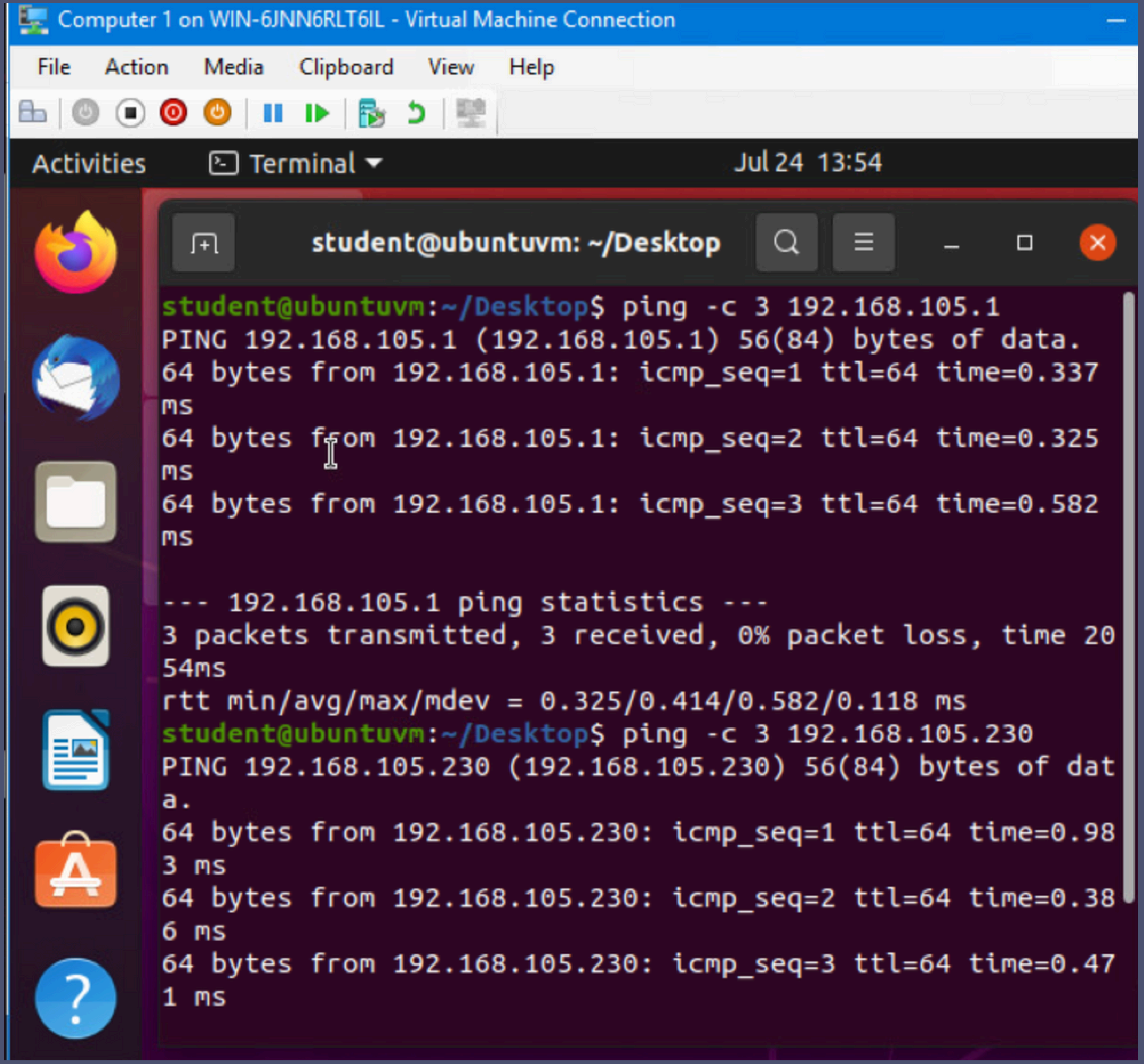
```
student@ubuntuvm:~/Desktop$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
mq state UP group default qlen 1000
    inet 192.168.105.230/24 brd 192.168.105.255 scope glob
al dynamic noprefixroute eth0
student@ubuntuvm:~/Desktop$ 
```

This screenshot shows the terminal window and the IPv4 address of the Computer 2 VM

SCREENSHOT OF THE TERMINAL WINDOW.

THIS SCREENSHOT SHOWS

- 1) THE CONNECTIVITY TEST FROM THE COMPUTER 1 VM TO THE SOHO ROUTER VM,
- 2) THE CONNECTIVITY TEST FROM THE COMPUTER 1 VM TO THE COMPUTER 2 VM.


Computer 1 on WIN-6JNN6RLT6IL - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Activities
Terminal
Jul 24 13:54
student@ubuntuvm: ~/Desktop

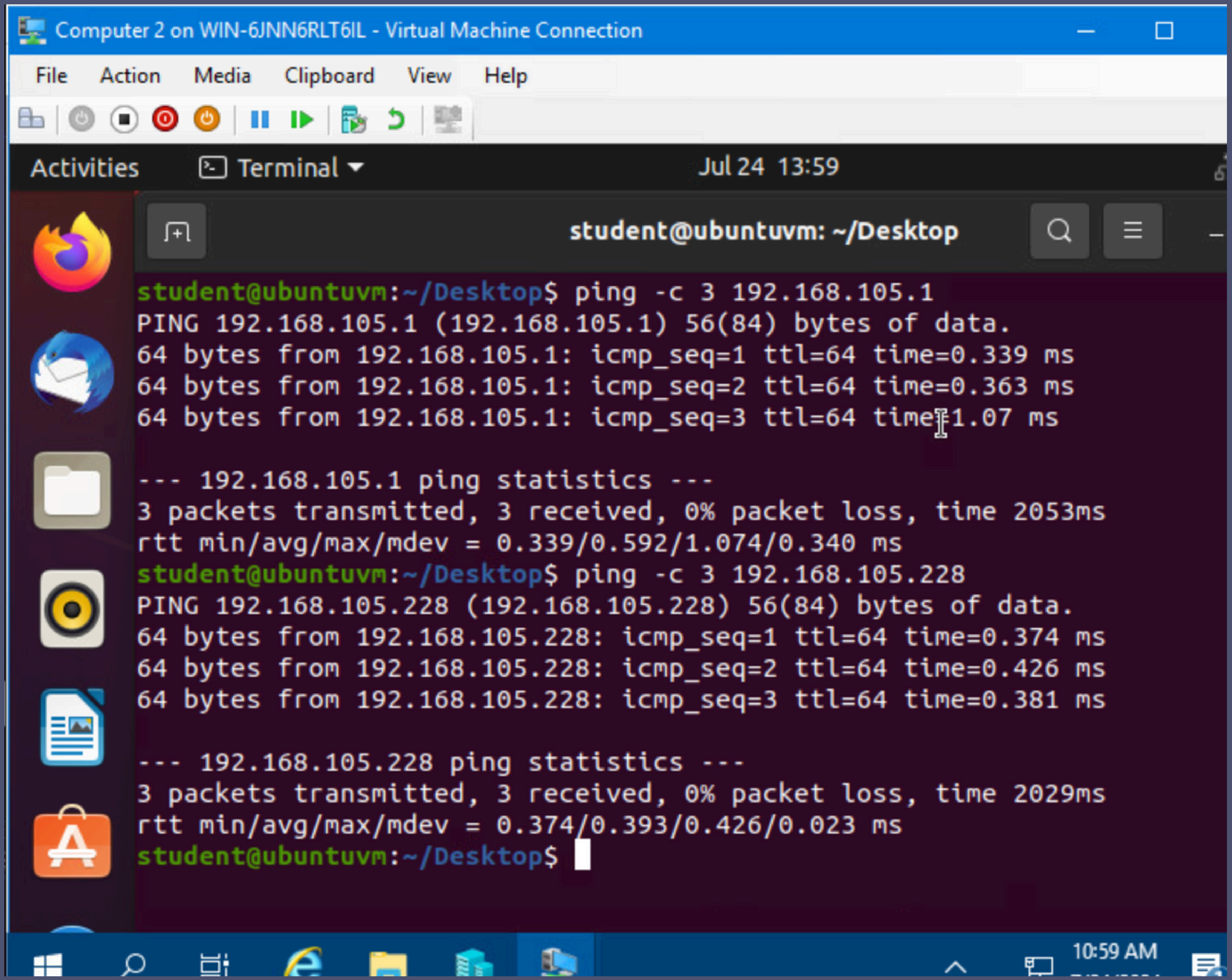
```
student@ubuntuvm:~/Desktop$ ping -c 3 192.168.105.1
PING 192.168.105.1 (192.168.105.1) 56(84) bytes of data.
64 bytes from 192.168.105.1: icmp_seq=1 ttl=64 time=0.337
ms
64 bytes from 192.168.105.1: icmp_seq=2 ttl=64 time=0.325
ms
64 bytes from 192.168.105.1: icmp_seq=3 ttl=64 time=0.582
ms

--- 192.168.105.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 20
54ms
rtt min/avg/max/mdev = 0.325/0.414/0.582/0.118 ms
student@ubuntuvm:~/Desktop$ ping -c 3 192.168.105.230
PING 192.168.105.230 (192.168.105.230) 56(84) bytes of dat
a.
64 bytes from 192.168.105.230: icmp_seq=1 ttl=64 time=0.98
3 ms
64 bytes from 192.168.105.230: icmp_seq=2 ttl=64 time=0.38
6 ms
64 bytes from 192.168.105.230: icmp_seq=3 ttl=64 time=0.47
1 ms
```

SCREENSHOT OF THE TERMINAL WINDOW.

THIS SCREENSHOT SHOWS

- 2) THE CONNECTIVITY TEST FROM THE COMPUTER 1 VM TO THE COMPUTER 2 VM.


Computer 2 on WIN-6JNN6RLT6IL - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Activities
Terminal
Jul 24 13:59
student@ubuntuvm: ~/Desktop
10:59 AM

```
student@ubuntuvm:~/Desktop$ ping -c 3 192.168.105.1
PING 192.168.105.1 (192.168.105.1) 56(84) bytes of data.
64 bytes from 192.168.105.1: icmp_seq=1 ttl=64 time=0.339 ms
64 bytes from 192.168.105.1: icmp_seq=2 ttl=64 time=0.363 ms
64 bytes from 192.168.105.1: icmp_seq=3 ttl=64 time=1.07 ms

--- 192.168.105.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2053ms
rtt min/avg/max/mdev = 0.339/0.592/1.074/0.340 ms
student@ubuntuvm:~/Desktop$ ping -c 3 192.168.105.228
PING 192.168.105.228 (192.168.105.228) 56(84) bytes of data.
64 bytes from 192.168.105.228: icmp_seq=1 ttl=64 time=0.374 ms
64 bytes from 192.168.105.228: icmp_seq=2 ttl=64 time=0.426 ms
64 bytes from 192.168.105.228: icmp_seq=3 ttl=64 time=0.381 ms

--- 192.168.105.228 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2029ms
rtt min/avg/max/mdev = 0.374/0.393/0.426/0.023 ms
student@ubuntuvm:~/Desktop$ 
```

NETW191 COURSE PROJECT

MODULE 4

IP SUBNETTING AND LOOPBACK INTERFACES

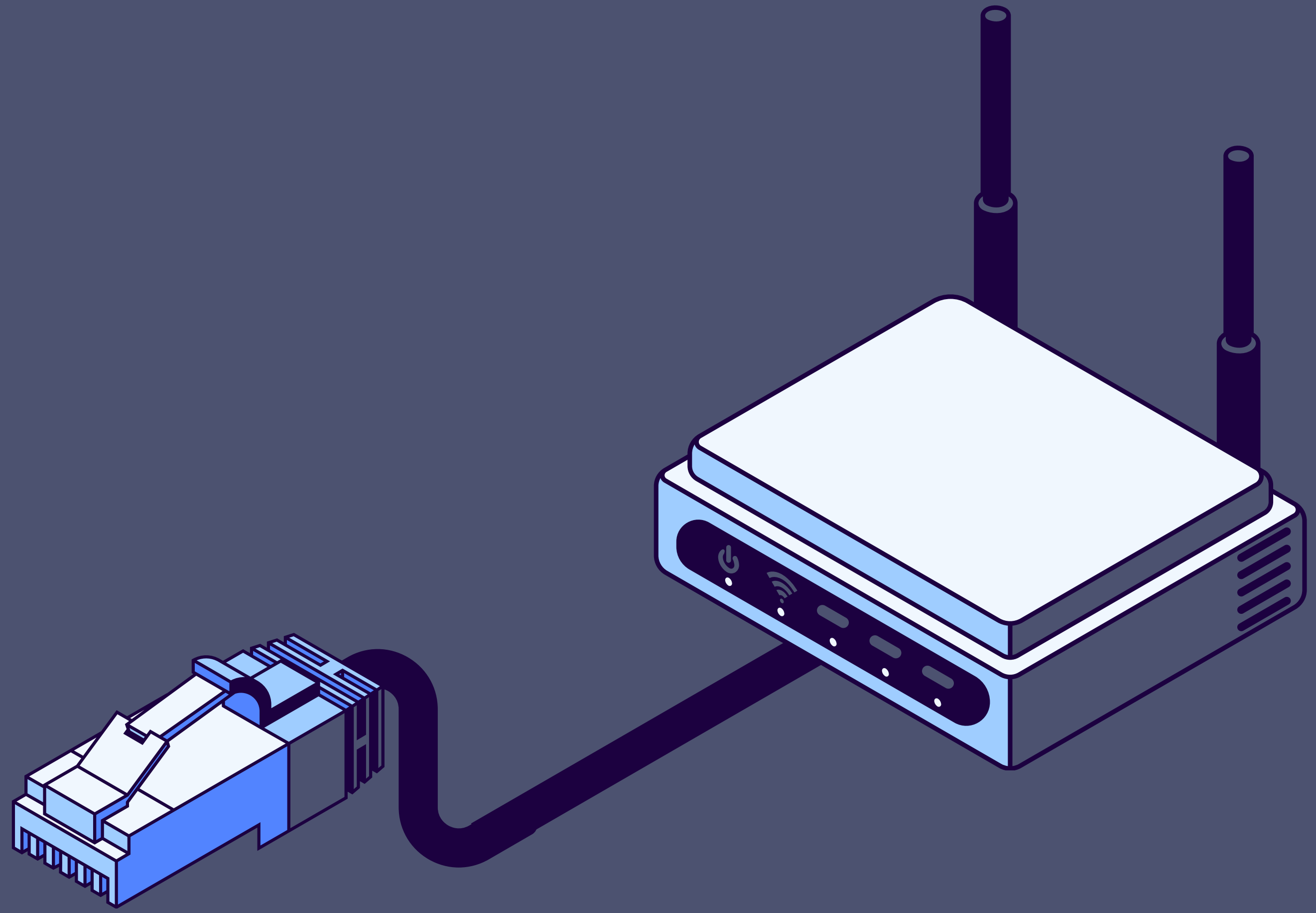
IN THIS PROJECT, WE FOCUSED ON SEVERAL KEY TASKS INVOLVING SUBNETTING AND INTERFACE CONFIGURATION:

- SUBNETTING AND ADDRESS DIVISION: WE LEARNED TO DIVIDE A CLASSFUL IP ADDRESS INTO TWO EQUAL SUBNETS. THIS WAS DEMONSTRATED THROUGH A SIMPLE ANALOGY OF DIVIDING STUDENTS INTO TWO GROUPS, ENSURING AN EQUAL DISTRIBUTION OF ADDRESSES.

- CONFIGURING LOOPBACK INTERFACES: WE SET UP TWO LOOPBACK INTERFACES (LOOPBACK 1 AND LOOPBACK 2) ON OUR NETWORK, CONFIGURING EACH WITH SPECIFIC IP ADDRESSES AND SUBNET MASKS.

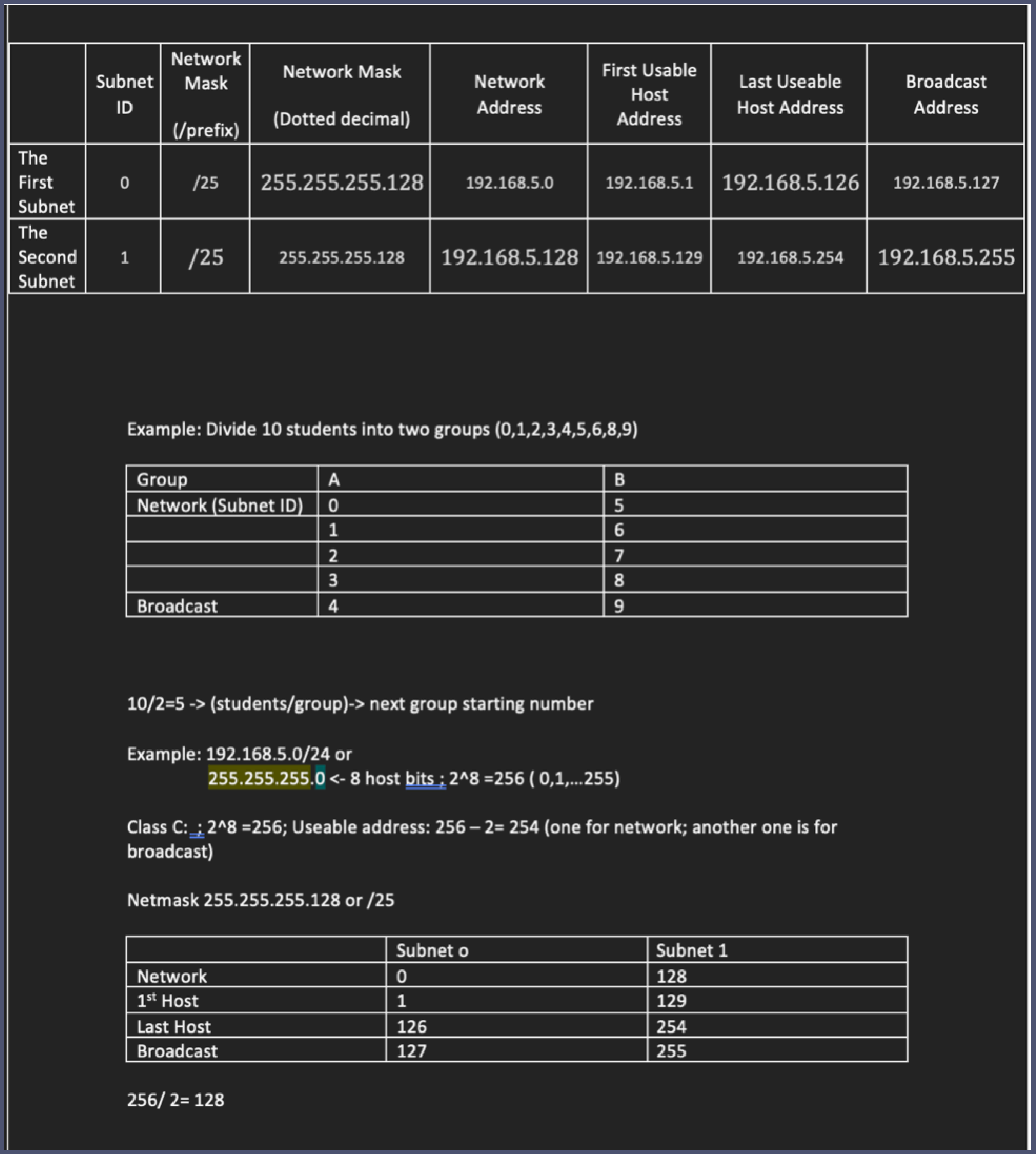
- THIS INVOLVED:
  ASSIGNING IP ADDRESSES AND SUBNET MASKS TO THE INTERFACES.
  VERIFYING THE CONFIGURATIONS THROUGH CONNECTIVITY TESTS.

- CONNECTIVITY TESTING: WE PERFORMED CONNECTIVITY TESTS USING PING COMMANDS TO ENSURE SUCCESSFUL COMMUNICATION BETWEEN THE CONFIGURED INTERFACES WITH NO PACKET LOSS.



In this section, I learned how to divide an IP address into smaller subnetworks, which is called subnetting. The idea is similar to dividing a group of students into smaller groups, where each group has a starting and ending number. In networking, this means splitting an IP address range into smaller ranges that can be used for different parts of a network.

Instructor’s Example:



	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	192.168.5.0	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

Example: Divide 10 students into two groups (0,1,2,3,4,5,6,8,9)

Group	A	B
Network (Subnet ID)	0	5
	1	6
	2	7
	3	8
Broadcast	4	9

10/2=5 -> (students/group)-> next group starting number

Example: 192.168.5.0/24 or
255.255.255.0 <- 8 host bits ; 2^8 =256 (0,1,…255)

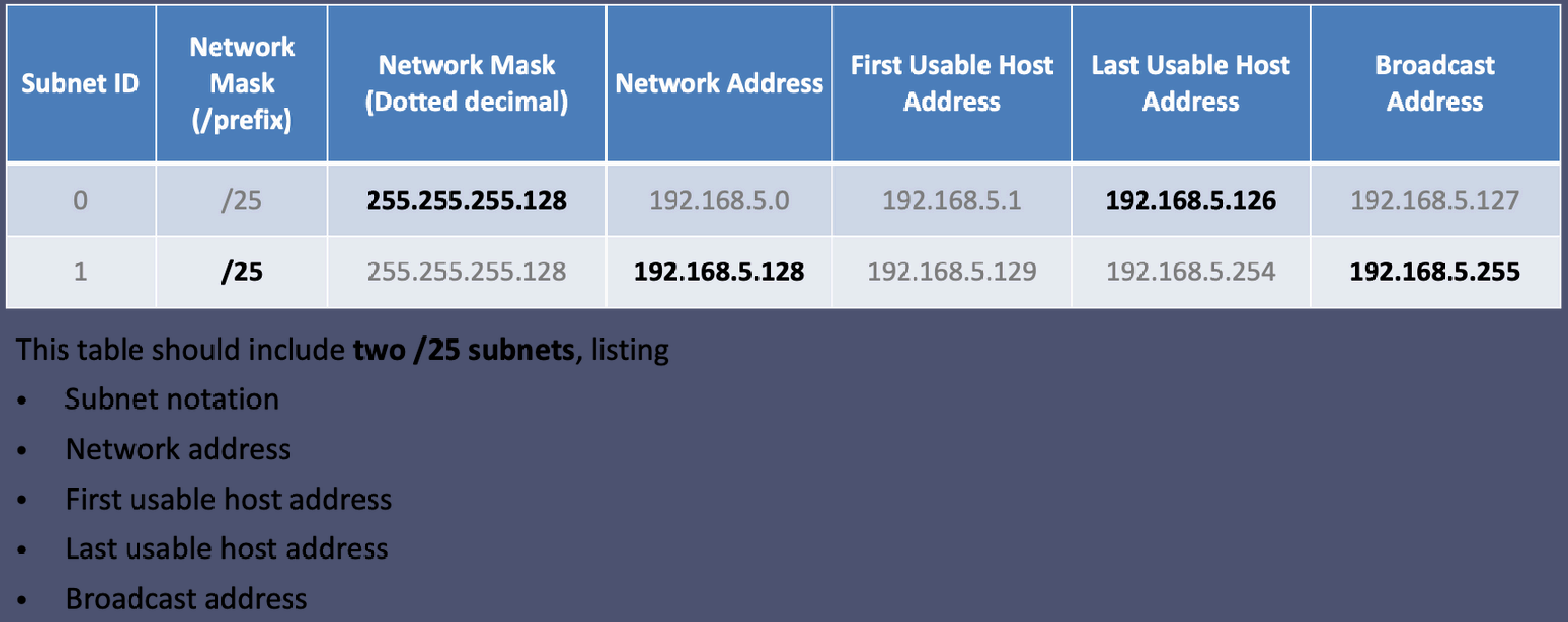
Class C: ; 2^8 =256; Useable address: 256 – 2= 254 (one for network; another one is for broadcast)

Netmask 255.255.255.128 or /25

	Subnet o	Subnet 1
Network	0	128
1^{st} Host	1	129
Last Host	126	254
Broadcast	127	255

256/ 2= 128

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	**192.168.5.128**	192.168.5.129	192.168.5.254	**192.168.5.255**

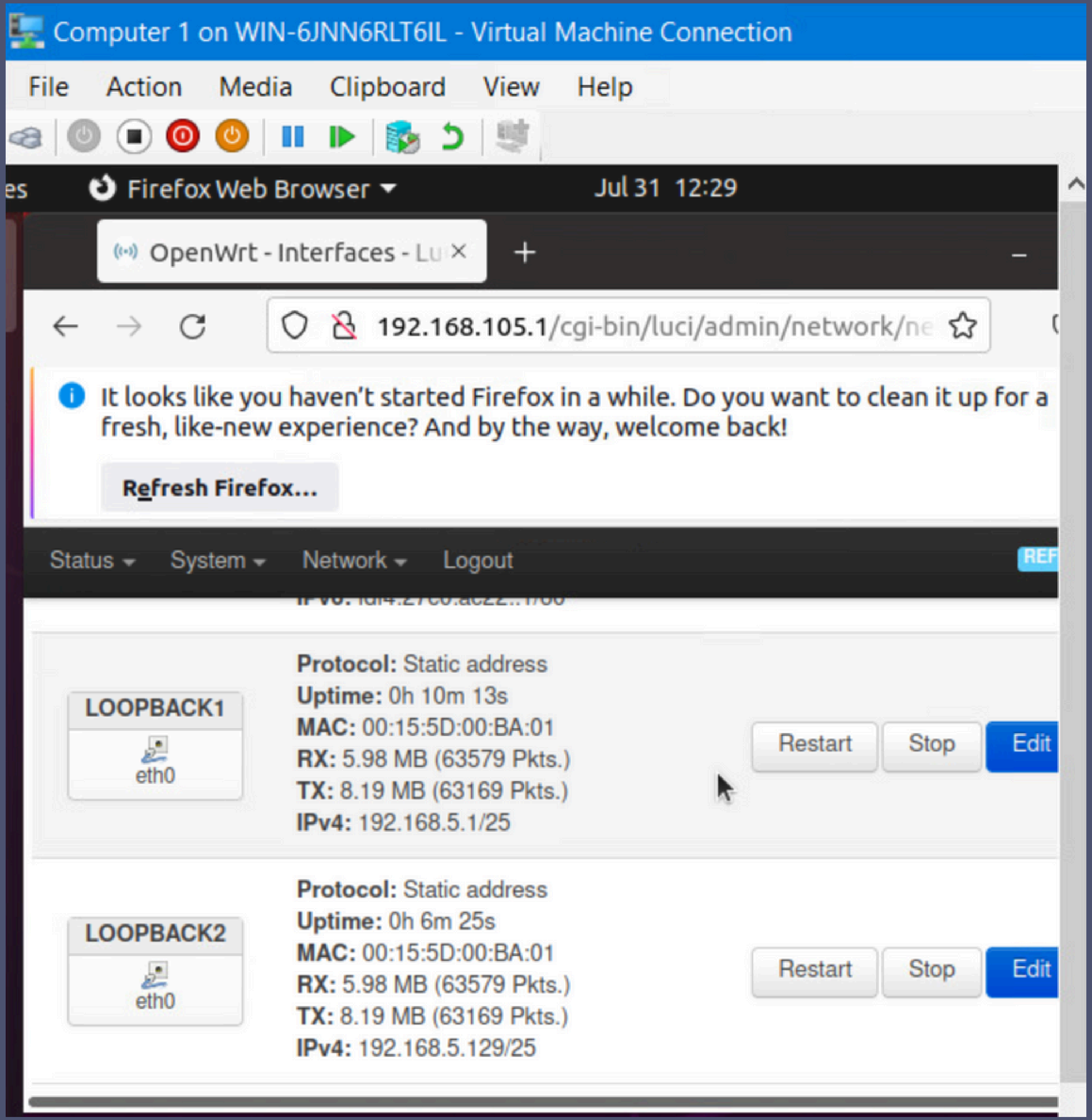
This table should include **two /25 subnets**, listing

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

I practiced creating two equal subnets from a given IP address, learned how to assign network and broadcast addresses, and identified the first and last usable IP addresses within each subnet.

This hands-on work helped me understand how to manage IP addresses more efficiently in a network, ensuring that devices can communicate properly while organizing the network in a way that makes it easier to manage.

THIS SCREENSHOT SHOWS BOTH LOOPBACK1 AND LOOPBACK2 INTERFACES AND THEIR CORRECT IPV4 ADDRESSES.



It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

LOOPBACK1
eth0

Protocol: Static address
Uptime: 0h 10m 13s
MAC: 00:15:5D:00:BA:01
RX: 5.98 MB (63579 Pkts.)
TX: 8.19 MB (63169 Pkts.)
IPv4: 192.168.5.1/25

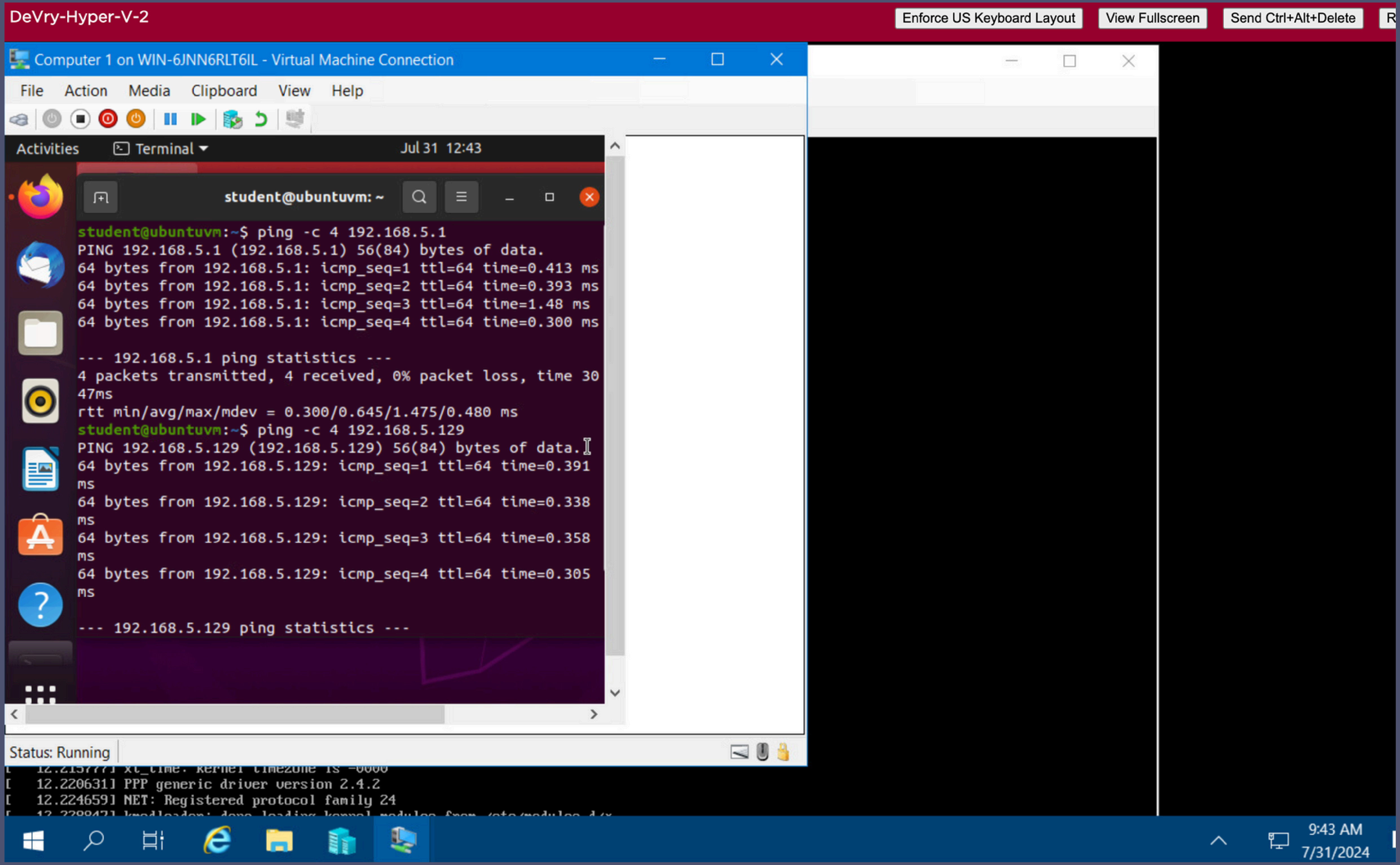
LOOPBACK2
eth0

Protocol: Static address
Uptime: 0h 6m 25s
MAC: 00:15:5D:00:BA:01
RX: 5.98 MB (63579 Pkts.)
TX: 8.19 MB (63169 Pkts.)
IPv4: 192.168.5.129/25

THIS SCREENSHOT SHOWS TWO SUCCESSFUL PING TESTS:

FROM THE COMPUTER 1 VM TO THE LOOPBACK 1 INTERFACE

FROM THE COMPUTER 1 VM TO THE LOOPBACK 2 INTERFACE



```
student@ubuntuvm:~$ ping -c 4 192.168.5.1
PING 192.168.5.1 (192.168.5.1) 56(84) bytes of data.
64 bytes from 192.168.5.1: icmp_seq=1 ttl=64 time=0.413 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=64 time=0.393 ms
64 bytes from 192.168.5.1: icmp_seq=3 ttl=64 time=1.48 ms
64 bytes from 192.168.5.1: icmp_seq=4 ttl=64 time=0.300 ms

--- 192.168.5.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 30
47ms
rtt min/avg/max/mdev = 0.300/0.645/1.475/0.480 ms
student@ubuntuvm:~$ ping -c 4 192.168.5.129
PING 192.168.5.129 (192.168.5.129) 56(84) bytes of data.
64 bytes from 192.168.5.129: icmp_seq=1 ttl=64 time=0.391
ms
64 bytes from 192.168.5.129: icmp_seq=2 ttl=64 time=0.338
ms
64 bytes from 192.168.5.129: icmp_seq=3 ttl=64 time=0.358
ms
64 bytes from 192.168.5.129: icmp_seq=4 ttl=64 time=0.305
ms

--- 192.168.5.129 ping statistics ---
```

```
[    12.215777] xt_time: kernel timezone is -0000
[    12.220631] PPP generic driver version 2.4.2
[    12.224659] NET: Registered protocol family 24
```

NETW191 COURSE PROJECT

MODULE 5

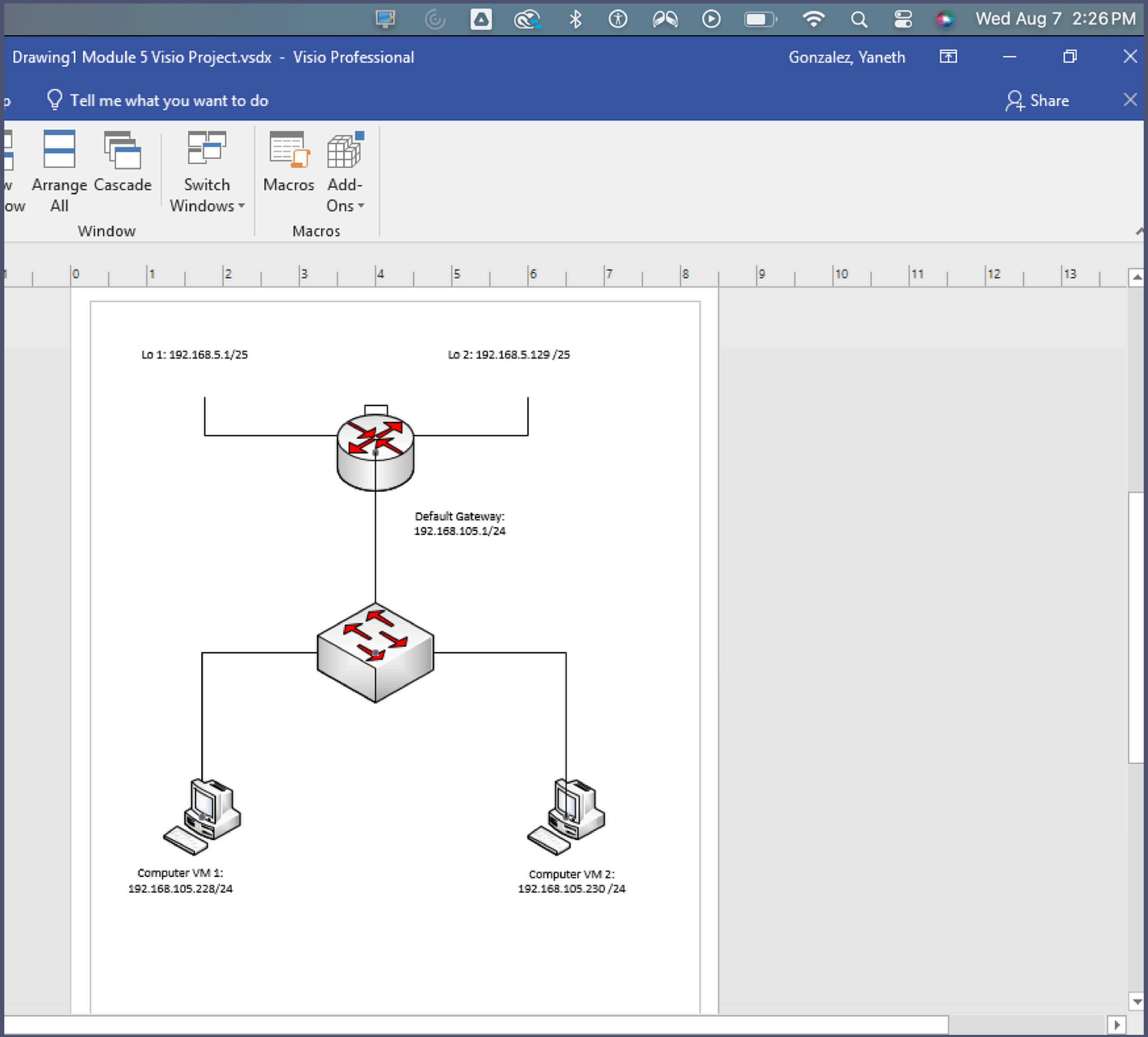
VISIO NETWORK DIAGRAM

IN THIS PROJECT, WE CREATED A NETWORK DIAGRAM USING MICROSOFT VISIO OR A SIMILAR TOOL.

WE STARTED BY DOWNLOADING AND INSTALLING MICROSOFT VISIO, FOLLOWING THE INSTRUCTIONS PROVIDED. FOR THOSE UNABLE TO INSTALL IT, WE USED THE WEB-BASED VERSION THROUGH VIRTUAL LAB CITRIX.

IN THE PROJECT, WE MADE A NETWORK DIAGRAM SHOWING HOW VIRTUAL MACHINES (VMS) CONNECT TO A ROUTER. WE INCLUDED ALL NECESSARY IP ADDRESSES AND LOOPBACK INTERFACES. THIS HELPED US UNDERSTAND HOW TO SET UP AND DOCUMENT A NETWORK ACCURATELY.

THIS DIAGRAM SHOULD ILLUSTRATE THE INTERCONNECTION OF THE COMPUTER 1 VM, THE COMPUTER 2 VM, AND THE SOHO ROUTER VM ALONG WITH PROPER IP ADDRESSES AND LABELING.



NETW191 COURSE PROJECT

MODULE 6

SOHO WIRELESS NETWORK SECURITY

IN THIS MODULE, WE EXPLORE KEY WAYS TO SECURE YOUR HOME OR SMALL OFFICE WIRELESS NETWORK. WE'LL START BY DISCUSSING WHY IT'S IMPORTANT TO CHANGE THE DEFAULT ROUTER USERNAME AND PASSWORD, WHICH ARE OFTEN EASY TO GUESS.

- NEXT, WE'LL LOOK AT THE BENEFITS OF USING STATIC IP ADDRESSES FOR BETTER CONTROL OF YOUR NETWORK. WE'LL ALSO COVER HOW MAC FILTERING HELPS YOU MANAGE WHICH DEVICES CAN CONNECT.

- ADDITIONALLY, WE'LL EXPLAIN THE IMPORTANCE OF USING STRONG ENCRYPTION LIKE WPA2 WITH AES.

- FINALLY, WE'LL TOUCH ON EXTRA SECURITY STEPS LIKE SETTING UP A GUEST NETWORK, USING VLANS, AND ADDING A VPN FOR PRIVACY.

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: ADMIN AND **PASSWORD:** ADMIN. THE PASSWORD IS TOO WEAK AND NOT STRONG, IT CAN ALSO BE SEARCHED ON THE INTERNET TO IDENTIFY THE DEFAULT USERNAME PLUS THE PASSWORD. NOT SECURE ENOUGH AND NOTICEABLE FOR EVERYONE TO SEE IT.

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:

IT'S CRITICAL FOR A SMALL NETWORK TO USE AN STATIC IP MANAGEMENT SINCE IT HAS MORE OVERHEAD AND NOT SCALABLE. IT ALSO ENSURES TO BE MORE SECURE AND UTILIZES LESS RESOURCES FOR DYNAMICALLY LEASING ADDRESSES.

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:

DENY: USE THIS TO BLOCK SPECIFIC DEVICES FROM ACCESSING YOUR WIRELESS NETWORK.
ALLOW: USE THIS WHEN YOU ONLY WANT SPECIFIC, KNOWN DEVICES TO CONNECT TO YOUR NETWORK.
ALSO IF DENY LIST IS EMPTY, IT WILL BE ACCESSIBLE TO EVERYONE
ALLOW THE STATIONS SPECIFIED BY ANY ENABLED ENTRIES IN THE LIST TO ACCESS FOR FILTERING RULES, AND THERE ARE NOT ANY ENABLE ENTRIES IN THE LIST, THUS, NO WIRELESS STATIONS CAN ACCESS THE AP.

4. WHAT WIRELESS SECURITY SETTINGS ARE DISPLAYED ON THE WIRELESS SECURITY PAGE? WHICH ONE IS RECOMMENDED BY THE VENDOR? WHY?

ANSWER:

DISABLE WIRELESS SECURITY - WPA/WPA2 - PERSONAL - SELECT WPA BASED ON PRE-SHARED PASSPHRASE.
WPA/WPA2 - ENTERPRISE - SELECT WPA BASED ON RADIUS SERVER.
WEP - SELECT 802.11 WEP SECURITY.

FOR NETWORK SECURITY, IT IS STRONGLY RECOMMENDED TO ENABLE WIRELESS SECURITY AND SELECT WPA2-PSK AES ENCRYPTION.
WPA2-PSK AES ENCRYPTION
WPA2 WITH AES IS THE STRONGEST OF ALL

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:

I RECOMMEND USING ALL THE SECURITY MEASURES TOGETHER AS PART OF A LAYERED DEFENSE STRATEGY.

USERNAME + PASSWORD: THIS IS A "WHAT YOU KNOW" SECURITY MEASURE FOR ACCESSING THE MANAGEMENT CONSOLE (ADMIN).

MAC FILTERING: THIS CONTROLS ACCESS BASED ON WHAT DEVICES YOU HAVE.

ENCRYPTED KEY: THIS PROTECTS YOUR DATA BY HIDING IT FROM NETWORK SNIFFING (ANOTHER FORM OF SOMETHING YOU KNOW).

6. WHAT WOULD YOU DO TO PROTECT YOUR WIRELESS NETWORK AT HOME? WHY?

ANSWER:

TO PROTECT MY HOME WIRELESS NETWORK, I WOULD DO THE FOLLOWING:

GUEST NETWORK: I'D CREATE A SEPARATE NETWORK FOR VISITORS, SO THEY CAN'T ACCESS MY PERSONAL DEVICES AND DATA.

VLAN: I'D ORGANIZE MY NETWORK INTO DIFFERENT SECTIONS, KEEPING THINGS LIKE SMART DEVICES SEPARATE FROM MY MAIN DEVICES, MAKING IT HARDER FOR ANY THREATS TO SPREAD.

VPN: I'D USE A VPN TO ENCRYPT MY INTERNET ACTIVITY, KEEPING MY ONLINE ACTIONS PRIVATE AND SECURE.

REGULARLY UPDATE FIRMWARE: KEEPING THE ROUTER'S FIRMWARE UP TO DATE ENSURES THAT I HAVE THE LATEST SECURITY PATCHES AND PROTECTIONS AGAINST KNOWN VULNERABILITIES. REGULAR UPDATES HELP SAFEGUARD THE NETWORK FROM POTENTIAL THREATS.

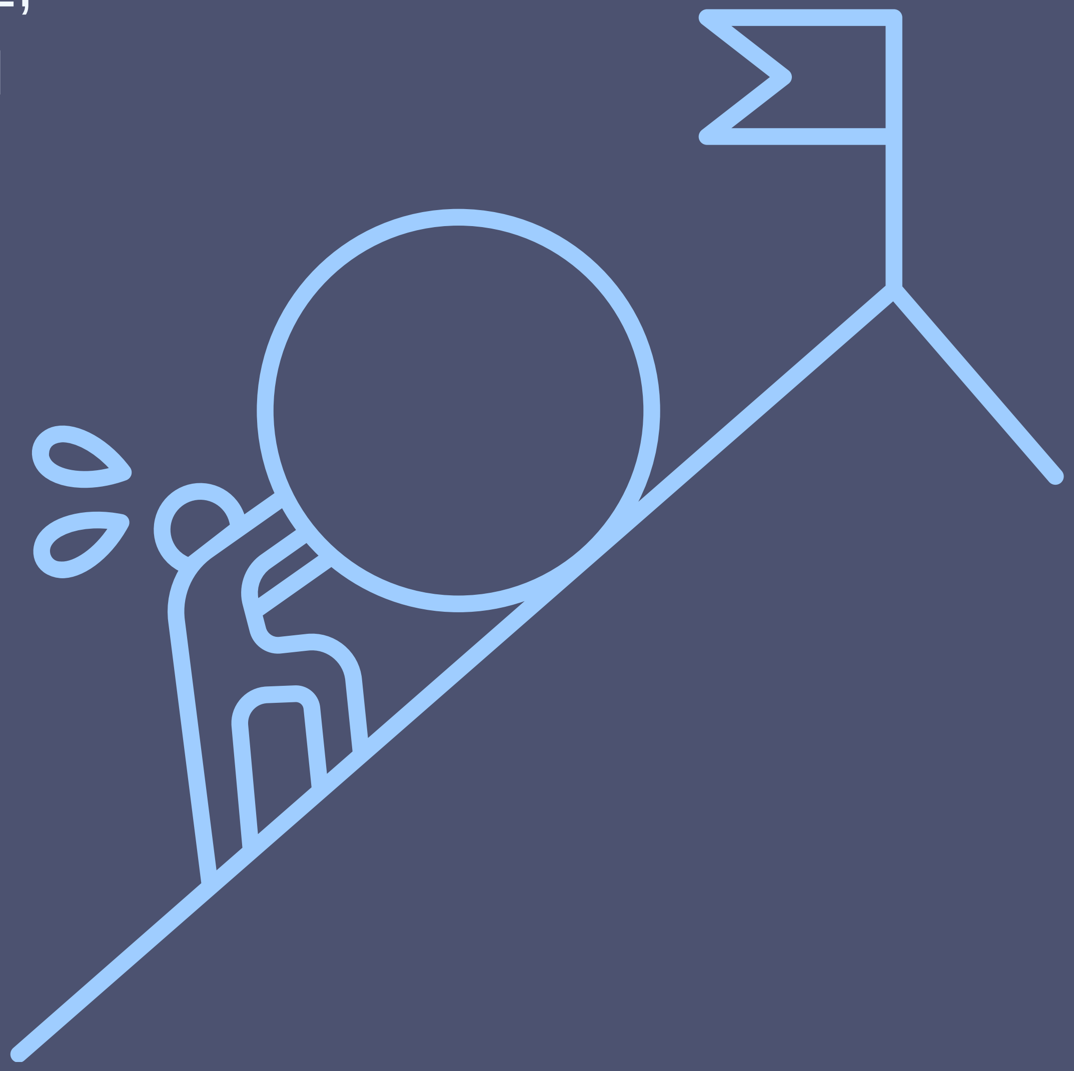
CHALLENGES

DURING THE COURSE, I FACED SEVERAL CHALLENGES THAT TAUGHT ME A LOT.
ONE CHALLENGE WAS CHANGING THE DEFAULT GATEWAY. RECONFIGURING THE DEFAULT GATEWAY IP ADDRESS AND MAKING SURE I FOLLOWED THE CORRECT STEPS WAS TRICKY.

ANOTHER CHALLENGE WAS RESETTING DEVICES. IF I MADE A MISTAKE, I HAD TO RESET THE DEVICES, WHICH TOOK TIME AND SLOWED DOWN THE PROCESS.

TYPING MANUAL COMMANDS IN THE TERMINAL WAS ALSO CHALLENGING. I HAD TO BE VERY CAREFUL TO TYPE EVERYTHING ACCURATELY, AS EVEN SMALL ERRORS COULD CAUSE PROBLEMS WITH THE CONFIGURATION.

DESPITE THESE CHALLENGES, EACH ONE HELPED ME IMPROVE MY SKILLS AND BECOME MORE CONFIDENT IN HANDLING NETWORK TASKS.



CAREER SKILL

THROUGHOUT THIS COURSE, I DEVELOPED SEVERAL IMPORTANT CAREER SKILLS:

NETWORK CONFIGURATION: I GAINED HANDS-ON EXPERIENCE IN CONFIGURING IPV4 ADDRESSES ON BOTH ROUTERS AND LINUX SYSTEMS. THIS PRACTICAL KNOWLEDGE IS ESSENTIAL FOR SETTING UP AND MANAGING NETWORKS.

PROBLEM-SOLVING: WHEN CONFIGURATIONS DIDN’T WORK AS EXPECTED, I LEARNED HOW TO TROUBLESHOOT EFFECTIVELY. THIS SKILL IS CRUCIAL FOR IDENTIFYING AND FIXING ISSUES IN REAL-WORLD NETWORK SETUPS.

ATTENTION TO DETAIL: I REALIZED THE IMPORTANCE OF FOLLOWING PRECISE STEPS AND CAPTURING ALL NECESSARY INFORMATION ACCURATELY. THIS ATTENTION TO DETAIL ENSURES THAT CONFIGURATIONS ARE DONE CORRECTLY AND HELPS PREVENT ERRORS.

TECHNICAL DOCUMENTATION: I LEARNED HOW TO DOCUMENT TECHNICAL STEPS AND OUTCOMES EFFECTIVELY. GOOD DOCUMENTATION IS KEY FOR FUTURE REFERENCE, TROUBLESHOOTING, AND ASSESSMENTS.

CONCLUSION

TO WRAP UP, THE FUNDAMENTALS OF TECHNOLOGY AND NETWORKING COURSE HAS GIVEN ME A SOLID UNDERSTANDING OF IMPORTANT NETWORKING CONCEPTS, ESPECIALLY IN SETTING UP AND MANAGING IPV4 ADDRESSES.

THROUGH HANDS-ON PROJECTS, I'VE LEARNED NOT ONLY THE TECHNICAL SKILLS BUT ALSO HOW CRUCIAL IT IS TO CAREFULLY SET UP, DOCUMENT, AND TROUBLESHOOT NETWORKS TO KEEP THEM RUNNING SMOOTHLY.

THIS COURSE HAS PREPARED ME TO HANDLE REAL-WORLD NETWORKING TASKS WITH MORE CONFIDENCE. I'M NOW READY TO APPLY THESE SKILLS IN FUTURE PROJECTS AND IN MY CAREER, HELPING TO BUILD AND MAINTAIN NETWORKS THAT ARE BOTH EFFICIENT AND SECURE.

THANK YOU FOR YOUR TIME, AND I'M EXCITED TO CONTINUE USING WHAT I'VE LEARNED.

Reference

(2022, JULY 2). NETW191 INFOSEC MODULE 2 PROJECT- JULY 2ND 2022, 4:25:47 PM [VIDEO]. HTTPS://DEVRYU.INSTRUCTURE.COM/COURSES/111164/EXTERNAL_TOOLS/9

(2022, JULY 2). NETW191 INFOSEC MODULE 2 PROJECT- JULY 2ND 2022, 4:25:47 PM [VIDEO]. HTTPS://DEVRYU.INSTRUCTURE.COM/COURSES/111164/EXTERNAL_TOOLS/9

[ALEX LEUNG]. (2023, NOVEMBER 14). NETW191 M4 PROJECT [VIDEO]. HTTPS://DEVRYU.INSTRUCTURE.COM/COURSES/111164/EXTERNAL_TOOLS/9

[ALEX LEUNG]. (2023, JANUARY 26). NETW191 MODULE 5 PROJECT (INFO SEC) [VIDEO]. HTTPS://DEVRYU.INSTRUCTURE.COM/COURSES/111164/EXTERNAL_TOOLS/9

[ALEX LEUNG]. (2021, OCTOBER 22). NETW191 MODULE 6 PROJECT- OCTOBER 22ND 2021, [VIDEO]. HTTPS://DEVRYU.INSTRUCTURE.COM. HTTPS://DEVRYU.INSTRUCTURE.COM/COURSES/111164/EXTERNAL_TOOLS/9

O'SULLIVAN, F., & HENGES, K. (2024, APRIL 21). THE BEST VPN SERVICES OF 2024. HTTPS://WWW.HOWTOGEEK.COM. HTTPS://WWW.HOWTOGEEK.COM/738071/BEST-VPN-SERVICES/

SOURCE (N.D.). TP-LINK EMULATORS. HTTPS://WWW.TP-LINK.COM. HTTPS://WWW.TP-LINK.COM/US/SUPPORT/EMULATOR/

SOURCE (N.D.). HOW TO LOGIN TO YOUR TP-LINK ROUTER. HTTPS://WWW.ROUTERPASSWORDS.COM. HTTPS://WWW.ROUTERPASSWORDS.COM/TP-LINK-DEFAULT-ROUTER-PASSWORD/

THANK YOU!

Presentation by Yaneth Gonzalez