

Designing a Secure Network Topology (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 03

Student:

Vidhi Kadakia

Email:

jinsukrishna108@gmail.com

Time on Task:

11 hours, 58 minutes

Progress:

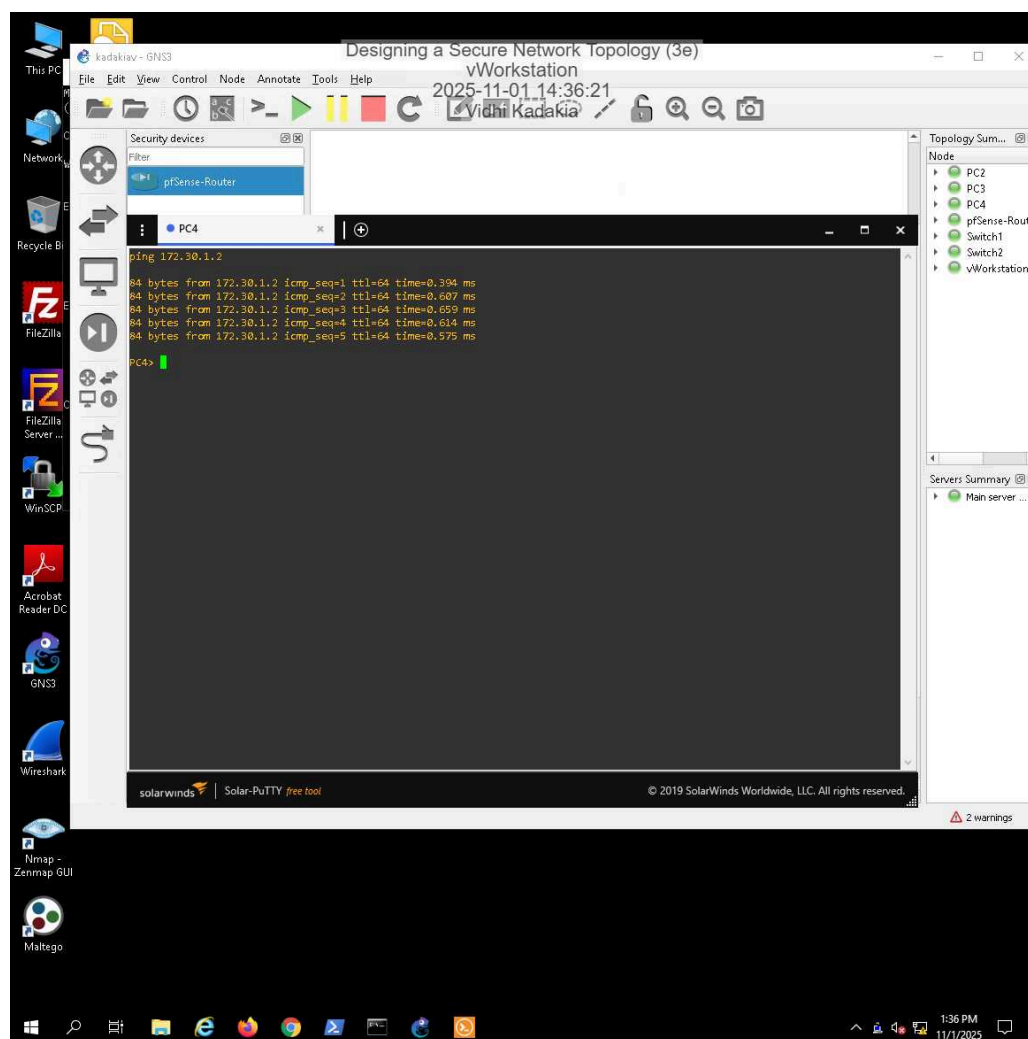
88%

Report Generated: Sunday, November 2, 2025 at 6:39 PM

Section 1: Hands-On Demonstration

Part 1: Design a Simple Network Topology

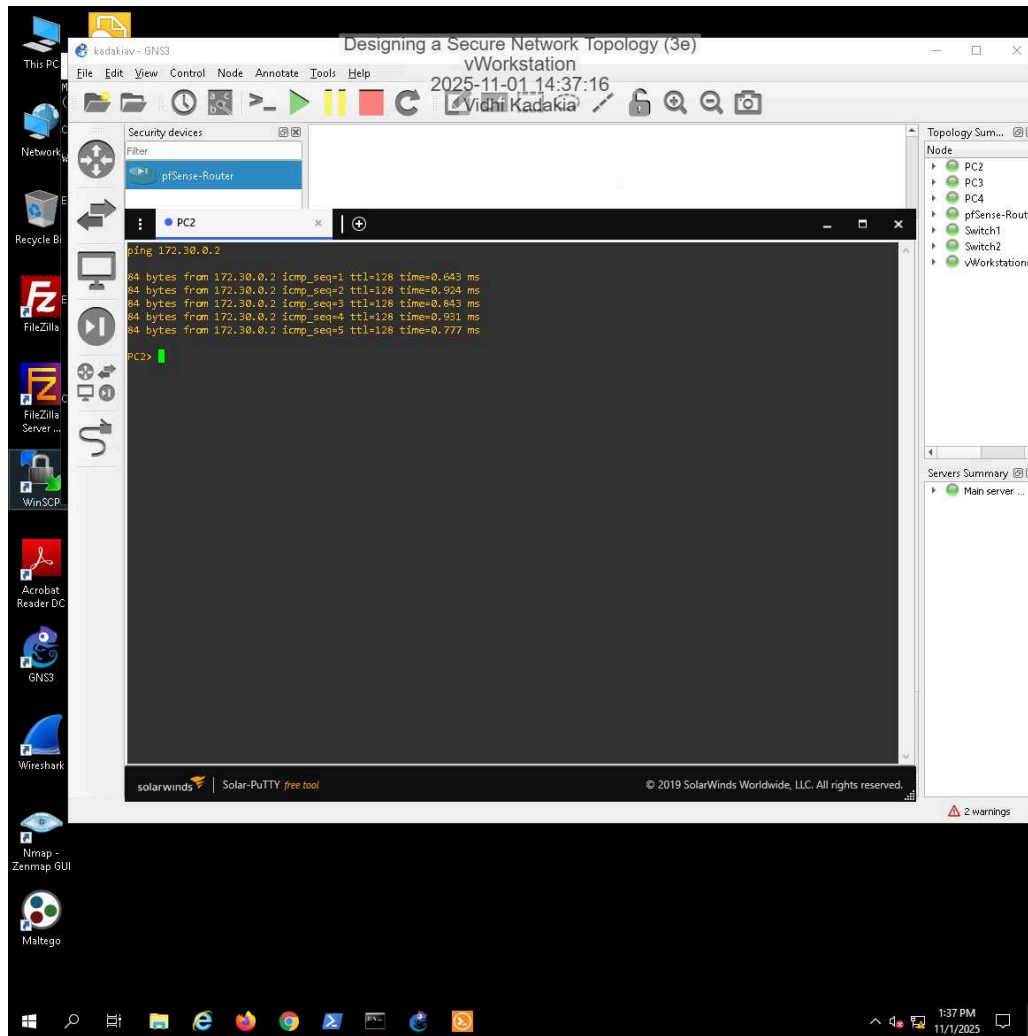
34. Make a screen capture showing the results of the ping attempt from PC4 to PC3.



Designing a Secure Network Topology (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 03

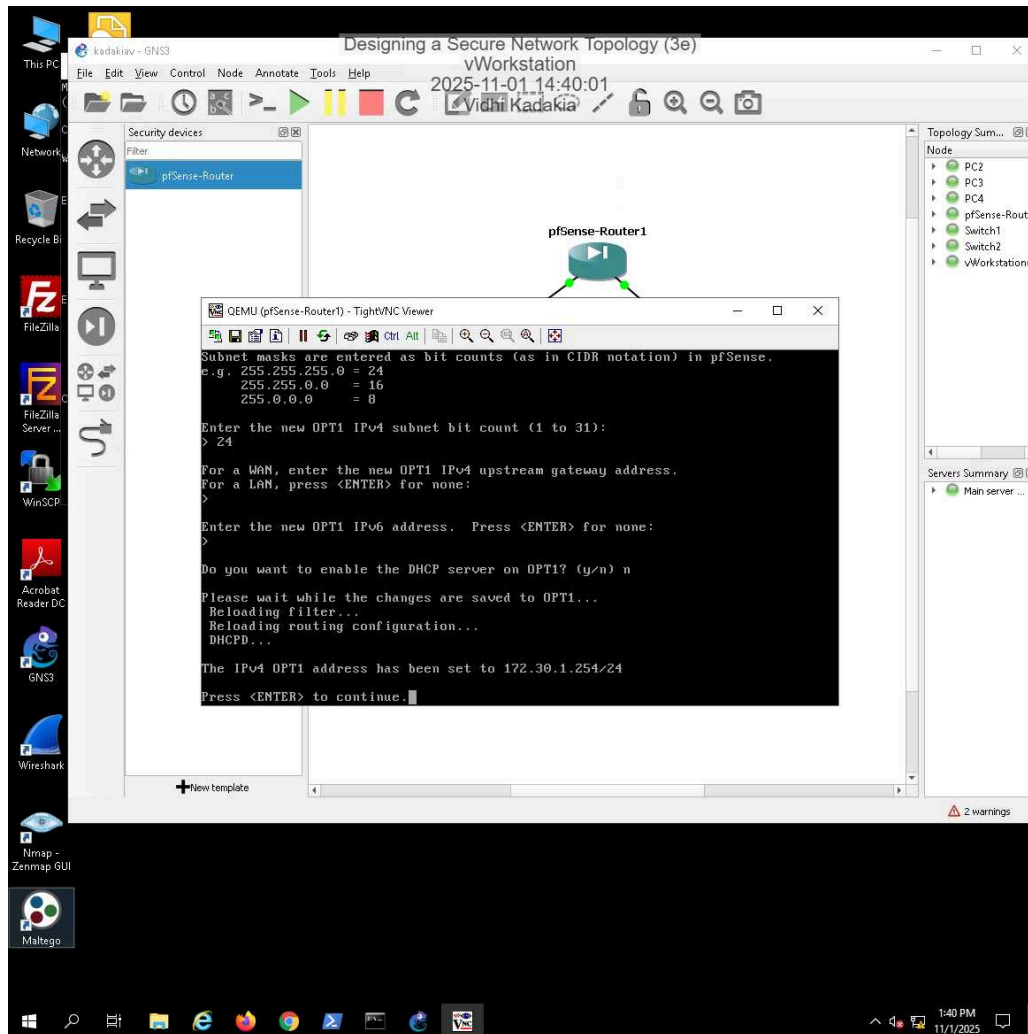
37. Make a screen capture showing the results of the ping attempt from PC2 to the vWorkstation (172.30.0.2).



Designing a Secure Network Topology (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 03

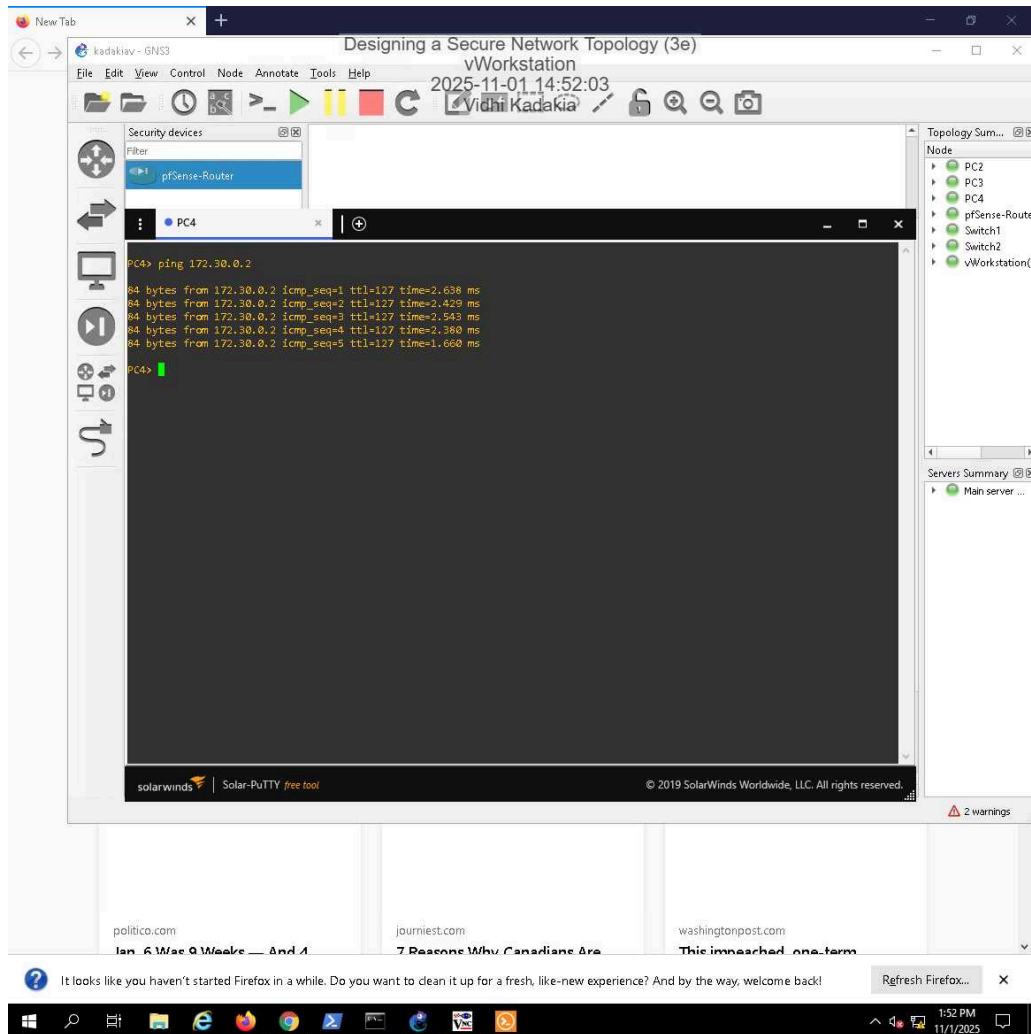
49. Make a screen capture showing the IP address assignments in the pfSense console.



Designing a Secure Network Topology (3e)

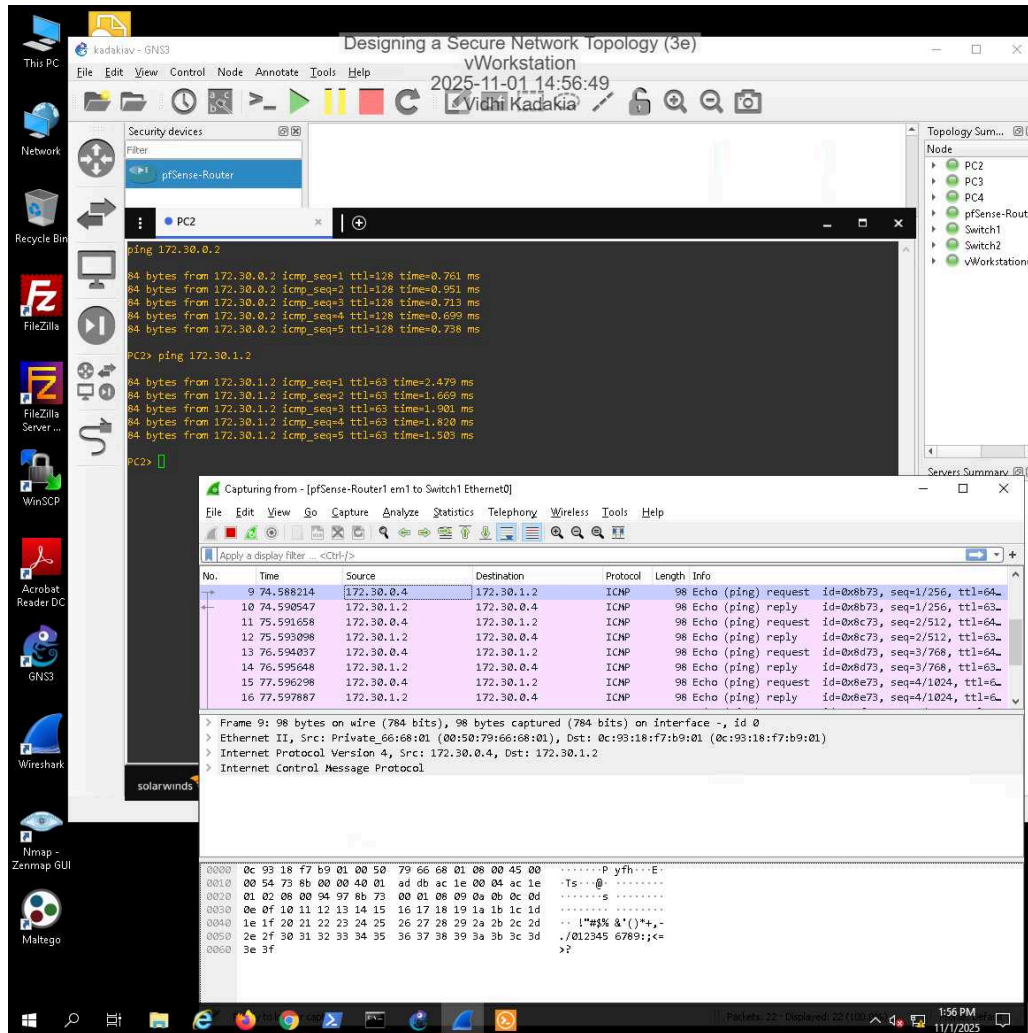
Network Security, Firewalls, and VPNs, Third Edition - Lab 03

72. Make a screen capture showing the **successful ping** from PC4 to the vWorkstation.



Part 2: Capture Network Traffic to Validate Connectivity

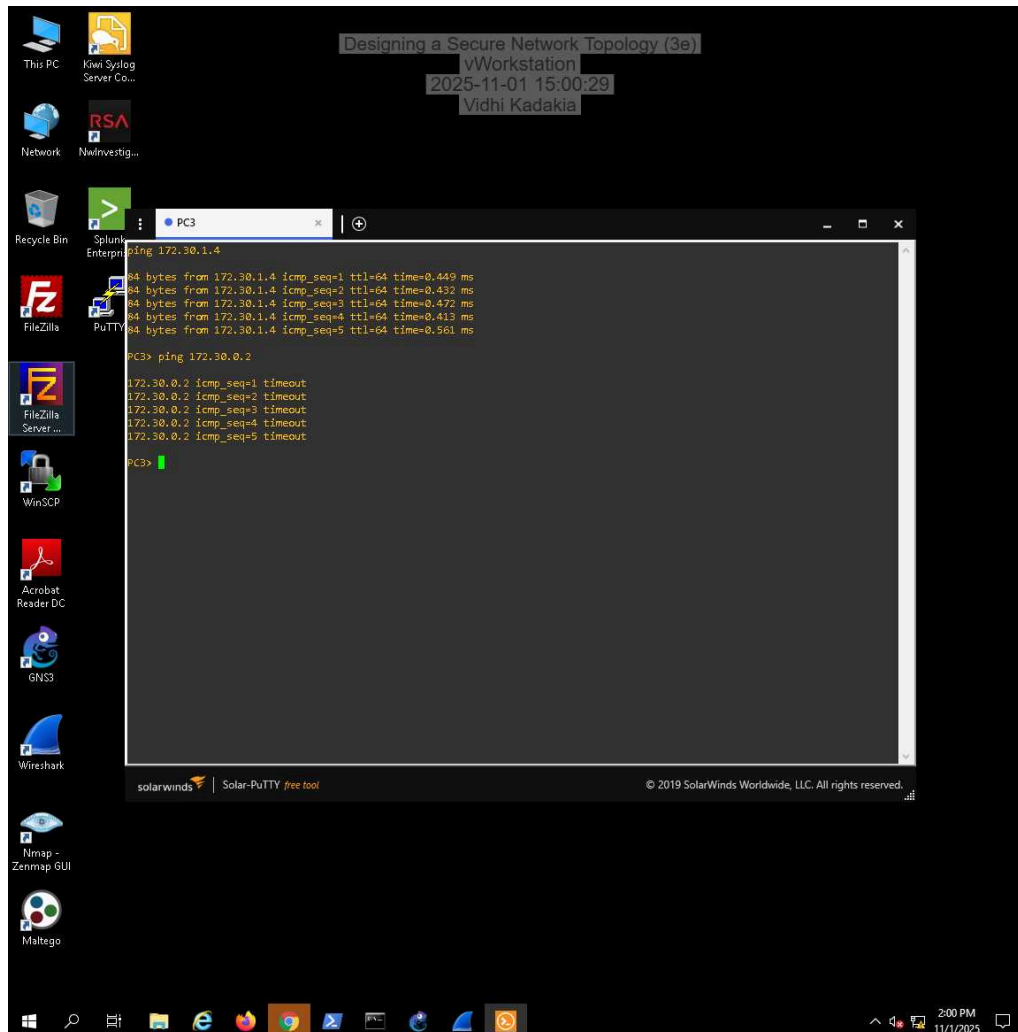
7. Make a screen capture showing the Wireshark capture for the PC2 to PC3 ping request.



Designing a Secure Network Topology (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 03

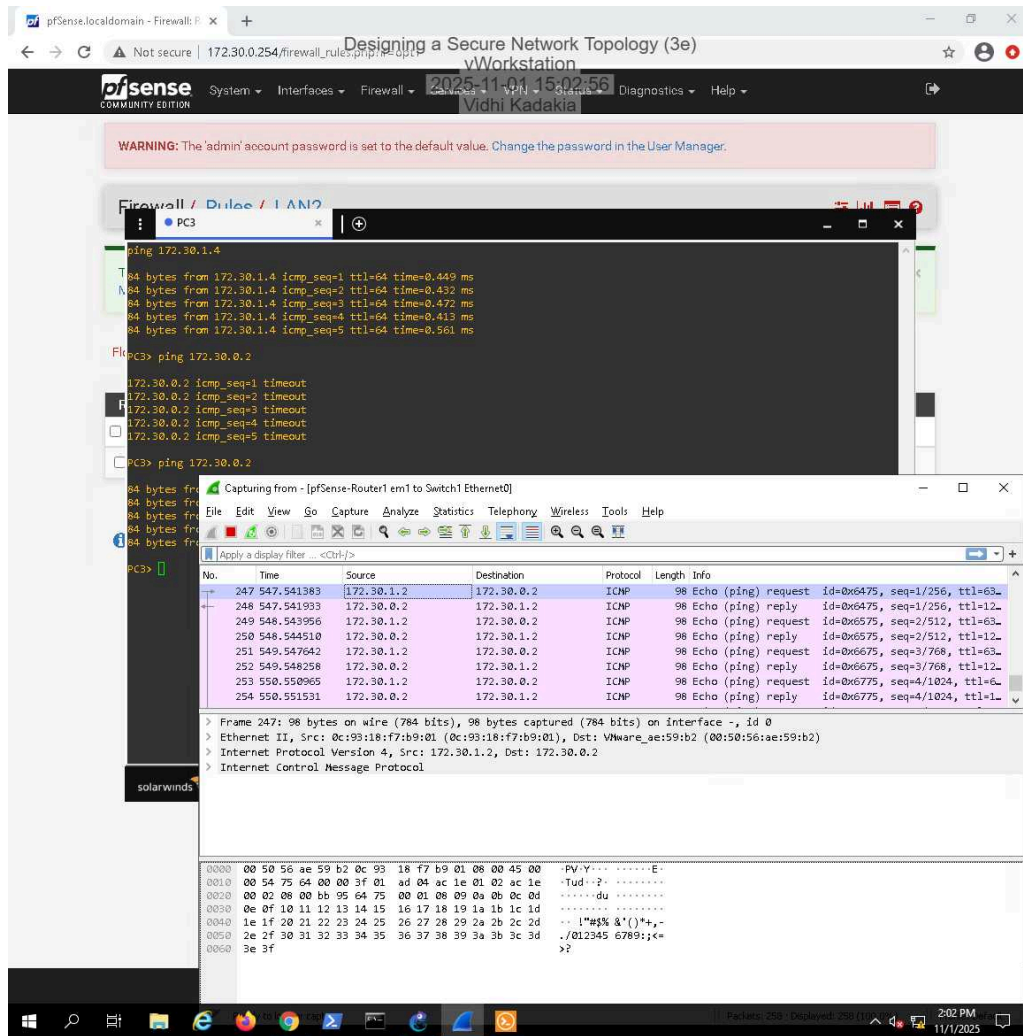
17. Make a screen capture showing the timed out ping request.



Designing a Secure Network Topology (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 03

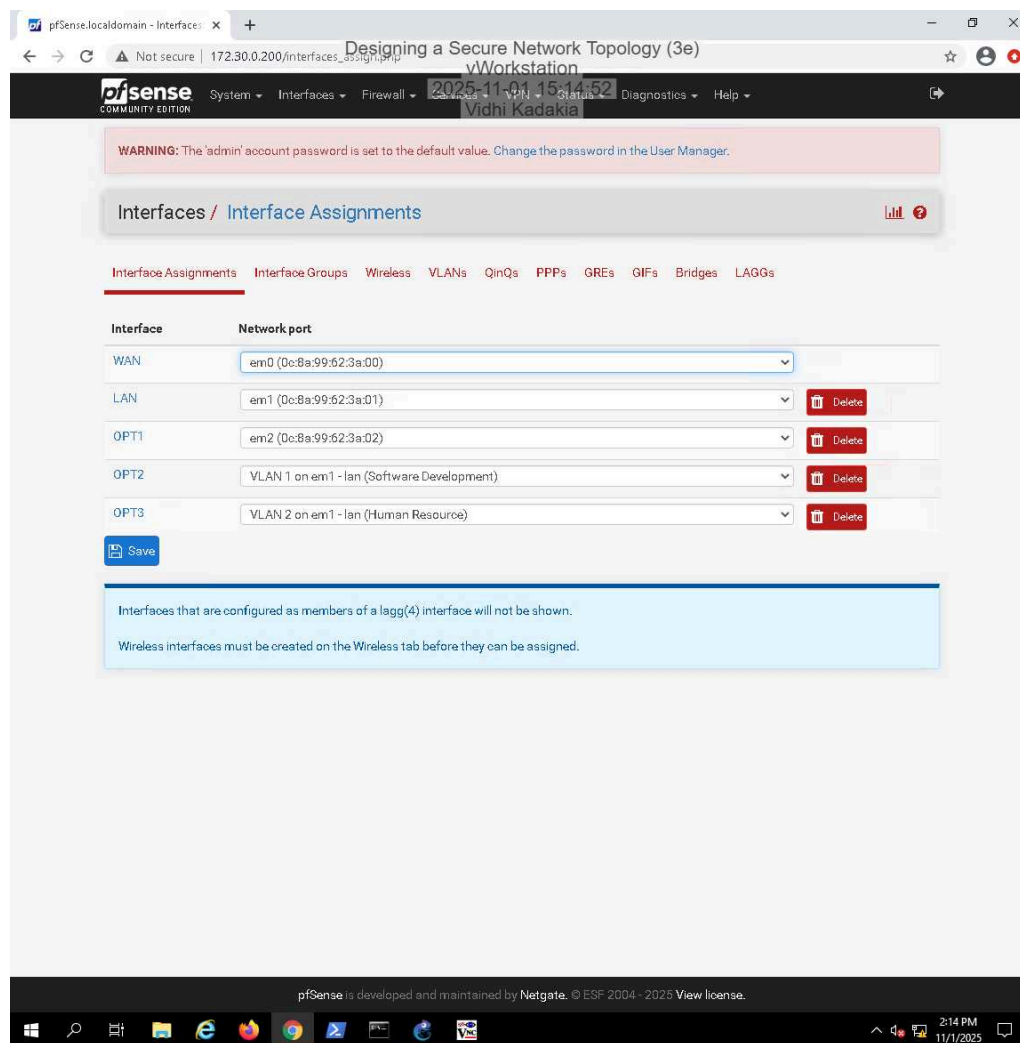
20. Make a screen capture showing the Wireshark capture for the PC3 to vWorkstation ping request.



Section 2: Applied Learning

Part 1: Design a More Complex Network Topology

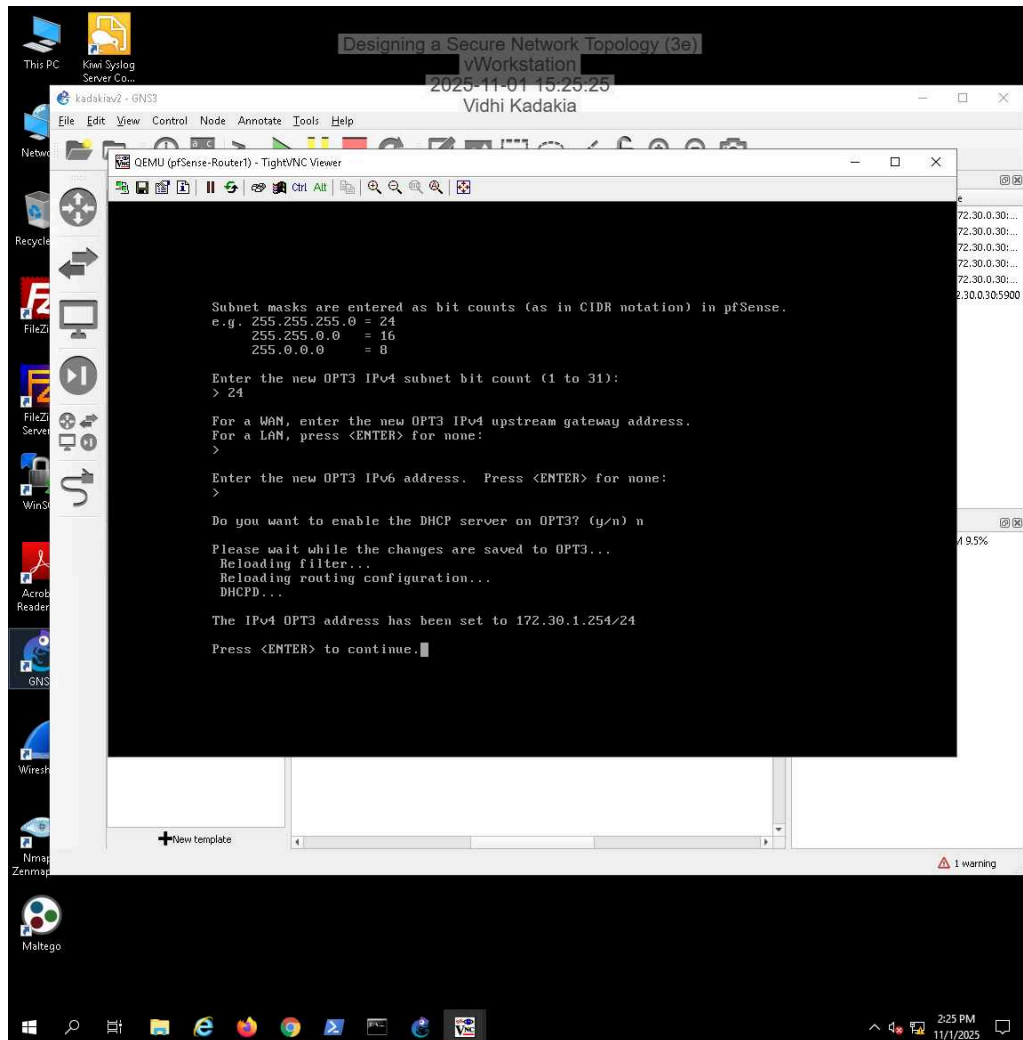
14. Make a screen capture showing the **Interface Assignments** page.



Designing a Secure Network Topology (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 03

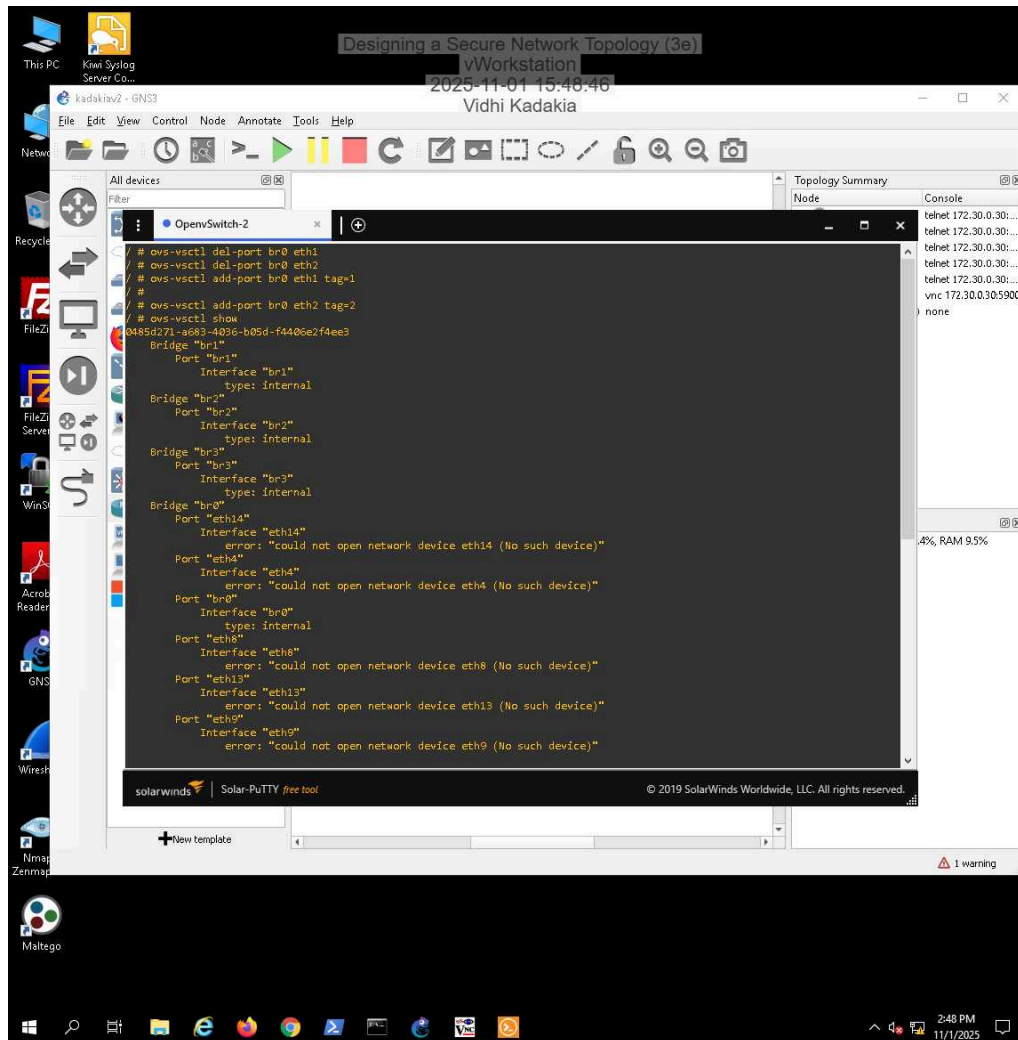
28. **Make a screen capture** showing the **updated pfSense router settings with the VLAN IP address assignments.**



Designing a Secure Network Topology (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 03

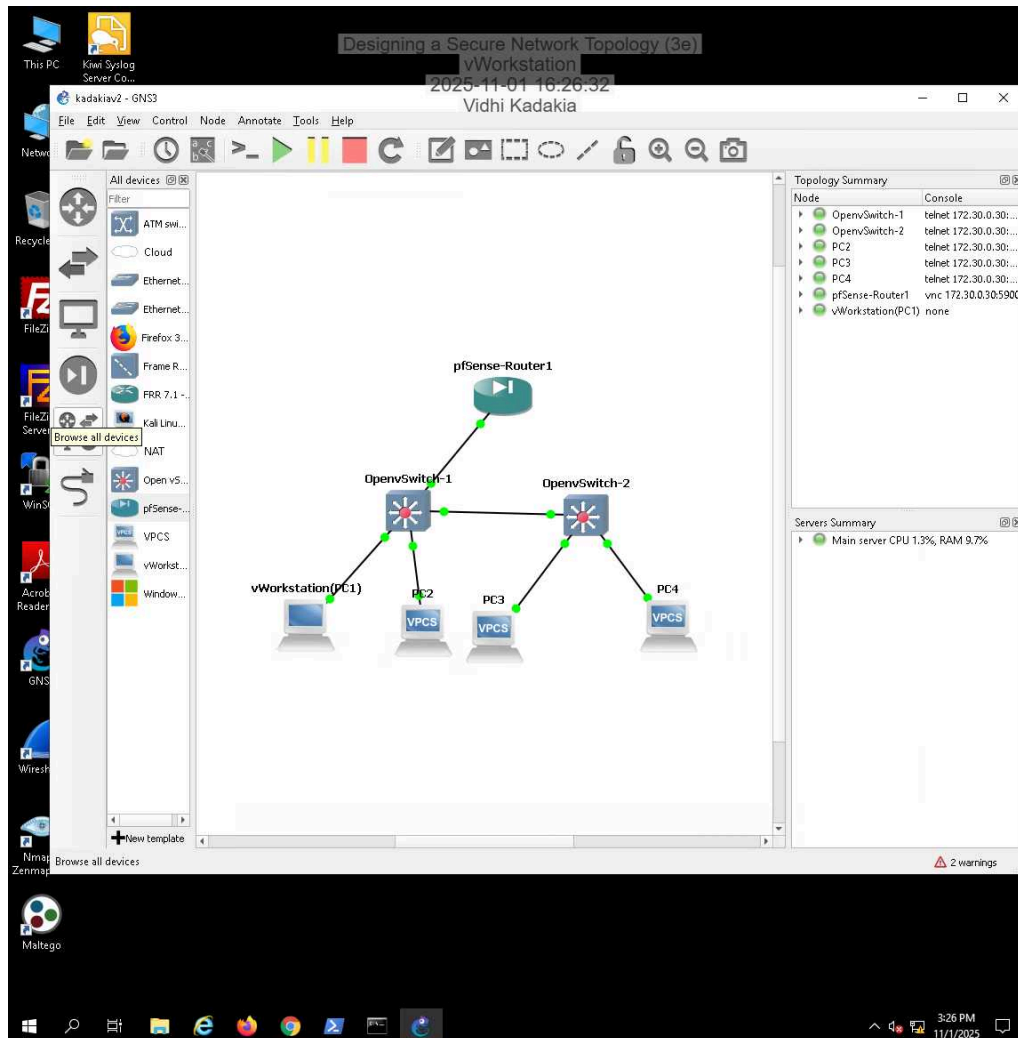
36. Make a screen capture showing the **eth1** and **eth2** interfaces with their assigned VLAN tags on Switch2.



Designing a Secure Network Topology (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 03

39. Make a screen capture showing the **completed topology**.



Part 2: Capture Network Traffic to Validate Connectivity

3. Make a screen capture showing the **Wireshark** capture for the vWorkstation to PC3 ping request.

Designing a Secure Network Topology (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 03

Capturing from - [pfSense-Router1 em1 to OpenvSwitch-1 eth0]

File Edit View Go Capture Analyze Settings Help

Designing a Secure Network Topology (3e)

Workstation

2025-11-01 19:01:36

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::b05a:a4ff:fe2f:91fa	ff02::2	ICMPv6	70	Router Solicitation from b2:5a:a4:2f:91:fa
2	6.144083	fe80::8a5:71ff:fe84::	ff02::2	ICMPv6	70	Router Solicitation from 0a:a5:71:84:61:4c
3	7.197953	172.30.0.2	172.30.0.255	BROWSER	259	Domain/Workgroup Announcement WORKGROUP, NT Workstation
4	8.191486	fe80::88ad:50ff:fe1::	ff02::2	ICMPv6	70	Router Solicitation from 8a:ad:50:17:b6:a8
5	12.292259	fe80::98e6:74ff:fe1::	ff02::2	ICMPv6	70	Router Solicitation from 9a:e6:74:f6:bb:44
6	14.879714	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
7	15.853325	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
8	16.852971	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
9	17.858517	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
10	18.852999	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
11	19.852837	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
12	20.857759	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
13	21.853078	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
14	22.853079	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
15	23.857875	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
16	24.852947	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
17	25.852928	VNware_ae:6d:7d	Broadcast	ARP	64	Who has 172.30.0.4? Tell 172.30.0.2
18	56.278430	fe80::20c:29ff:fe8f::	ff02::2	ICMPv6	74	Router Solicitation from 00:0c:29:8f:27:d7

> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface -, id 0
> Ethernet II, Src: b2:5a:a4:2f:91:fa (b2:5a:a4:2f:91:fa), Dst: IPv6mcast_02 (33:33:00:00:00:02)
> Internet Protocol Version 6, Src: fe80::b05a:a4ff:fe2f:91fa, Dst: ff02::2
> Internet Control Message Protocol v6

0000 33 33 00 00 00 02 b2 5a a4 2f 91 fa 86 dd 00 00 33Z ./...
0010 00 00 00 10 3a ff fe 80 00 00 00 00 00 b0 5a ..:.....Z
0020 a4 ff fe 2f 91 fa ff 02 00 00 00 00 00 00 00 .../.....
0030 00 00 00 00 00 02 85 00 ae 24 00 00 00 00 01 01\$.
0040 b2 5a a4 2f 91 faZ./..

Frame (frame), 70 bytes

Packets: 18 · Displayed: 18 (100.0%)

Profile: Default

Wireshark

Nmap - Zenmap GUI

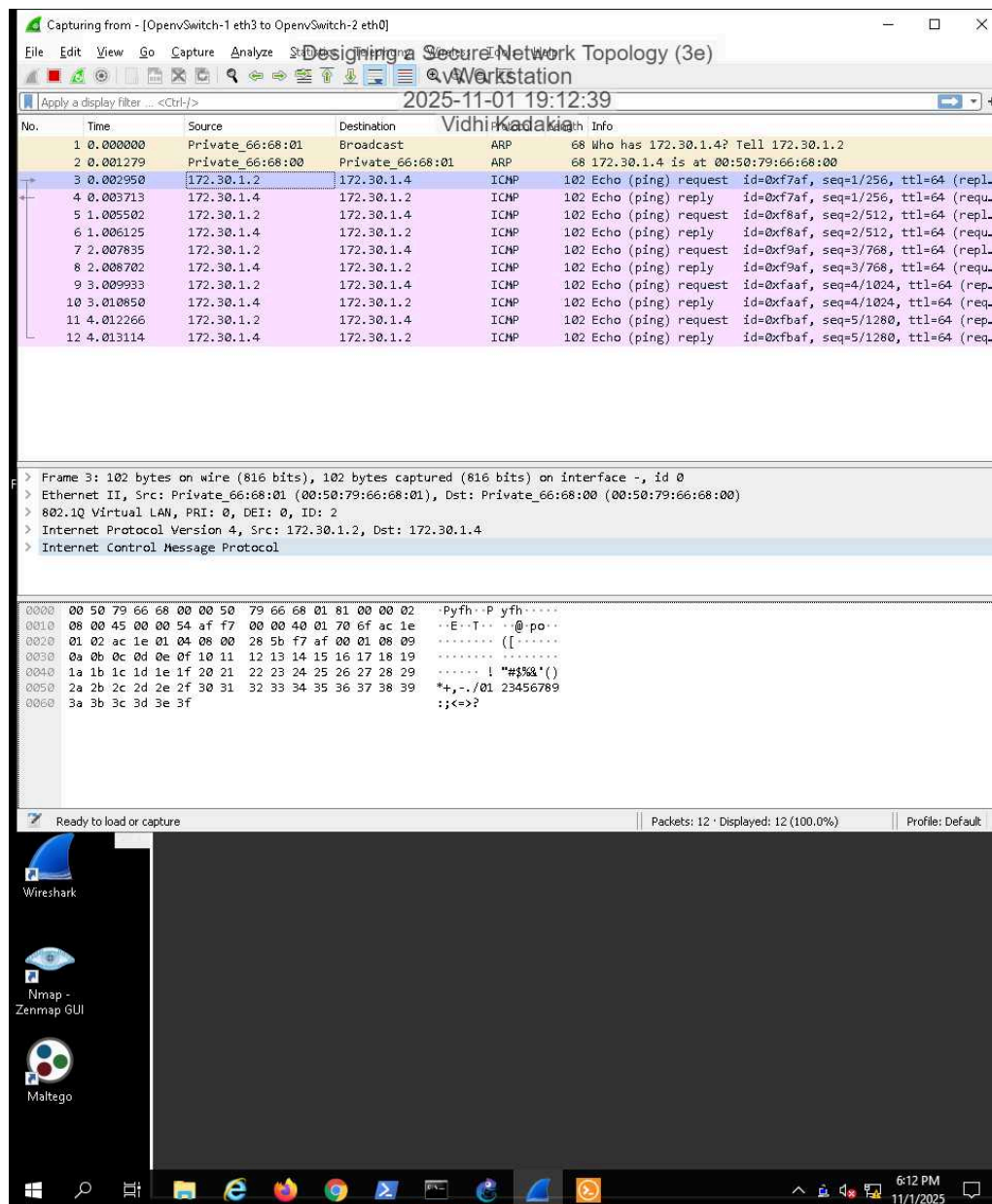
Maltego

6:01 PM 11/1/2025

5. Make a screen capture showing the Wireshark capture for the PC2 to PC4 ping request.

Designing a Secure Network Topology (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 03



7. Make a screen capture showing the Wireshark capture for the vWorkstation to PC2 ping request.

Designing a Secure Network Topology (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 03

Designing a Secure Network Topology (3e)

2025-11-01 19:19:33

Vidhi Kadakia

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.30.0.2	172.30.0.255	BROWSER	259 Domain/Workgroup Announcement WORKGROUP, NT Workstati
2	13.585805	172.30.0.2	172.30.1.2	ICMP	78 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (-
3	13.587237	0c:8a:99:62:3a:01	Broadcast	ARP	46 Who has 172.30.1.2? Tell 172.30.1.254
4	13.588640	Private_66:68:01	0c:8a:99:62:3a:01	ARP	64 172.30.1.2 is at 00:50:79:66:68:01
5	13.589055	172.30.0.2	172.30.1.2	ICMP	78 Echo (ping) request id=0x0001, seq=5/1280, ttl=127 (-
6	13.589713	172.30.1.2	172.30.0.2	ICMP	78 Echo (ping) reply id=0x0001, seq=5/1280, ttl=64 (r-
7	13.589967	0c:8a:99:62:3a:01	Broadcast	ARP	42 Who has 172.30.0.2? Tell 172.30.0.200
8	18.155050	VMware_ae:6d:7d	0c:8a:99:62:3a:01	ARP	64 Who has 172.30.0.254? Tell 172.30.0.2
9	18.156072	0c:8a:99:62:3a:01	VMware_ae:6d:7d	ARP	46 172.30.0.254 is at 0c:8a:99:62:3a:01
10	18.170737	172.30.0.2	172.30.1.2	ICMP	78 Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (-
11	18.171512	172.30.0.2	172.30.1.2	ICMP	78 Echo (ping) request id=0x0001, seq=6/1536, ttl=127 (-
12	18.172161	172.30.1.2	172.30.0.2	ICMP	78 Echo (ping) reply id=0x0001, seq=6/1536, ttl=64 (r-
13	18.172690	0c:8a:99:62:3a:01	Broadcast	ARP	42 Who has 172.30.0.2? Tell 172.30.0.200
14	23.170704	172.30.0.2	172.30.1.2	ICMP	78 Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (-
15	23.171643	172.30.0.2	172.30.1.2	ICMP	78 Echo (ping) request id=0x0001, seq=7/1792, ttl=127 (-
16	23.172394	172.30.1.2	172.30.0.2	ICMP	78 Echo (ping) reply id=0x0001, seq=7/1792, ttl=64 (r-
17	23.173038	0c:8a:99:62:3a:01	Broadcast	ARP	42 Who has 172.30.0.2? Tell 172.30.0.200
18	28.170945	172.30.0.2	172.30.1.2	ICMP	78 Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (-
19	28.171885	172.30.0.2	172.30.1.2	ICMP	78 Echo (ping) request id=0x0001, seq=8/2048, ttl=127 (-
20	28.172855	172.30.1.2	172.30.0.2	ICMP	78 Echo (ping) reply id=0x0001, seq=8/2048, ttl=64 (r-
21	28.173365	0c:8a:99:62:3a:01	Broadcast	ARP	42 Who has 172.30.0.2? Tell 172.30.0.200
22	28.737220	fe80::88ad:50ff:fe1...	ff02::2	ICMPv6	70 Router Solicitation from 8a:ad:50:17:b6:a8
23	73.331000	172.30.0.2	172.30.0.255	NBNS	96 Name query NB WPAD<00>
24	73.355848	172.30.0.2	172.30.0.255	NBNS	96 Name query NB WPAD<00>
25	73.356225	172.30.0.2	224.0.0.251	MDNS	74 Standard query 0x0000 A wpad.local, "QN" question
26	73.356562	172.30.0.2	224.0.0.251	MDNS	74 Standard query 0x0000 A wpad.local, "QN" question
27	73.356831	172.30.0.2	224.0.0.252	LLMNR	68 Standard query 0x1836 A wpad
28	73.357245	172.30.0.2	224.0.0.252	LLMNR	68 Standard query 0x47ec A wpad
29	73.399647	172.30.0.2	239.255.255.250	SSDP	219 M-SEARCH * HTTP/1.1
30	73.808670	172.30.0.2	224.0.0.252	LLMNR	68 Standard query 0x47ec A wpad
31	73.810641	172.30.0.2	224.0.0.252	LLMNR	68 Standard query 0x1836 A wpad
32	74.089860	172.30.0.2	172.30.0.255	NBNS	96 Name query NB WPAD<00>
33	74.105903	172.30.0.2	172.30.0.255	NBNS	96 Name query NB WPAD<00>
34	74.356309	172.30.0.2	224.0.0.251	MDNS	74 Standard query 0x0000 A wpad.local, "QN" question
35	74.404712	172.30.0.2	239.255.255.250	SSDP	219 M-SEARCH * HTTP/1.1
36	74.844403	172.30.0.2	172.30.0.255	NBNS	96 Name query NB WPAD<00>

Frame 2: 78 bytes on wire (624 bits) 78 bytes captured (624 bits) on interface - id 0

wireshark_-_20251101181529_a05784.pcapng

Packets: 101 · Displayed: 101 (100.0%) Profile: Default

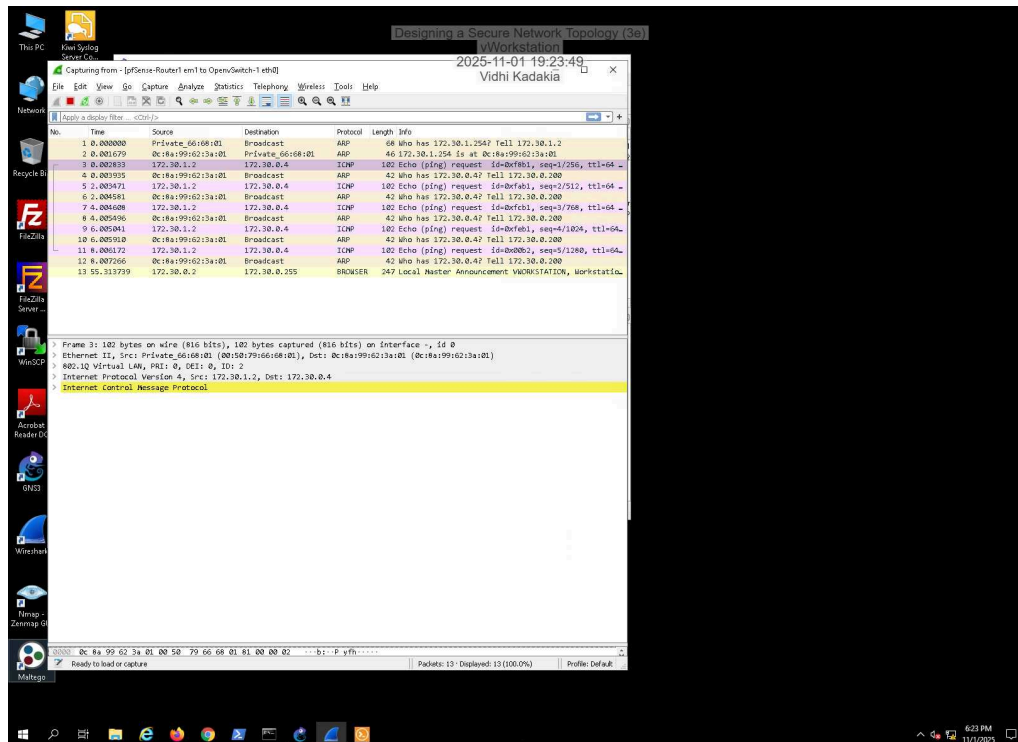
Wireshark

Nmap - Zenmap GUI

Maltego

6:19 PM 11/1/2025

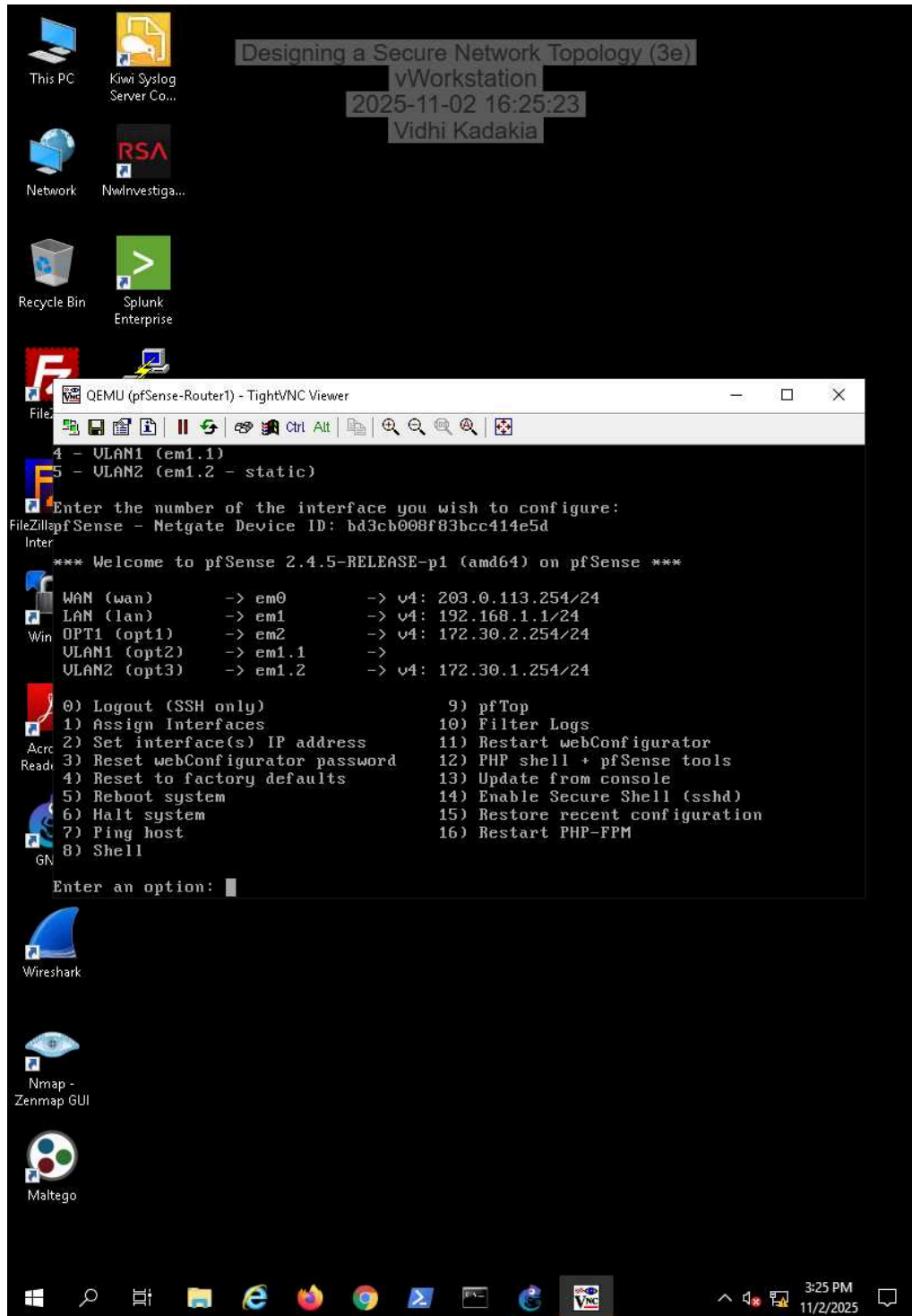
9. Make a screen capture showing the Wireshark capture for the PC2 to PC3 ping request.



Section 3: Challenge and Analysis

Part 1: Enhance the Network Topology with a DMZ

Make a screen capture showing the interface configurations in the pfSense console.



Make a screen capture showing the **firewall rule on the WAN interface in the pfSense webConfigurator**.

Incomplete

Part 2: Validate DMZ Connectivity

Make a screen capture showing the **results of both pings**.

Incomplete