

Designing a Secure Network Topology (4e)

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

Student:

Shoumya Rayamajhi

Email:

sxr230169@utdallas.edu

Time on Task:

3 hours, 4 minutes

Progress:

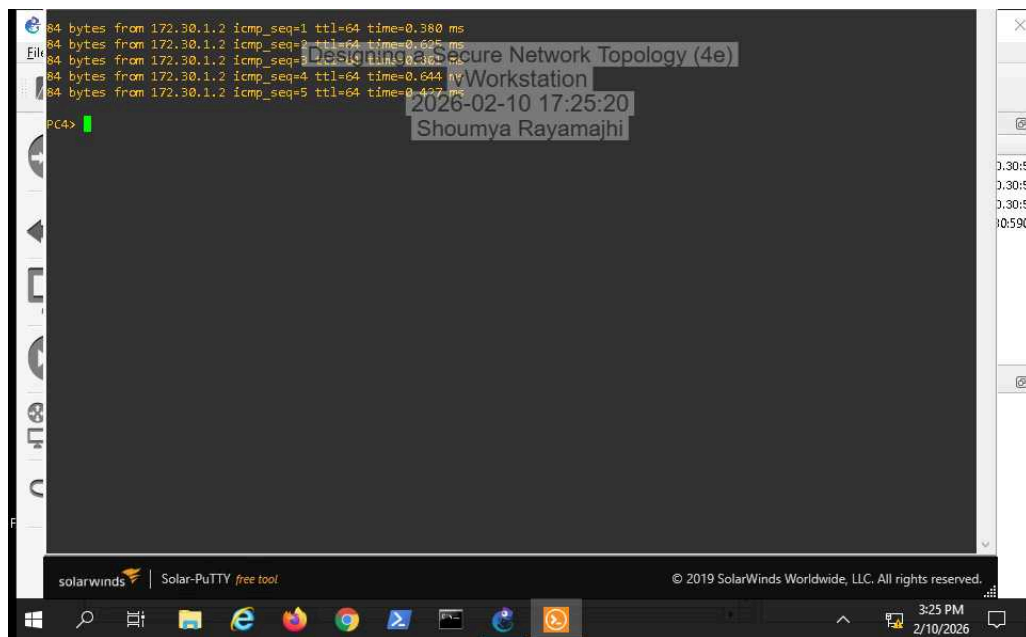
100%

Report Generated: Sunday, February 22, 2026 at 12:35 AM

Hands-On Demonstration

Part 1: Design a Simple Network Topology

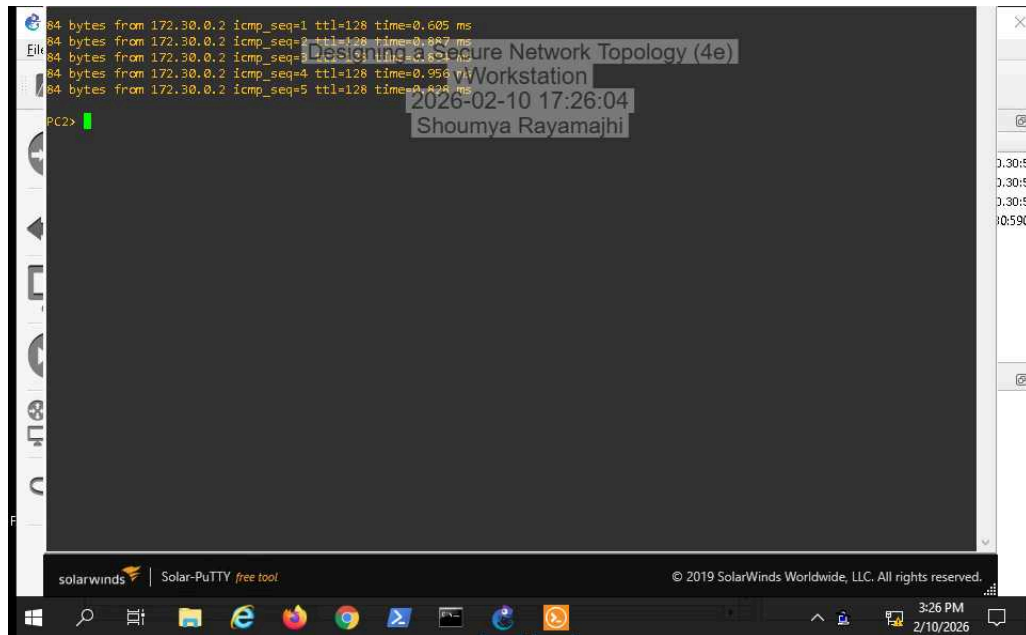
34. Make a screen capture showing the results of the ping attempt from PC4 to PC3.



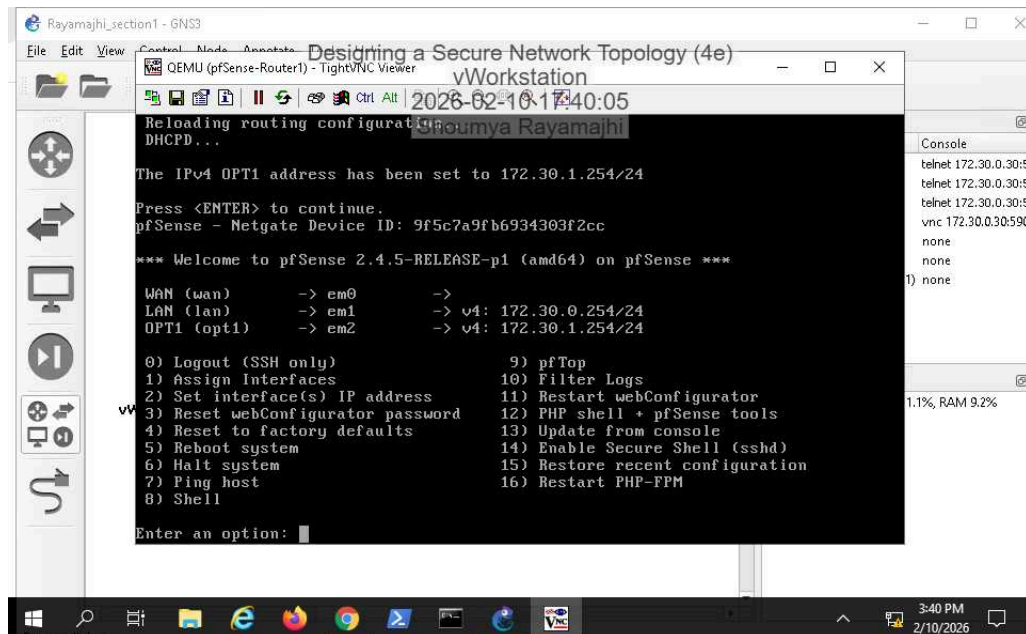
Designing a Secure Network Topology (4e)

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

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



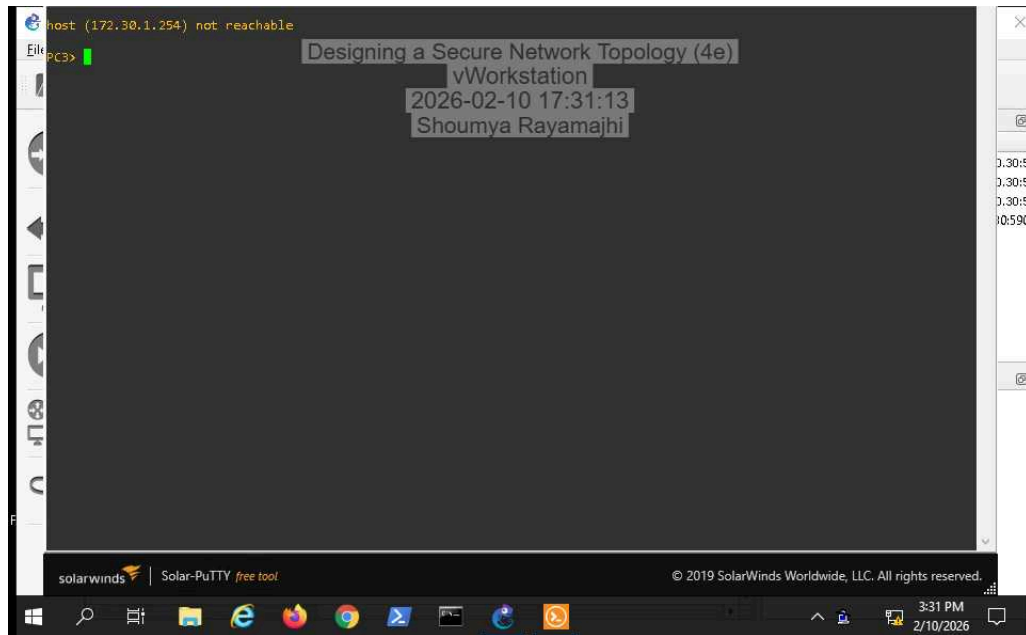
49. Make a screen capture showing the IP address assignments in the pfSense console.



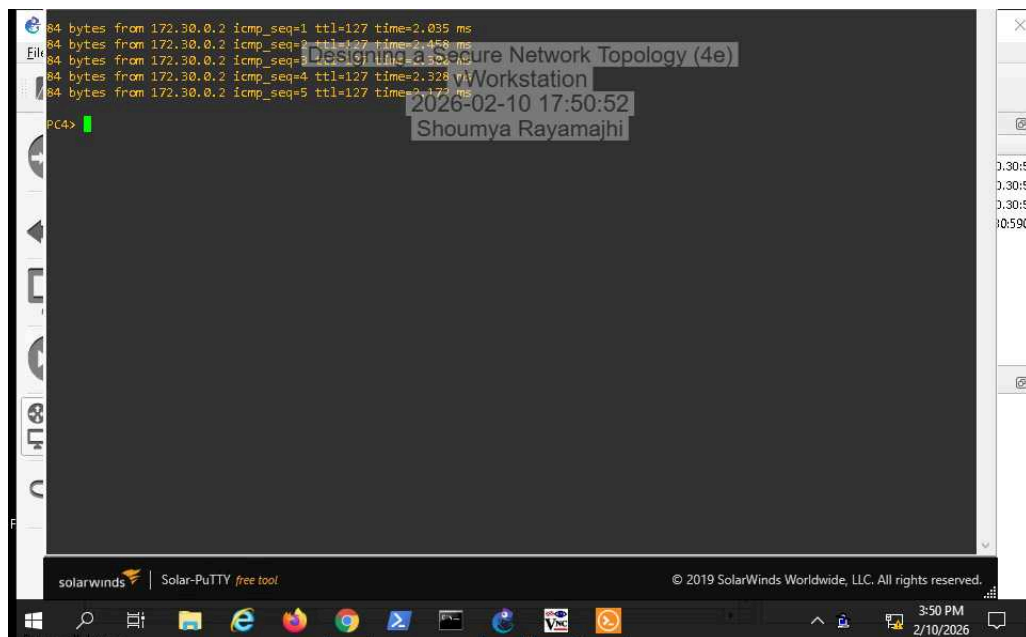
Designing a Secure Network Topology (4e)

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

53. Make a screen capture showing the **ICMP timeout message**.



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

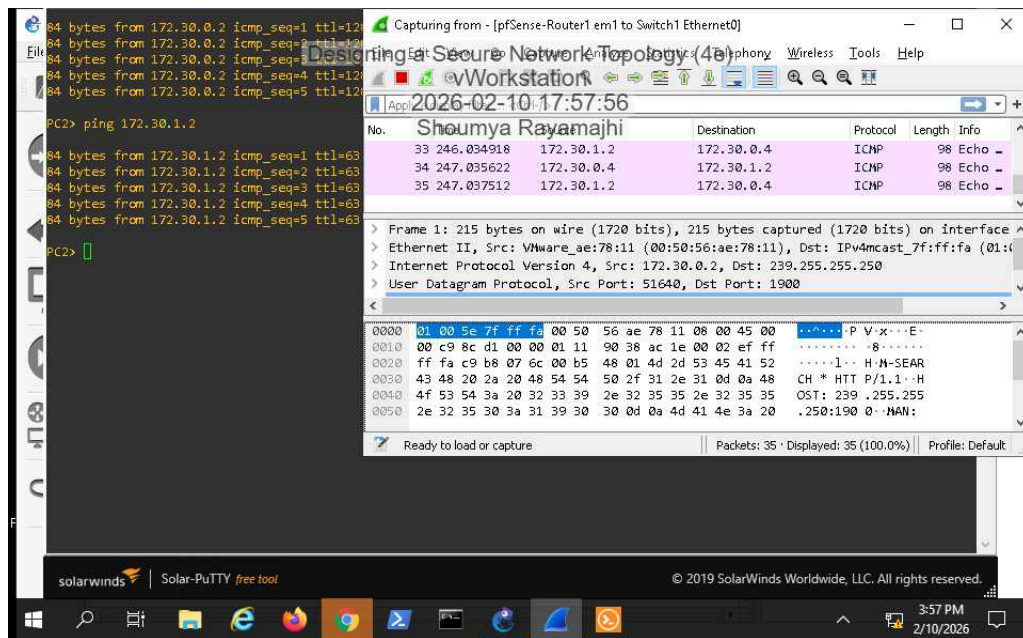


Part 2: Capture the Network Traffic to Validate Connectivity

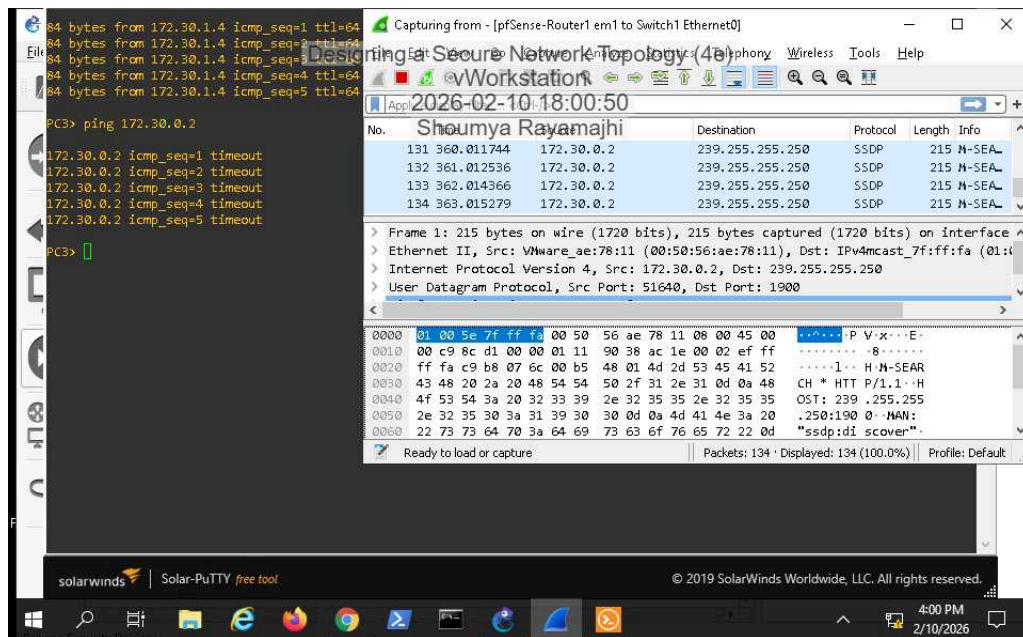
Designing a Secure Network Topology (4e)

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

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



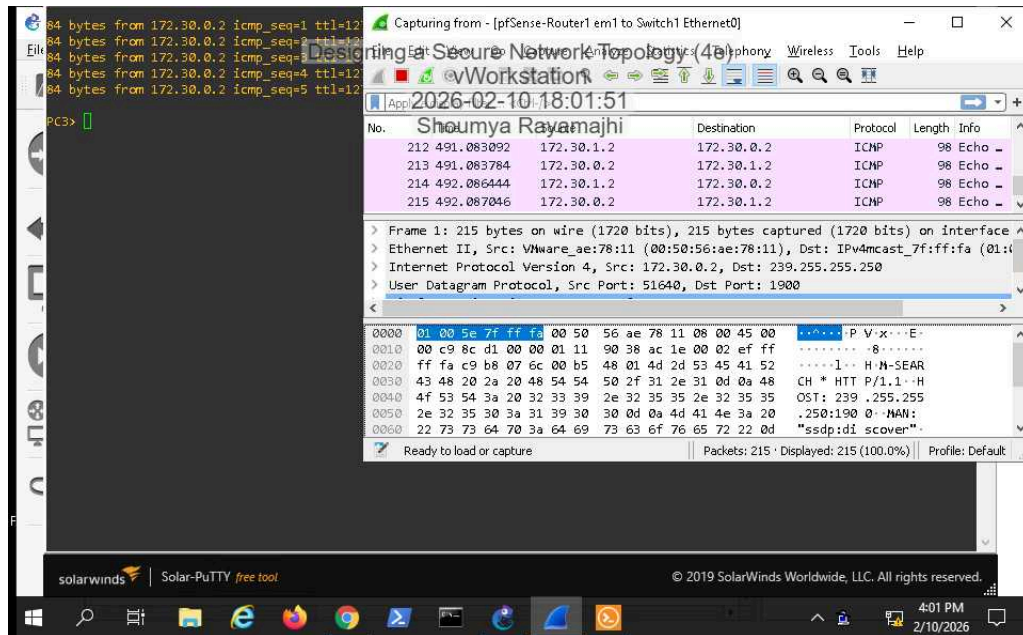
17. Make a screen capture showing the timed out ping request.



Designing a Secure Network Topology (4e)

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

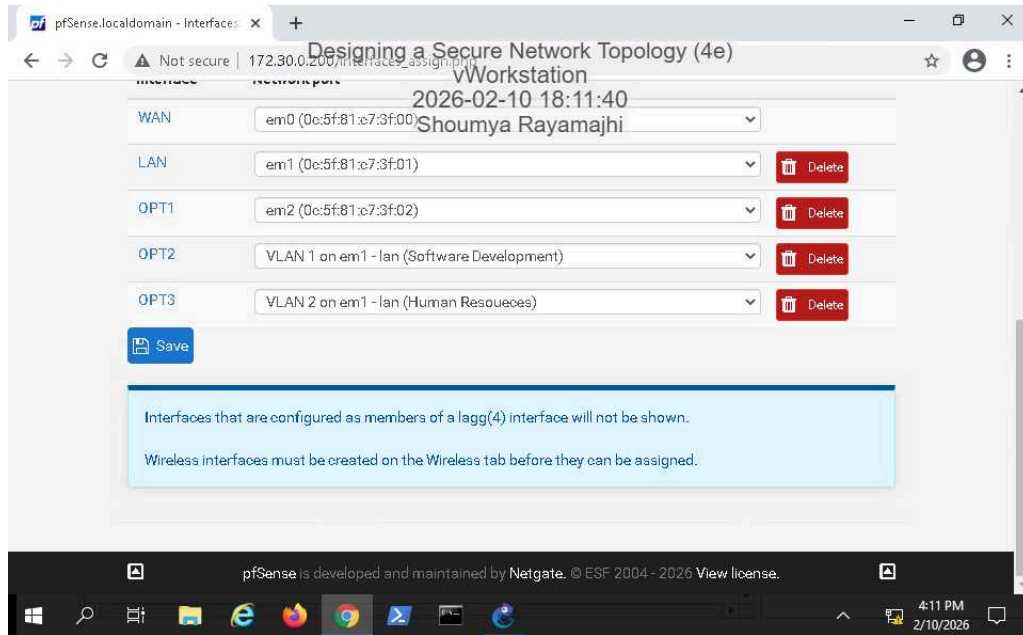
20. Make a screen capture showing the **Wireshark** capture for the **PC3** to **vWorkstation** ping request.



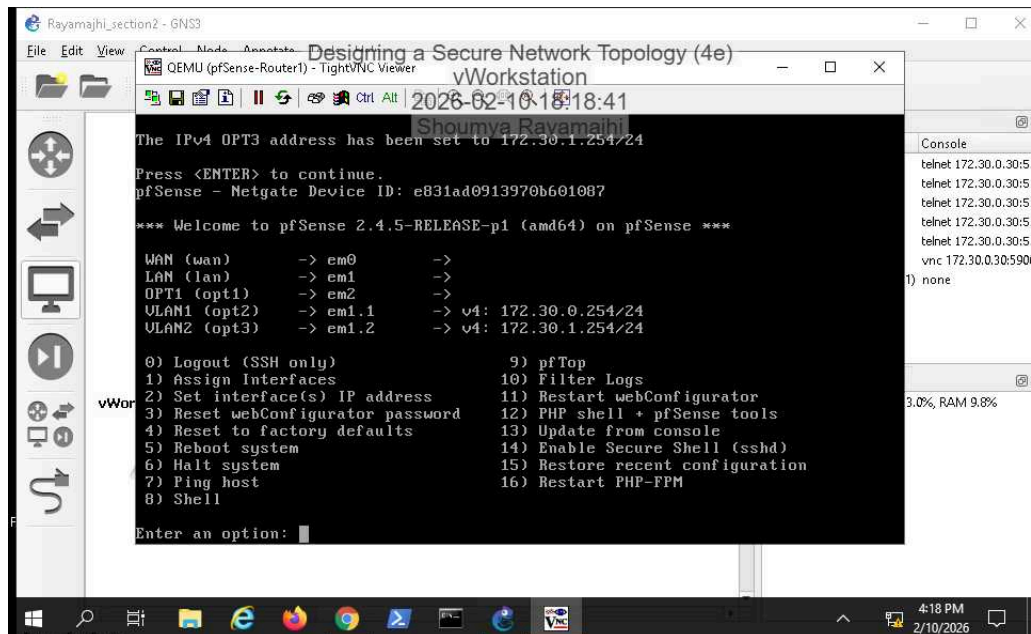
Applied Learning

Part 1: Design a More Complex Network Topology

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



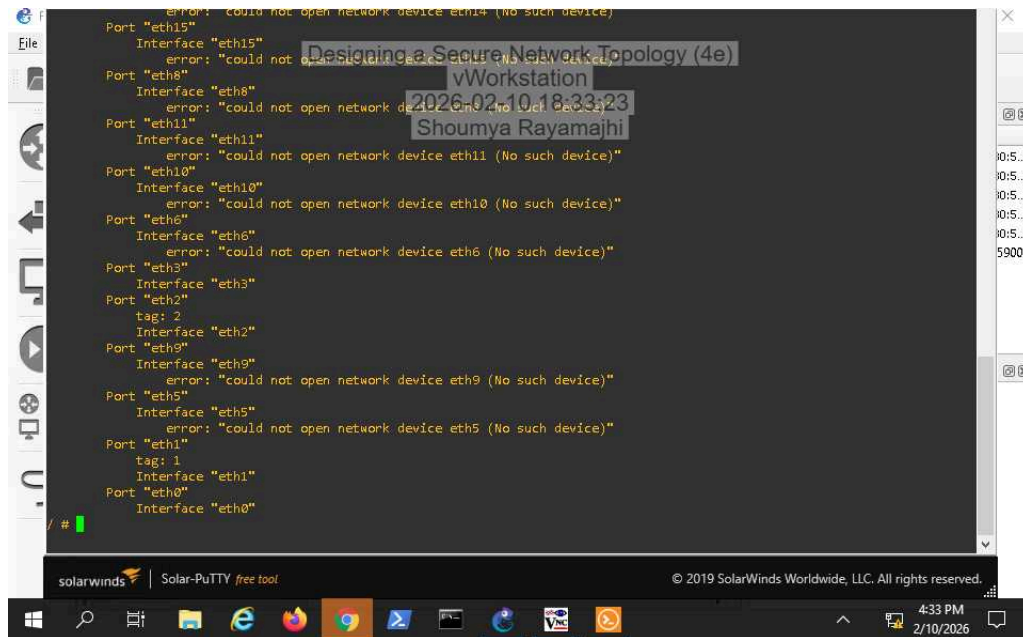
28. Make a screen capture showing the **updated pfSense router settings with the VLAN IP address assignments.**



Designing a Secure Network Topology (4e)

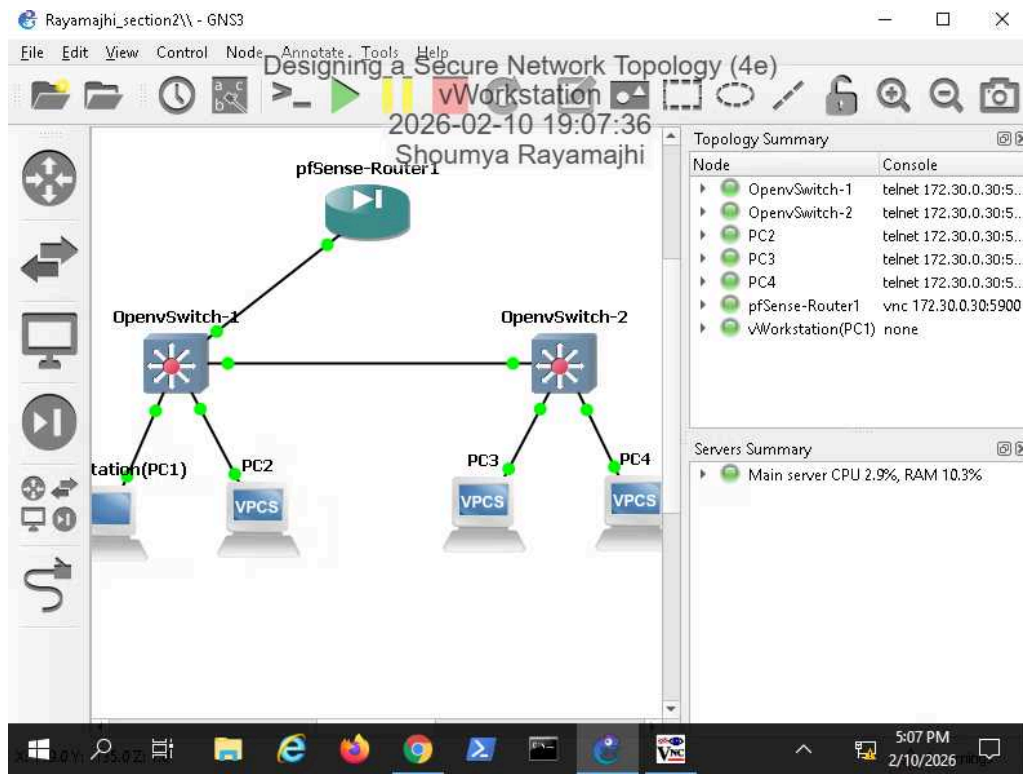
Network Security, Firewalls, and VPNs, Fourth Edition - Lab 03

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



```
error: "could not open network device eth14 (No such device)"
Port "eth15"
Interface "eth15"
error: "could not open network device eth15 (No such device)"
Port "eth8"
Interface "eth8"
error: "could not open network device eth8 (No such device)"
Port "eth11"
Interface "eth11"
error: "could not open network device eth11 (No such device)"
Port "eth10"
Interface "eth10"
error: "could not open network device eth10 (No such device)"
Port "eth6"
Interface "eth6"
error: "could not open network device eth6 (No such device)"
Port "eth3"
Interface "eth3"
Port "eth2"
tag: 2
Interface "eth2"
Port "eth9"
Interface "eth9"
error: "could not open network device eth9 (No such device)"
Port "eth5"
Interface "eth5"
error: "could not open network device eth5 (No such device)"
Port "eth1"
tag: 1
Interface "eth1"
Port "eth0"
Interface "eth0"
/ #
```

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



Part 2: Capture Network Traffic to Validate Connectivity

Designing a Secure Network Topology (4e)

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

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

The screenshot shows the Wireshark interface with a capture filter set to 'OpenvSwitch-1 eth0 to pfSense-Router1 em1'. The capture list shows four packets, all of which are SSDP M-SEARCH requests from 172.30.0.2 to 239.255.255.250. The packet details pane for the first packet shows the following layers:

- Frame 1: 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits) on interface -, id 0
- Ethernet II, Src: VMware_ae:78:11 (00:50:56:ae:78:11), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
- 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1
- Internet Protocol Version 4, Src: 172.30.0.2, Dst: 239.255.255.250
- User Datagram Protocol, Src Port: 54802, Dst Port: 1900
- Simple Service Discovery Protocol

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, 802.1Q header, IP header, UDP header, and SSDP payload. The SSDP payload is an M-SEARCH request for HTTP/1.1 services.

Ready to load or capture | Packets: 4 · Displayed: 4 (100.0%) | Profile: Default

Designing a Secure Network Topology (4e)

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

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

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Designing a Secure Network Topology (4e)

2026-02-10 19:09:51

Shounya Rayamajhi

No.	Time	Source	Destination	Protocol	Length	Info
3	2.023379	172.30.0.2	239.255.255.250	SSDP	219	M-SEARCH * HTTP/1.1
4	3.023554	172.30.0.2	239.255.255.250	SSDP	219	M-SEARCH * HTTP/1.1
5	87.288208	172.30.0.2	172.30.0.255	NBNS	96	Name query NB VWORKSTATION<1c>
6	88.044732	172.30.0.2	172.30.0.255	NBNS	96	Name query NB VWORKSTATION<1c>
7	88.817593	172.30.0.2	172.30.0.255	NBNS	96	Name query NB VWORKSTATION<1c>
8	100.659107	Private_66:68:01	Broadcast	ARP	68	Who has 172.30.1.4? Tell 172.30.1.4

> Frame 1: 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits) on interface -, id 0

> Ethernet II, Src: VMware_ae:78:11 (00:50:56:ae:78:11), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1

> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 239.255.255.250

> User Datagram Protocol, Src Port: 54802, Dst Port: 1900

> Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa 00 50 56 ae 78 11 81 00 00 01 ...P V...
0010 08 00 45 00 00 c9 8d 69 00 00 01 11 8f a0 ac 1e ...E...i...
0020 00 02 ef ff ff fa d6 12 07 6c 00 b5 3b a7 4d 2d1.;M-
0030 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
0040 31 0d 0a 48 4f 53 54 3a 20 32 33 39 2e 32 35 35 1..HOST: 239.255
0050 2e 32 35 35 2e 32 35 30 3a 31 39 30 30 0d 0a 4d .255.250:1900..M
0060 41 4e 3a 20 22 73 73 64 70 3a 64 69 73 63 6f 76 AN: "ssd p:discov
0070 65 72 22 0d 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 er".MX: 1..ST:
0080 75 72 6e 3a 64 69 61 6c 2d 6d 75 6c 74 69 73 63 urn:dial-multisc
0090 72 65 65 6e 2d 6f 72 67 3a 73 65 72 76 69 63 65 reen-org :service

Ready to load or capture

Packets: 8 · Displayed: 8 (100.0%)

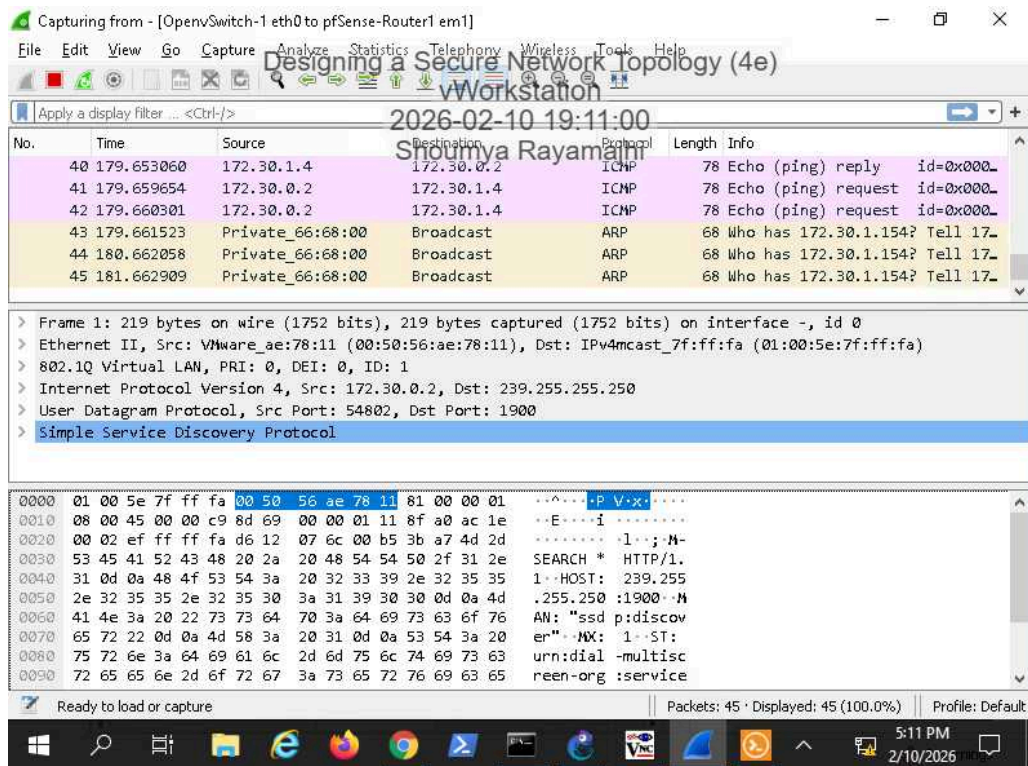
Profile: Default

5:09 PM
2/10/2026

Designing a Secure Network Topology (4e)

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

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



Designing a Secure Network Topology (4e)

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

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

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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Designing a Secure Network Topology (4e)

2026-02-10 19:11:45

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

No.	Time	Source	Destination	Protocol	Length	Info
66	224.039260	172.30.0.4	172.30.1.2	ICMP	102	Echo (ping) reply id=0x4dd...
67	224.039723	172.30.0.4	172.30.1.2	ICMP	102	Echo (ping) reply id=0x4dd...
68	225.040750	172.30.1.2	172.30.0.4	ICMP	102	Echo (ping) request id=0x4ed...
69	225.042030	172.30.1.2	172.30.0.4	ICMP	102	Echo (ping) request id=0x4ed...
70	225.043258	172.30.0.4	172.30.1.2	ICMP	102	Echo (ping) reply id=0x4ed...
71	225.043809	172.30.0.4	172.30.1.2	ICMP	102	Echo (ping) reply id=0x4ed...

> Frame 1: 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits) on interface -, id 0

> Ethernet II, Src: VMware_ae:78:11 (00:50:56:ae:78:11), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1

> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 239.255.255.250

> User Datagram Protocol, Src Port: 54802, Dst Port: 1900

> Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa 00 50 56 ae 78 11 81 00 00 01 ...P V x...

0010 08 00 45 00 00 c9 8d 69 00 00 01 11 8f a0 ac 1e ...E...i...

0020 00 02 ef ff ff fa d6 12 07 6c 00 b5 3b a7 4d 2d1.;M-

0030 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.

0040 31 0d 0a 48 4f 53 54 3a 20 32 33 39 2e 32 35 35 1..HOST: 239.255

0050 2e 32 35 35 2e 32 35 30 3a 31 39 30 30 0d 0a 4d .255.250 :1900..M

0060 41 4e 3a 20 22 73 73 64 70 3a 64 69 73 63 6f 76 AN: "ssd p:discov

0070 65 72 22 0d 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 er".MX: 1..ST:

0080 75 72 6e 3a 64 69 61 6c 2d 6d 75 6c 74 69 73 63 urn:dial-multisc

0090 72 65 65 6e 2d 6f 72 67 3a 73 65 72 76 69 63 65 reen-org :service

Ready to load or capture

Packets: 71 · Displayed: 71 (100.0%)

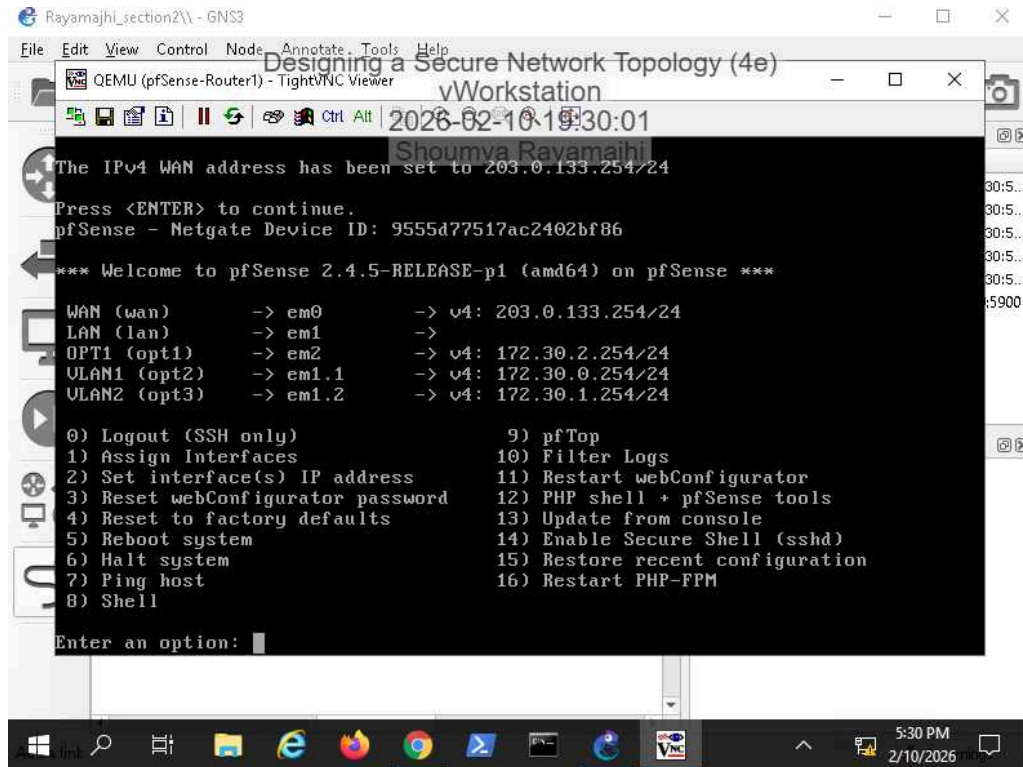
Profile: Default

5:11 PM
2/10/2026

Challenge and Analysis

Part 1: Enhance the Network Topology with a DMZ

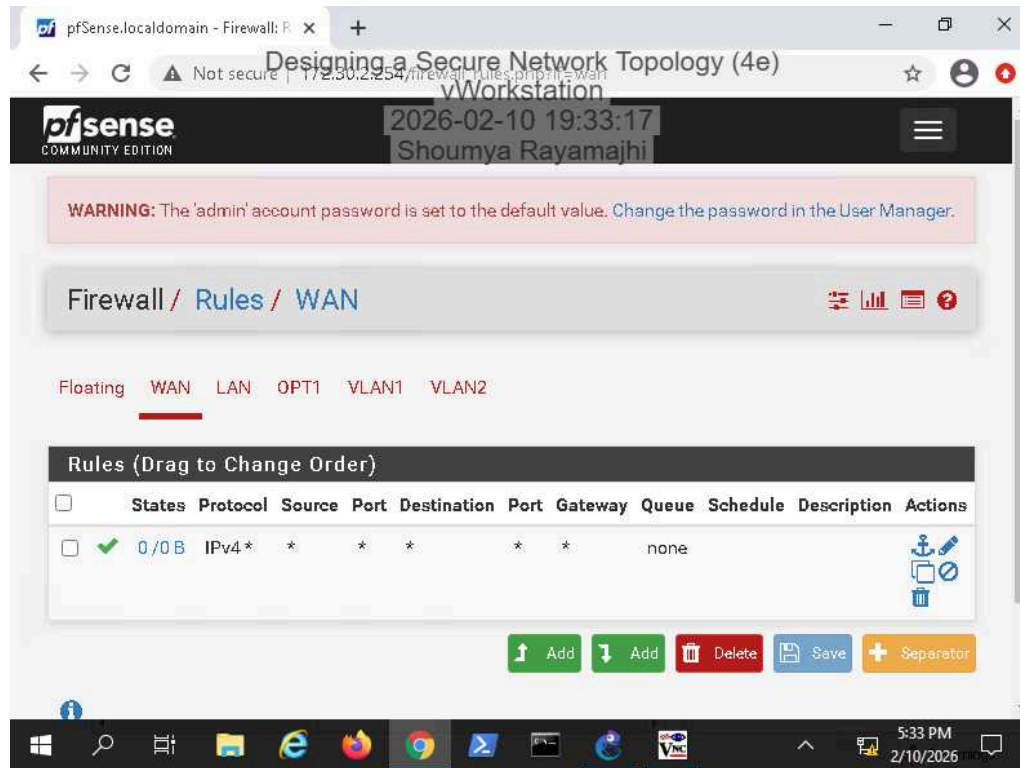
1. Make a screen capture showing the interface configurations in the pfSense console.



Designing a Secure Network Topology (4e)

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

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



Part 2: Validate DMZ Connectivity

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

