LAB REPORT

LAB TITLE: Troubleshooting Common Network Issues

Name: Gabriel Miracle Nwauche

PSU ID: GMN5192@psu.edu

Course: IST 220

Instructor: Nick Giacobe

Date: 4/25/2023

General Context

The purpose of this Lab is to identify and troubleshoot functions in a system to properly concatenate their corrections. Once the user is introduced to the local network, the user will examine the networking issues with the LAN and WAN to discover why the network is preventing the user from accessing the device from the outside in. Like many of the previous labs the user will have to access the PuTTy command line interface to configure codes and access the information needed for these corrections through inputs and outputs. The main Protocol that will be used is the RIP. Various codes in the command line will be fitted for showing the IP configuration and the routing tables that the RIP protocol takes place in.

Furthermore, the routing tables will be examined by the user to determine which of the values are incorrect in the system. For example, In the OpenVPN the user will be prompted to change the port from *443 TCP* to *1194 UDP* in order for the correct connection to be established. Those were corresponding to the network troubleshooting. Then comes the troubleshooting for the DNS. The way we figured out the DNS could not locate a specific website in the browser was by using the *nslookup* command in the command prompt of the Window's system. Then the user had to navigate to the pfsense web page to see the DNS settings and if they were configured correctly in the first place. After reviewing the settings on the site, the user is supposed to find a typo in the website name which when corrected results in a successful *nslookup* configuration in the command prompt window.

Technical Context

Troubleshooting in a system can prove to be very *troublesome*, but that was the complete opposite in this lab's guidelines and description. When a novice network administrator hears "Identify, isolate, and remediate network issues on a LAN and WAN, and issues on a OpenVPN remote access network" they would probably think they're in for a long day at work. Not so much in this case. Using the Windows Command Prompt, the user is going to start off using commands like *ipconfig, ping, arp, tracert, nslookup,* etc. These baseline commands can provide for lasting information on what needs to be done in the system to first: locate the problem, and second: execute the correct procedure to find a solution for the problem. Using the routing table the user configured in the PuTTy application, that will designate the user to instill a new RIP-provided route that corresponds to the interfaces on the system, ending it with a successful traceroute ping command from the system.

Moving forward, the web browser will help lead the way for other ways a network administrator can use troubleshooting to their advantage for solutions. In the pfsense web page, the display for the rules in the firewall will show the user that there are many blocked connections pertaining to the *202.20.1.2* (which was pinged as well). This is when the user will

send a ping request to the RemoteWindows01 machine successfully and get a new default gateway for the system. Even though the troubleshooting options could seem countless, many of them work together in favor of the administrator.

SECTION 1: Part 1: Troubleshoot Connectivity Issues on the LAN

8. **Make a screen capture** showing the **Student connection details in the Student Status window**.

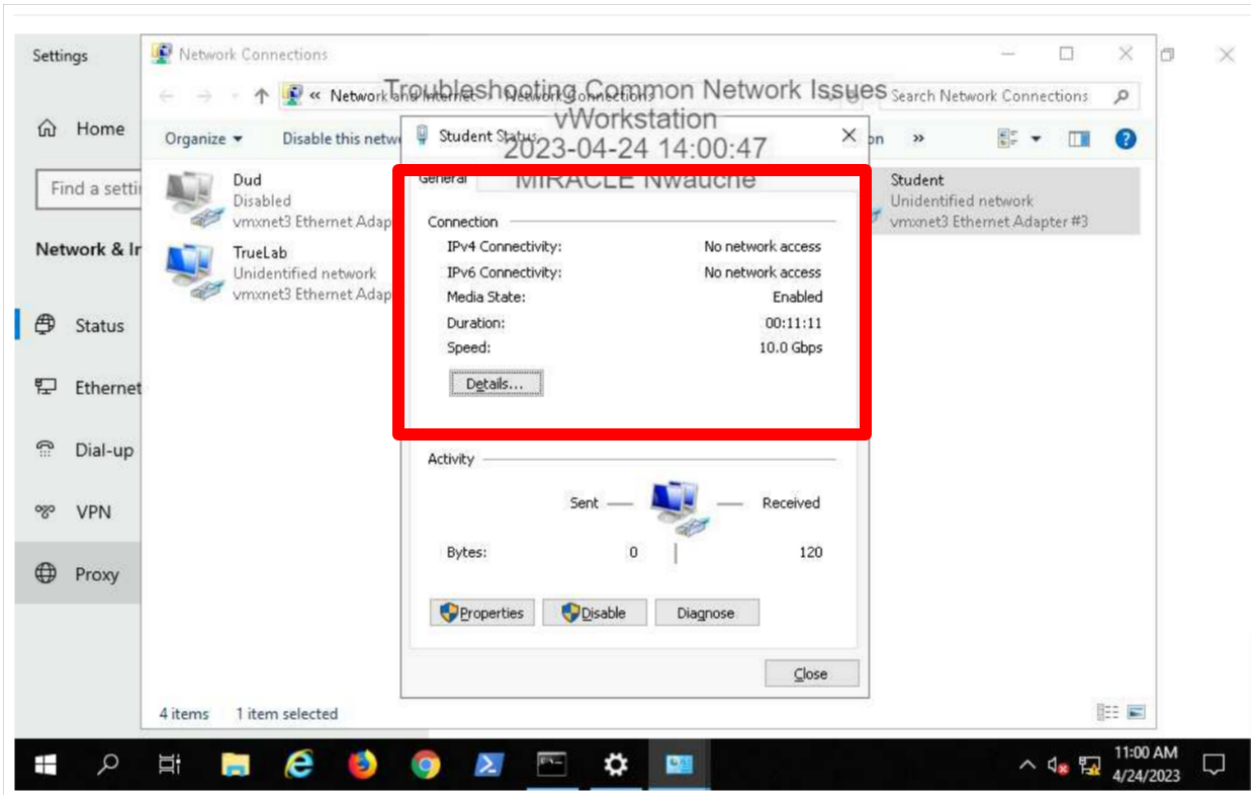

Figure 1, Section 1, Part 1: When opening the Network Connections in the Windows OS and navigating to *Student* the user will be able to access the properties for the connectivity in the network. In this case, the Ipv4 and the Ipv6 are not connected, although the Media State for the connection says it is enabled. The device is physically connected but not necessarily ready for the other OSI layers just yet.

14. **Make a screen capture** showing the **successful localhost ping**.

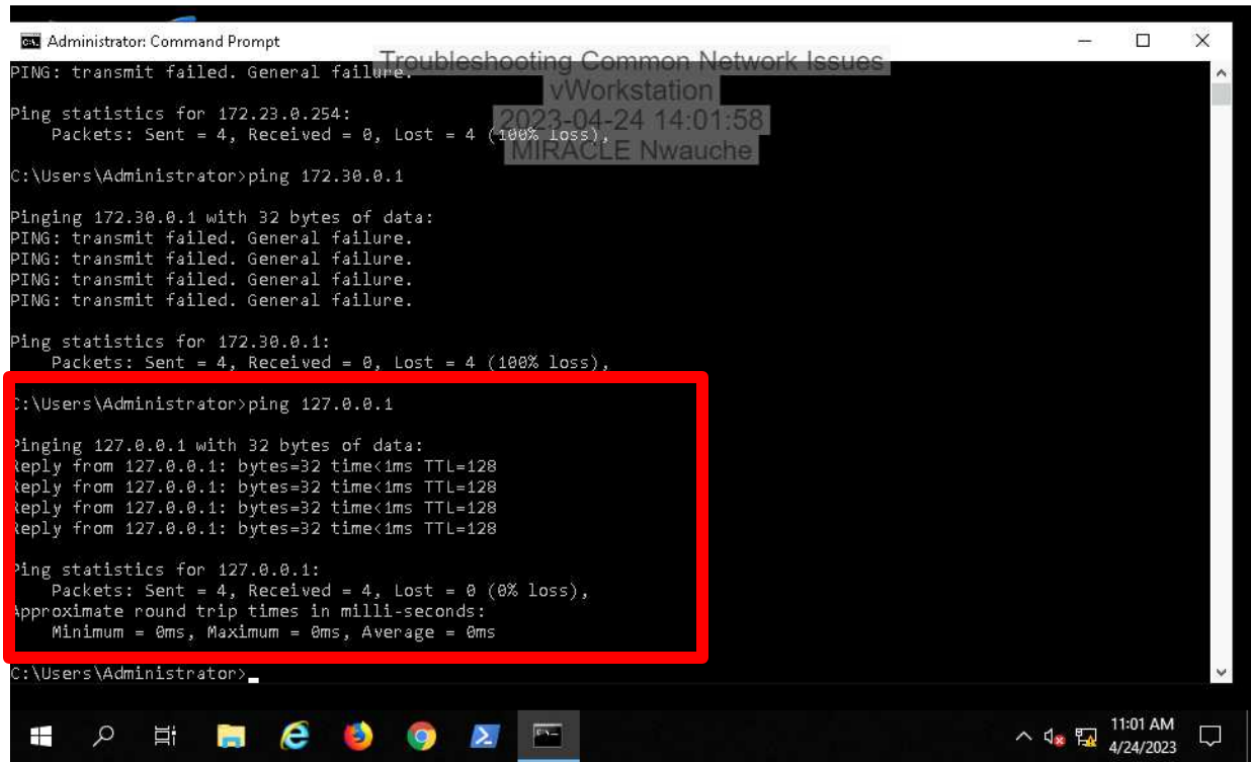

Figure 2, Section 1, Part 1: In the Windows command prompt the user will execute a *ping* command that will attempt to ping the localhost on the network. This is going to confirm that there is functionality in the first 3 layers of the OSI model and the next task will be for the user to make sure everything is functioning properly. This will not always happen in the localhost depending on how the network is configured and reacting.

28. **Make a screen capture showing the current ARP cache for the vWorkstation machine.**

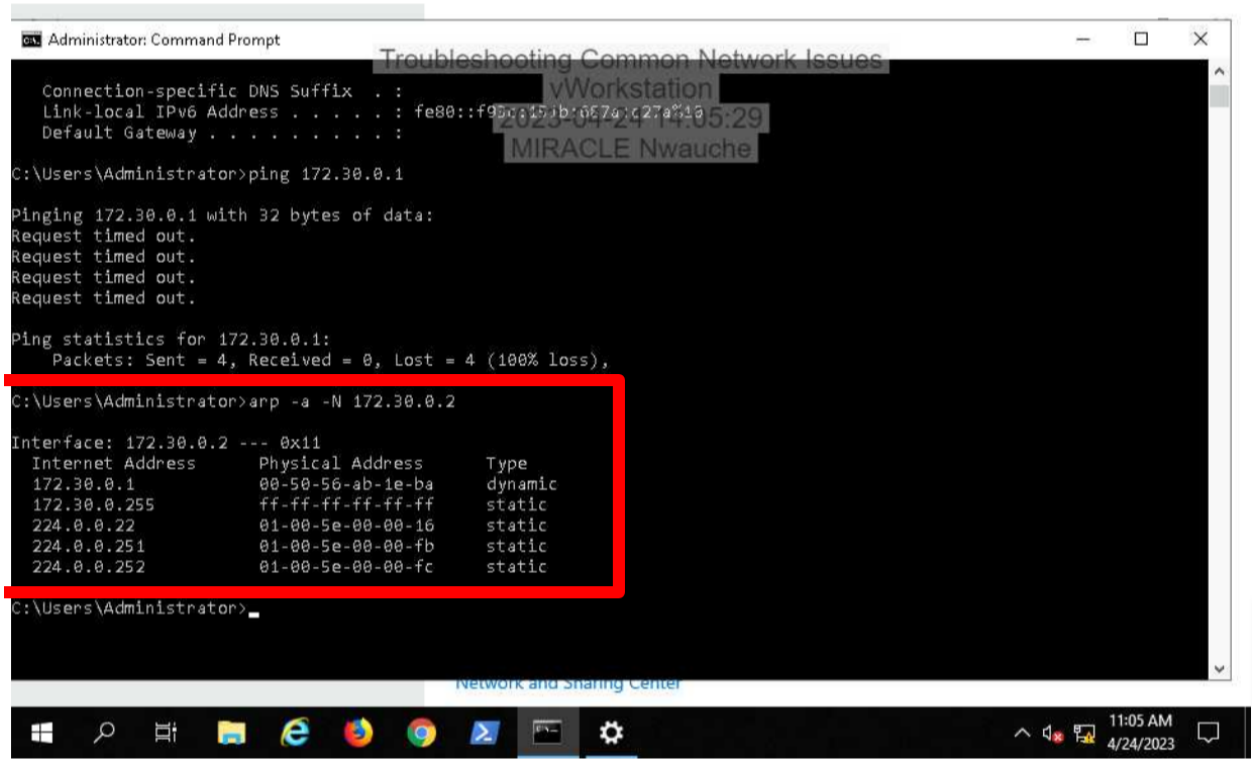

Figure 3, Section 1, Part 1: Here is the *arp cache* activated by the command in the highlighted box. This is going to show the IP addresses of various devices, their MAC addresses and their type whether that may be dynamic or static. Since this is in communication with the *Student* interface that was looked at before, the ARP request is in accordance with if the networking is correctly configured.

PART 2: Troubleshoot Connectivity Issues on the WAN

7. **Make a screen capture showing the router1 ARP cache.**

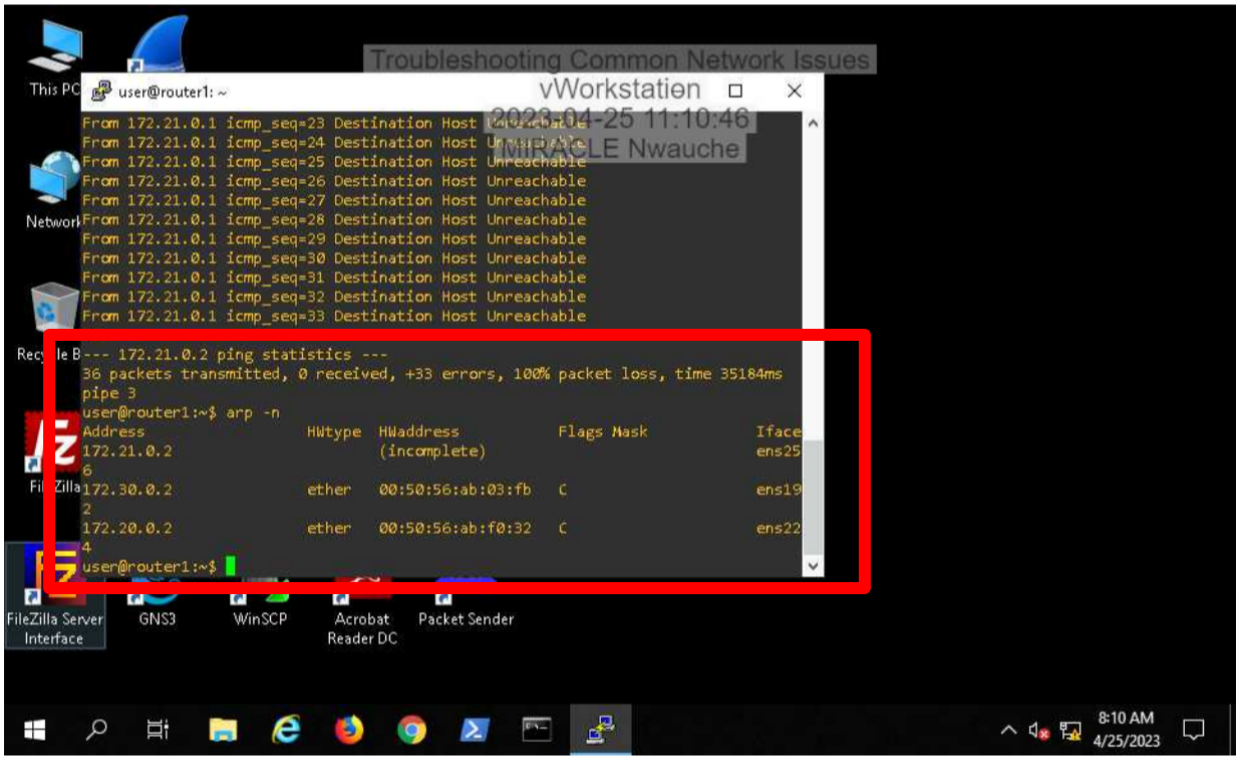

Figure 4, Section 1, Part 2: Here is where the user is going to access the PuTTy command line interface. This arp cache command is going to look much different because this command line gives some of its own data that Windows can not produce with this specific command. The PuTTy application will show categories like flags, HWtype and will show the interfaces names that are corresponding to the network they are configured to.

11. Make a screen capture showing the current routing table on router1.

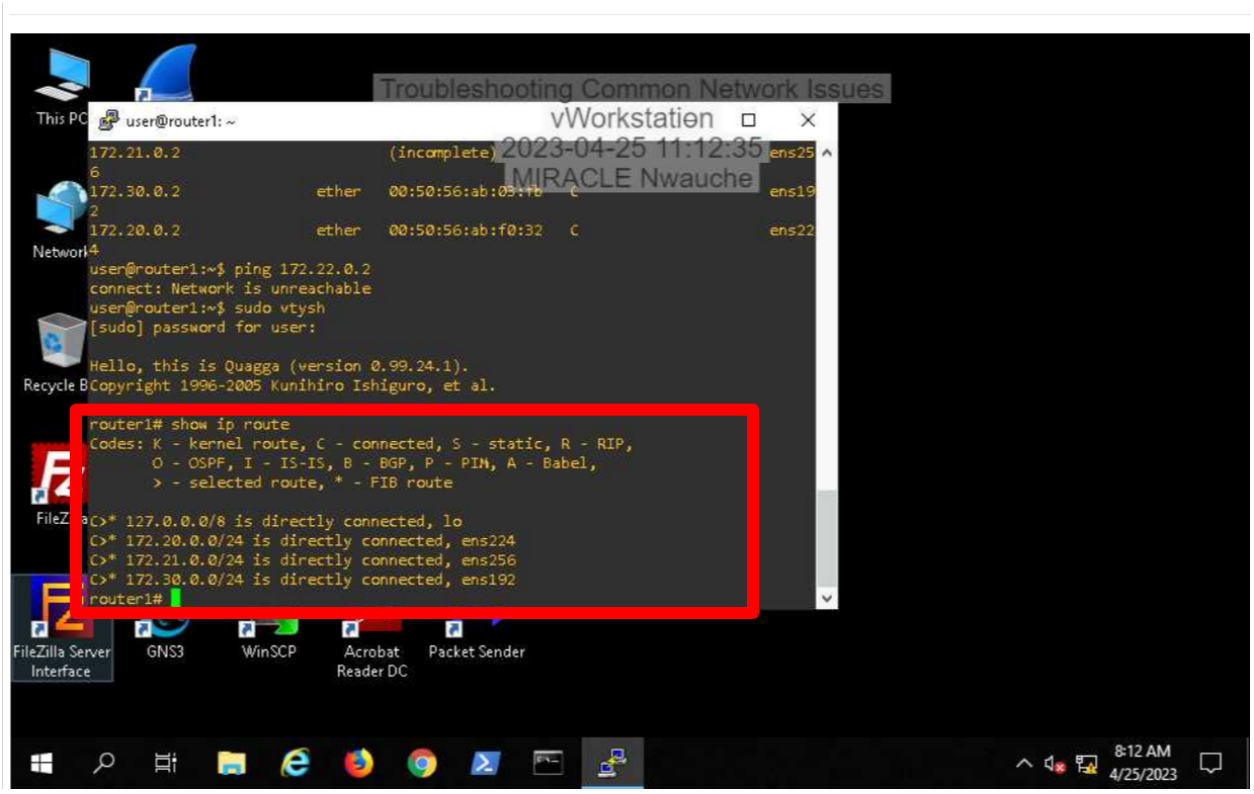

Figure 5, Section 2, Part 1: As a network administrator, you're probably going to have to familiarize yourself with the routes between routers in the networks you will be trying to connect. So it is important to know which interfaces are passing through what subnet masks. For this example, the routes show that router1 and router2 will be connected but maybe router3 is not connecting correctly, resulting in the RIP causing problems in the traffic.

21. Make a screen capture showing the output of your RIP status command.

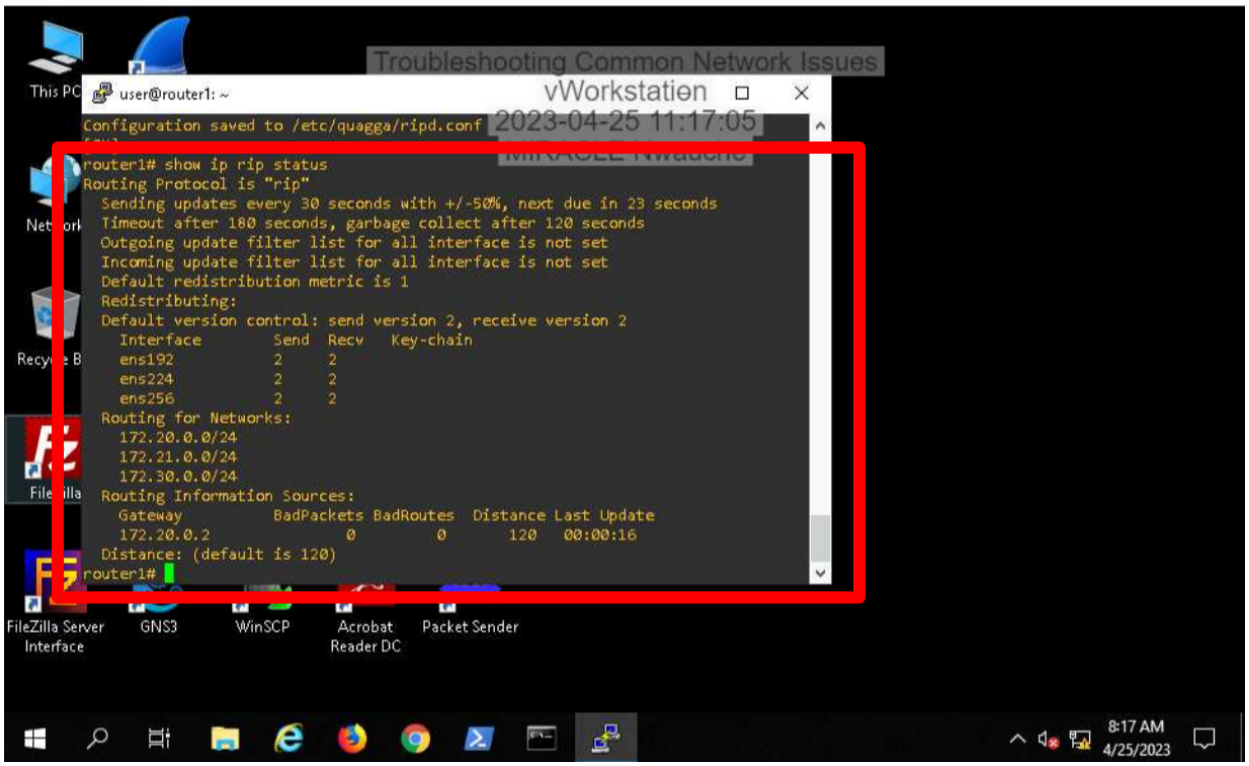

Figure 6, Section 1, Part 2: Using the RIP status command *shows ip rip status* is going to give the user multiple forms of information including the interface ids, the routing for the Networks with the corresponding IP networks, and some more in Routing Information Sources. Now we know that there is no issue and it will be made available for any new updates.

23. **Make a screen capture showing the new RIP-provided route.**

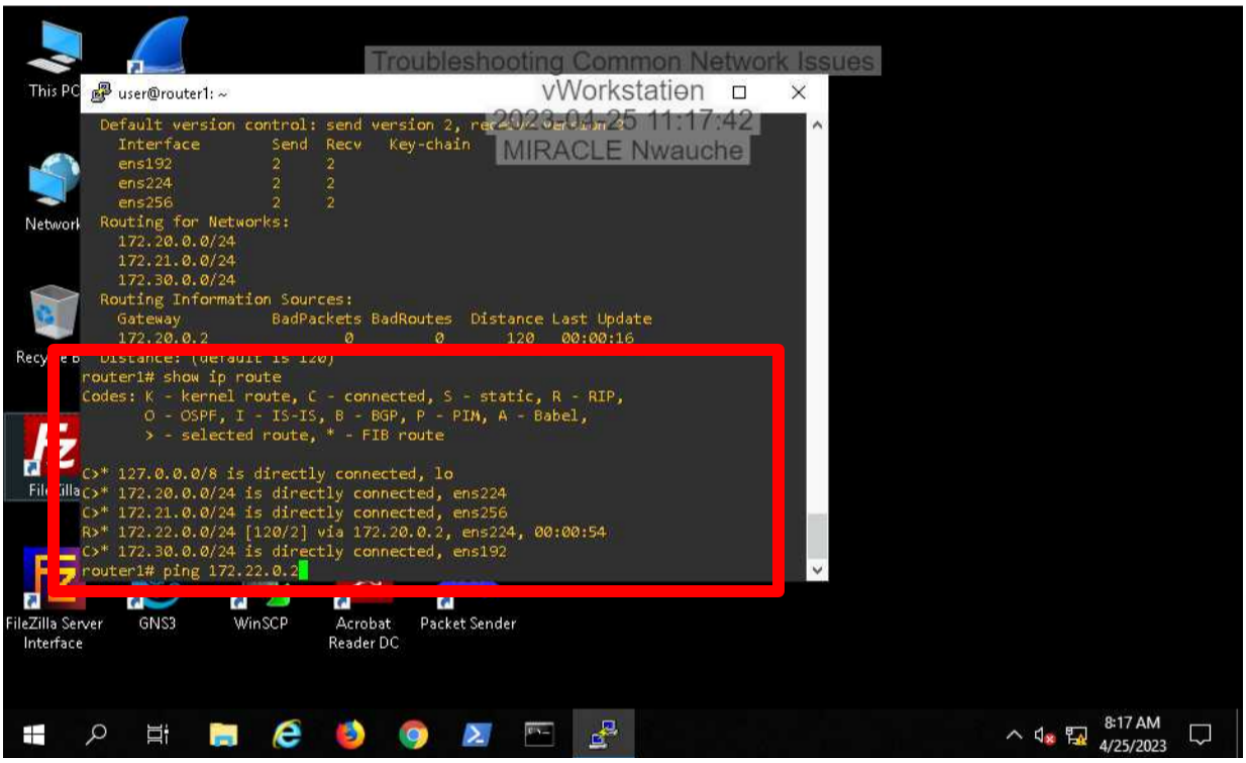

Figure 7, Section 1, Part 2: The *show ip route* will show the RIP-provided route in the table, the "R" in the table shows that the connection for the IP route 172.22.0.0/24 for the ens224 is unreachable unlike the other interfaces in the network. This will show that all of the other interfaces are correctly connected.

39. **Make a screen capture showing the successful traceroute to pfSense from the vWorkstation.**

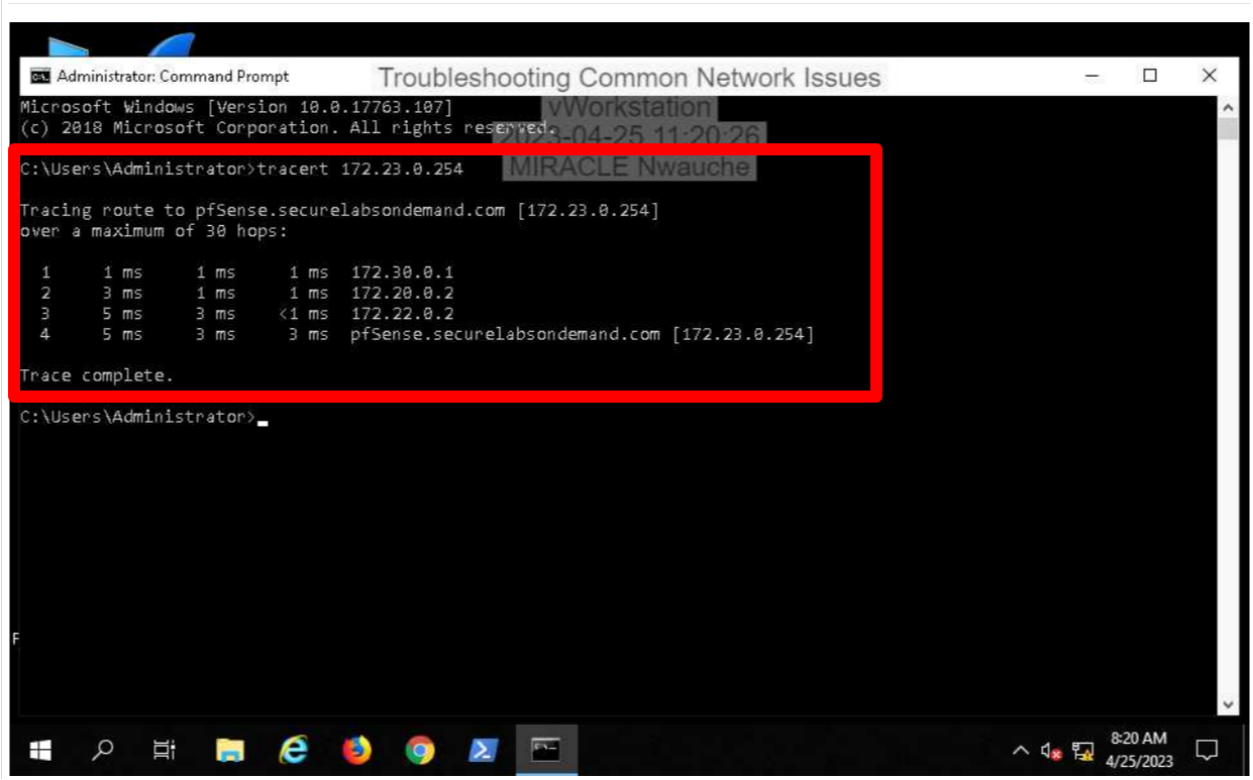

Figure 8, Section 1, Part 2: Using the tracert command with the IP address pfsense, the hops are designated for the connections that are corresponding to the interfaces in the systems. Now we know that the interfaces are correctly connected to each other in the network that must mean all of the interfaces share the same passphrase for the RIP connection. The output shows the RIP routes were successful.

SECTION 2, PART 1: Troubleshoot VPN Issues

8. **Make a screen capture showing the blocked connections from 202.20.1.2 in the firewall logs.**

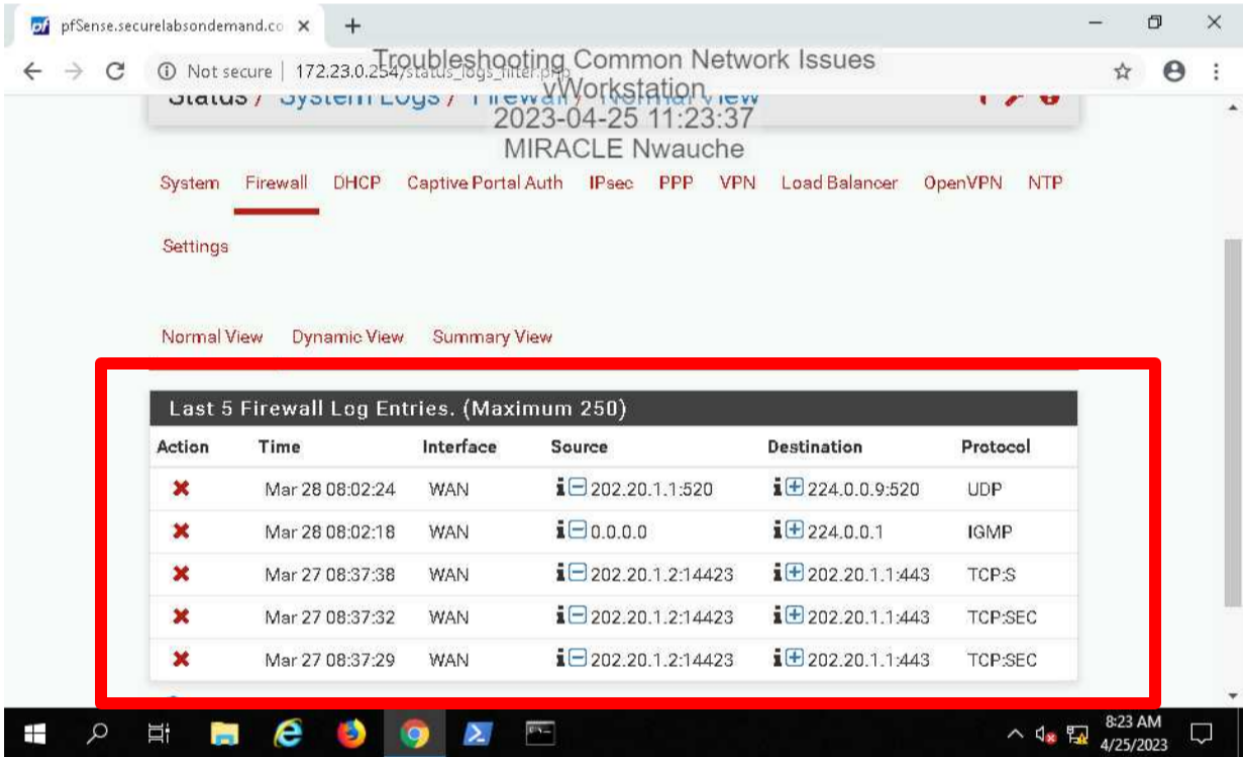

Figure 9, Section 2, Part 1: In the pfsense web page, the user will navigate to the System logs, then into Firewall to see the blocked connections pertaining to the 202.20.1.2. The firewall logs can be a good way of finding out which of the ports are causing inconsistencies in the network, but in this particular case it is all of the ports associated with the firewall. This leads to more investigation.

18. **Make a screen capture showing the current IP configuration on RemoteWindows01.**

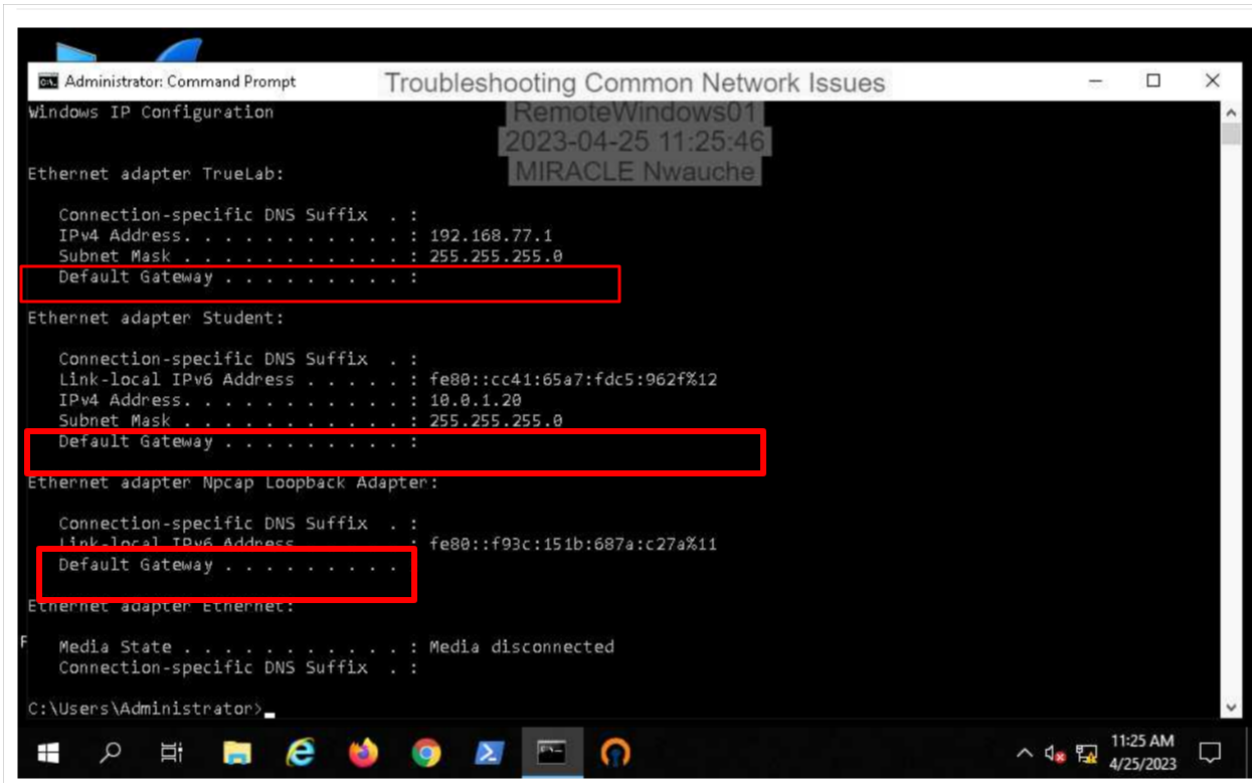

Figure 10, Section 2, Part 1: Thus, will lead to the typical IP configuration in the Windows Command Prompt, this is where we see the details of the networks that are connected in the system the user is operating on. Now we see that there is no default gateway configuration when the command is executed. This should be part of the problems that are being represented, in the coming screenshots will be the solution for this.

22. **Make a screen capture showing the successful ping to the RemoteWindows01 machine's default gateway.**

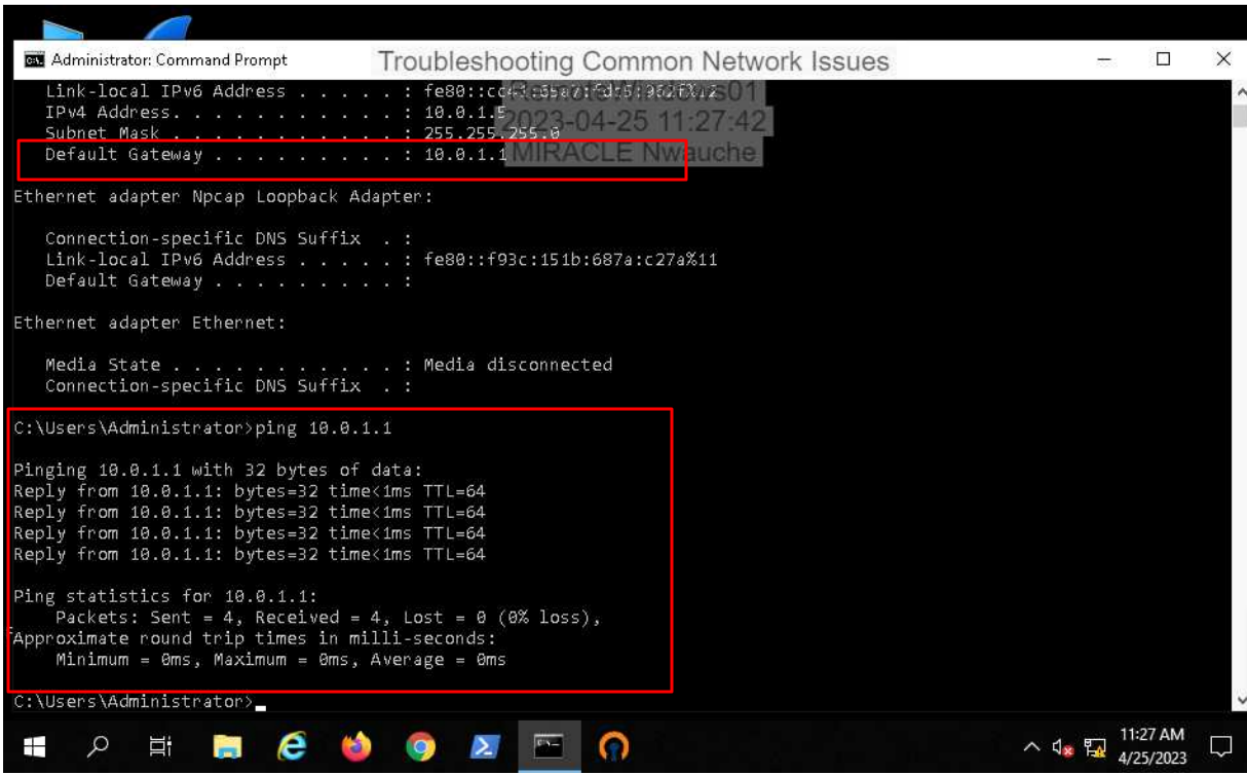

Figure 11, Section 2, Part 1: We will establish a ping command to the *RemoteWindows01* operating system in hopes that the default gateway will be included in the IP configuration command that will be run with it. Once that is found, the user will access a ping command to the default gateway to ensure that it is connected to the correct gateway with the results that are shown in the screenshot above.

31. Make a screen capture showing the OpenVPN Connection window.

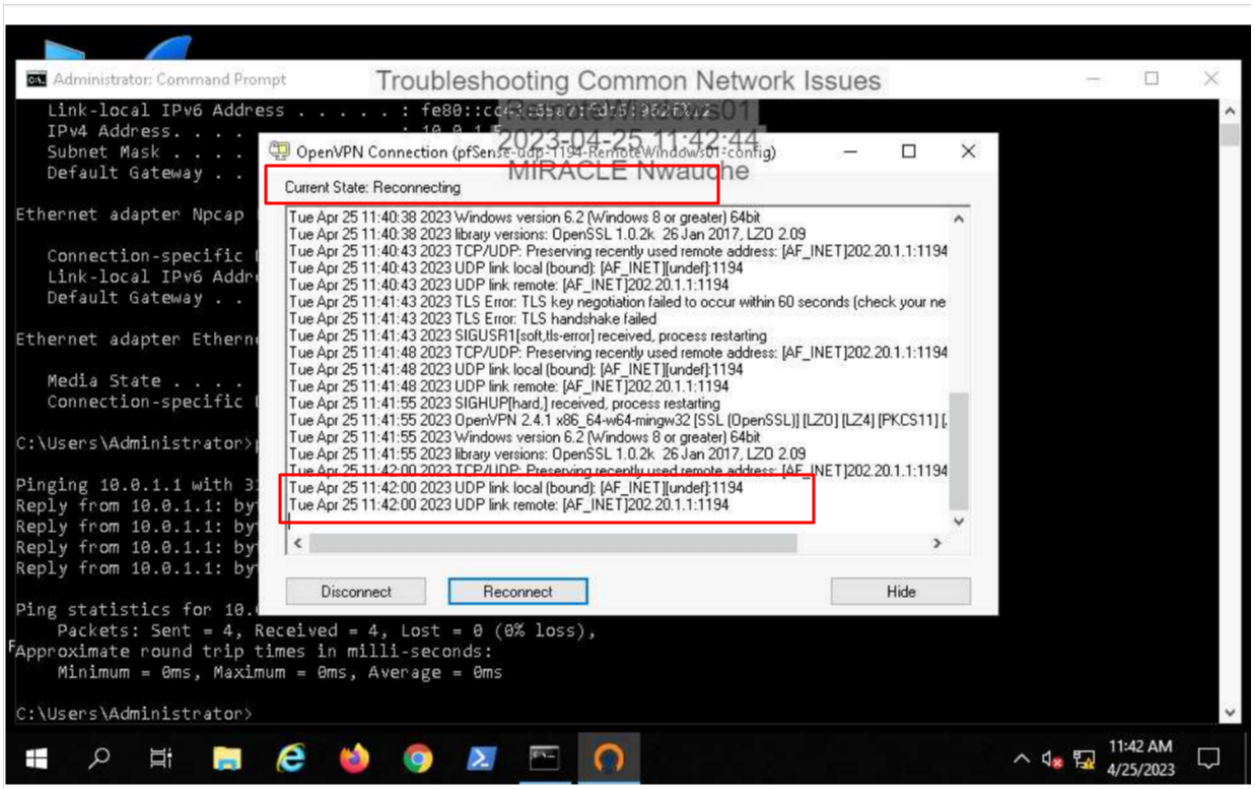

Figure 12, Section 2, Part 1: This was one of the most confusing parts in the lab, not even the steps to get to this, but the results it kept giving me. After editing the logs by right clicking the OpenVPN symbol (using the caret), I changed the TCP port to a *1194 UDP* port which did not work in my favor because the VPN just kept trying to reconnect without actually working.

PART 2: Troubleshoot DNS Issues

15. **Make a screen capture showing the output of your ping and nslookup executions.**

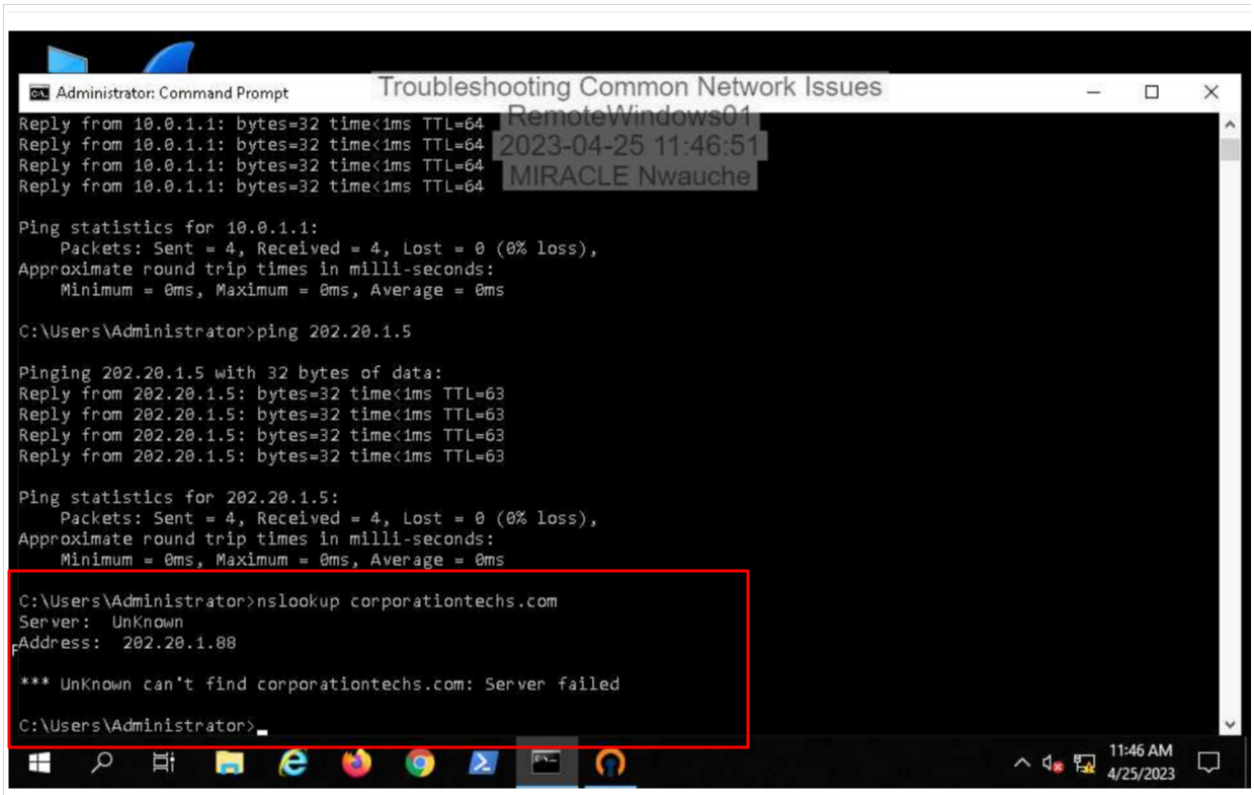

Figure 13, Section 2, Part 2: Now we get to the command that corresponds to the DNS in our Windows Command Prompt and we will see how it will turn out to be unsuccessful in the long run. This is going to show that there is a problem with the DNS records (which in later screenshots we will see why). Notice how the server says it is unknown for right now, but the IP address is displayed.

22. **Make a screen capture showing the successful connection to the corporationtechs.com website.**

Figure 14, Section 2, Part 2: This was weird because even before the typo was fixed in the pfsense, I was able to access the Corporation Techs website as you will be able to see in the first tab on the browser. I guess when you try to use the nslookup in the command prompt, it will not be operational but when it comes to accessing a web browser should work just fine.

25. **Make a screen capture showing the successful record lookup of corporationtechs.com.**

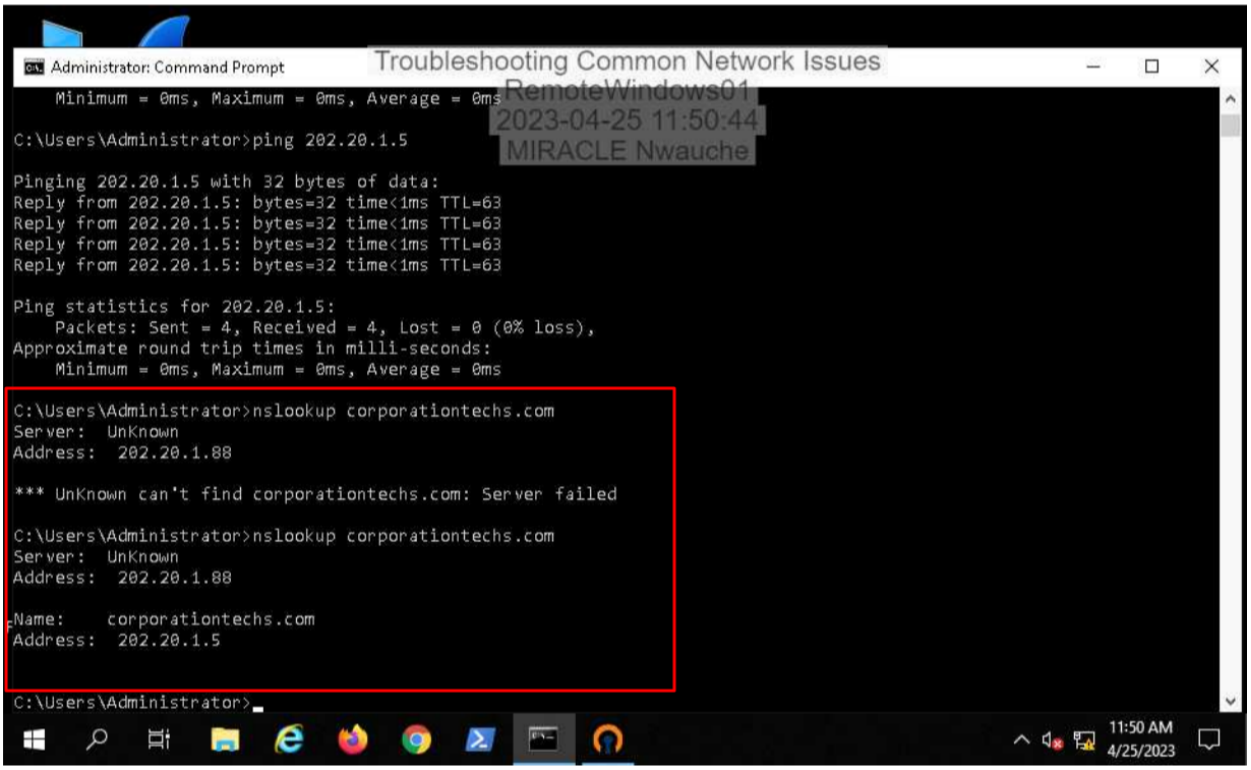

Figure 15, Section 2, Part 2: The highlighted capture is going to show the previous outcome of the *nslookup* command and the present outcome of the command. After that typo was fixed in the setting of the DNS on the pfsense web page, the Windows Command Prompt is able to identify the DNS name with the corresponding IP address that it was given in the system. This is a successful outcome, rather than not being able to find the DNS name like earlier.

SECTION 3, PART 1: Continue Troubleshooting Connectivity Issues

Describe the networking problem you have identified.

The ens192 interface is down, and does not have a respective IP address associated to it.

Make a screen capture showing the command output that corroborates your problem description.

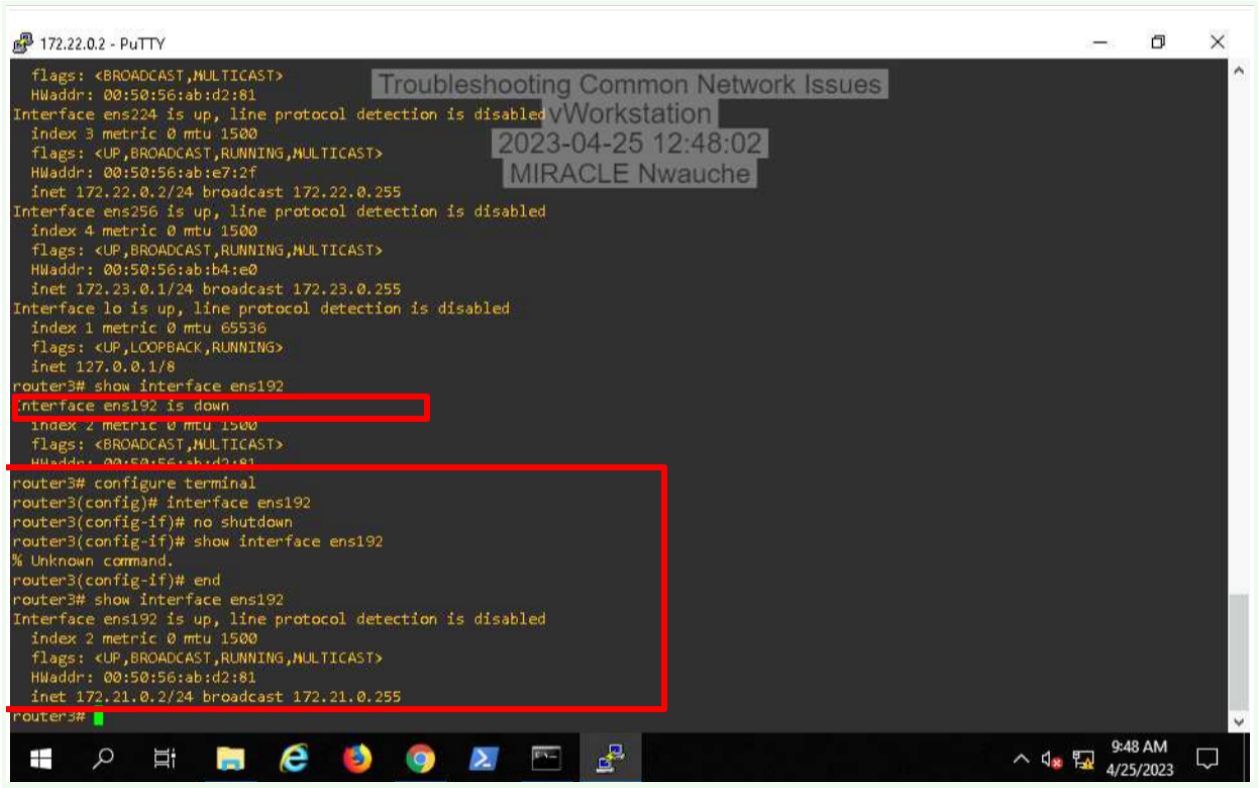

Figure 16, Section 3, Part 1: After seeing the requirements for the interfaces and making sure everything else was correct like the IP addresses, subnet masks, passphrases for the interface, etc. The only thing that I encountered that was not correct is interface ens192 is down when all of them were supposed to be up. This is a quick fix that can be corroborated by using a series of commands. First you will like to configure the terminal to access the interface, then show the interface, and reverse the shutdown so it looks like it never happened. Then the interface will be up and running.

SECTION 3, PART 2: Resolve the Connectivity Issues

Make a screen capture showing the output of your status command.

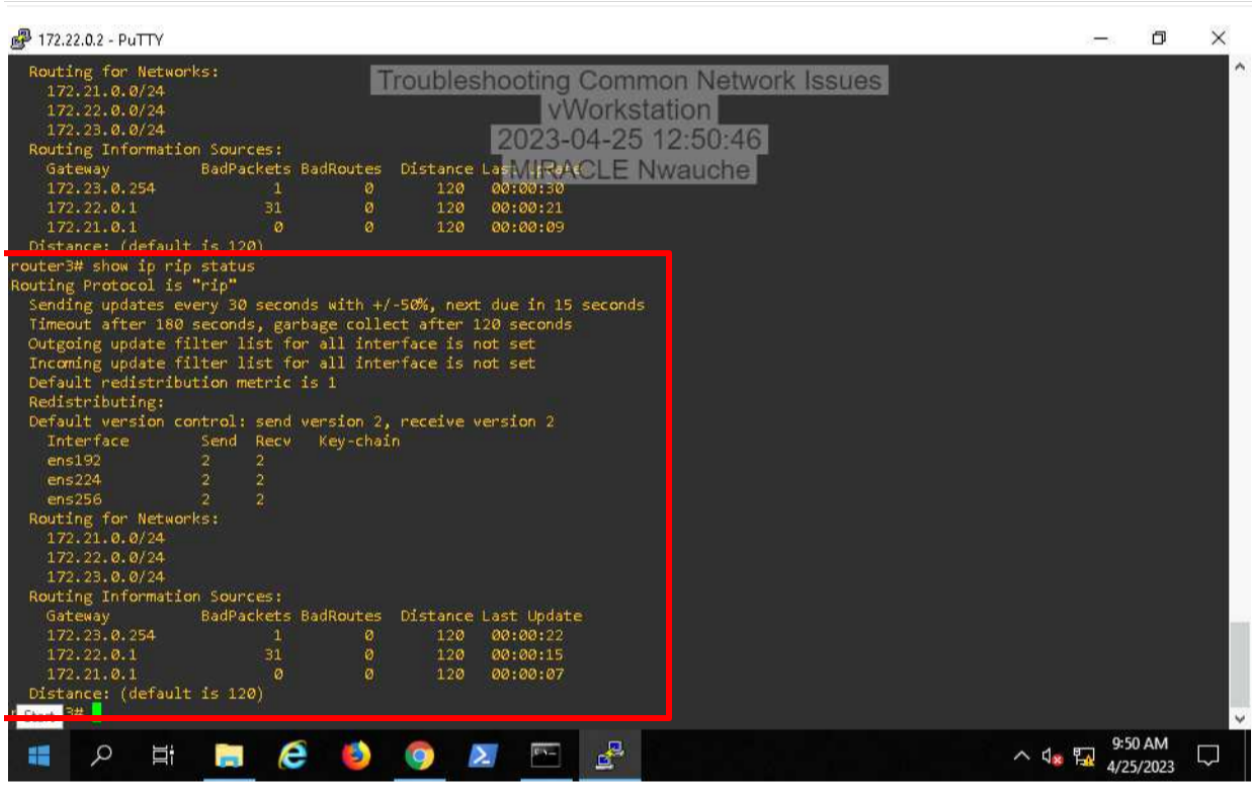

Figure 16, Section 3, Part 2: Once again the user will access the routing information and the RIP status in the interfaces to make sure all of the interfaces have their corresponding addresses and the connection to 172.21.0.1 is smooth in the system with no bad packets being transferred.