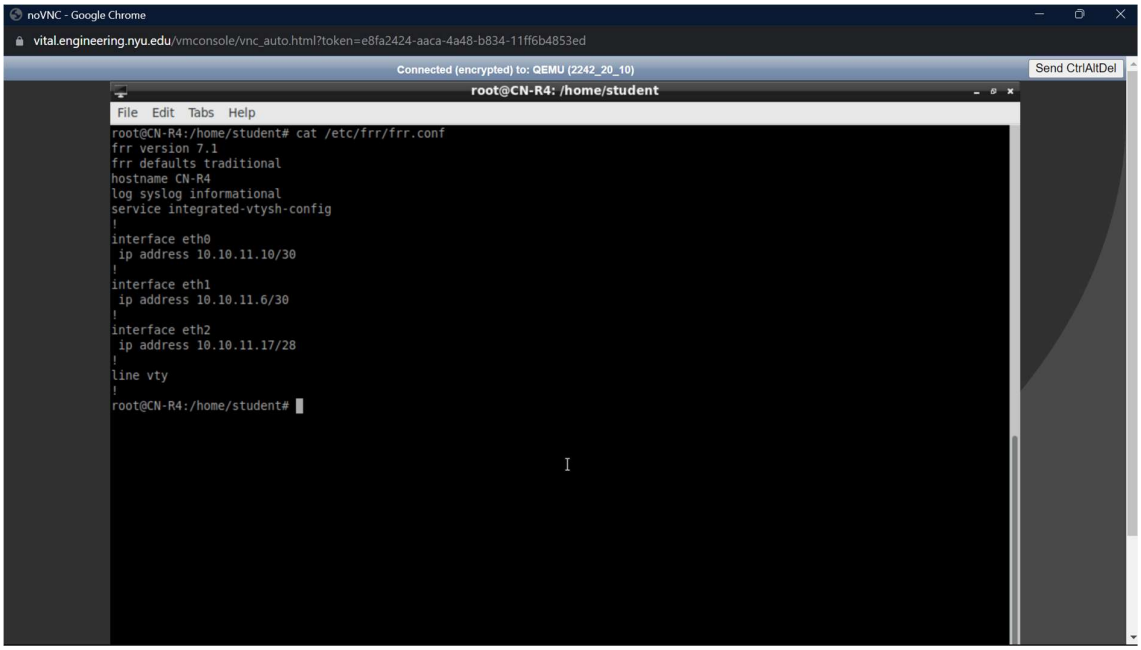
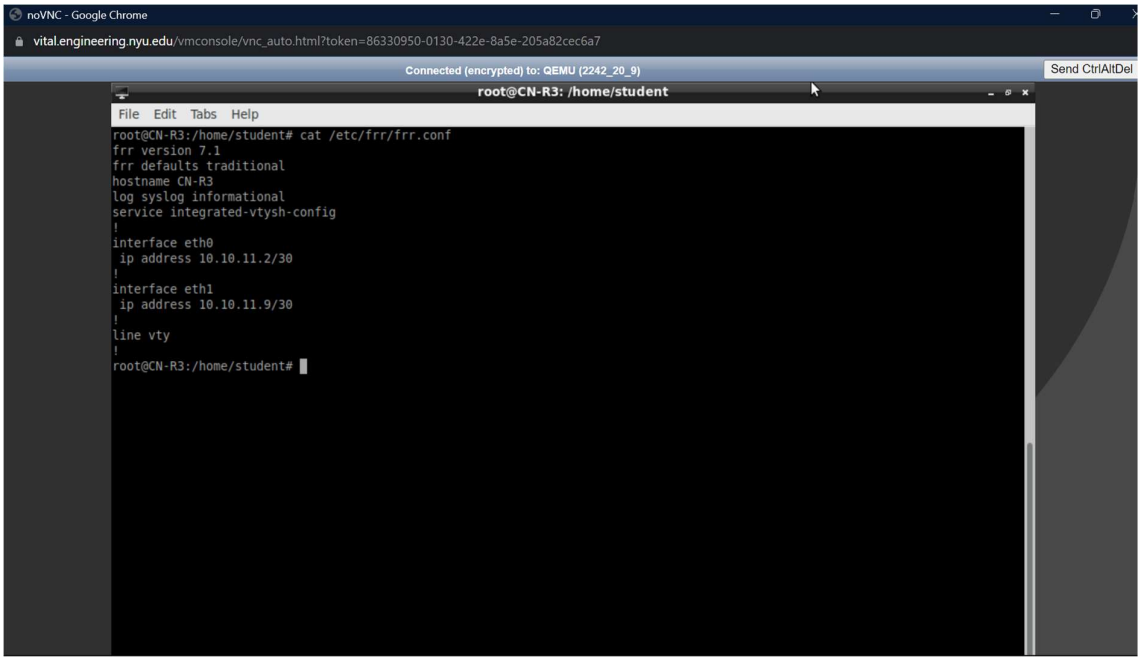
Submissions

Screenshots of the .conf file under /etc/frr/frr.conf from R2, R3, and R4

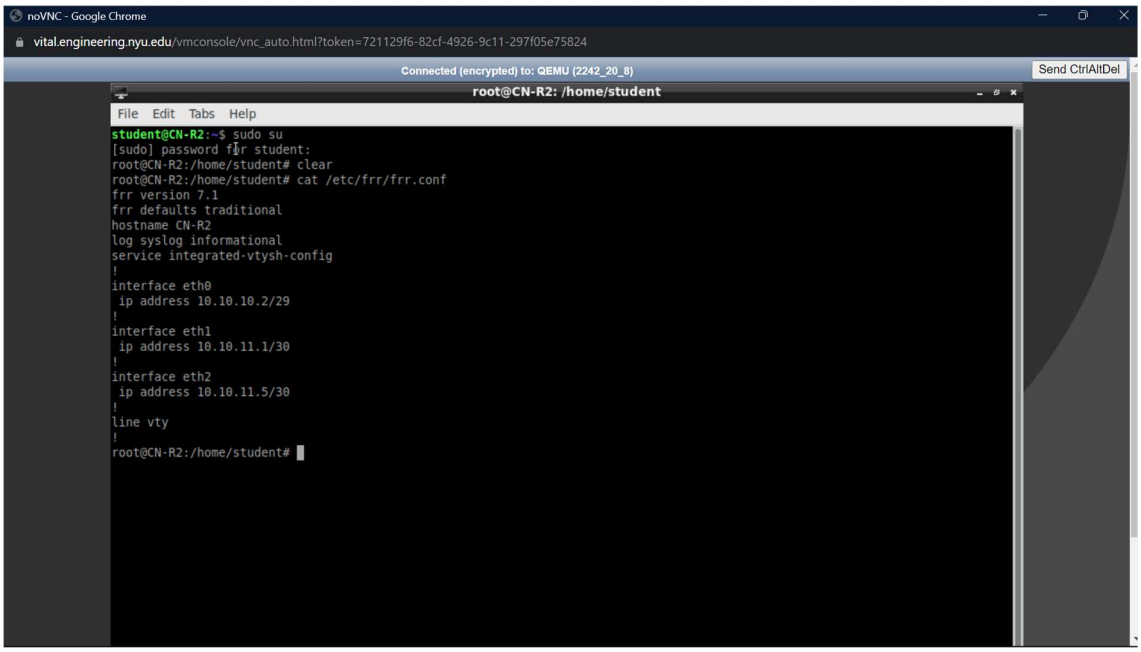
Screenshot of .conf file of R4



Screenshot of .conf file of R3



Screenshot of .conf file of R2



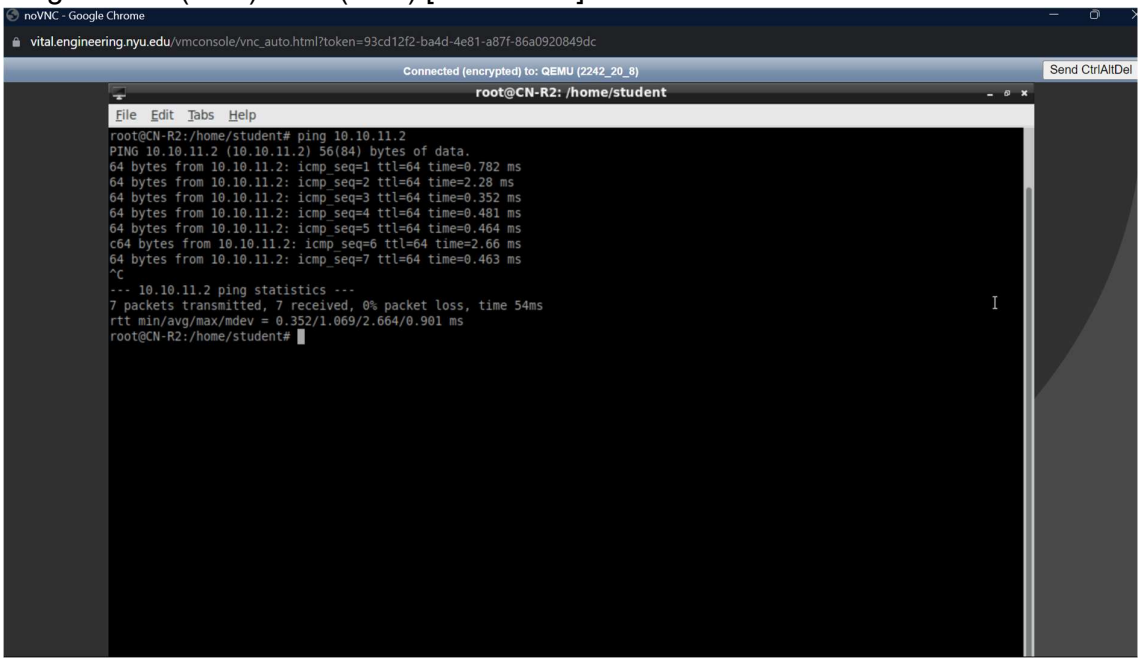
IP subnet table

VM (interface)	IP Address	Network Address	Broadcast Address	Range (usable addresses)
R2 (eth1)	10.10.11.1	10.10.11.0/30	10.10.11.3	10.10.11.1 - 10.10.11.2
R3 (eth0)	10.10.11.2			
R2 (eth2)	10.10.11.5	10.10.11.4/30	10.10.11.7	10.10.11.5 - 10.10.11.6
R4 (eth1)	10.10.11.6			
R3 (eth1)	10.10.11.9	10.10.11.8/30	10.10.11.11	10.10.11.9 - 10.10.11.10
R4 (eth0)	10.10.11.10			
R4 (eth2)	10.10.11.17	10.10.11.16/28	10.10.11.31	10.10.11.17 - 10.10.11.30

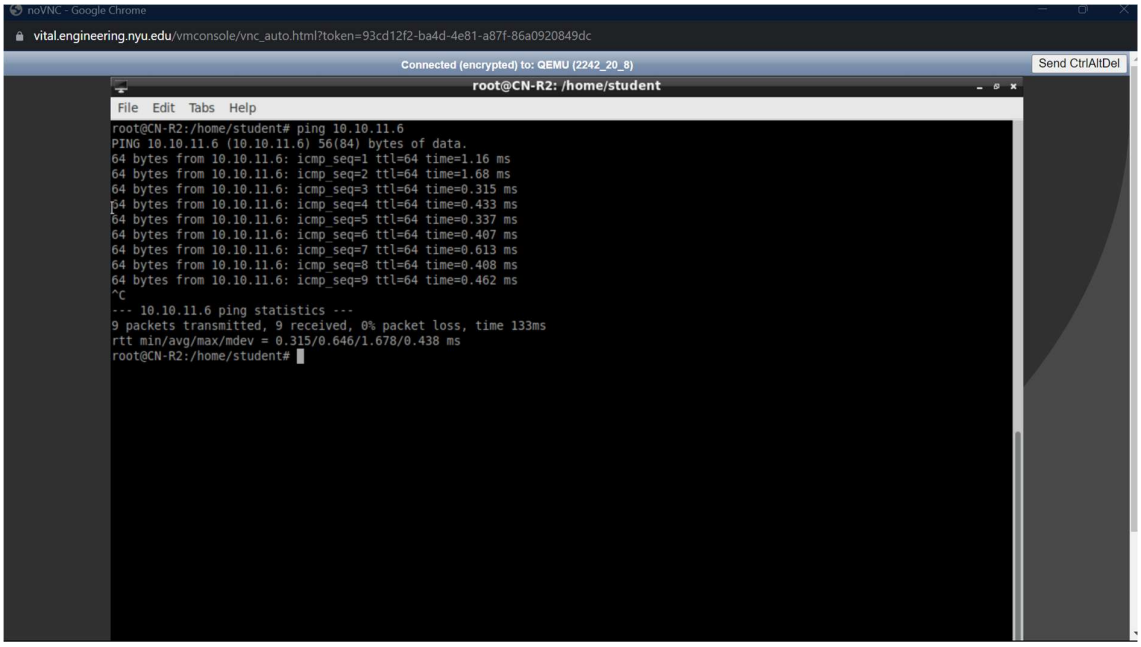
Screenshot showing that pinging works between R2, R3, and R4

R2

Ping from R2(eth1) to R3(eth0) [10.10.11.2]

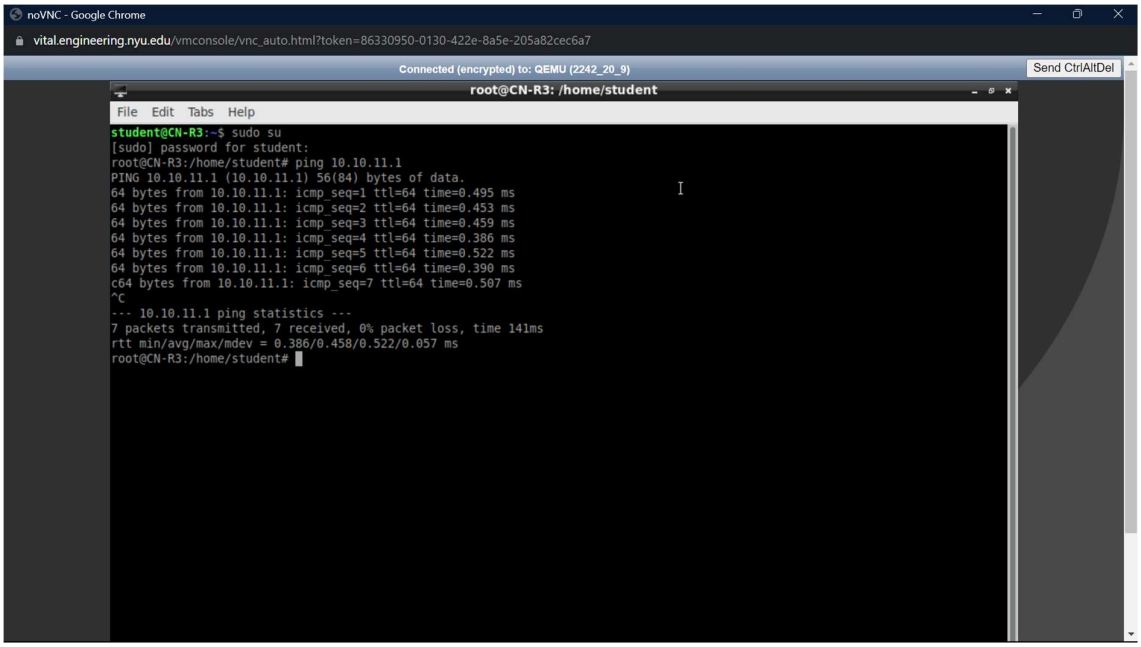


Ping from R2 to R4 (eth1) [10.10.11.6]

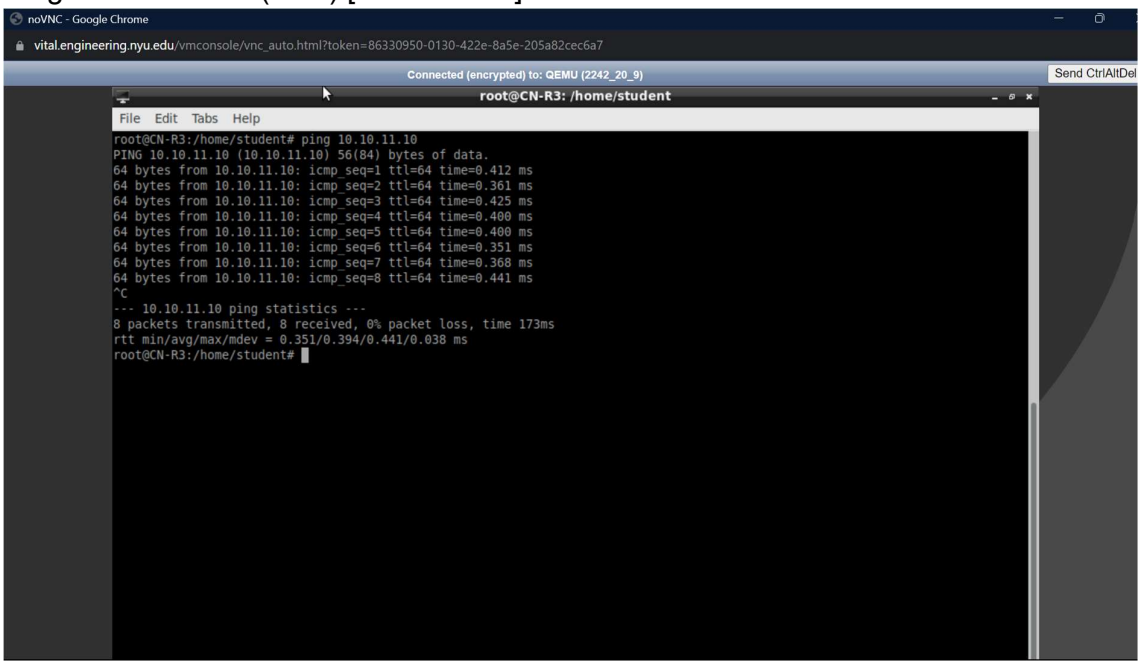


R3

Ping from R3 to R2(eth1) [10.10.11.1]

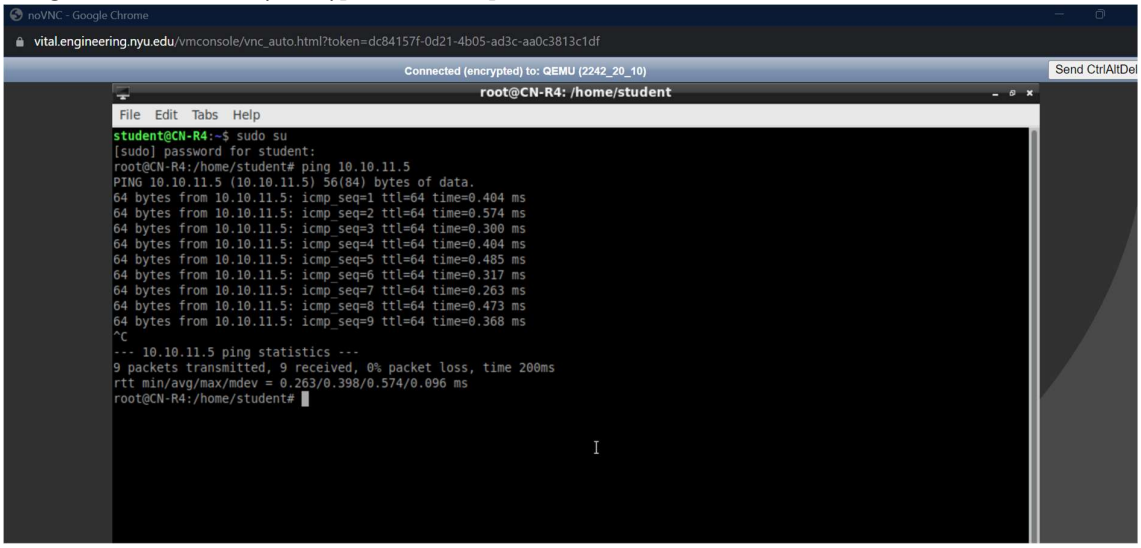


Ping from R3 to R4(eth0) [10.10.11.10]

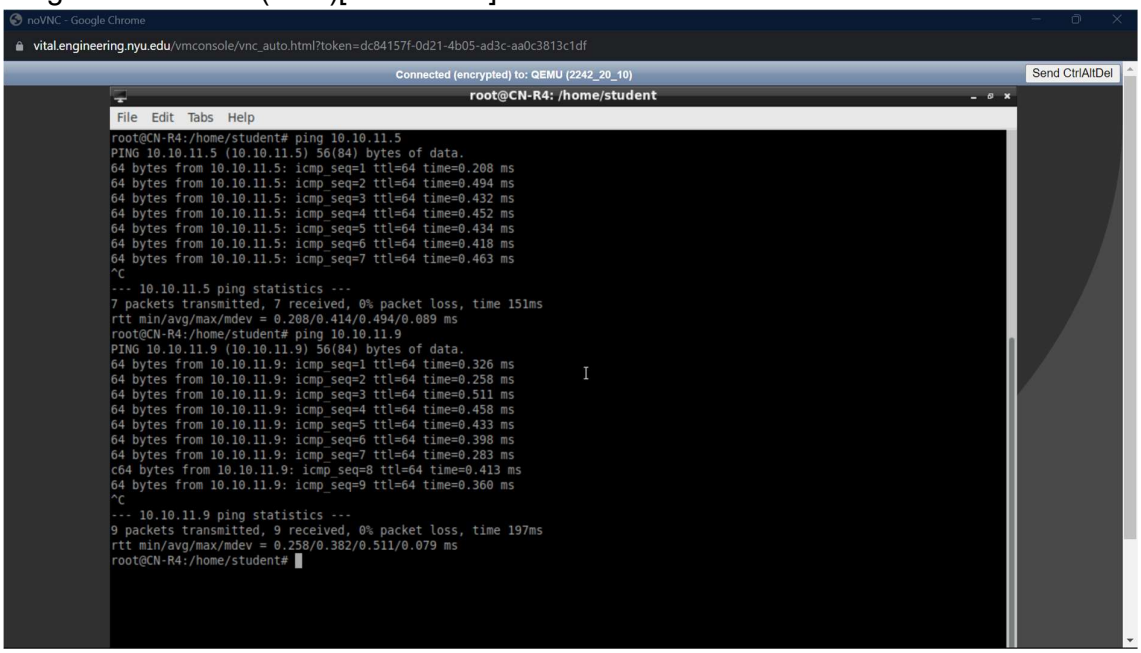


R4

Ping from R4 to R2(eth2)[10.10.11.5]

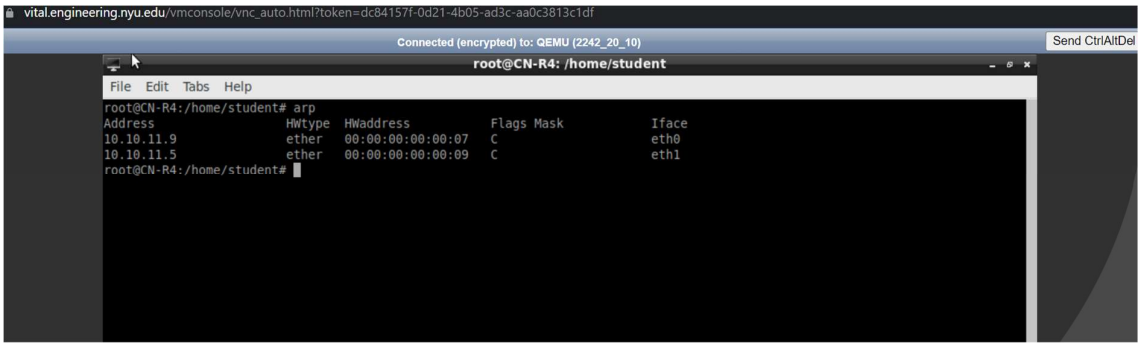


Ping from R4 to R3(eth1)[10.10.11.9]

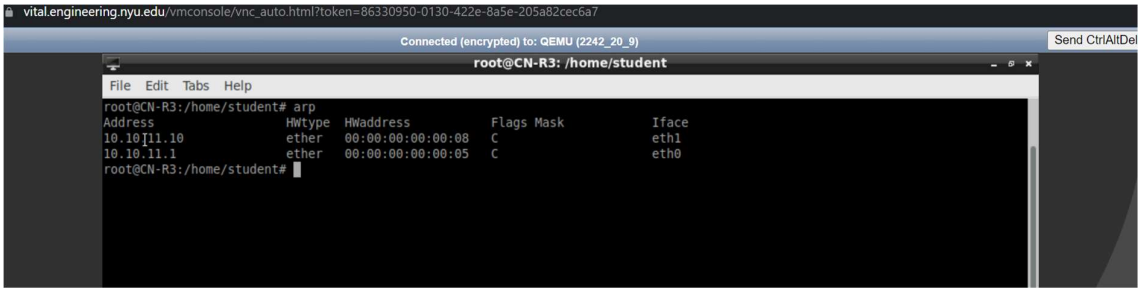


Screenshot of the ARP tables on R2, R3, and R4

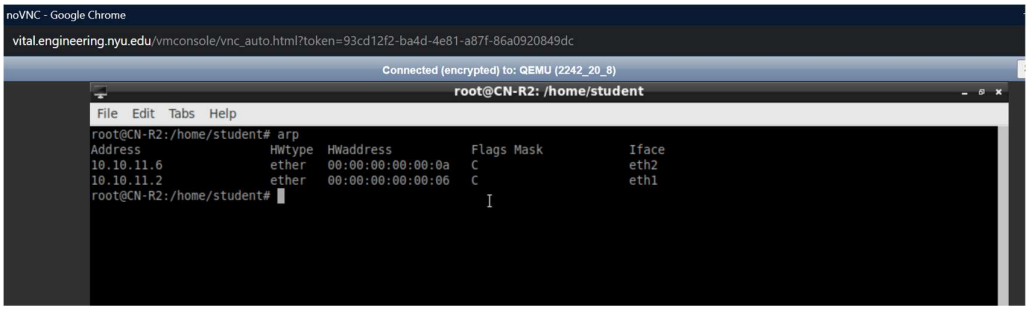
R4



R3



R2



Part 2: Questions

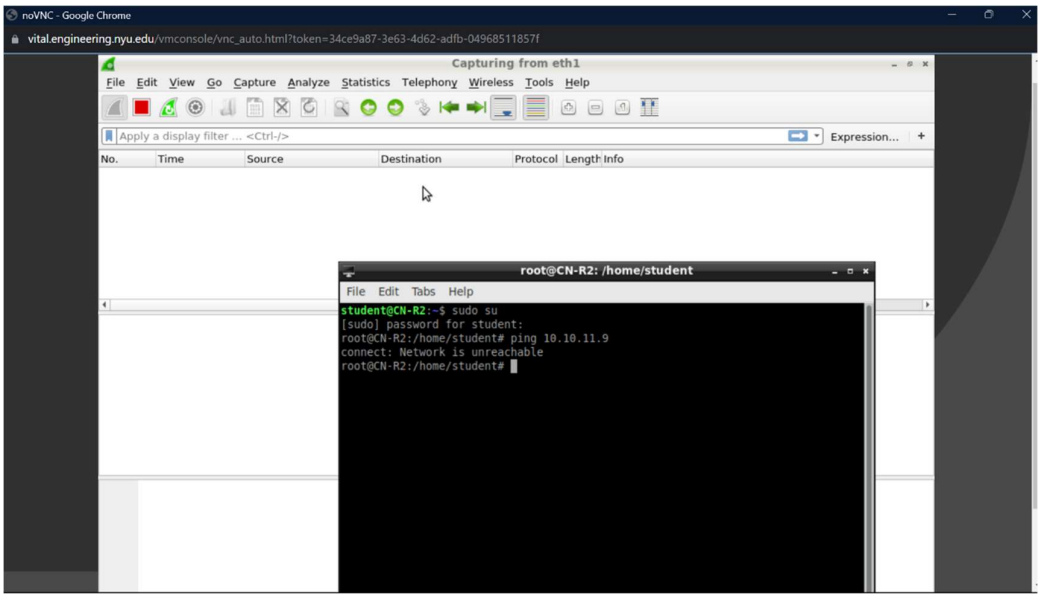
a) Why must we ensure that our subnets do not overlap? Discuss one example of something that could go wrong.

Ans: When the same IP address is assigned to more than one application or node on a network, or when the same range of IPs is implemented on various networks,

overlapping subnets occur. Overlapping subnets should be avoided since they can cause a variety of problems, including:
Network Confusion: If two devices inside an overlapping subnet are assigned the same IP address, the network may become confused about where to send data. As a result, data may not arrive at its intended location, resulting in broken connections or delayed network performance.
Faulty Traffic Flows: Traffic flows caused by overlapping subnets might be faulty or unpredictable. For example, if two networks share the same IP range and are linked, a router may loop messages back into the same network rather than delivering them to the other network. This can cause massive network outages.
Security Concerns: Overlapping subnets might also cause security concerns. If a malicious actor acquires access to one network, they may be able to gain access to other networks with overlapping subnets.

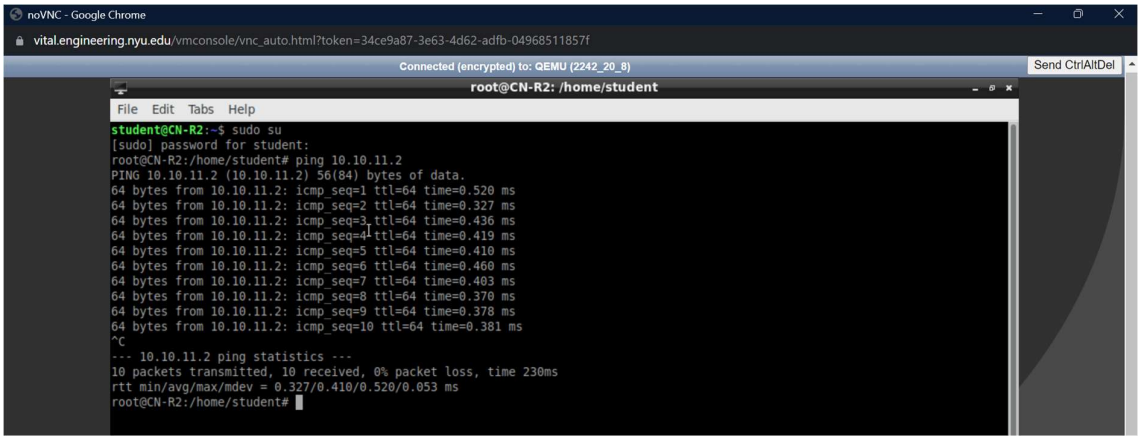
b) Suppose there is another Router (R5) directly connected to the HUB between R3 and R4. Explain whether or not we would need to reconfigure the IP subnets on R3 and R4 in order to communicate with R5.
When another router is physically connected to the hub between R3 and R4, the IP subnets on R3 and R4 must be configured in order to interact with R5. Before R5, the subnet size was /30, which allowed just two hosts. So, in order to accommodate another host, we must update the configuration to /29.

c) Run Wireshark on R2 (eth1). Now ping R3(eth1) from R2. Identify what type of packet is used in ping. Why is R2 unable to reach R3 (eth1)?
No packets are captured in Wireshark since R2 is unable to reach R3. R2 is unable to reach R3 (eth1) since both the interfaces are in different subnets and are connected via a hub. The packets used are ARP and ICMP.
After pinging R3(eth1) from R2(eth1)



d) Briefly describe how Wireshark results compare when you ping R3 (eth0) from R2 (eth1).

When we ping R3 (eth0) from R2 (eth1), we can see ICMP packets being captured by Wireshark. This is because R3 (eth0) gets successfully pinged by R2. They have the same broadcast address. When R3 detects that the request is meant for it, they start communicating using ICMP packets and R3 sends R2 it's Mac address.
In the Wireshark readings, we can see that first R2(eth1) sends R3(eth0) an ARP request asking who has that IP address.



Wireshark shows ICMP packets exchanged between R2 and R3