Lab 0 - Enterprise Network Report

Learn the basics of LAN cabling:

Determine the type of cable needed to connect the following devices:

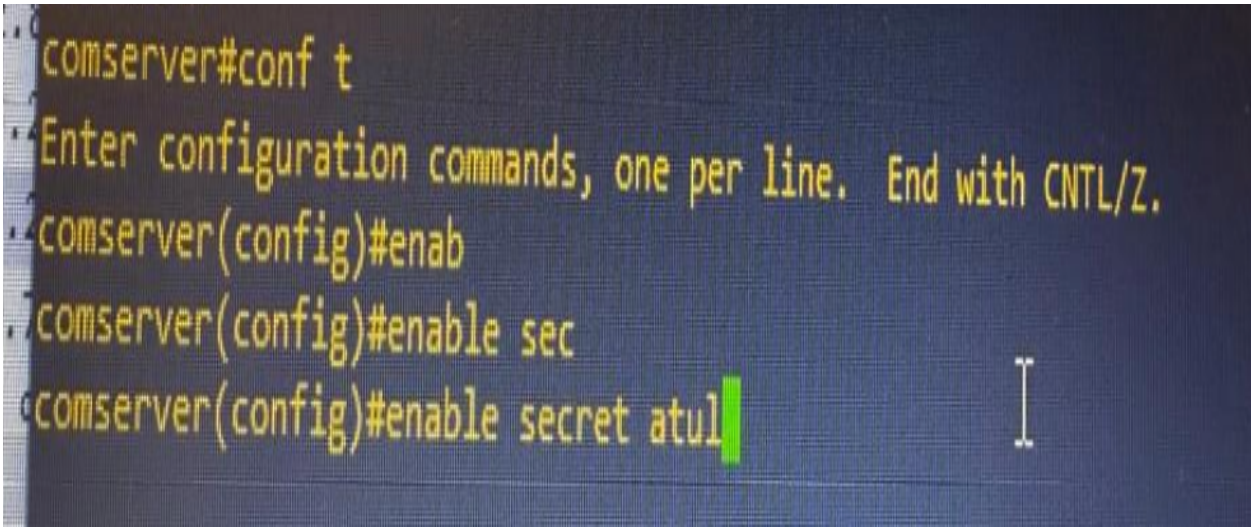
- PC to a Router - Straight Through Cable
- PC to a PC - Cross Over Cable
- Router to Router - Cross Over Cable
- Router to Switch - Straight Through Cable
- Switch to Switch - Cross Over Cable
- Hub to Switch - Straight Through Cable
- PC to Hub - Straight Through Cable
- PC to Switch - Straight Through Cable

Learn how to secure a router/switch

Setup different passwords for enable and console levels -

Enable password and console password will be set in the configuration mode on the device by using below commands –

Enable Secret - This ensures the password is saved in configuration in hashes.

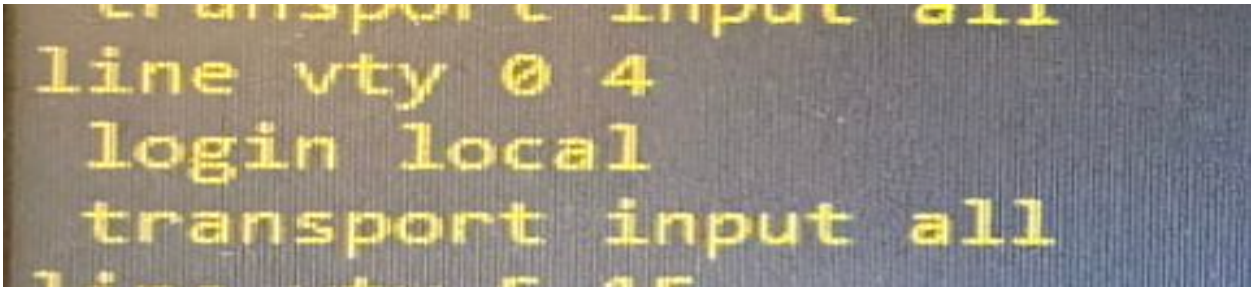


Lab 0 - Enterprise Network Report

How to connect to a router remotely via Telnet

Configure Telnet on your router(**Commands**):

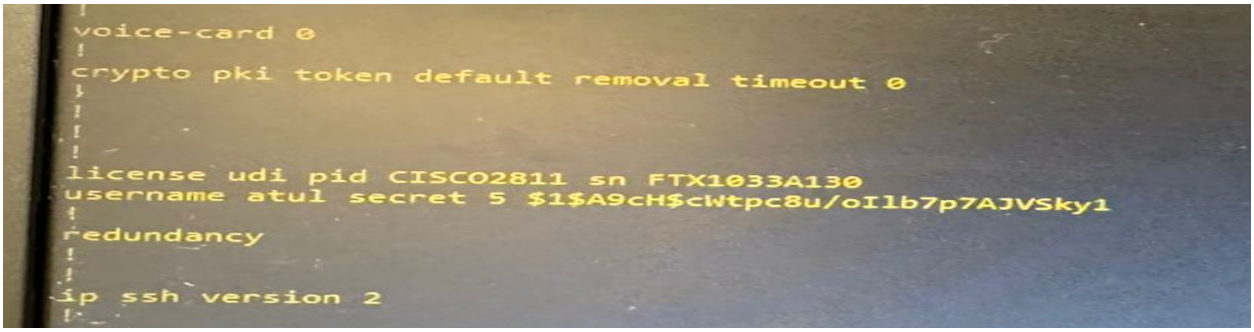
line vty 0 4
transport input telnet
login local



Configure SSH on your router(**Commands**):

generate rsa (It will prompt for key size, and I used 2048)
ip ssh version 2
transport input ssh
login local

We can configure the username and password as below which will be used by SSH or telnet –



Check whether telnet is working If not, report the problem and how to fix

If we limited the transport type to either SSH or Telnet - we could only login using on protocol - so I used the keyword all to allow telnet and SSH on same virtual lines.

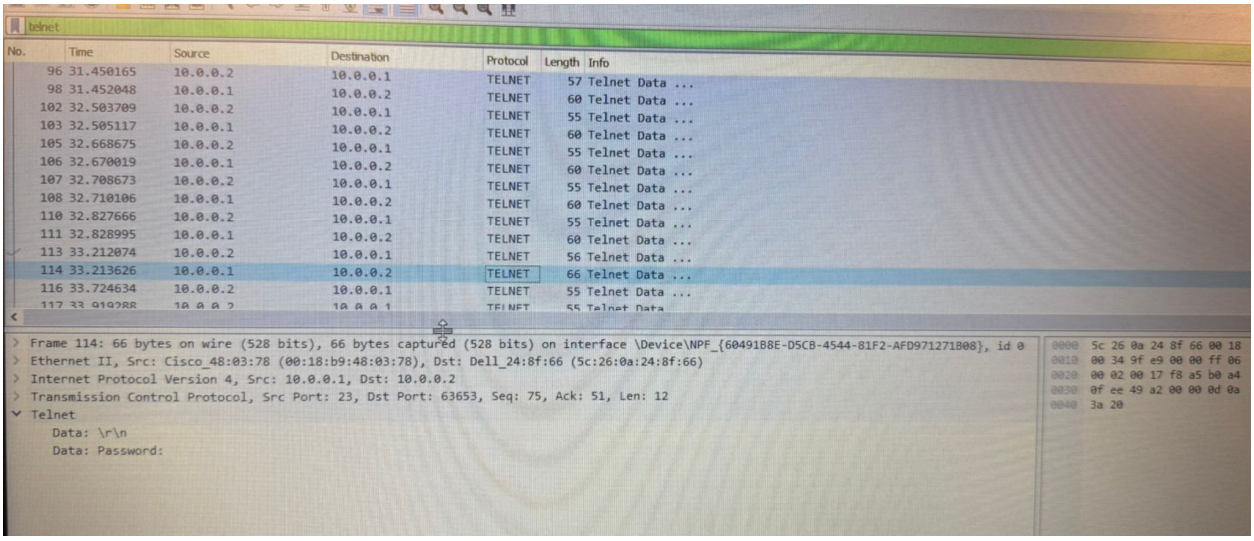
Lab 0 - Enterprise Network Report

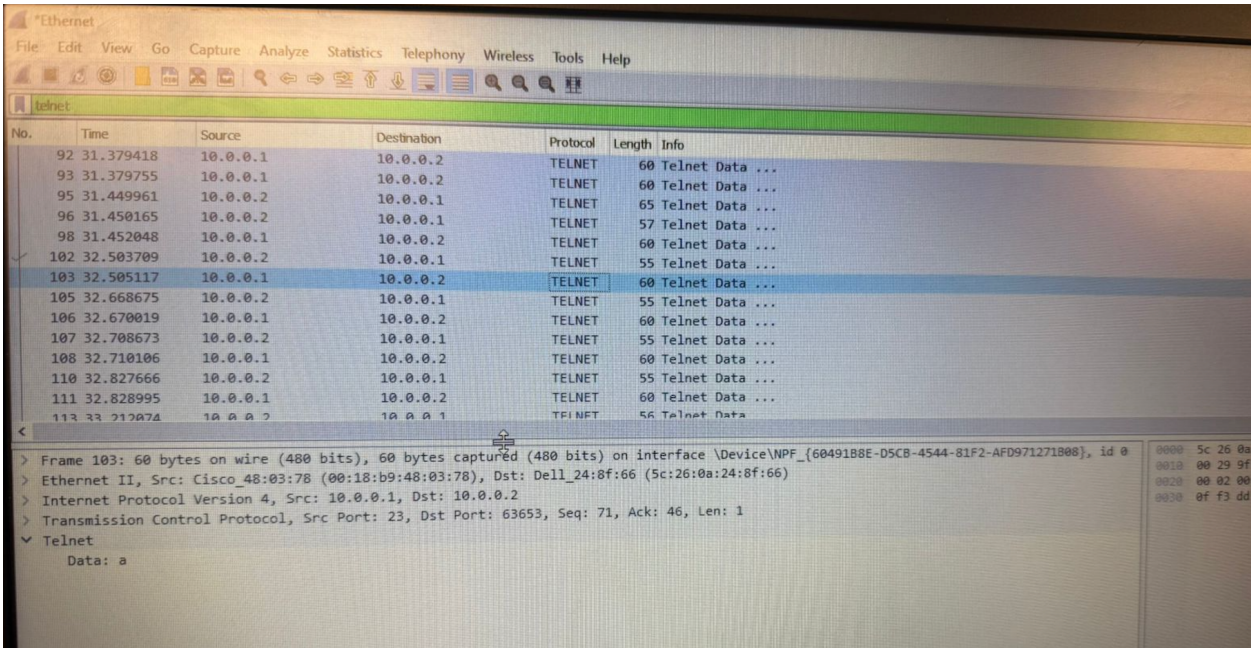
Learn the use of Wireshark packet sniffer

Use Wireshark on PC2 to obtain the Telnet Password of the Network Administrator (when he/she tries to login).

** Dissect appropriate frames/packets used by telnet, highlight password info and include in your report.

Ans - Telnet is un-secure so password exchanged during the session will be captured in Wireshark as highlighted below - the best recommendation is to use the SSH which allows safeguards against these type of issues.

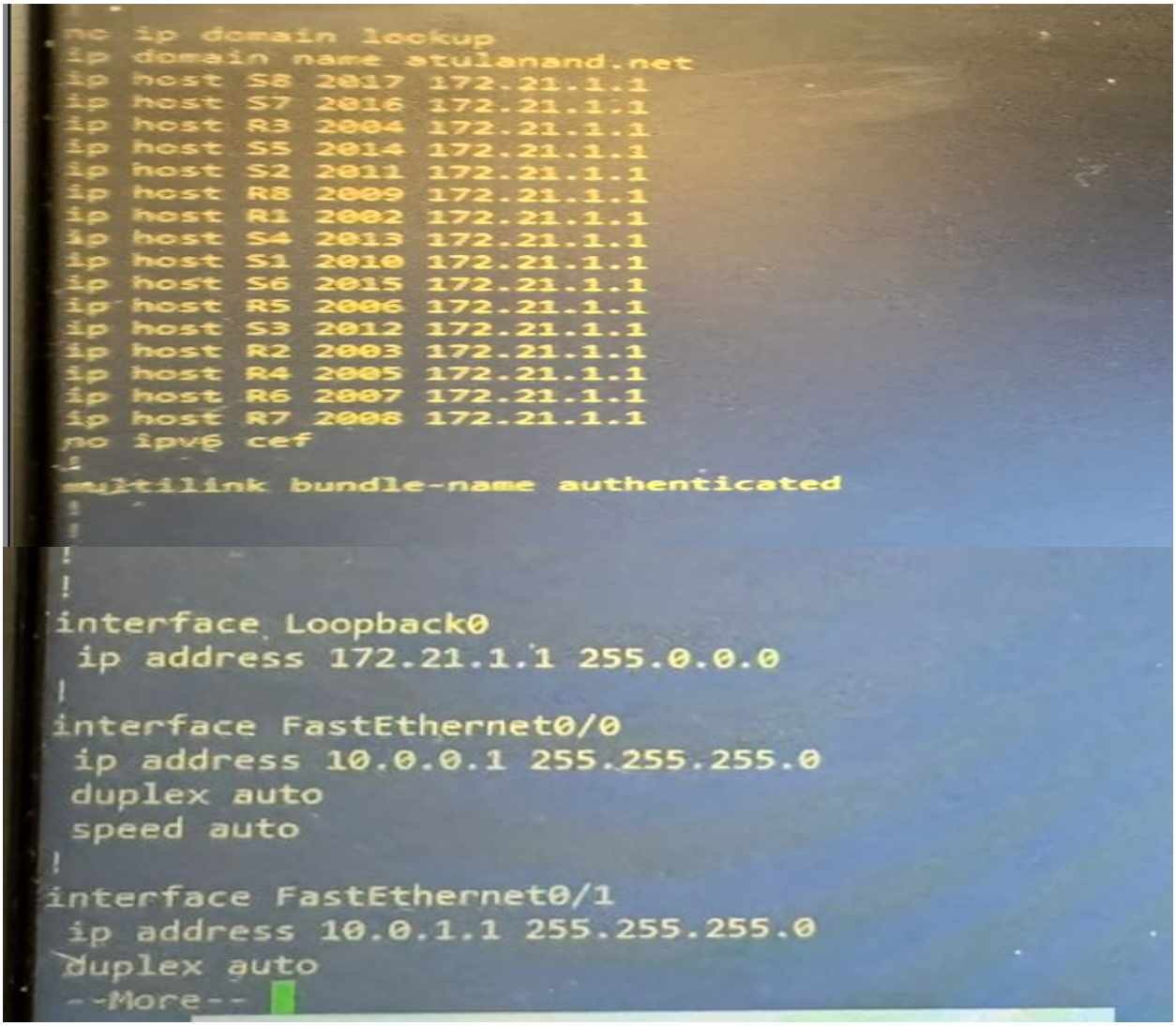




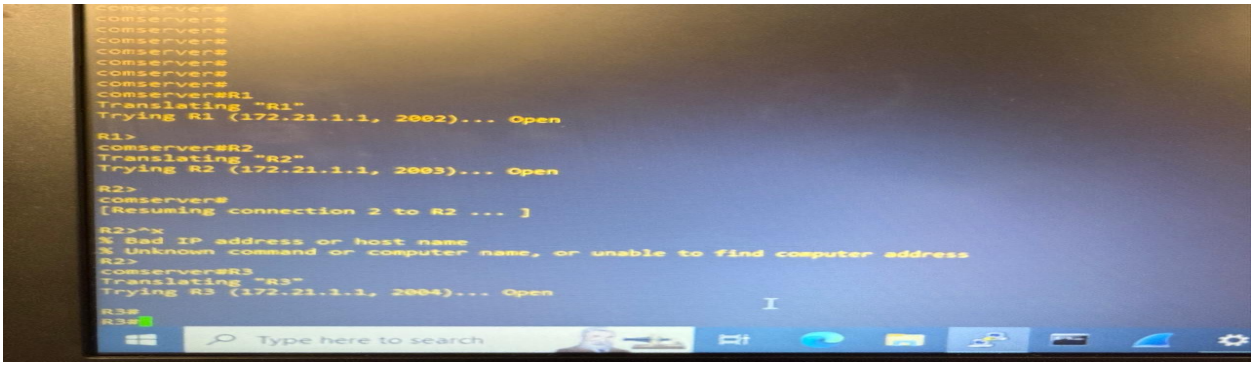
Lab 0 - Enterprise Network Report

Learn how to use a COMM server for connectivity

Complete the connections from the commserver to the 3 Cisco 3600 routers



Telnet into the 3 routers

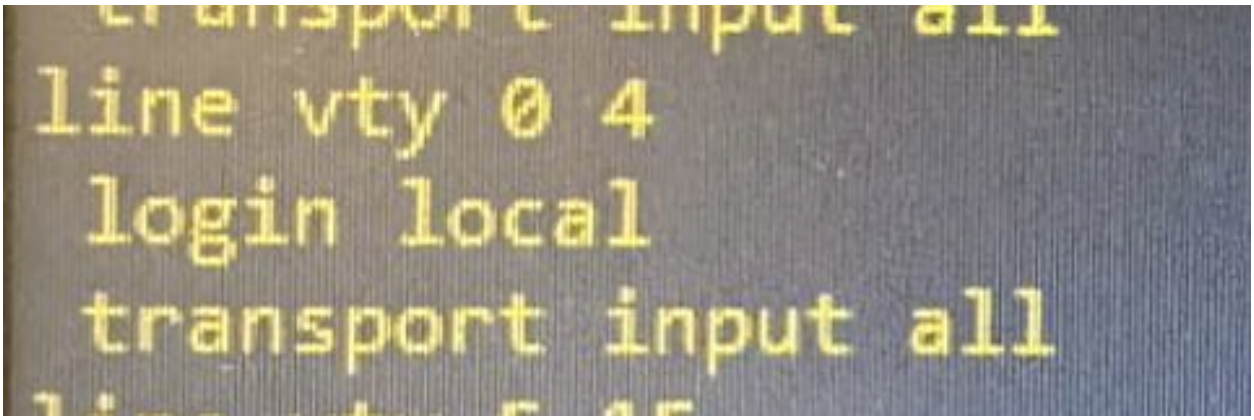


Lab 0 - Enterprise Network Report

Learn How to Telnet to Commserver

How many sessions can you open? Explain Why?

Ans - Number of sessions is directly related to how many VTY was configured so I configured 0 4 means total 5 sessions can be established via telnet.

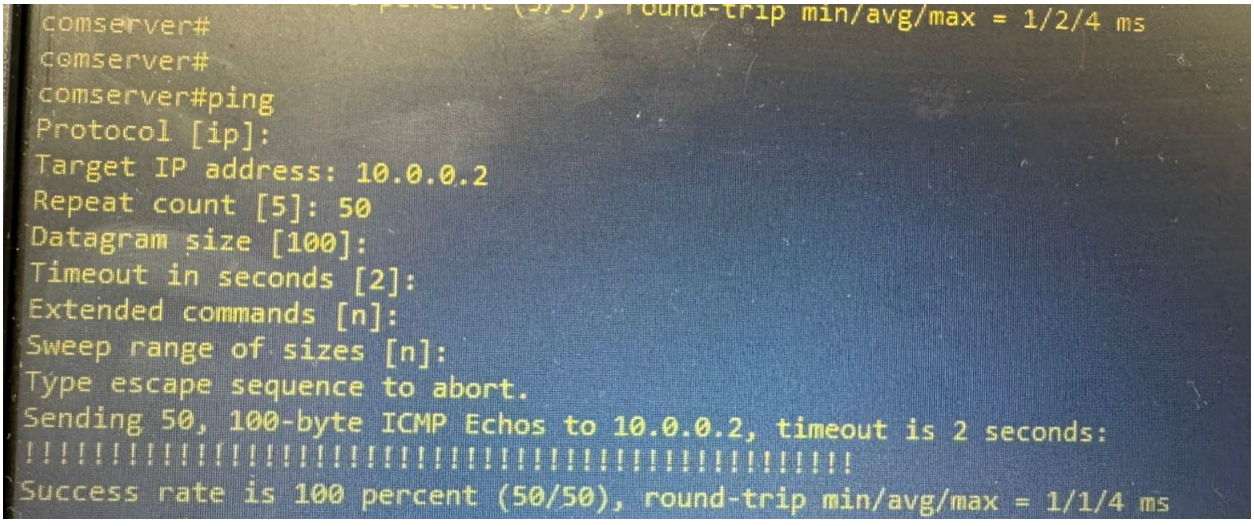


How many line VTY's session can be configured in commserver.

Ans - Total 16 VTY sessions can be configured on router from 0 to 15

Extended Ping with options in Windows and Cisco.

Use ping command with options in Cisco Router command prompt



Lab 0 - Enterprise Network Report

Use ping command with options in windows command prompt

Ans - I used the MacBook commands and here -s means size and -D is for settings the DF bit.

```
[atan8167@OIT-FVFFG1NCQ6LW ~ % ping -s 1472 -D google.com
PING google.com (142.250.72.14): 1472 data bytes
1480 bytes from 142.250.72.14: icmp_seq=0 ttl=115 time=32.305 ms
1480 bytes from 142.250.72.14: icmp_seq=1 ttl=115 time=28.822 ms
1480 bytes from 142.250.72.14: icmp_seq=2 ttl=115 time=28.252 ms
1480 bytes from 142.250.72.14: icmp_seq=3 ttl=115 time=17.263 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 17.263/26.660/32.305/5.643 ms
```

Learn to calculate Path MTU and GIANT Packets

Explain what are runt and giant packet types and how to troubleshoot those packets?

Runt Packets - The packet which is smaller than the allowed minimum size on the network

These are primarily caused by the collisions or faulty NIC or SFP or other related failures.

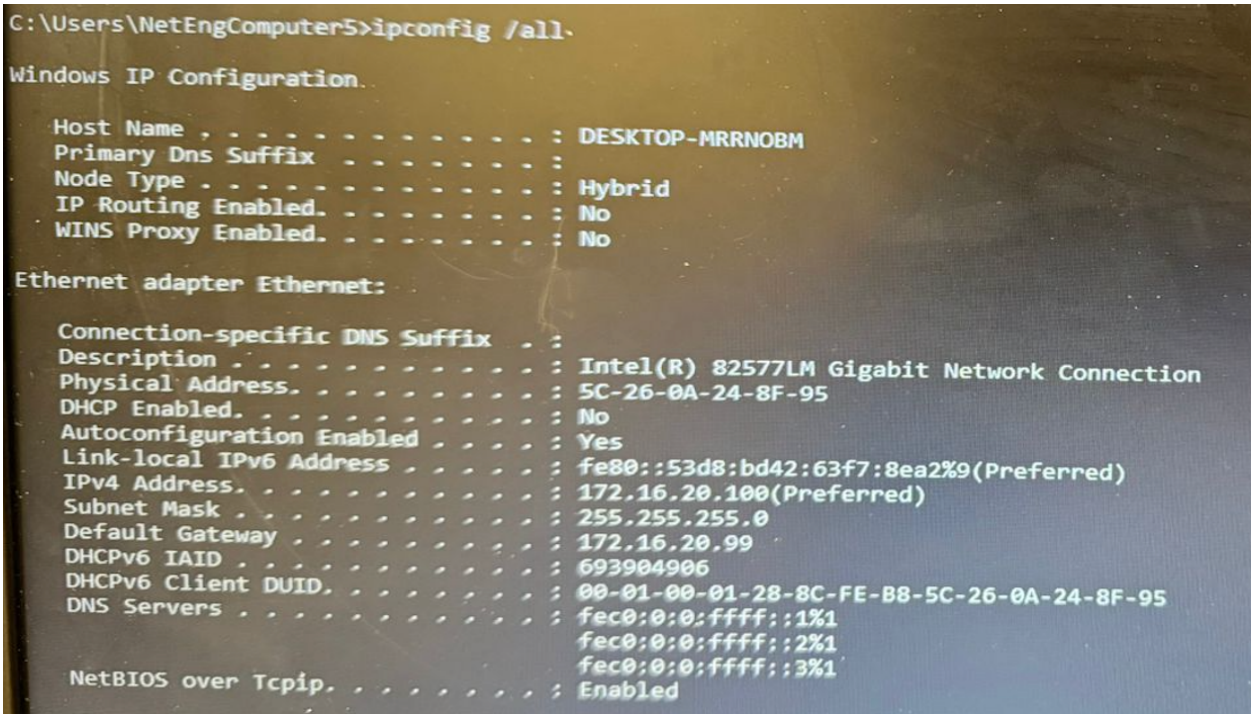
Giant Packets - The packet which is bigger than then allowed maximum limit on the network is called as Giant packets and usually these are fragmented by the device if DF bit is not explicitly set on the packet by the sender. Below screenshot shows the F bit set with giant packets which is dropped due to fragmentation not allowed.

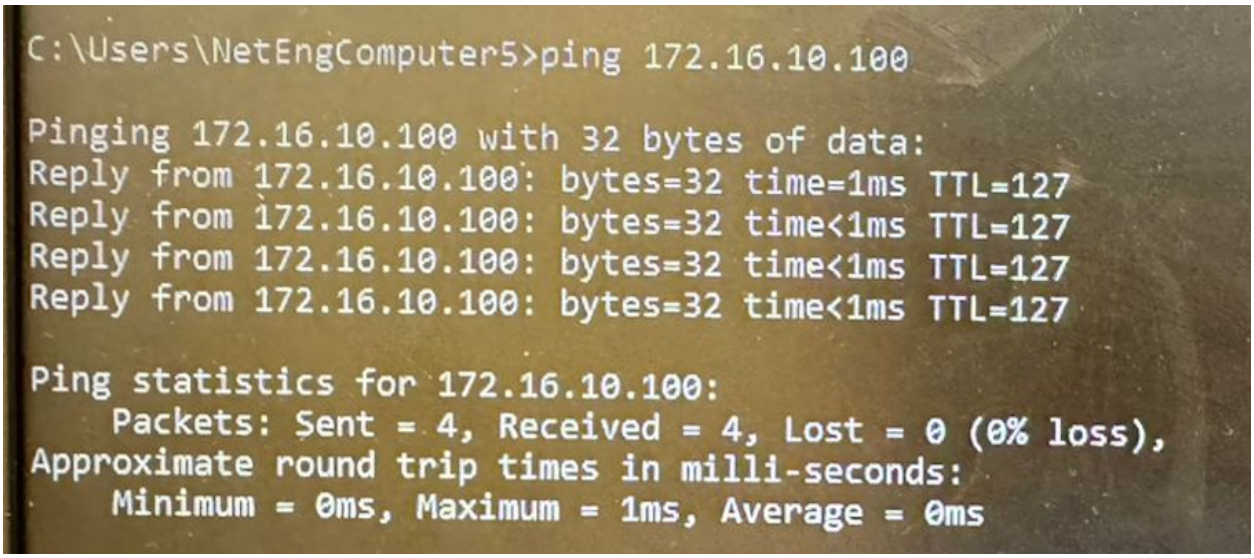
```
[atan8167@OIT-FVFFG1NCQ6LW ~ % ping -s 1500 -D google.com
PING google.com (142.250.72.14): 1500 data bytes
ping: sendto: Message too long
Request timeout for icmp_seq 0
ping: sendto: Message too long
Request timeout for icmp_seq 1
ping: sendto: Message too long
Request timeout for icmp_seq 2
ping: sendto: Message too long
Request timeout for icmp_seq 3
ping: sendto: Message too long
Request timeout for icmp_seq 4
ping: sendto: Message too long
Request timeout for icmp_seq 5
^C
--- google.com ping statistics ---
7 packets transmitted, 0 packets received, 100.0% packet loss
```

Lab 0 - Enterprise Network Report

Learn how Proxy ARP works.

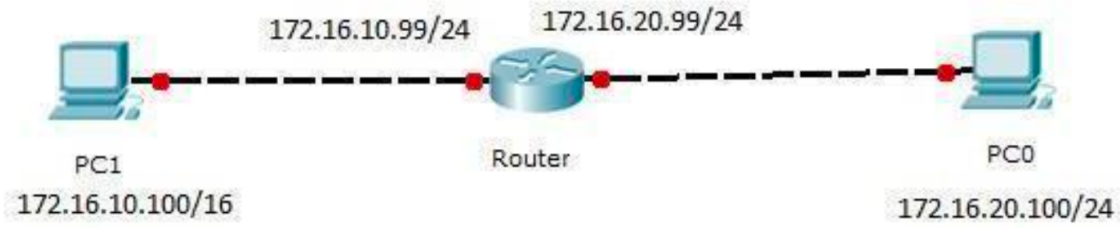
Ping from PC1 to PC2.





Lab 0 - Enterprise Network Report

Configure the no ip proxy-arp command on the router interface. Ping from PC1 to PC2. Explain the result?



In the diagram above, client PC1 is part of a /16 subnet. When we ping PC2, the host treats it as a device on the same network and sends an ARP packet to discover the MAC address. This packet is received by the router interface. Since the router has the requested network directly connected, it responds with its own MAC address by default, as proxy ARP is enabled on Cisco devices. This allows the host to ping PC2.

However, if we disable proxy ARP, the router discards the ARP request, causing the ping to fail and resulting in a connectivity failure.