**NETWORKS NOTES:**

* Class A: N.H.H.H 🡺 Binary: Start with “0” Decimal: 0-127

Class B: N.N.H.H 🡺 Binary: Start with “10” Decimal: 128-191

Class C: N.N.N.H 🡺 Binary: Start with “110” Decimal: 192-223

**Ex:** The network address of 172.16.0.0/19 provides how many subnets and hosts?

**Answer:**

Firstly, we look 172 and it is between 128-191 so this is Class B Network.

CIDR=19 it means there will be 19 bits in Binary networking;

11111111.11111111.11100000.00000000 🡺Total 19 number 1 available.

N N 3🡪1 and 13 🡪0 available.

2^3=8 Subnets 2^13-2(reserved IP) = 8190 Hosts

* **traceroute/tracert 🡺** Trace the packet while it reaches to website
* **man “command”🡺** Information about command
* **ipconfig 🡺** Protocol information about the website

**ipconfig/all 🡺** More details

**ifconfig 🡺** For Linux/Mac

* **ping “hostname/IP” 🡺** To check if host is active and it can accessible
* **arp 🡺** Display and modifies ARP tables

**arp -a**

* **nslookup “Domain/Website name”** 🡺 Give the IP address of domain
* **mtr 🡺** combine command (trace and ping) for Linux and Mac
* **nmap 🡺** Finds open port on the server (Hackers are using)- Port scanning

**Need installment:** sudo yum install nmap

* **route** 🡺 Manipulate network routing table
* **netstat** 🡺 Checks out the inbound/outbound TCP/IP connections on your machine

**netstat -e**

**netstat -a**

* **tcpdump 🡺** Captured packets comes/goes to computer from the network

**windump** for windows

* **ftp**: File transfer protocol

**sudo yum install ftp -y**

[**ftp.gnu.org**](ftp://ftp.gnu.org) **🡺** Connect to the gnu.org ftp server

**open** [**ftp.gnu.org**](ftp://ftp.gnu.org) **:**Public ftp folders here. Authentication user name**: anonymous**

**quit:** To exit from ftp

**get a.txt** 🡺 Download to any file

**put a.txt 🡺** Upload the file to the server

* **ssh user-name@host(IP or Domain Name)**
* **scp -i firtskey.pem ec2-user@Public IP:/home/ec2-user/test.txt testfile.txt**

Copy the test.txt file from home/ec2-user paste to my local as testfile.txt

* **scp -i firstkey.pem readm.txt ec2-user@Public IP:/home/ec2-user**

Copy the readm.txt file from my local to the home/ec2-user

* **curl “url(raw)”:** Copy the data from server (github etc.)

**curl “URL” -o readme.txt:** Copy the data to my local as readme.txt

* **widget:** Use for set up file or different file except txt files.
* **Difference of widget and curl;** Curl copy only the type data, widget get some secret character behind. Better to use curl for copy information on the website.