# Module 4: Networking Refereshser

*LAYER 3: ROUTING*

**Ip addresses**
Linux: inet = ipv4
32 bits = 2^32 = 4,294,967,296 (# possible IPs)

```
Linux: inet6 = ipv6
        128 bits = 2^128 = 3.4028x10^38 (# possible IPs)
```

inet 192.168.57.139 (Each set of numbers is 8 bits, 32 bits total= 4 bytes)

*bits are binary (1's and 0's)

128, 64, 32, 16, 8, 4, 2, 1 = (when added total number is 255)

**NAT** - Network Address Translation:
Assigns Private IP addresses
Any IPs that start with 192.168 are private
Private IPs are not anywhere on the public net

**Network Classes | Network # | # of Networks | Network Hosts**

Class A(Large 10.0.0.0 126 16,646,144
medium Business)

Class B 172.16.0.0- 16,383 65,024
172.31.0.0

Class C 192.168.0.0- 2,097,151 254
(Household) 192.168.255.255

*LAYER 2: SWITCHING*

MAC Address - Media Access Control
-switches work over this address
-anything that has a network Interface Card (NIC) uses a MAC address

TCP- Transmission Control Protocol: Connection oriented protocol
-Most common, High Reliability (HTTPS, websites, ssh, ftp)

```
        Works on a 3way handshake

        syn (saying Hi) -> syn ack (neighbor says hi back) -> ack (we know
we can start converstation)
```

UDP- User Datagram Protocol: Connectionless protocol
-Streaming, etc

Pentesters scan both TCP and UDP

Port: Item that can be open on a machine
Ex. HTTP: port 80
HTTPs: Port 443

```
WIRESHARK capture traffic on NIC (Network Interface Card)
```

**common ports and protocols**

TCP
-FTP (21) "FILE TRANSFER PROTOCOL"
-SSH (22) "ENCRYPTED VERSION OF ABILITY TO LOG INTO A MACHINE REMOTE"
-Telnet (23) "ABILITY TO LOG INTO A MACHINE REMOTE"
-SMTP (25) "MAIL"
-DNS (53) "A WAY TO RESOLVE IP ADDRESSES TO NAMES"
-HTTP (80) "WEBSITE" NOT ENCRYPTED
-HTTPS (443) "WEBSITE"ENCRYPTED
-POP3 (110) "MAIL"
-SMB (139 + 445) 'SAM-BUH' MOST COMMON PORT AS A PENTESTER "FILE SHARES"
-IMAP (143) "MAIL"

UDP
-DNS (53)
-DHCP (67,68) "ASSOCIATES YOU WITH AN IP"
-TFTP (69)
-SNMP (161) "SIMPLE NETWORK MANAGEMENT PROTOCOL"

**THE OSI MODEL**

1 P Physical Layer - Data cables, Cat6
2 D Switching Layer - MAC addresses
3 N Network Layer - IP addresses, routing
4 T Transport layer - TCP/UDP
5 S Session Layer - Session management
6 P Presentation Layer - WMV, JPEG, MOV
7 A Application - HTTP, SMTP

**SUBNETTING P1&P2**

*see resources folder for Subnetting Sheet
Subnetting in 7 Seconds: https://www.youtube.com/watch?v=ZxAwQB8TZsM
IPaddressguide.com