OSI Model

1. P= Physical- data cables, cat 6
2. D= Data- Switching, Mac Addresss
3. N= Network- IP addresses, routing
4. T= Transport- TCP/UDP
5. S= Session- Session management
6. P= Presentation- WMV,JPEG,MOV
7. A= Application- HTTP, SMTP

Please Do Not Throw Sausage Pizza Away

Subnetting

Allows number of hosts for a network by locking in the static and dynamic bits

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.232.121  netmask 255.255.255.0  broadcast 192.168.232.255
        inet6 fe80::2598:38a3:b85c:a1d8  prefixlen 64  scopeid 0x20<link>
        inet6 2402:3a80:4398:a43:259b:48c5:202d:3a32  prefixlen 64  scopeid 0x0<global>
        ether 58:6c:25:f8:6e:2a  txqueuelen 1000  (Ethernet)
        RX packets 1222786  bytes 1510168152 (1.4 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 220171  bytes 57192755 (54.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Structure of netmask:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL
1	128	64	32	16	8	4	2	1		128	64	32	16	8	4	2	1		128	64	32	16	8	4	2	1		128	64	32	16	8	4	2	1			
2	1	1	1	1	1	1	1	1		1	1	1	1	1	1	1	1		1	1	1	1	1	1	1	1		0	0	0	0	0	0	0	0		/24	
3									255									255									255									0		
4																																						
5																																						
6																																				Hosts	2^8	
7																																				Hosts	256	
8																																						

same structure as ip address (octals), but the bits can only be turned on in order.

The turned on bits are fixed and cannot be changed by any nic or networking device, ex: wifi devices cannot be assigned to these addresses/ any protocol cannot modify these values.

for ex: a wifi base address with 192.168.232.0 and netmask 255.255.255.0 signifies the first 24 bits are turned on(all 255) hence when assigning ip address, these cannot be changed. i.e 192.168.232 are fixed values and cannot be changed by router or anything.

hence the effective address that can be allocated to devices on the network are 192.168.232.0-255 i.e 256 hosts (2^8 as the last 8 bits are left unset and these places can be used) hence 254 devices can be connected to this network (first and last address are reserved for network id and broadcast)

since the first 24 bits are set, the address and the subnet can be represented as: 192.168.232.0/24 where the /24 signifies the number of set bits.

ex: 192.168.0.0/23 signifies only 23 bits are set, i.e: 11111111.11111111.11111110.00000000=255.255.254.0

therefore (2^9) 512 hosts can be accomodated out of which the last decimal can range from 0-255 (2^8 unset bits) and the 2nd last can range 0-1 (2^1 unset bits)

hence possible ip ranges are 192.168.0.0-255, 192.168.1.0-255

	1	2	3	4	5	6	7	8	255.0.0.0
	9	10	11	12	13	14	15	16	255.255.0.0
	17	18	19	20	21	22	23	24	255.255.255.0
	25	26	27	28	29	30	31	32	
Hosts	128	64	32	16	8	4	2	1	
Subnet	128	192	224	240	248	252	254	255	

Structure of subnet mask

No. of unset bits

Corresponding subnet mask value

The Cyber Mentor's Subnetting Sheet

	Subnet x.0.0.0							
CIDR	/1	/2	/3	/4	/5	/6	/7	/8
Hosts	2,147,483,648	1,073,741,824	536,870,912	268,435,456	134,217,728	67,108,864	33,554,432	16,777,216
Class A	Subnet 255.x.0.0							
CIDR	/9	/10	/11	/12	/13	/14	/15	/16
Hosts	8,388,608	4,194,304	2,097,152	1,048,576	524,288	262,144	131,072	65,536
Class B	Subnet 255.255.x.0							
CIDR	/17	/18	/19	/20	/21	/22	/23	/24
Hosts	32,768	16,384	8,192	4,096	2,048	1,024	512	256
Class C	Subnet 255.255.255.x							
CIDR	/25	/26	/27	/28	/29	/30	/31	/32
Hosts	128	64	32	16	8	4	2	1
Subnet Mask (Replace x)	128	192	224	240	248	252	254	255

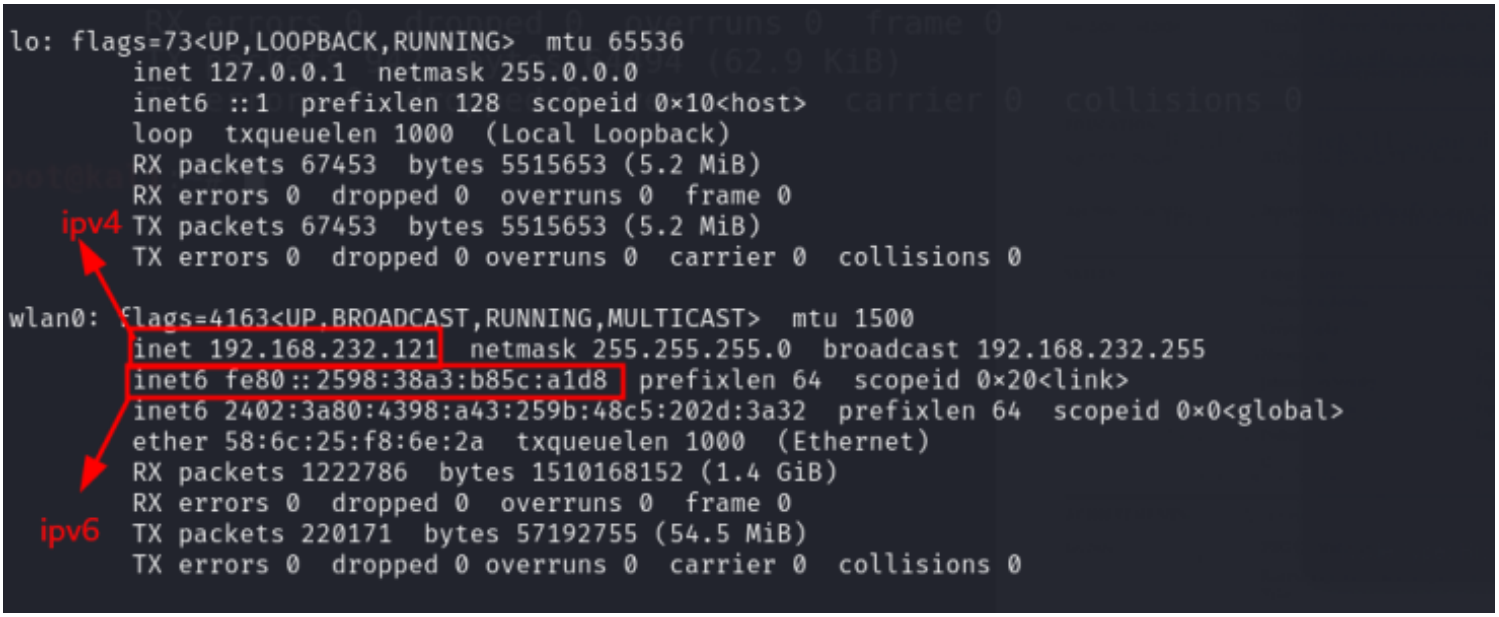
Notes:
*Hosts double each increment of a CIDR
*Always subtract 2 from host total:
Network ID - First Address
Broadcast - Last Address

	Subnet	Hosts	Network	Broadcast
192.168.1.0/24	255.255.255.0	254	192.168.1.0	192.168.1.255

Addresses

IP Address

ifconfig



layer3 of osi model (router)

public and private ip addresses exist, translation is done by NAT

ipv4

Decimal notation

1 and 0 put together for human readable format

ex: 192.168.57.139, each number is just decimal representation on a binary octal. ex: 11111111.11111111.11111111.11111111=255.255.255.255 (4*8=32 bits)

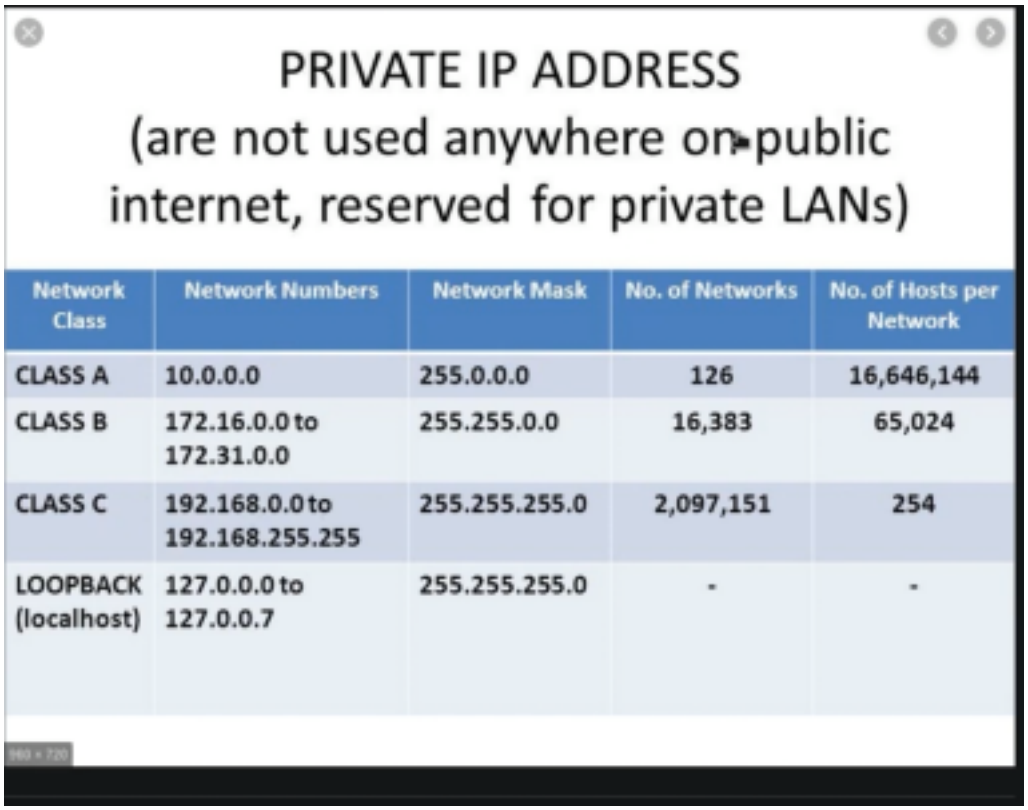
approx 4 billion addresses (2^32) , almost all are used up, hence we use NAT

ipv6

hexadecimal notation (128 bits, possible combinations, 2^128)

NAT

Network Address translation



Translates private address to public address since limited number of ipv4 address available

various private address are interfaced to single public address using nat

public addresses are brought by various organisation such as isp

MAC Address

Media access control

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.232.121  netmask 255.255.255.0  broadcast 192.168.232.255
        inet6 fe80::2598:38a3:b85c:a1d8  prefixlen 64  scopeid 0x20<link>
        inet6 2402:3a80:4398:a43:259b:48c5:202d:3a32  prefixlen 64  scopeid 0x0<global>
        ether 58:6c:25:f8:6e:2a  txqueuelen 1000  (Ethernet)
        RX packets 1222786  bytes 1510168152 (1.4 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 220171  bytes 57192755 (54.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

physical address: comes with network interface cards(nic) and allows for physical switches to read and transport messages

Layer 2 (switching)

MAc Adddress: first three pairs are identifiers, i.e: 58:6c:25

Protocols

Layer 4 of the OSI model (transport layer)

utilizes ports for communication (65k+ ports)

TCP

Transmission control protocol

connection oriented . ex: http, https, ftp, ssh

Works on 3 way handshake

UDP

User datagram protocol

Connection less, ex: voip,dns

3 way handshake

SYN > SYN ACK> ACK

SYN: Synchronize (initiate connection)
ACK: Acknowledge

ports

Common Ports and Protocols

- TCP
  - FTP (21)
  - SSH (22)
  - Telnet (23)
  - SMTP (25)
  - DNS (53)
  - HTTP (80) / HTTPS (443)
  - POP3 (110)
  - SMB (139 + 445)
  - IMAP (143)
- UDP
  - DNS (53)
  - DHCP (67, 68)
  - TFTP (69)
  - SNMP (161)

ARP

Address resolution protocol