Host -- A computer or other device on a TCP/IP network.

Network Layer: (Anything involves TCP/IP protocol actions happens here. EG: put in wrong IP address)

- Specifies an addressing scheme for the network (IP addressing), and how packets should be routed through the network
- Also responsible for the end to end delivery of packets
- Process of encapsulation occurs here
- Contains protocols which govern how messages flow around network.

Encapsulation:

- Is the process of where data created application layer and is send down to all the layers (Application → Physical layer). It does that by adding information (headers) required to ensure the transmission reaches the destination. All layers will interact with each other. Steps
    - Adds header to **data** in Layer 7 (**Application)** and sends it down to presentation layer now called segment
    - Adds header to **segment** in **Transport layer** and sends it down to network layer
    - Adds header to **Packets** in **Network layer** and sends it down to data link layer
    - Adds header and trailer to **Frame** in **Data layer** and sends down to Physical layer now called Bit

The IP Hourglass Model:

- Idea everything runs over Ip and Ip runs over everything. So IP becomes the domain protocol and is central

Network Layer Protocols:

- Internet Protocol version 4 (IPv4)
- Internet Protocol version 6 (Ipv6)
- ICMP: used for pinging
- IPX
- Appletalk

Internet Protocol:

- Governs how the packet flows/transmission from source to destination based off IP address (Unicast, Multicast Broadcast)
    - **Unicast Transmission:** Where packets send for only one host/device ***<u>*Important: Devices are now called host</u>***
    - **Multicast Transmission:** Transmission will reach more than one host but not all
    - **Broadcast:** Packets are destined for all other host within *subnet* eg: lms to everyone
- Ip communication are **connectionless** so no setup is required like handshake

- Similar to UDP, IPV4 is best effort meaning doesn't mean unreliable but reliability must come from another layer of network stack
- Can function over cooper, air, fibre
- Ipv4 is media independent
- *Supports- different types of transmission

IP Protocol Headers: (fields/characteristics)

- Source Address: The originating host address. Where we send packets
- Destination Address: The destination host address
- Version: Ipv4 or Ipv6
- Protocol (What transport layer protocol either TCP or UDP)
- Time to live (TTP): how far can we send packets before it gets dropped

IP Address:

- Is an address is a 32 bit numerical label assigned to each devices connected on network that uses Internet Protocol for communication.

- Decimal: 32 Bit Numbers split into 4 (parts) numbers each (parts) number are separated by dot → 111**.**111.111.111 (Notice 4 (parts) Numbers 111 x 4)
    - The (parts) numbers can only range from 0 to 255
- Octet: is the binary name for individual (parts) numbers and represent 8 bits (binary digits)
    - 32 comes from (8 binary bits x 4 octet)

- Contains **Public Ip address**: A public Ip address is the IP address that is used to identify your home network to the external world.
- Contain **Private Ip addresses**: A private Ip address is the Ip address given to each network device on your home network and it can identify the different devices on your network. The Isp offers the public ip address while the router assigns the private Ip address to networking devices connected to it
- These ranges can be used inside private networks and packets addressed to these can't be routed on the internet [Public are
    - 10.0.0.0 – 10.255.255.255
    - 169.254.0.0 – 169.254.255.255
    - 172.16.0.0 – 172.31.255.255
    - 192.168.0.0 – 192.168.255.255
- Issue: Packets that come from private Ip addressing must undergo Nat (network address translation) to be routed over internet

IP Address Ranges Assignment:

- Private is above
    - 10.0.0.0 – 10.255.255.255

  - 169.254.0.0 – 169.254.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
- Loopback: 127.0.0.1 to 127.255.255.255
  - Used for virtual network interface for testing. Send data to yourself
- Link Local: 169.254.0.1 to 169.254.255.255
  - Communication for local subnet only
- Documentation: 192.0.2.0 →192.0.2.255
- Public anything outside so think: 132 etc

Ip address Hierarchy:

- Allows host to send data across the internet without needing to know about every other host on network. So it reduces traffic which improve performance
- We can also use IP address hierarchy to reduce size of routing tables

Decimal to Binary Conversion:

- Write out powers of 2 horiziontal
- Then subtract the decimal number and add a one below if it can be subtracted (So bit must be smaller
- 112: 01110000

Binary to Decimal Conversion:

- Addition of Bits (other way around)
- 0111111: (n + 1) – 1) → N is the number of bits + 1 at the start of the leading ones
  - Eg: 32 (the 1 is at 16 but one more) – 1 = 31

Subnetting:

- Is breaking a large range of IP address down into small sub networks/subnet. A router allows this since it allows different networks together (Different network ID ie different subnets)
- Purpose:
  - Security- allows different security polices to be applied to groups of users. This is so we can contain security incidents or faults
  - Performance- reduces performance overhead caused by excessive broadcast. So reduces broadcast traffic

Classful network vs Classless addressing (VLSM):

- Where Ip addressing is helped determined by class the subnet mask is based on the IP. Bad because size of each block of ip addressing. Classless addressing is where block of ip address can be assigned by an organisation based on their size. These blocks can be further

subdivided by network administrator. Efficient because we reduce chance of running out of ipv4

- **Important:**
  - **VLSM (Classesless Addressing) → different subnet mask**
  - **Classeful → Same subnet mask for all sub networks**

Packet forwarding occurs here Network Layer (On a different ANS sheet. Refer there)

General Process Subnetting:

Method 1: xxx.xxx.xxx.xxx (subnetMask)

-

Method 2: VLSM subnetting (So find Ip of each new sub network)

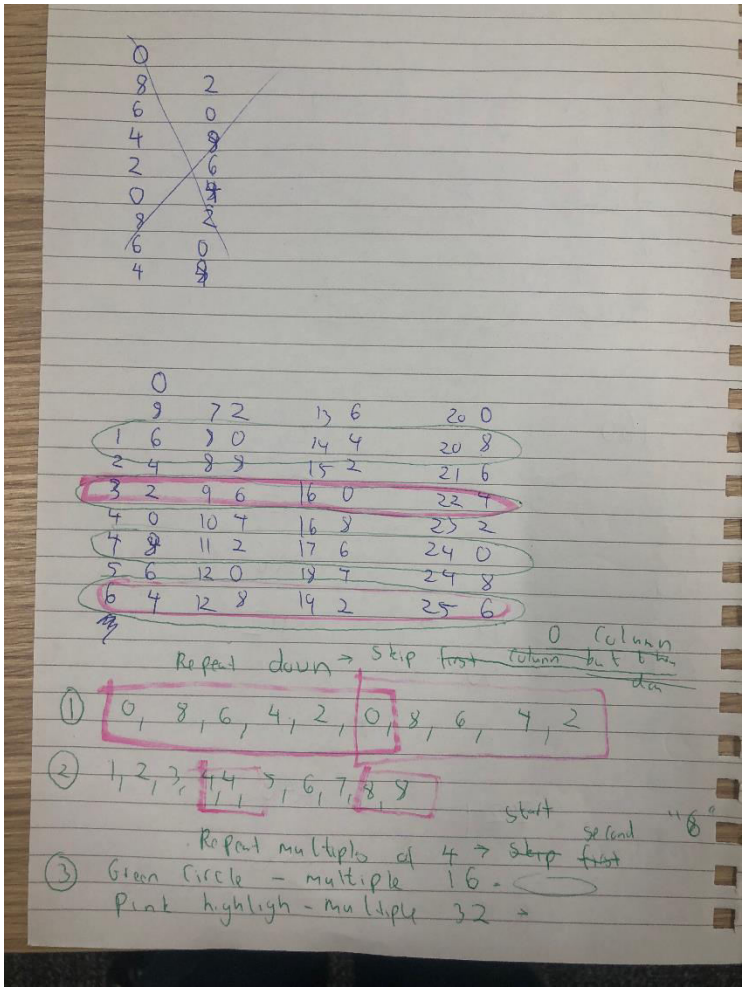
- **Find info like broadcast etc**

/18 = 18 on bits from the start

Method 1: Subnetting:

10.4.211.66/18

4094	2046	1022	510	254	126	62	30	14	6	2	Nil	Nil	**Actual no. of hosts** that can be assigned and used by a device (Host-2)
4096	2048 **8	1024 **4	512 **2	256 **1	128	64	32	16	8	4	2	1	**No. of host/IP**
2^12	2^11	2^10	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	**No of host bits** n in (2^n)
/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32	**Subnet Mask** (CIDR or /Notation)
240	248	252	254	255	128	192	192+32 =224	224+16 =240	248	252	254	255	**Subnet Mask (dotted decimal)** 255.255.255.X *Note: It's The previous no add by next number of host on right. ***/27 && /28 work out**



Before Begin:

Magic Number to Increment = /19 →No of host

1) **Work out what class/cut it will be**

So to work out cut line ip original ip up with subnet in dotted decimal

10.4.235.99 **255.255.**224.0 *This is just /18converted to dotted decimal

Notice 255 in first and second octet therefore it is that class

Answer = 255.255.x.x → these two changes

2) **Reset/Increment by Magic No/Host OR DRAW 2 TABLES → Multiplication table + Subnet Table**

Reset to 0 (VLSM no Reset) → **Increment by Magic No/Host**

If Host > 128 then

Host = 128 64 32 16 8 4 2 1 ← Starting

Incremented Table

10.4.0.0 → (63)
10.4.64.0 → (127)
10.4.128.0 → (191)
10.4.192.0 → (255.255)
10.4.256.0 = 10.5.0.0 (Max 255)
10.5.64.0

Subnet/CIDR: This is the subnet given →18

***#ip/Host:** 2^n = → READ TABLE BASED ON SUBNET MASK /18

Network Address: First IP not usable → READ INCREMENTED CLOSET START IP 10.4.211.66 closest to 10.4.192.0

Broadcast Address: Last Ip not usable → READ INCREMENTED CLOSEST START IP 10.4.211.66 CLOSEST IS 255 = 1 less then next network ***Think VLSM

First usable ip: Refer to incremented table → 10.4.192.1

Last usable ip: Refer to incremented → 10.4.255.254

Next Network/Start of Next: Refer to incremented table 10.5.0.0

No. Host bits: 2^n number: READ CHART BASED OF SUBNET MASK /26 OR CONVERTED

DO: http://www.subnettingquestions.com/

What is the last valid host on the subnetwork 172.25.102.0 255.255.254.0?

Answer: 172.25.103.254

***Valid = usable so without broadcast/network**

Method 2: VLSM Subnetting:

Question: use vlsm subnet

eakdown of employees by department.

Department	Number of Employees
Administrative Support	108
Accounts	86
Human Resources	22
IT Support	58
Research & Development	642
Sales	255
Security Services	31

Network IP: 203.5.80.0/20

3) Draw Table

4094	2046	1022	510	254	126	62	30	14	6	2	Nil	Nil	**Actual no. of hosts** that can be assigned and used by a device (Host-2)
4096	2048 **8	1024 **4	512 **2	256 **1	128	64	32	16	8	4	2	1	***No. of host/IP
2^12	2^11	2^10	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	***No of host bits n in (2^n)
/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32	***Subnet Mask (CIDR or /Notation)
240	248	252	254	255	128	192	192+32 =224	224+16 =240	248	252	254	255	**Subnet Mask (dotted decimal)** 255.255.255.X *Look below

Octet 3 Octet 4

***= Need for Exam

IF HOST IS > 128 Always Increase 128 64 32 16 8 4 2 1 not 512 etc

For octet 4 the min increment is 4

- No reset

4) **Write host and work out subnet mask (Highest to lowest)**

*See what the host fit into actual **no of hosts**

642 = Fits into 1022 → /22
255 = Fits into 510 → /23
108 etc
86
58
31
22

5) **Work out what class/cut it will be**

So to work out cut line ip original ip up with subnet in dotted decimal

203.5.80.0
255.255.240.0 *This is just /20 converted to dotted decimal

Notice 255 in first and second octet therefore it is that class

Answer = 255.255.x.x → these two changes

6) **Do questions/INCREMENT → Network address for subnet + Broadcast address**

- See what the host fit into actual **no of hosts**
- **Increment** the 255.255.x.x (x part) by **NO. OF HOST (DYNAMIC SO WILL CHANGE)**
    - Always 128 64 32 16 8 4 2 1 even IF HOST IS > 128
    - For octet 4 the min increment is 4
    - No reset

Research and development network subnet (642):

203.5.80.0/22 → 203.5.83.255 **/22 comes from above and the second part is broadcast address as well

Notice: One less for 255.255.x.255 is always the 255 one

Sales (255):

203.5.84.0 /23 → 203.5.85.255

Administrative (108):

203.5.86.0/25 → 203.5.86.127

Wan Link: NOT REAL HYPOTHETICAL

This is router to other host/router. Always 2 host → increment by 4 host since remember for octet 4

Router → Admin

203.5.86.128 /30 REMEMBER ALWAYS 4 HOST →

Router → Sales

Etc

****NOTE: WHEN IT IS A CLASS B THE THIRD AND FOURTH OCTET DON'T TURN TO 0 MEANING THE VALUES ARE STILL THE SAME IE. 128.10.1.0 → Host: 1.0 (So third octet starts at 1 not 0)**

- **Class:** Helps us identify the network and host ID cut **this will be compared 203.5.80.0/20 to /20 = **255.255.240. 0**
  203.5.80.0 **255.255.240. 0** (THIS indicates cut)

- **Subnet: Ip/subnet mask:** First subnet 203.5.80.0 /(Largest No of host device mask)

- **Subnet Mask:** (/20) is a number **helps** that tells computer which addresses are local (part of the subnetwork) or are outside a subnetwork. Without it all ip addresses will be trying to *broadcast propagate* with one another. It splits the Ip address into and
  - *Network Identification*: (203.5)
    - Doesn't Change because we are subnetting a major network (aka making a large network smaller). So some part of the large network has to have same IP bits
    - Indicates if device is on the sub network
  - *Host Identification:* (0.0): Changes in order to give a device a unique IP.

***IF THERE IS A SUBNETMASK ASSUME THAT THE NETWORK HAS SUB NETWORKS IN IT OR THE QUESTION DEALS WITH SUB NETWORKS**

- **Network address:** (203.5.80.0) starting point Ip address of a network/subnetwork. *can't be assign to host device or pc

- **Broadcast address:** (203.5.83.255) the final ip address on the network/subnetwork used to send packet to everyone on local subnet *can't assign to host device or pc

- **Host address:** First and last useable IP address in-between network and broadcast (not including them)
- **No of subnet host:** Given to you when you/Typology when you do VLSM question
- **No. subnet host bits:** 2^n number: READ CHART BASED OF SUBNET MASK /26 OR CONVERTED

Convert CIDR to Dot Decimal

First off understand → /32

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 4 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 1 1 1 1 1 1 1 1 1

- /32 means 32 all turned on therefore

(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)

255.255.255.255

Second Question → /28

11111111 11111111 11111111 11110000

- /28 means: 8 (switched on in octet) x 3 = 24 Therefore → 4 Turned on in octet 4

255.255.255.(128+64+32+16)

255.255.255.240

Last Question → /21

11111111 11111111 11111000 00000000

- /21 means: 8 x 2 = 16 Therefore 5 Turned on in octet 3

255.255.(128+64+32+16+8).***0***

255.255.248.0

Ip Address class:

Address Class	First Octet Range	First Octet Bits	Subnet Mask	Network / Host Portions	Number of Hosts
A	1—127	**0**0000001—**0**1111111	255.0.0.0	N.H.H.H	16,777,214
B	128—191	**10**000000—**10**111111	255.255.0.0	N.N.H.H	65,534
C	192—223	**110**00000—**110**11111	255.255.255.0	N.N.N.H	254
D	224—239	**1110**0000—**1110**1111	-	N/A (Multicast)	-
E	240—255	**1111**0000—**1111**1111	-	N/A (Experimental)	-

Concepts learnt:

- **VLSM IP scheme includes → Network address**

https://www.reddit.com/r/explainlikeimfive/comments/qnc2g/eli5_subnet_masks/