INTRODUCTION

Topic syllabus discussion.

Network

Two or more devices connected to each other and sharing its information and resources.

Diagramatical representations .

Cisco Device Icons

- The following table lists the specific icons Cisco uses to represent network devices and connections.

Icon	Represents
	Hub
	Bridge
	Switch
	Router
	Access point
	Network cloud
	Ethernet connection
	Serial Line connection
	Wireless connection

NETWORK DEVICES

1.Hub - A network hub serves **as a connection point for all devices in a LAN**. It is basically a multiple-port repeater because it repeats an electrical signal that comes in one port out all other ports (except the incoming port).

2.Switch – Modular switch / Non modular switch , L2 switch L3 switch .
3.Router -- **router** is hardware device designed to receive, analyze and move incoming packets to another network.
4.Firewall – it's a device that protects network form unauthorized access , controls incoming and outgoing traffic based on set of rules
5.Wireless access point – is a device that allows other Wi-Fi devices to connect to a wired network
6.WLC – Device which controls AP .

CISCO

CISCO SYSTEMS INC. IS THE WORLDWIDE LEADER in networking for the Internet. The company was founded in 1984 by two computer scientists from Stanford University seeking an easier way to connect different types of computer systems.

Cisco Systems shipped its first product in 1986 and is now a multi-national corporation, with over 35,000 employees in more than 115 countries. Today, Cisco solutions are the networking foundations for service providers, small to medium business and enterprise customers which includes corporations, government agencies, utilities and educational institution

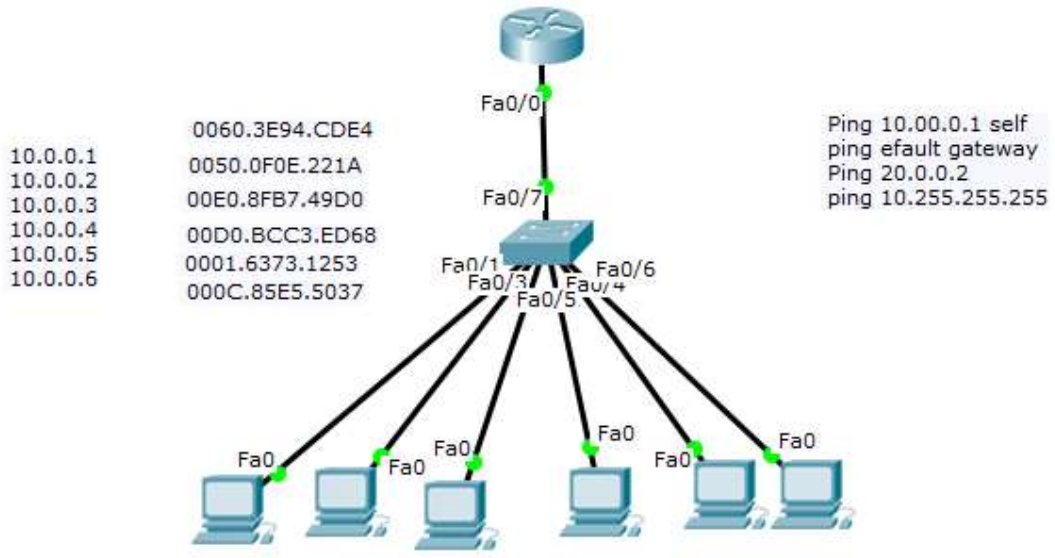
Common network types

PAN – Personal area network . Set of end devices connected to each other within 2 – 3 meter s
LAN – Set of devices connected with the same location
MAN – 2 or more LAN within the city limits
WAN – 2 or more LAN outside the city limits

BASIS FOR COMPARISON	HUB	SWITCH
Operates on	Physical layer	Data link layer
Type of transmission	Broadcast	Unicast, multicast, broadcast.
Number of ports	4 (more or less)	24 - 28 (depending on the type of switch).
Collision domain	Only one	Different ports have separate collision domain.
Transmission mode	Half duplex	Full duplex
Filtering	No provision of packet filtering	Provided

ARP

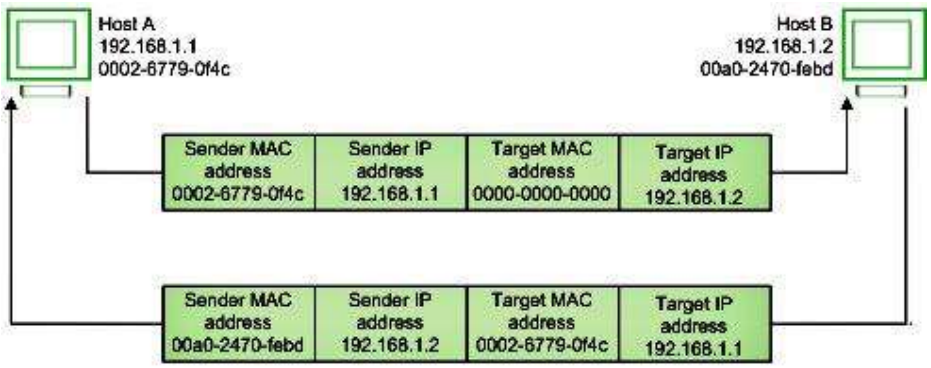
The Address Resolution Protocol is a communication protocol used to find MAC address using an IPv4 address.



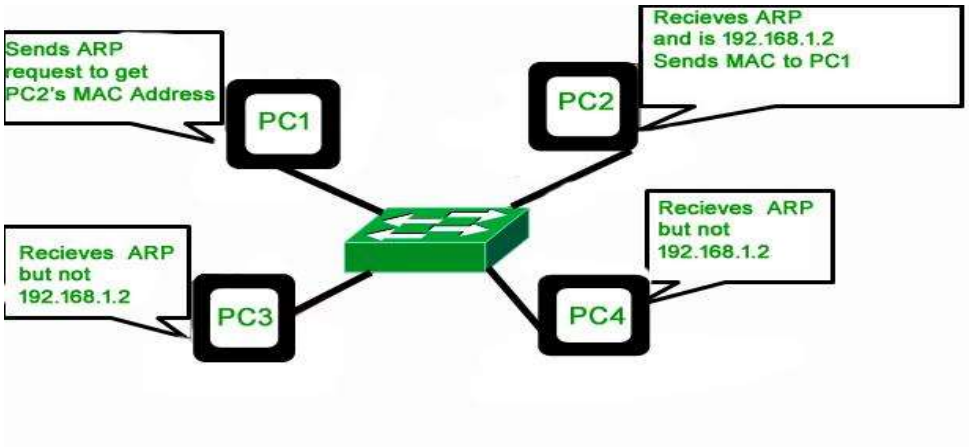
Arp –a , Arp –d ,Show mac address table .

1. Address Resolution Protocol (ARP) –

Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address.
In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.



Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.



Types of cables

Types of cables

1. Coaxial cable – Used for cable connections

2. Twisted pair cable **Twisted-pair cable** is a type of **cabling** that is used for telephone communications and most modern Ethernet **networks**. A **pair** of wires forms a circuit that can transmit data. The **pairs** are **twisted** to provide protection against crosstalk, the noise generated by adjacent **pairs**.

Types of Ethernet cables .1 . Straight through , 2 . Cross over . 3 Rolled over

3. Fiber optic cable - They're designed for long distance, high-performance data**networking**, and telecommunications. Compared to wired**cables**, **fiber optic cables** provide higher bandwidth and can transmit data over longer distances.

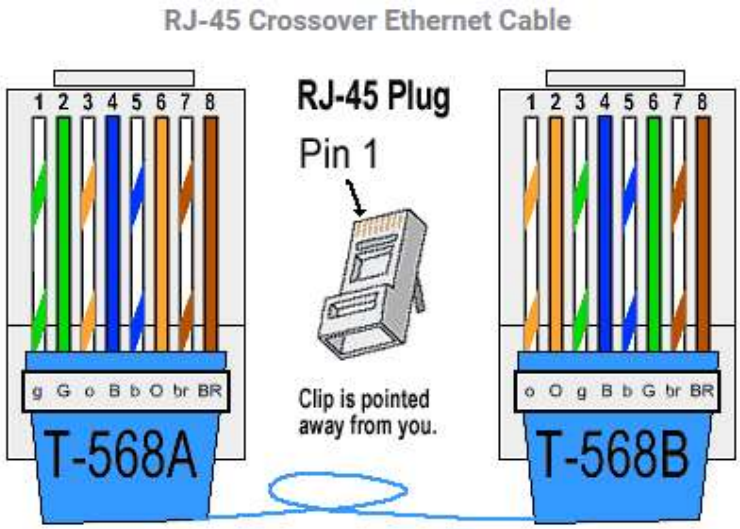
Coaxial cable

Twisted pair

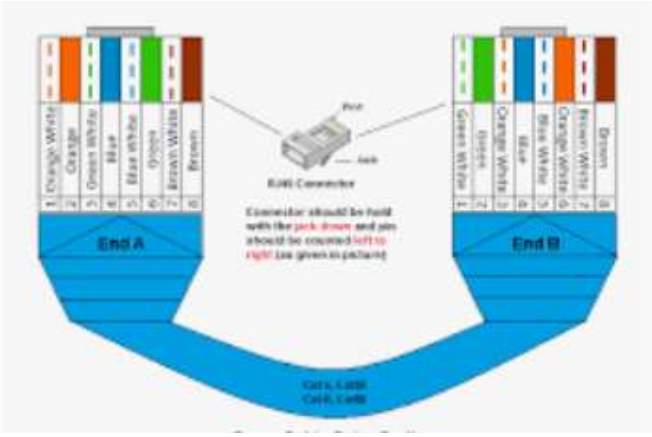
Ethernet : A system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems

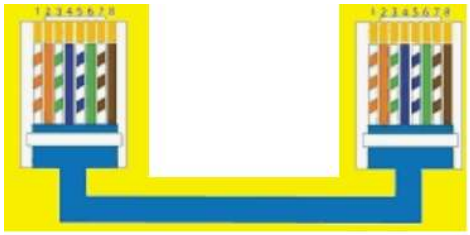
Types of Ethernet cables .1 . Straight through , 2 . Cross over . 3 Rolled over

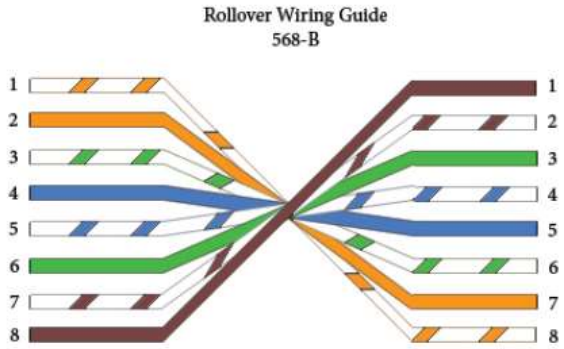
Color coding of cables
T-568A + T568A – Straight through cable
T-568B + T568B - Straight through able
T-568A + T568B – cross over cable



Some Examples.







RJ45 and RJ11 – Connectors

Communication between hosts can be classified into three types:

- **Unicast** – Communication from one host to another host only.
- **Broadcast** – Communication from one host to all the hosts in the network.
- **Multicast** – Communication from one host to few hosts only.

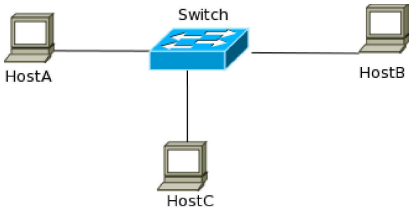
CD – How many devices can communicate at a time

A collision domain is **a network segment connected by a shared medium or through repeaters where simultaneous data transmissions collide with one another**. The collision domain applies particularly in wireless networks, but also affected early versions of Ethernet.

BD – How far a Packet travels when a broadcast is done .

A broadcast domain is **a logical division of a computer network**, in which all nodes can reach each other by broadcast at the data link layer. A broadcast domain can be within the same LAN segment or it can be bridged to other LAN segments. ... Routers and other higher-layer devices form boundaries between broadcast domains.

- **Figure 1-3** *A switched network*



- **Figure 1-4** *Collision Domains – 1*

Figure 1-4 Collision Domains – 1

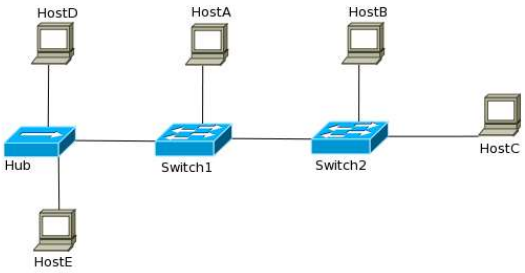
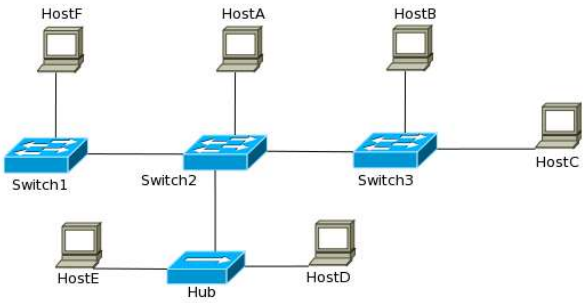
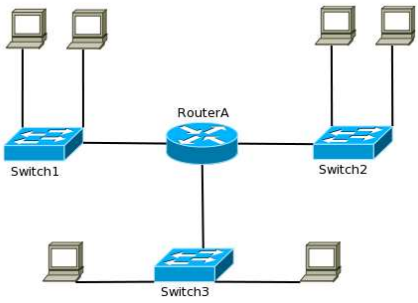
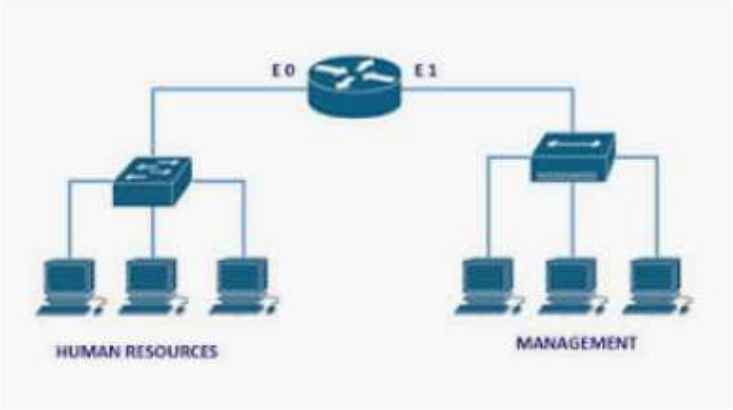
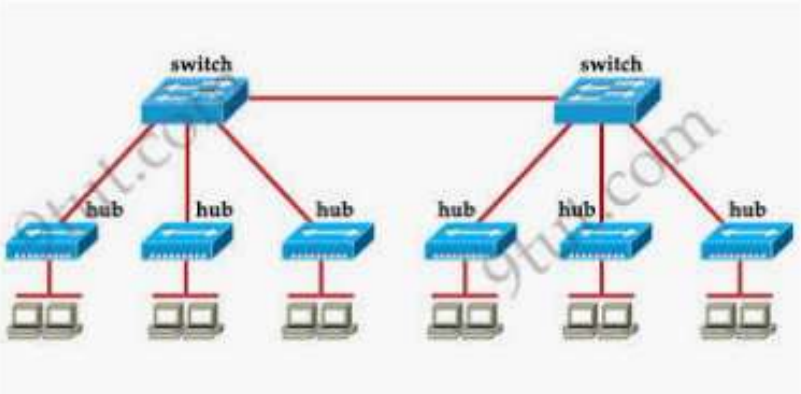


Figure 1-5 *Collision Domains – 2*









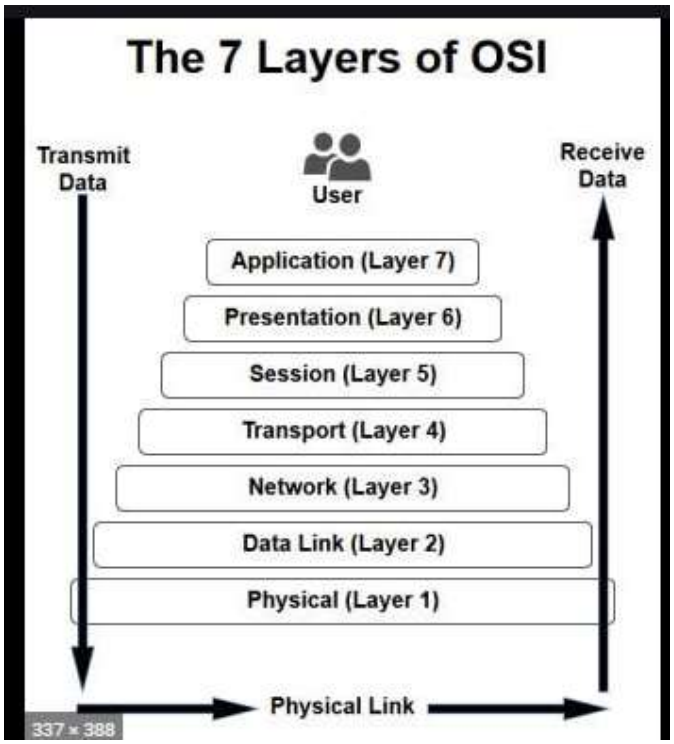
Switches break collision domains and routers break broadcast domains

Fundamentals Review

OSI Layers

1.OSI 7 Layers and its Functionalities
2.OSI Layers and TCP Suite .

OSI MODEL AND TCP / IP MODEL –
OSI Model is a reference model which was developed by ISO which consists of 7 layers , We use OSI only as a reference , But when we talk about the **TCP**/IP model, it was designed and developed by Department of Defense (DoD) / ARPA it has 4 layers . (practically we use TCP/IP model , Theoretically for a reference we use OSI model) . OSI layer tells how the communication happens between two or more networking devices within the organization or internet . Each layer defines a set of functions in data communications.. Internet runs on TCP/IP model .



APPLICATION LAYER.

Provides user interface for the users to interact with application services or Network services.

Presentation Layer (Layer 6)

- responsible for defining a standard format for the data.
- It deals with data presentation.

Encoding – Decoding
Encryption – Decryption
Compression – Decompression

.jpeg, .Doc, Zip files.

Session Layer (Layer 5)

- It is responsible for establishing, maintaining and terminating the sessions.
- It deals with sessions or Interactions between the applications.
- Session ID is used to identify a session or interaction

You can see the list of sessions created through cmd prompt using NETSTAT command
Will see what are port number.

Here comes the real networking part .

Transport Layer (Layer 4)

Responsible for end-to-end transportation of data between the applications.

The major functions described at the Transport Layer are...

- Identifying Service
- Multiplexing & De-multiplexing
- Segmentation
- Sequencing & Reassembling
- Error Correction
- Flow Control

\\Segmantation
Sequencing and Reassembling
Multiplexing and de multiplexing
Identifying the service
Flow control
Error correction

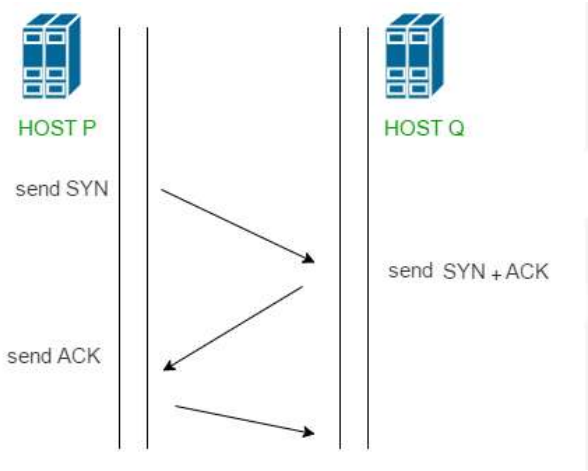
This layer breaks up the data from sending host and then reassembles it in the receiver
Data coming from session layer , will be divided in to chunks these chunks are called as segments , the size of the chunks is called MSS maximum segment size

In this layer
First MAIN thing what happens is segmentation , when the segments reach the destination reassembling has to be done , to do reassembling we need to know the Sequence numbers . so each segment will have a

seq number , Transport layer adds header in to the segment called transport layer header .
Second MAIN thing what happens is to find out Tcp or Udp ,
There are 2 types of header , TCP header and UDP Header .
1.These transport layer will have sequence numbers and other stuffs , Now what are the other stuffs ,
2.This is the second biggest thing that happens in transport layer , ie whether the data has to be sent reliably [TCP – connection oriented] or non-reliably [UDP Connectionless],

Reliable - TCP
Seq 1 ---→
----<<< ack 2
Seq 2 -→
If ack not coming then again
Seq 2 -→ will be sent .

Before all these sending and receiving , a connection will be established called , 3 way handshake



after which all the above will happen .

Non Reliable

In UDP seq 1-→
Seq 2 --→
Seq 3 -→

No ack just sending continuous data . If data is lost in the middle its lost forever , Now the question is who wants to loose the data ,
ANS : UDP will be used , when the time is imp than the DATA itself .

TCP is used when DATA is imp that time .

TCP protocols
UDP protocols
Data communication between two devices either has to be TCP or UDP, however

There are some other protocols which neither uses TCP or UPD ,
Question : Is there any protocol that doesn't use TCP and UDP ????
Yes
Ex: EIGRP or OSPF has its own protocols

Each and every protocol [Only TCP and UDP] uses port number ,
Port number is a 16 bit number used by protocols that either uses TCP(6) or UDP (17) . for ex HTTP : 80 HTTPS 443
SO
Question What is the port number of EIGRP and OSPF .
There are no port numbers for the above two .
3.Port number :

Now PDU in Transport layer is called Segment ,

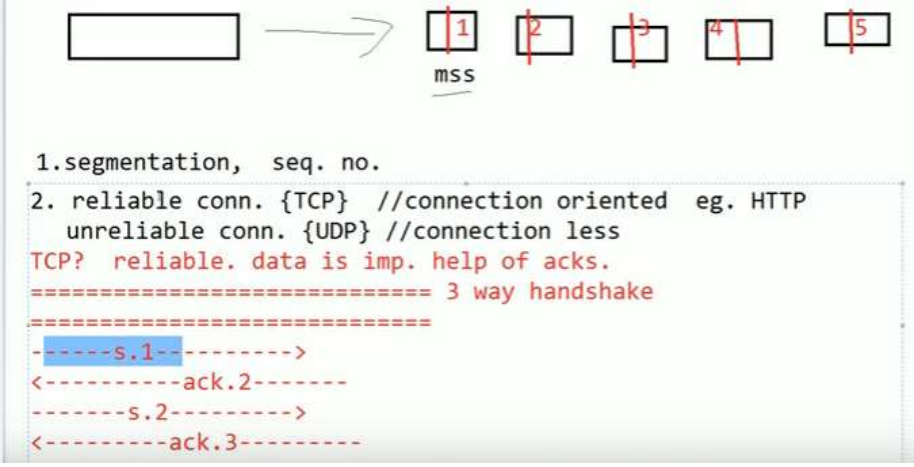
.....

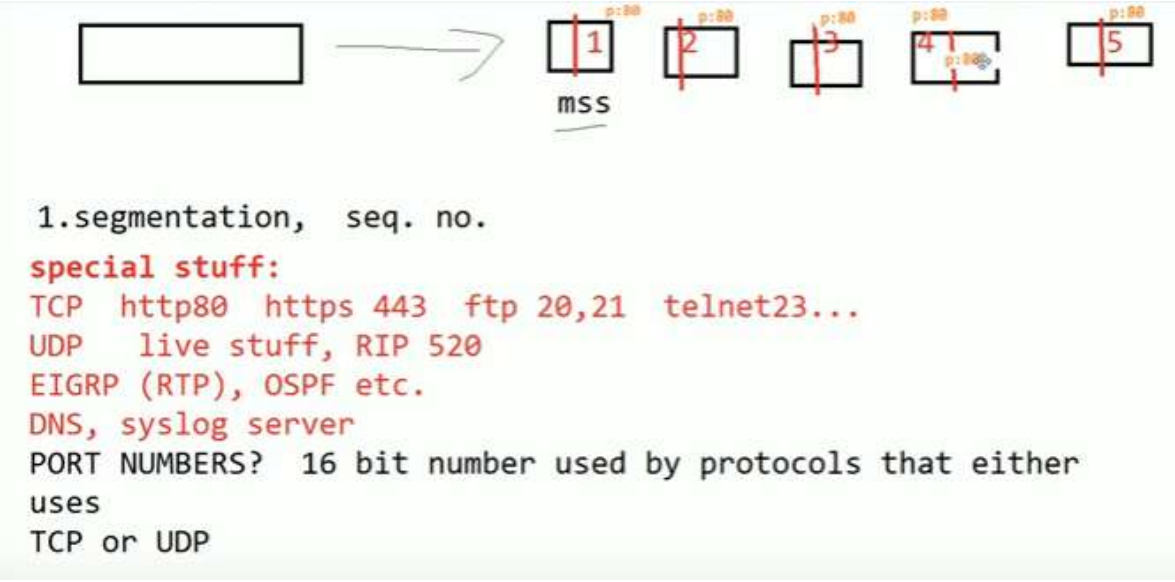
MSS – Maximum segment size
Minimum packet size 30 bytes to 1500 bytes
Ip header size is 20 bytes

- The layer 1 (Physical layer) PDU is the bit
- The layer 2 (Data link layer) PDU is the frame.
- The layer 3 (Network layer) PDU is the packet.

- The layer 4 (Transport layer) PDU is the segment for TCP or the datagram for UDP.

In Layer 5 and above, PDU is referred to as data.





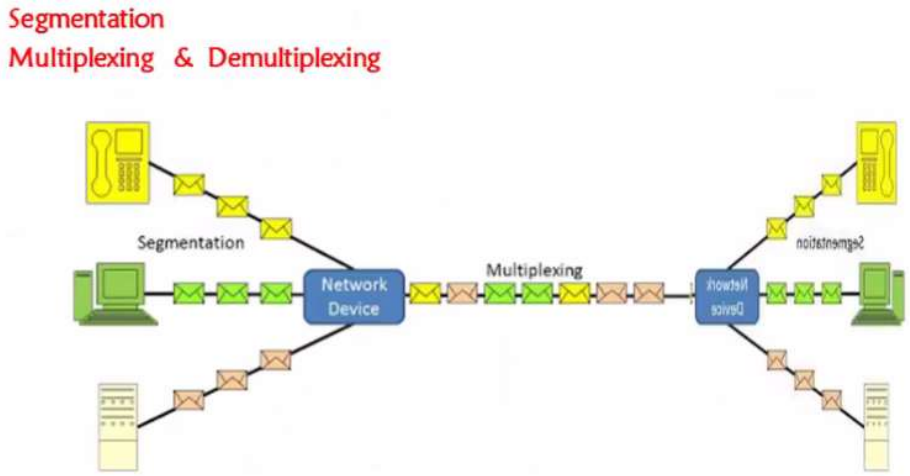
- Protocol No is 6
- Eg: HTTP, FTP, SMTP

- Protocol No is 17
- Eg: DNS, DHCP, TFTP

1.Identifying the service - TCP or UDP .

TCP	UDP
• Transmission Control Protocol • Connection Oriented • Reliable communication(with Ack's) • Slower data Transportation • Protocol No is 6 • Eg: HTTP, FTP, SMTP	• User Datagram Protocol • Connection Less • Unreliable communication(no Ack's) • Faster data Transportation • Protocol No is 17 • Eg: DNS, DHCP, TFTP

Segmentation
Multiplexing and DE multiplexing – Different types of traffic which is identified using different frequencies .FBD-TBD Frequency based division and Time based division



Sequencing and reassembling .

Hello how are you

Hello	how	are	you
1/4	2/4	3/4	4/4

To control the flow **Sliding window protocol** was found . I am sending data at 100 mbps speed but the other side he has capacity to receive only 10 mbps . sliding window protocol resolves this issue .

Network Layer
Network header will be added here , In this layer it makes

1.Logical Addressing
2.Best path selection using routing
so S IP add and D IP address will be added here .

Network Layer (Layer 3)

- It is responsible for end-to end Transportation of data across multiple networks
- Logical addressing & Path determination (Routing) are described at this layer.
- The protocols works at Network layer are

Routed Protocols:

- Routed protocols acts as data carriers and defines logical addressing.
- IP, IPX, AppleTalk... Etc

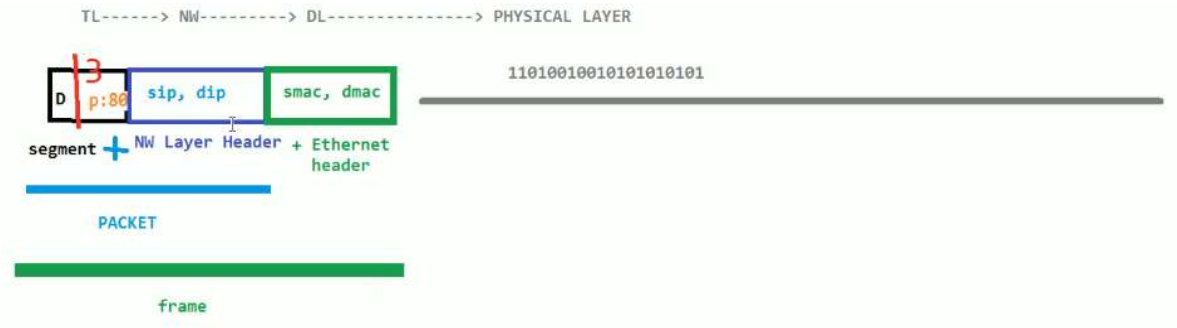
Routing Protocols:

- Routing protocols performs Path determination (Routing).
- RIP, IGRP, EIGRP, OSPF.. Etc
- Devices works at Network Layer are Router, Multilayer switch etc..

Routing protocols finds the best path
Routed protocols are the actual carriers .

1. Logical addressing
2. Path determination

Routed protocols and routing protocols



Data-link Layer (Layer 2)

It is responsible for end-to-end delivery of data between the devices on a LAN Network segment. Data link layer comprises of two sub-layers.

- It deals with hardware addresses (MAC addresses).
- It also provides ERROR DETECTION using CRC (Cyclic Redundancy Check) and FRAMING (Encapsulation).

Devices works at Data link layer are Switches.

Physical Layer (Layer 1)

- It deals with physical transmission of Binary data on the given media (copper, Fiber, wireless...).
- It also deals with electrical, Mechanical and functional specifications of the devices, media.. etc

◦ Copper media	:	Electrical signals of different voltages
◦ Fiber media	:	Light pulses of different wavelengths
◦ Wireless media	:	Radio frequency waves

For More detailed Study

https://www.geeksforgeeks.org/layers-of-osi-model/

TCP / IP Model

TCP/IP Model was developed and proposed by ARPA (Advanced Research Projects Agency), This model was mainly created to connect military Network.

What made Tcp/ip come in to existence is

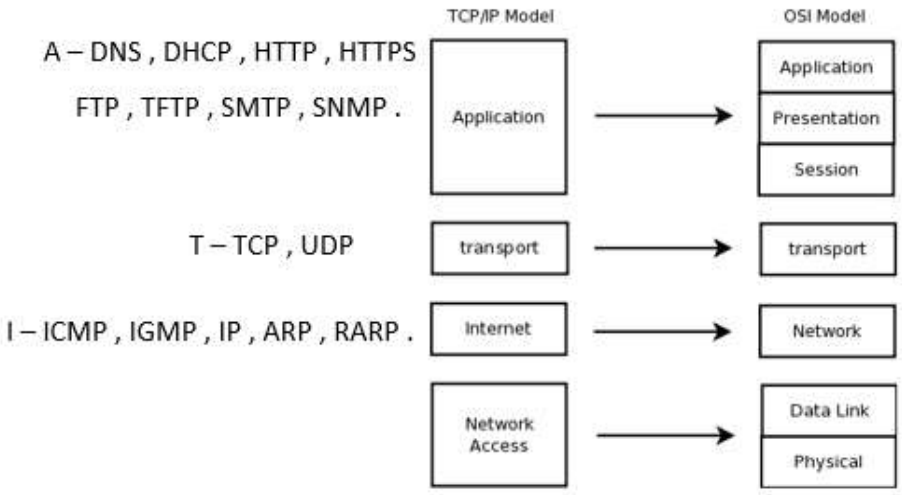
1.How to transmit data across the network

2.How to format the data so that the other side understands it .

Two key features of TCP/IP Model

1. Dynamic routing : end nodes can transfer data over multiple paths and network chooses the best path for individual data transfer .

2.Fine node verification : Only the two end points are responsible for successful data transmission



Application Protocol	Transport Protocol	Port Number
HTTP	TCP	80
HTTPS	TCP	443
FTP (control)	TCP	21
FTP (data)	TCP	20
SSH	TCP	22
Telnet	TCP	23
DNS	TCP, UDP	53
SMTP	TCP	25
TFTP	UDP	69

Network Addressing Scheme

Binary : 0 and 1
Decimal : 0 1 2 3 4 5 6 7 8 9
Hexa decimal : 0 1 2 3 4 5 6 7 8 9 10 [A] , 11[B] , 12 [C] , 13[C] , 14 [D], 15[E] .

DATA REPRESENTATION FORMATS

Binary **- Binary** is used for calculating **network** masks
Decimal **- Decimal** is the human **numbering system** we display IPv4 addresses
Hexa decimal **- hexadecimal** is used to display Ethernet MAC addresses and IPv6 addresses

So expertize in converting of all these is very much required .

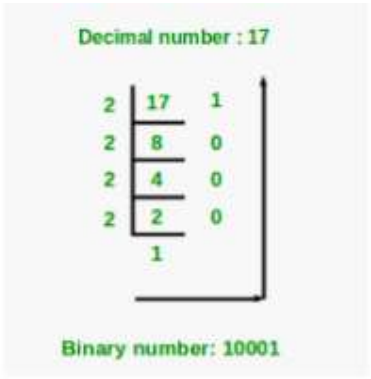
BINARY TO DECIMAL

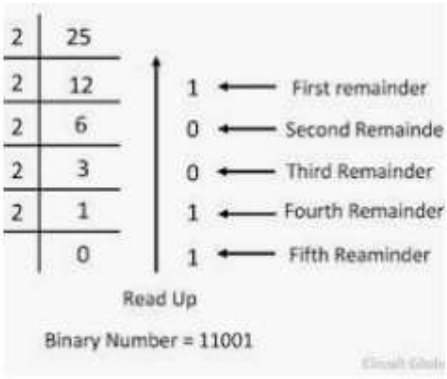
Representation of a Binary Number

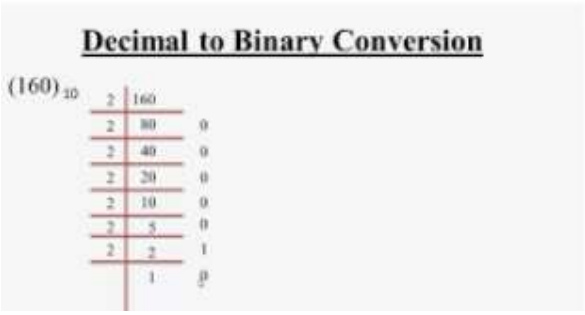
MSB	Binary Digit							LSB
2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
256	128	64	32	16	8	4	2	1

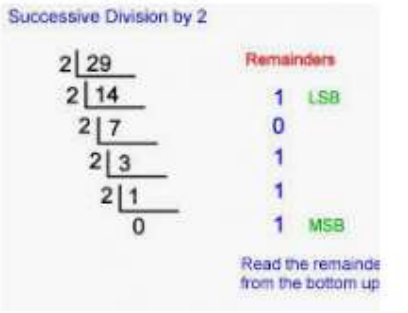
Decimal Digit Value	256	128	64	32	16	8	4	2	1
Binary Digit Value	1	0	1	1	0	0	1	0	1

DECIMAL TO BINARY









128	64	32	16	8	4	2	1	
			1	0	0	0	1	17
		0	1	1	0	0	1	25
1	0	1	0	0	0	0	0	160
			1	1	1	0	1	29

Convert hex to binary and decimal

**********END OF CONVERSION**********

IP addresses

Protocol

set of rules to have proper communication

Network protocols

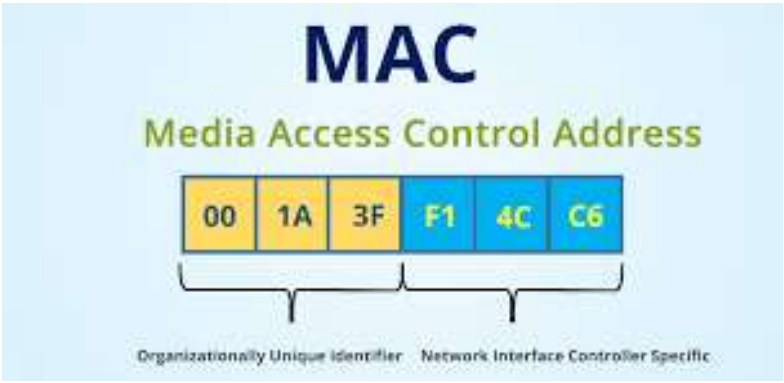
TCP/IP	DOD
IPx/SPx	NOVELL
Appletalk	APPLE
Netbios	MICROSOFT
OSI	ISO

What is TCP/IP?

- TCP/IP is a standard protocol used between computers and network devices for communication.

If I want to access or communicate any one through internet then it has to support tcp / ip protocol.
Inside the tcp / ip it has its own addressing of every device which we call it as IP ADDRESS.
When it comes to addressing there are two types of addresses
1.MAC address
2.IP address

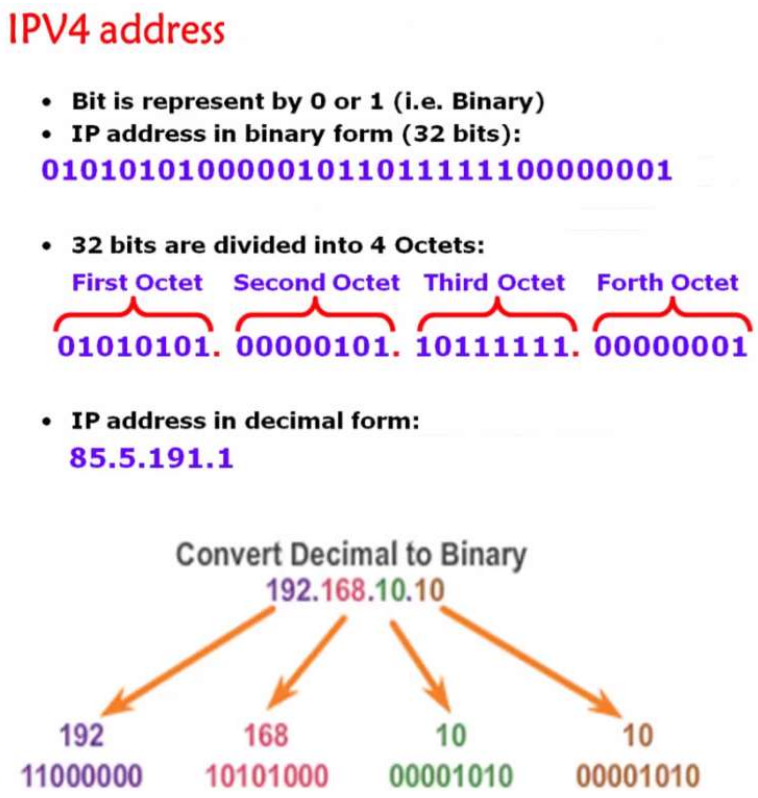
1. Mac address : A media access control **address** (**MAC address**) of a device is a unique identifier assigned to a network interface controller
   It is a 48 bit binary number represented in hexa decimal format .
   Mac / physical / Hardware / Burnt in address .



2.IP ADDRESS : IP addresses are 32 bit binary number represented in decimal format . AND DIVIDED in to 4 octet s .

- IP Address is Logical Address given to each and every device in the network.
- It is a Network Layer address (Layer 3)
- Two Versions of IP:
  - IP version 4
  - IP version 6

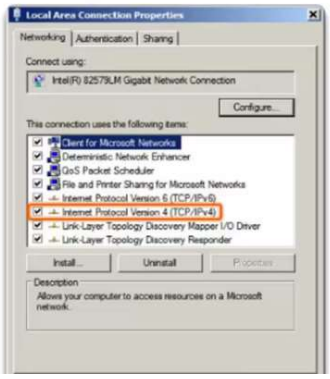
IP Address = 2 raise 32 ip address = 32billion – internet grew shortage IP address , To overcome the shortage of IPV4 , IPv6 128 bit



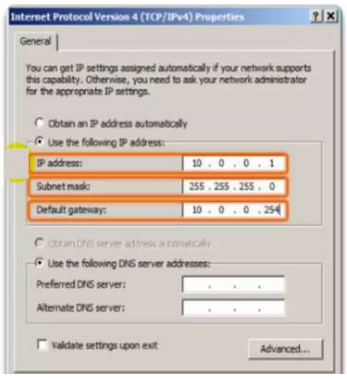
How to give IP address manually in your PC

Assigning a Static IPv4 Address to a Host

LAN Interface Properties



Configuring a Static IPv4 Address



Control panel , Network and sharing . In real time – DHCP

Range of IPv4 address

Taking Example for First Octet :
Total 8 bits, Value will be 0's and 1's
i.e. 2^8 = 256 combination

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
0	0	0	0	0	0	0	0	= 0
0	0	0	0	0	0	0	1	= 1
0	0	0	0	0	0	1	0	= 2
0	0	0	0	0	0	1	1	= 3
0	0	0	0	0	1	0	0	= 4
1	1	1	1	1	1	1	1	= 255

Total IP Address Range
0 . 0 . 0 . 0
to
255.255.255.255

IP Address Classification

IP Addresses are divided into 5 Classes

CLASS A	0-127	Used in LAN & WAN
CLASS B	128 - 191	
CLASS C	192-223	
CLASS D	224-239	Reserved for Multicasting
CLASS E	240-255	Reserved for Research & Development

169.254.0.0 to 169.254.255.255 – APIPA Ip addresses .
Unicast , Multicast and broadcast .

Network & Host portions

IP address is divided into Network & Host Portion

CLASS A	N.H.H.H
CLASS B	N.N.H.H
CLASS C	N.N.N.H
Host:	a specific device in the network
Network:	set of devices

If two devices has to communicate then network part should be same .

256 IP addresses
256 raise 2 = 65536
256 raise 3 = 16777212

Network & Broadcast Address

Network ID :

- Identify complete network
- First IP of the range
- All ZERO's in the host portion

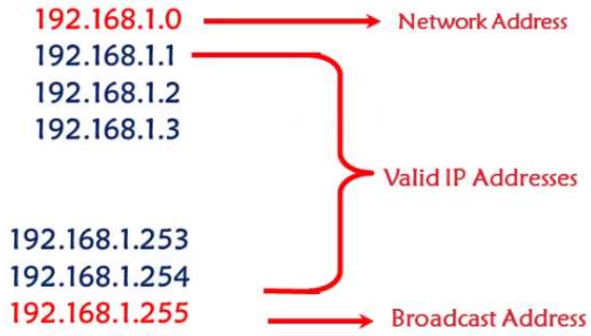
Broadcast address

- Used to send broadcast to all with in the same network
- Last IP address of the range
- All ONE'S in the host portion

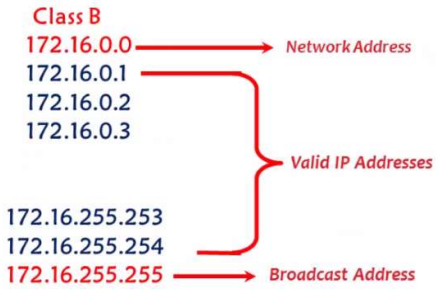
Valid IP

- Valid IP Addresses lie between the Network Address and the Broadcast Address.
- Only Valid IP Addresses are assigned to hosts/clients

Example - Class C



Example - Class B



Subnet-mask

Subnet Mask differentiates Network portion and Host Portion

- 1 represent network
- 0 represent hosts

Class A	N.H.H.H	255.0.0.0
Class B	N.N.H.H	255.255.0.0
Class C	N.N.N.H	255.255.255.0

PRIVATE IP

- Used with the LAN or within the organization
- Not recognized on internet
- Given by the administrator
- Unique within the network or organization
- Free
- Unregistered IP

PUBLIC IP

- Used on public network(INTERNET)
- Recognized on internet
- Given by the service provider (from IANA)
- Globally unique
- Pay to service provider (or IANA)
- Registered

Private IP Address

- There are certain addresses in each class of IP address that are reserved for Private Networks. These addresses are called private addresses.

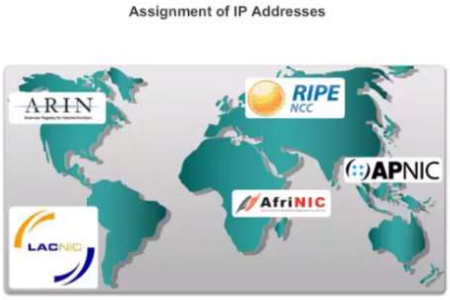
Class A
10.0.0.0 to 10.255.255.255 (10.x.x.x)

Class B
172.16.0.0 to 172.31.255.255

Class C
192.168.0.0 to 192.168.255.255 (192.168.x.x)

Assignment of IP Addresses

Regional Internet Registries (RIRs)
The major registries are:
(IANA.org)
http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml



https://www.iana.org/

https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml

What is Discontiguous vs. Contiguous?

Connected through an unbroken sequence". Therefore discontiguous might be thought of as "fragmented" or "separated".
So based on this we could say that a given network, separated by other networks, is discontiguous.

What is Major Network Number
Majot Network Number is nothing but the Network ID.

Major Network Mask is always assigned by the class of the IP addresses used on the network.
If a network has **Class A** IP Addresses assigned to hosts, **Major Network Mask** is 255.0.0.0
Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0

Subnetting

A subnetting, or sub networking, is the process of splitting a single large network into two or more strands. This means that an otherwise mammoth network can be subdivided into smaller, more localized networks

Subnetting benefits.

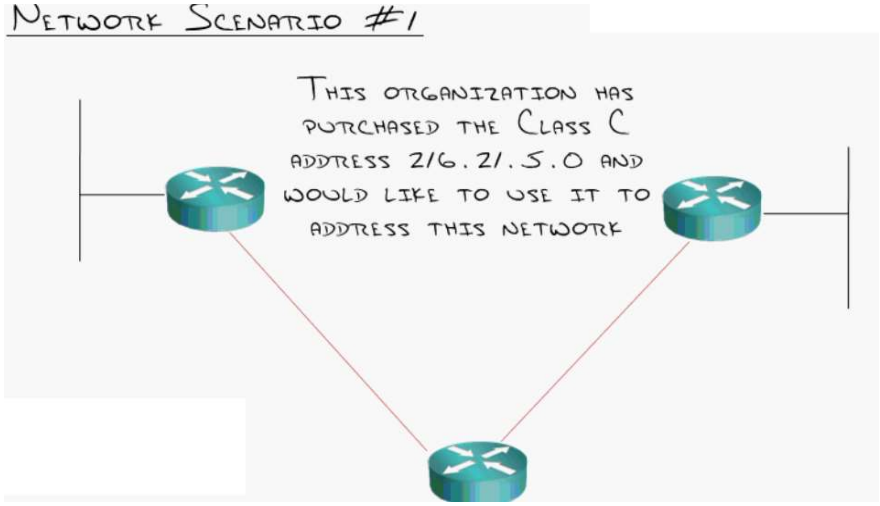
1. **Improve network performance and speed**
2. **Control network growth**
3. **Ease administration**

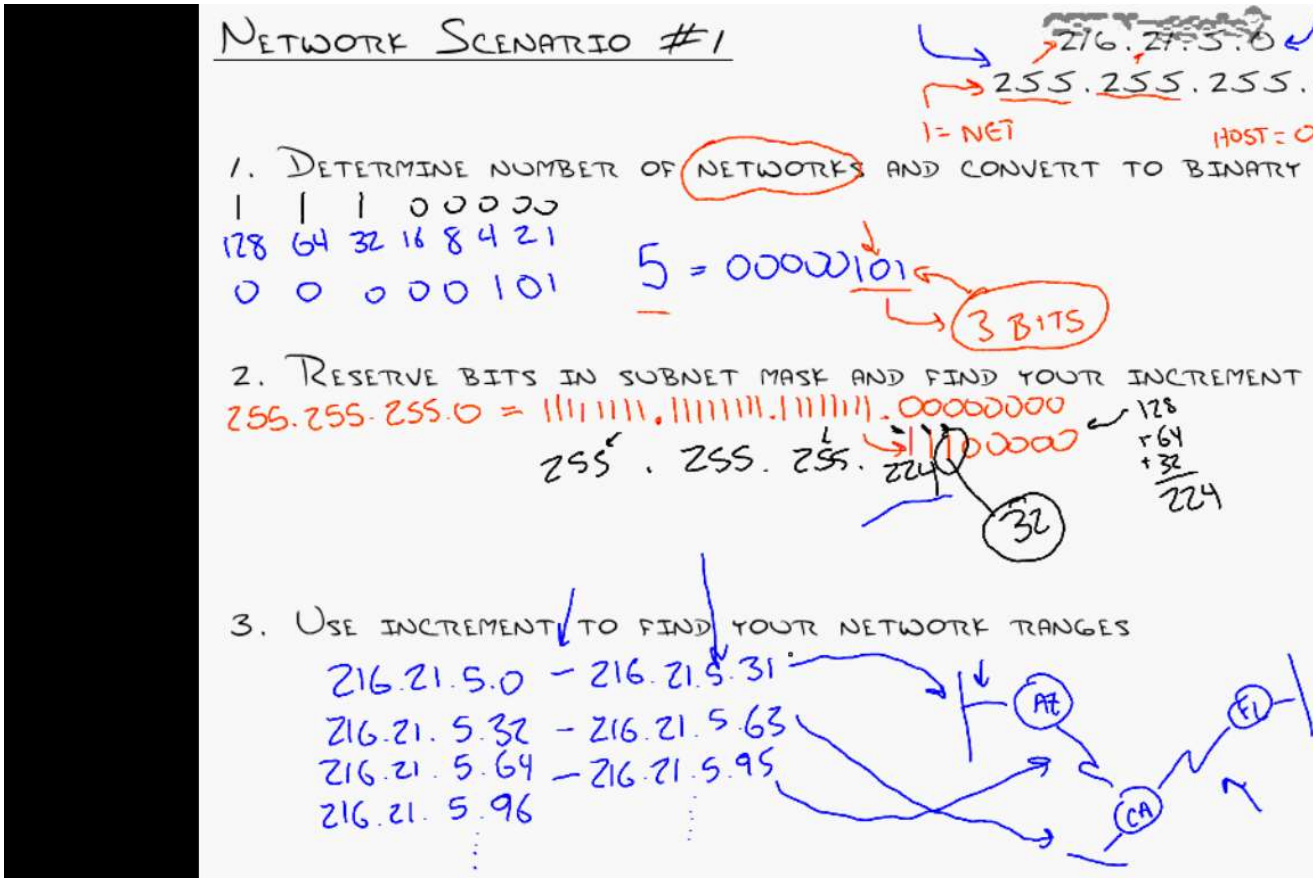
128 64 32 16 8 4 2 1

CONVERT THE NUMBER OF NETWORKS REQUIRED IN TO BITS
AND FIND OUT - HOW MANY BITS REQUIRED TO GET THAT NUMBER

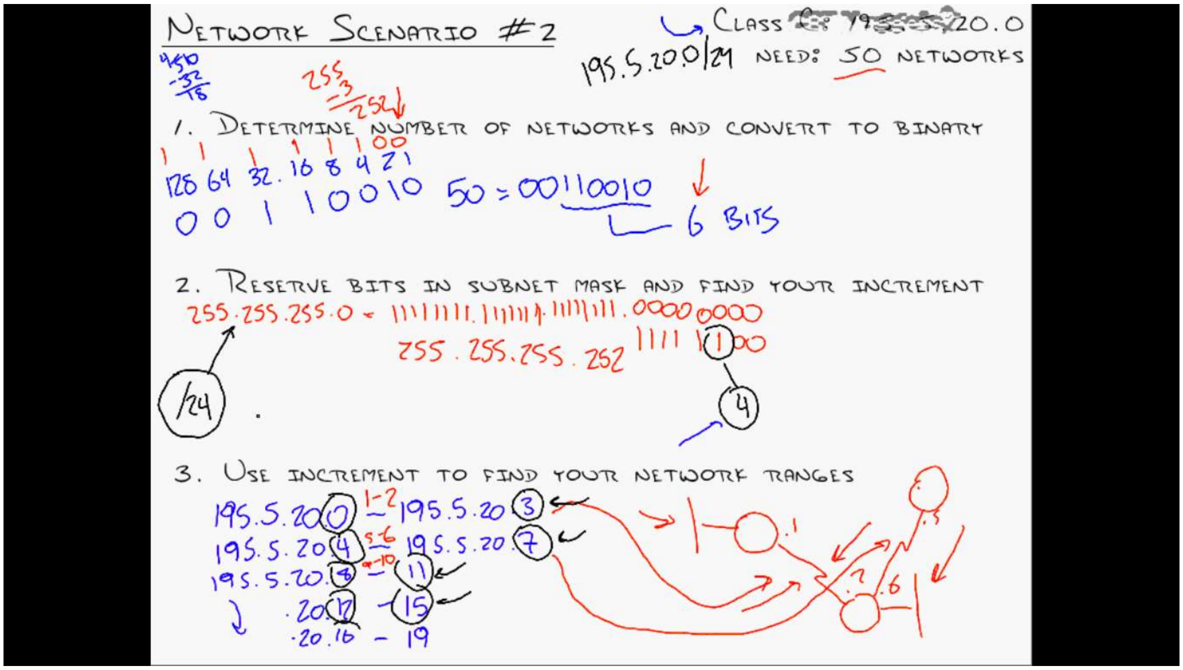
REVERSE THE BITS AND FIND THE INCREMENT

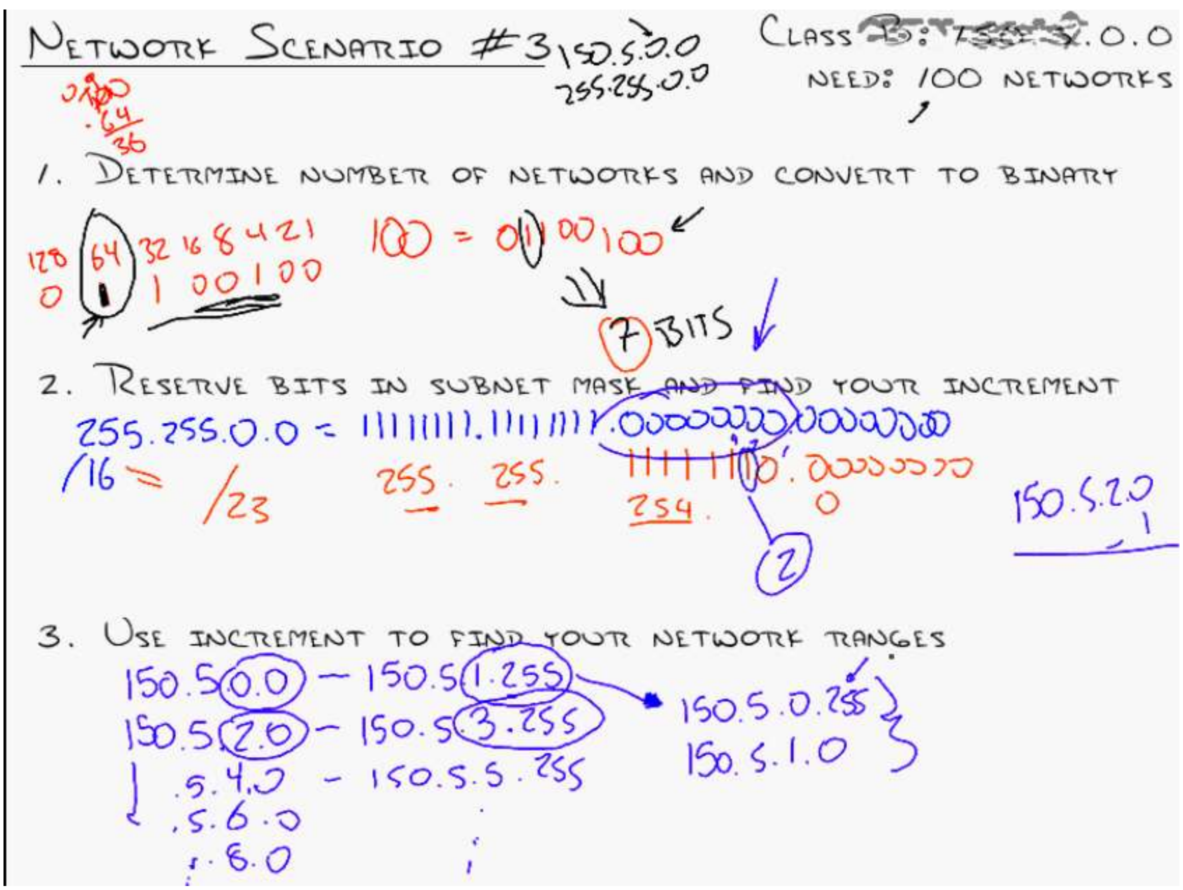
USING THE INCREMENT GET THE SUBNETWORKS





STEP 2 : How many bits does it take to get the number 5 .
2 RAISE on bits – Total number of Subnetworks
2 raise off bits - Total number of hosts.


NETWORK SCENARIO #2
CLASS 20.0
195.5.20.0/24 NEED: 50 NETWORKS
1. DETERMINE NUMBER OF NETWORKS AND CONVERT TO BINARY
128 64 32 16 8 4 2 1
0 0 1 1 0 0 1 0
50 = 00110010
6 BITS
2. RESERVE BITS IN SUBNET MASK AND FIND YOUR INCREMENT
255.255.255.0 = 11111111.11111111.11111111.00000000
255.255.255.252
/24
3. USE INCREMENT TO FIND YOUR NETWORK RANGES
195.5.20.0 - 195.5.20.3
195.5.20.4 - 195.5.20.7
195.5.20.8 - 11
.20.12 - 15
.20.16 - 19


NETWORK SCENARIO #3
150.5.0.0
255.255.0.0
CLASS .0.0
NEED: 100 NETWORKS
1. DETERMINE NUMBER OF NETWORKS AND CONVERT TO BINARY
128 64 32 16 8 4 2 1
100 = 01100100
7 BITS
2. RESERVE BITS IN SUBNET MASK AND FIND YOUR INCREMENT
255.255.0.0 = 11111111.11111111.00000000.00000000
/16 = /23
255.255.254.0
3. USE INCREMENT TO FIND YOUR NETWORK RANGES
150.5.0.0 - 150.5.1.255
150.5.2.0 - 150.5.3.255
.5.4.0 - 150.5.5.255
.5.6.0
.5.8.0
150.5.0.255
150.5.1.0

NETWORK SCENARIO #4

CLASS A: [redacted].0.0

NEED: 500 NETWORKS

500
-256

1. DETERMINE NUMBER OF NETWORKS AND CONVERT TO BINARY

512 256 128 64 32 16 8 4 2 1

(1)

500 - 9 BITS

(2^8)

2. RESERVE BITS IN SUBNET MASK AND FIND YOUR INCREMENT

255.0.0.0 = 11111111.00000000.00000000.00000000

255.255.128.0

/17

11111111.10000000.

128

128
+128
256

3. USE INCREMENT TO FIND YOUR NETWORK RANGES

10.0.0.0 - 10.0.127.255
10.0.128.0 - 10.0.255.255
10.1.0.0 - 10.1.127.255
10.1.128.0 - 10.1.255.255
10.2.0.0 ⋮

ON YOUR OWN:

[redacted]

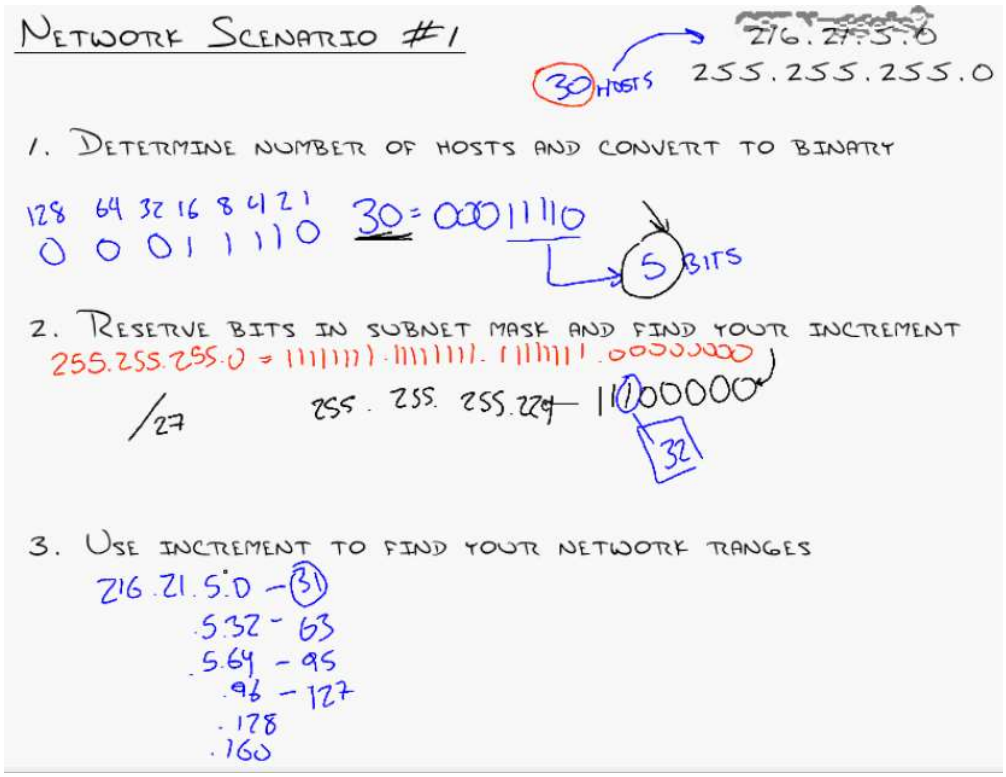
1. (C) 200.1.1.0, BREAK INTO 40 NETWORKS

2. (C) 199.9.10.0, BREAK INTO 14 NETWORKS

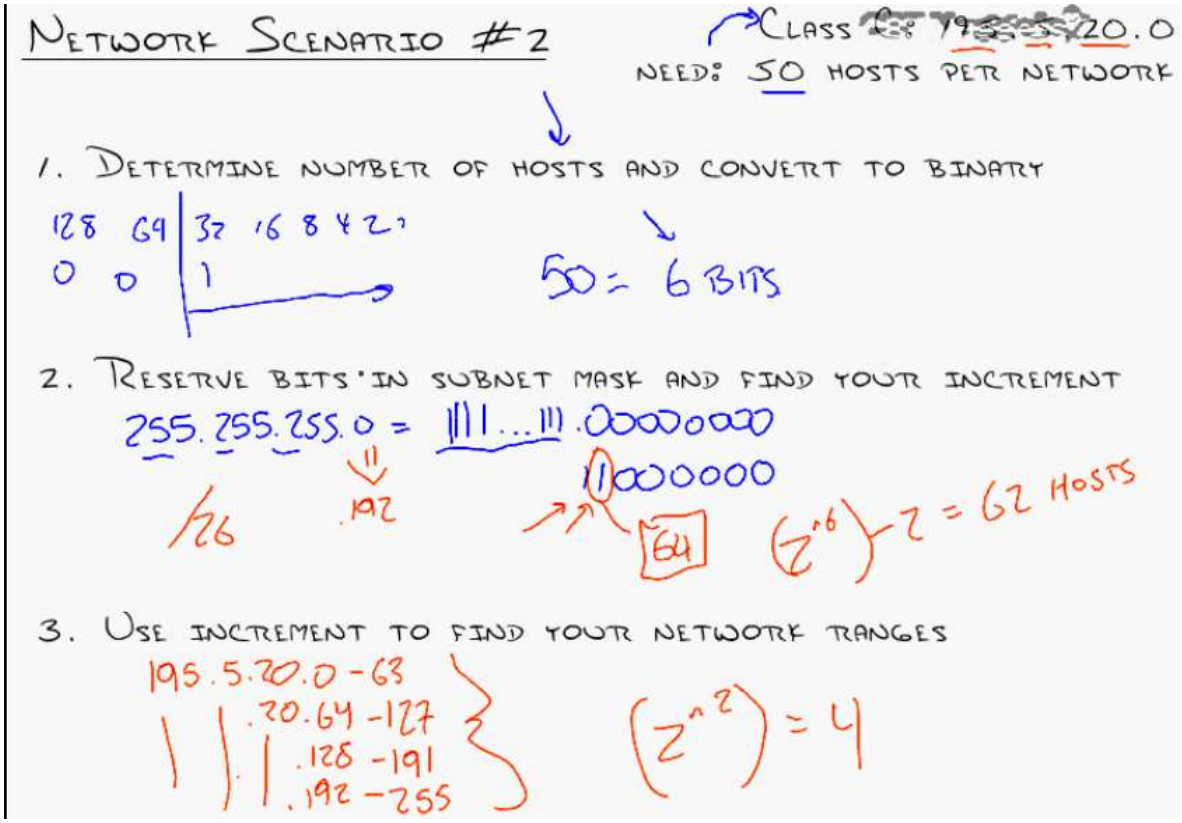
3. (B) 170.50.0.0, BREAK INTO 1000 NETWORKS

4. (A) 12.0.0.0, BREAK INTO 25 NETWORKS

SUBNETTING BASED ON HOSTS



Save the hosts .



NETWORK SCENARIO #3

CLASS B: [redacted].0.0

NEED: 500 HOSTS PER NETWORK

1. DETERMINE NUMBER OF HOSTS AND CONVERT TO BINARY

512 [256 128 64 32 16 8 4 2 1]
1

500 = 9 BITS

2. RESERVE BITS IN SUBNET MASK AND FIND YOUR INCREMENT

255.255.0.0 ⇒ 111...11.00000000.00000000

255.255.254.0 .11111110.00000000

/23

(2)

3. USE INCREMENT TO FIND YOUR NETWORK RANGES

150.5.0.0 – 150.5.1.255
150.5.2.0 – 150.5.3.255
.5 4.0 – 5.5
.6.0

NETWORK SCENARIO #4

CLASS A: [redacted].0.0

NEED: 100 HOSTS PER NETWORK

1. DETERMINE NUMBER OF HOSTS AND CONVERT TO BINARY

128 [64 32 16 8 4 2 1]
1

100 = 7 BITS

2. RESERVE BITS IN SUBNET MASK AND FIND YOUR INCREMENT

255.0.0.0 = 111...00000000.00000000.00000000

255.255.255.128 11111111.10000000

128

3. USE INCREMENT TO FIND YOUR NETWORK RANGES

10.0.0.0 – 127
10.0.0.128 – 255
10.0.1.0 – 127
1.128 – 1.255
2.0
2.128

On Your Own:

1. (C) 200.1.1.0, break into networks of 40 hosts each

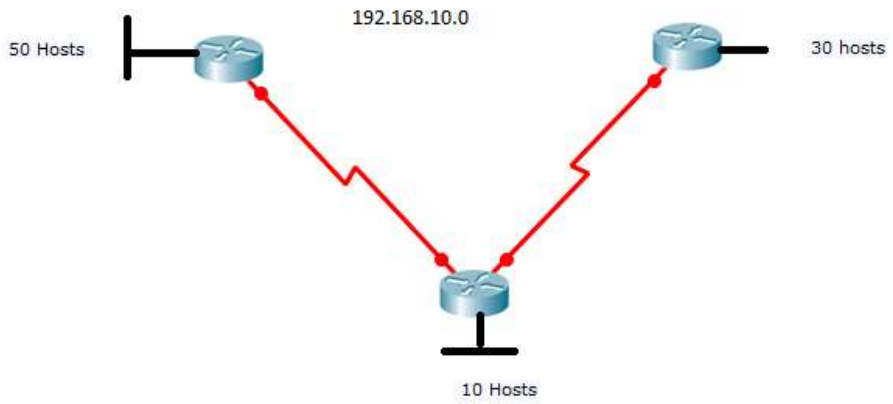
2. (C) 199.9.10.0, break into networks of 12 hosts each

3. (B) 170.50.0.0, break into networks of 1000 hosts

4. (A) 12.0.0.0, break into networks of 100 hosts each

VLSM

Very important as it is used in real time



Finds lots of Sub netting Questions here:

http://www.subnettingquestions.com/

Question: *Which subnet does host 172.31.139.1/23 belong to?*

Answer: 172.31.138.0

Question: *What is the last valid host on the subnetwork 172.18.117.128/27?*

Answer: 172.18.117.158

Question: *Which subnet does host 172.28.132.194/20 belong to?*

Answer: 172.28.128.0