**NETWORK ESSENTIALS / CCNA COURSE INTRODUCTION**

About The Instructor –

About the course-

Course Prerequisites – NA

**INTRODUCTION**

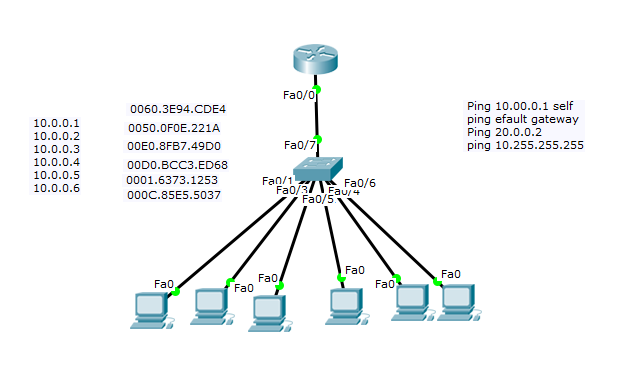
Topic syllabus discussion.

**Network**

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

**ARP**

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



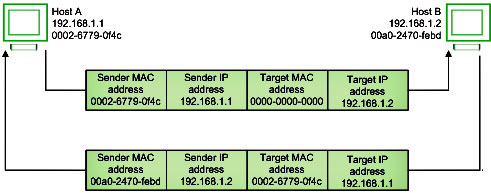
Arp –a , Arp –d ,Show mac address table .

# **ARP, Reverse ARP(RARP), Inverse ARP (InARP), Proxy ARP and Gratuitous ARP**

we will discuss about whole ARP-family, which are ARP, RARP, InARP, Proxy ARP and Gratuitous ARP. Let’s try to understand each one by one.

### 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.

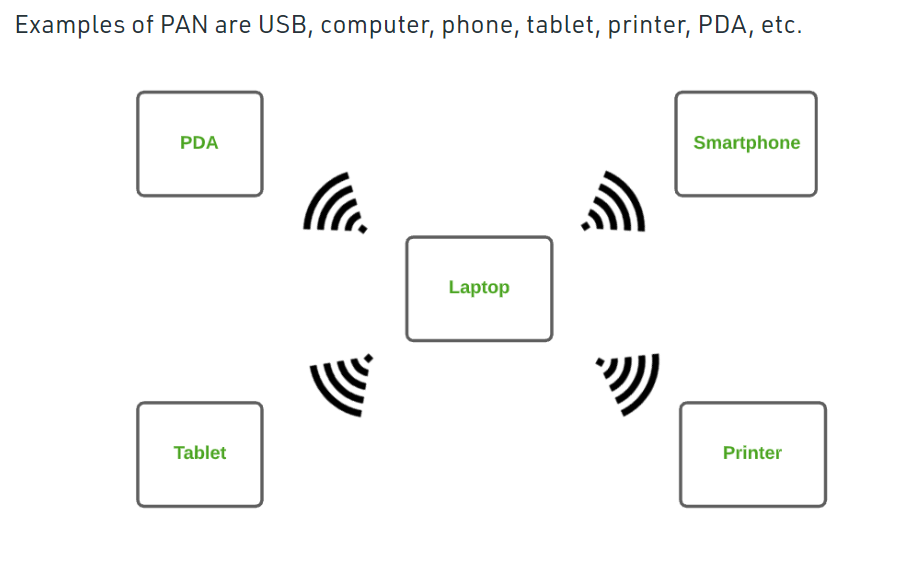


**Common network types**

PAN – Personal area network . Set of end devices connected to each other within 2 – 3 meter s

### ****1. Personal Area Network (PAN)****

[PAN](https://www.geeksforgeeks.org/overview-of-personal-area-network-pan/) is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centered only on an individual’s workspace. PAN offers a network range of 1 to 100 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost.



LAN – Set of devices connected with the same location

### ****Local Area Network (LAN)****

LAN is the most frequently used network. A [LAN](https://www.geeksforgeeks.org/lan-full-form/)is a computer network that connects computers through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are [Ethernet](https://www.geeksforgeeks.org/local-area-network-lan-technologies/)and [Wi-fi](https://www.geeksforgeeks.org/what-is-wi-fiwireless-fidelity/).  It ranges up to 2km & transmission speed is very high with easy maintenance and low cost.

Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.

WAN – 2 or more LAN outside the city limits

### ****Wide Area Network (WAN)****

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. [WAN](https://www.geeksforgeeks.org/wan-full-form/) can also be defined as a group of local area networks that communicate with each other with a range above 50km.

Here we use Leased-Line & Dial-up technology. Its transmission speed is very low and it comes with very high maintenance and very high cost.

**NETWORK DEVICES**

1.hub

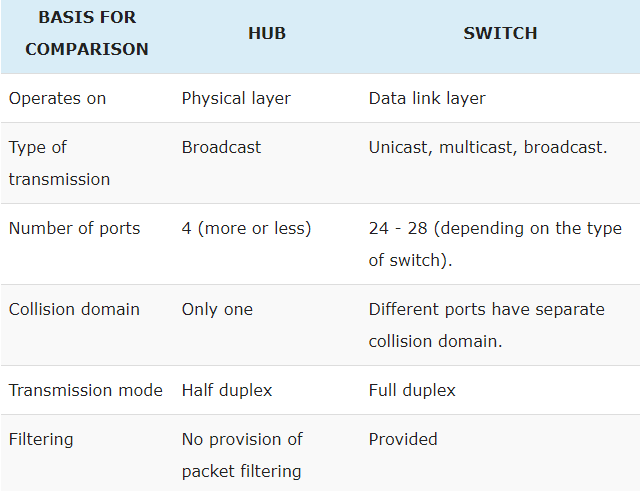
2.Switch – Modular switch / Non modular switch , L2 switch L3 switch .

3.Router --  **router** is [hardware](https://www.computerhope.com/jargon/h/hardware.htm) device designed to receive, analyze and move incoming [packets](https://www.computerhope.com/jargon/p/packet.htm) to another [network](https://www.computerhope.com/jargon/n/network.htm).

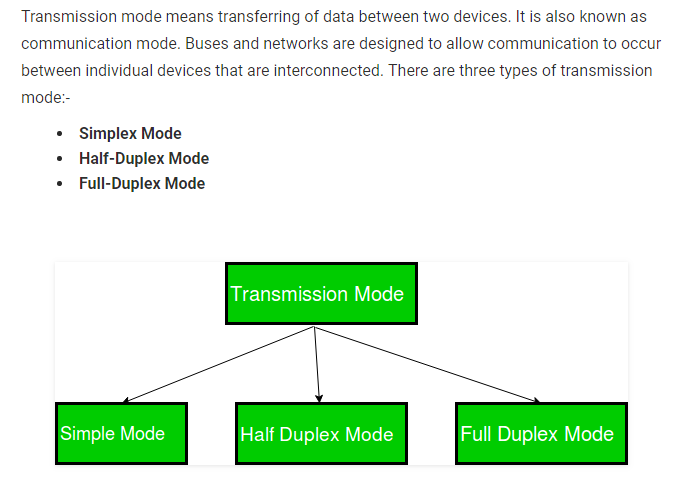
4.Firewall – it’s a device that protects network form unauthorized access , controls incoming and outgoing traffic based on set of rules

5.Wireless access point – is a device that allows other [Wi-Fi](https://en.wikipedia.org/wiki/Wi-Fi) devices to connect to a wired network

6.WLC – Device which controls AP .



**Transmission Modes.**

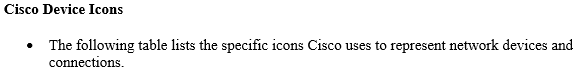


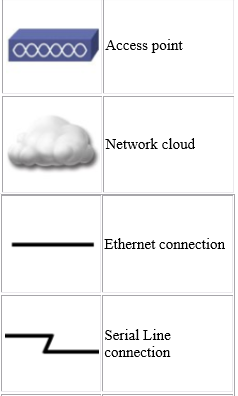
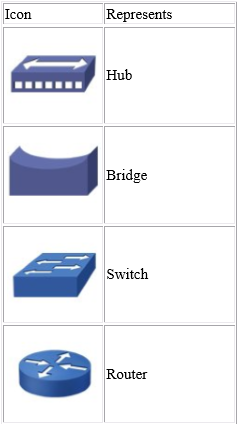
Simplex – One direction – Keyboard

Half duplex – Either send or receive , Walkie- talkie in which message is sent one at a time and messages are sent in both the directions.

Full Duplex – Telephone.

**Diagramatical representations .**

****





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

1. 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.



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

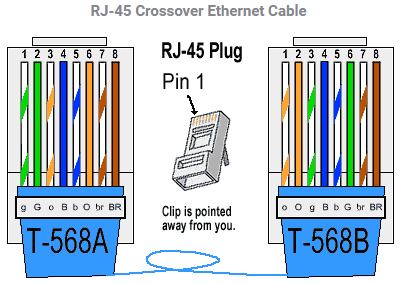
Types of Ethernet cables .1 . Straight through , 2 . Cross over . 3 Rolled over

Color coding of cables

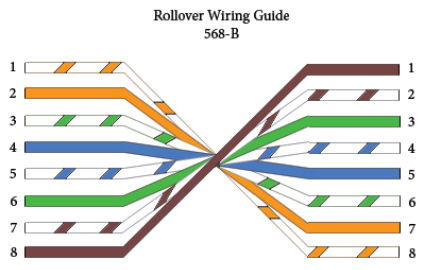
T-568A + T568A – Straight through cable

T-568B + T568B - Straight through able

T-568A + T568B – cross over cable

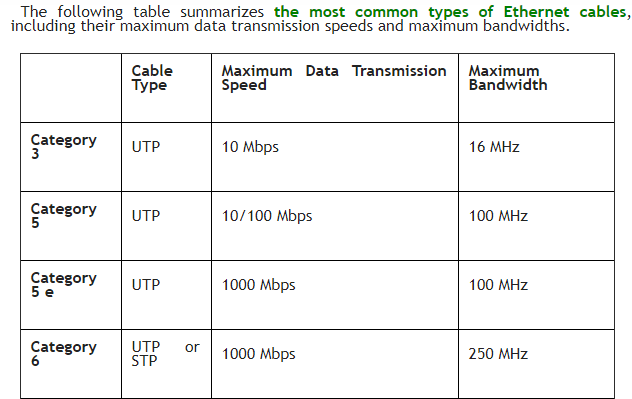


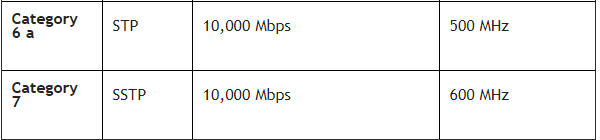
### NOT SOO IMPORTANT……………………start



RJ45 and RJ11 – Connectors

### NOT SOO IMPORTANT……………………start





### NOT SOO IMPORTANT……………………END

**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.

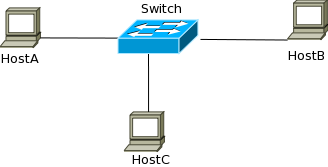
Cisco Systems shipped its first product in 1986 and is now a multi-national corporation, with over 35,000 employees in more than 115 countries. Today, Cisco solutions are the networking foundations for service providers, small to medium business and enterprise customers which includes corporations, government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

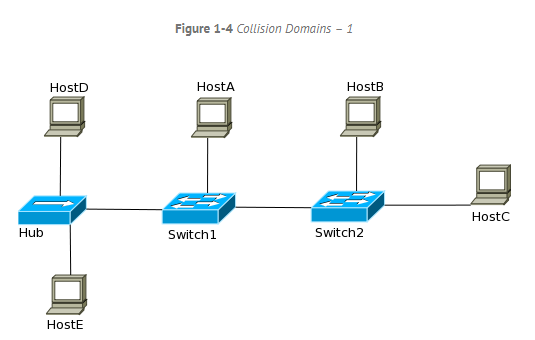
Communication between hosts can be classified into three types:

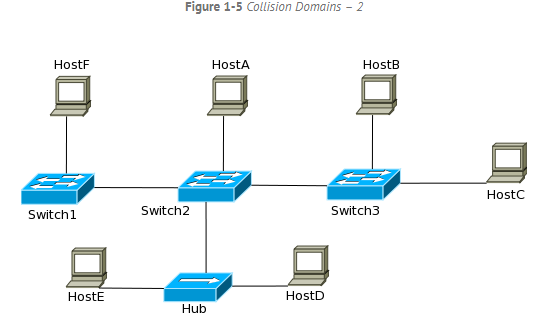
* **Unicast** – Communication from one host to another host only.
* **Broadcast** – Communication from one host to all the hosts in the network.
* **Multicast** – Communication from one host to few hosts only.

**CD** – How many devices can communicate at a time

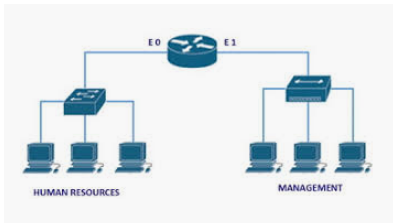
BD – How far a Packet travels when a broadcast is done .

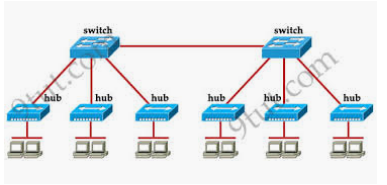
* **Figure 1-3** *A switched network*
* **
* **Figure 1-4** *Collision Domains – 1*











Switches break collision domains and routers break broadcast domains

**SYLLABUS STARTS… IMPORTANT**

**OSI Layers / Host to Host communication model.**

1.OSI 7 Layers and its Functionalities

2.OSI Layers and TCP Suite .

OSI MODEL AND TCP / IP MODEL.

**DEFINETION**: OSI / TCP-IP - model tells how the communication happens between two or more networking devices - within the organization or in the internet.

Each layer defines a set of functions in data communications.

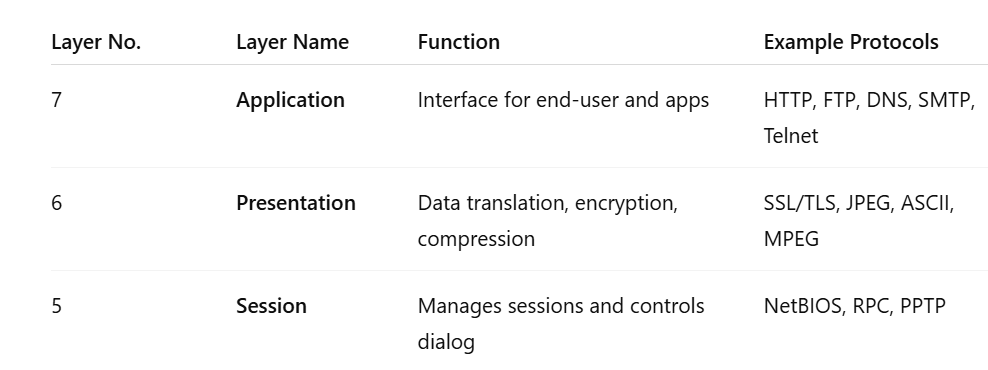
**OSI Model** is a reference model which was developed by **ISO** which consists of 7 layers

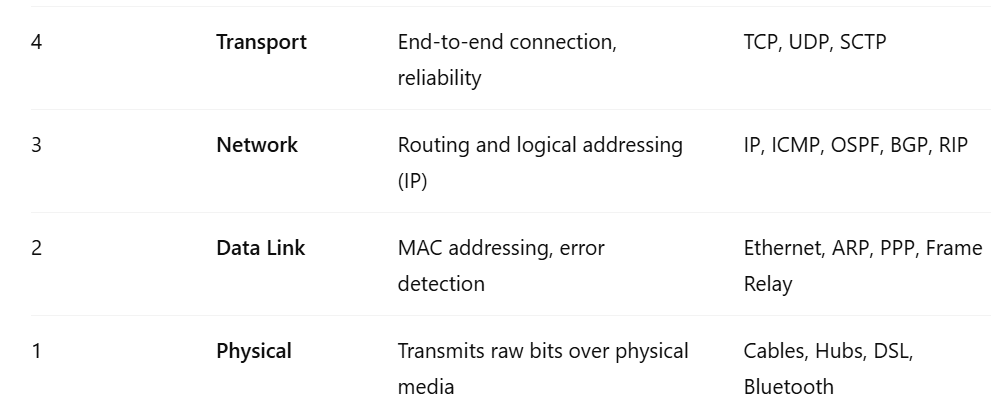
We use OSI only as a reference ,

But when we talk about the **TCP**/IP model, it was designed and developed by Department of Defense (DoD) it has 4 layers . (practically we use TCP/IP model Theoretically for a reference we use OSI model ) .

NOTE : INTERNET works on TCP/IP model.

OSI Layers. There are 7 Layers.





**APPLICATION LAYER. Layer 7**

The **Application Layer** is the **7th layer** in the **OSI (Open Systems Interconnection) model** It Provides user interface for the users to interact with application services or Network services.

Example - Google Chrome, Putty , whats app etc.

**PRESENTATION LAYER - 6**

The **Presentation Layer** is the **6th layer** in the **OSI (Open Systems Interconnection) model**

It is responsible for defining a standard format for the data.

.jpeg, .Doc, Zip files.

PDU – the data is in which form is called PDU – user data

PDU in presentation layer – Formatted data

**SESSION LAYER – 5**

The **Session Layer** is the **5th layer** in the **OSI (Open Systems Interconnection) model**

It is responsible for Establishing, maintaining and terminating sessions.

It deals with interactions between the applications,

Session ID s are used to identify a session

You can use the list of sessions created in cmd prompt using NETSTAT command

Here comes the real networking part .

**TRANSPORT LAYER**

The **Transport Layer** is the **4th layer** in the **OSI (Open Systems Interconnection) model**, responsible for **end-to-end communication** and **data delivery** between devices across a network –(def is imp don’t get confused with Def of DATA link layer)

Identifying the service and adding port number.

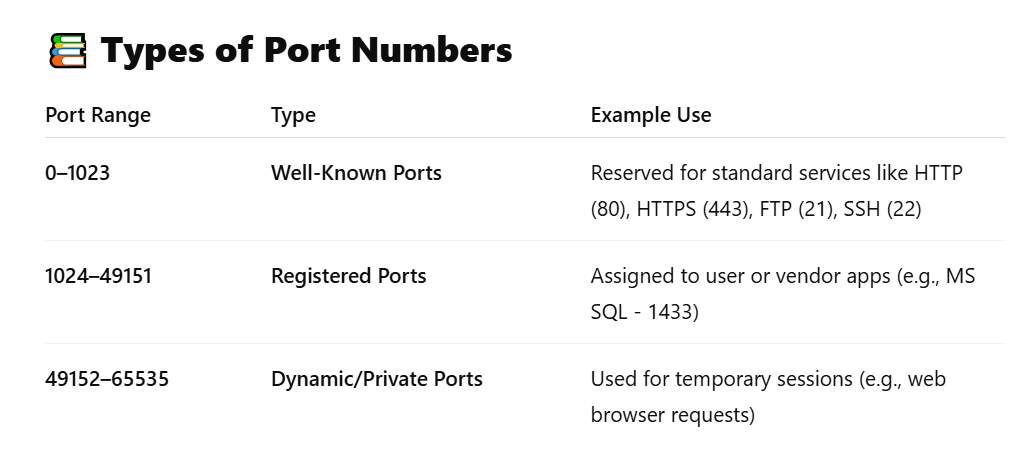
PORT NUMBERs

A **port number** is a **logical number** within a device that helps identify **specific applications or services** running on it. It works with IP addresses to make sure data reaches the **correct program**.

: Each and every service is identified using a port number

All protocols that comes under software layers will have port numbers but not protocol numbers.

Protocols that come under transport layer and below will have protocol numbers but not port numbers.



Functionalities of Transport Layer

Segmantation

Sequencing and Reassembling

Multiplexing and de multiplexing

Identifying the service

Flow control

Error correction

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 by default it is 1500 bytes.

There are 2 types of header , TCP header and UDP Header .

Transport layer decides 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 .

Unreliable – UDP – Continuous flow of traffic without any ack.

In UDP seq 1-🡪

Seq 2 --🡪

Seq 3 -🡪

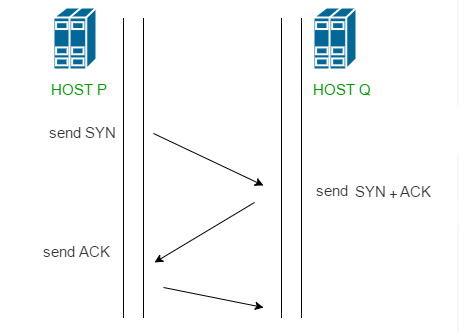
No ack just sending continuous data . If data is lost in the middle its lost forever , Now the question is who wants to loose the data ,

ANS : UDP will be used , when the time is imp than the DATA itself .

TCP is used when DATA is imp that time .

Before sending data a connection will be established called ,

3 way handshake



after which traffic will start flowing.



TCP protocols

UDP protocols

Almost all the protocols comes under TCP / UDP

Here's a clear breakdown of which common **application-layer protocols** using **TCP** or **UDP** as their **transport protocol**.

## ****Protocols That Use TCP****

These protocols require **reliable, connection-oriented communication**:

| **Protocol** | **Port** | **Description** |
| --- | --- | --- |
| **HTTP** | 80 | Web browsing |
| **HTTPS** | 443 | Secure web browsing |
| **FTP** | 21 | File Transfer Protocol |
| **SFTP** | 22 | Secure FTP over SSH |
| **SMTP** | 25 | Sending email |
| **POP3** | 110 | Retrieving email |
| **IMAP** | 143 | Email access (more advanced than POP3) |
| **SSH** | 22 | Secure remote login |
| **Telnet** | 23 | Remote terminal access (insecure) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## ****Protocols That Use UDP****

These are used when **speed is more important than reliability**:

| **Protocol** | **Port** | **Description** |
| --- | --- | --- |
| **DNS** | 53 | Resolving domain names (can also use TCP for large queries) |
| **DHCP** | 67/68 | Dynamic IP assignment |
| **TFTP** | 69 | Simple, lightweight file transfer |
| **SNMP** | 161 | Network management protocol |
| **RIP** | 520 | Routing Information Protocol |
| **NTP** | 123 | Time synchronization |
| **VoIP** | Varies | Used for voice calls (e.g., SIP uses UDP 5060) |
| **Syslog** | 514 | Logging from network devices |
| **mDNS** | 5353 | Local network name resolution |
| **BOOTP** | 67/68 | Bootstrap Protocol (older version of DHCP) |

but

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

Only TCP and UDP uses port number, Port number is a 16 bit number used by protocols that either uses TCP or UDP .

for ex HTTP : 80 HTTPS 443

Question What is the port number of EIGRP and OSPF .

There are no port numbers for the above two .

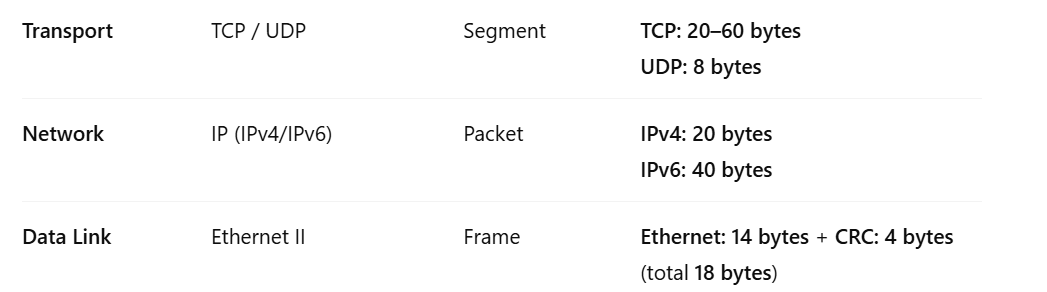
…..

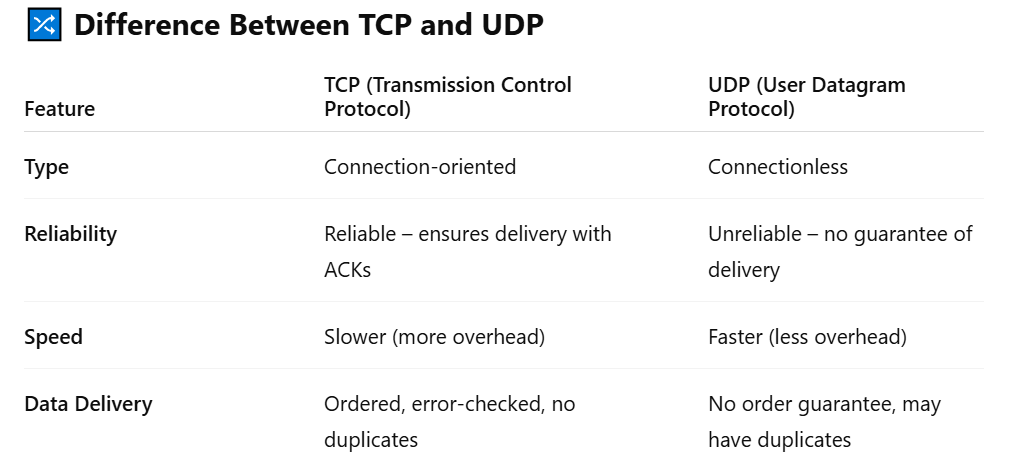
### ****PDU (Protocol Data Unit) of Each OSI Layer****

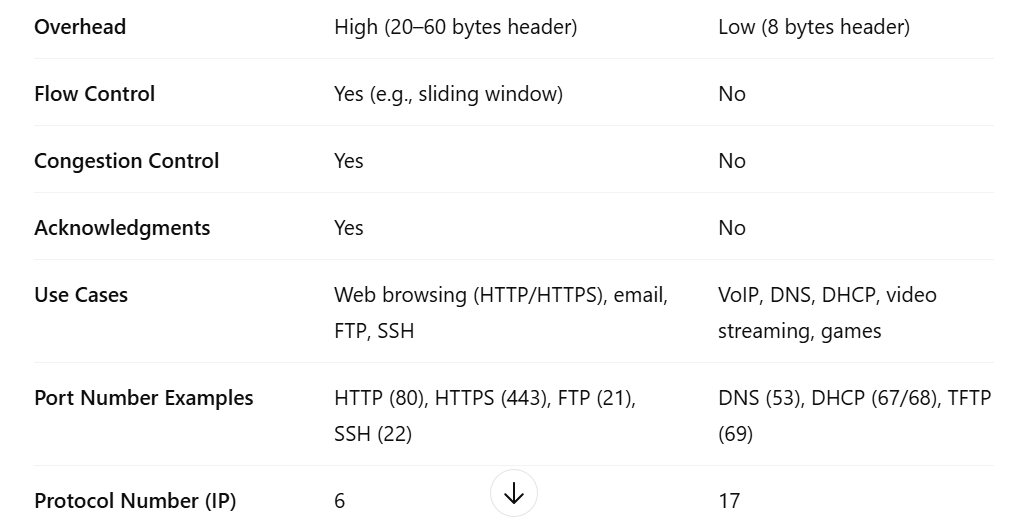
In networking, a **PDU (Protocol Data Unit)** is the name given to data at each layer of the OSI model. It changes as data moves through the layers during transmission.

| **OSI Layer No.** | **Layer Name** | **PDU Name** | **Description** |
| --- | --- | --- | --- |
| 7 | Application Layer | **Data** | User-generated data (e.g., message, file) |
| 6 | Presentation Layer | **Data** | Data formatting, encryption, compression |
| 5 | Session Layer | **Data** | Session control data |
| 4 | Transport Layer | **Segment** | Adds TCP/UDP headers, port info |
| 3 | Network Layer | **Packet** | Adds logical addressing (IP headers) |
| 2 | Data Link Layer | **Frame** | Adds MAC addresses, error checking |
| 1 | Physical Layer | **Bits** | Transmits raw bits (0s and 1s) over cable |

Header Sizes.





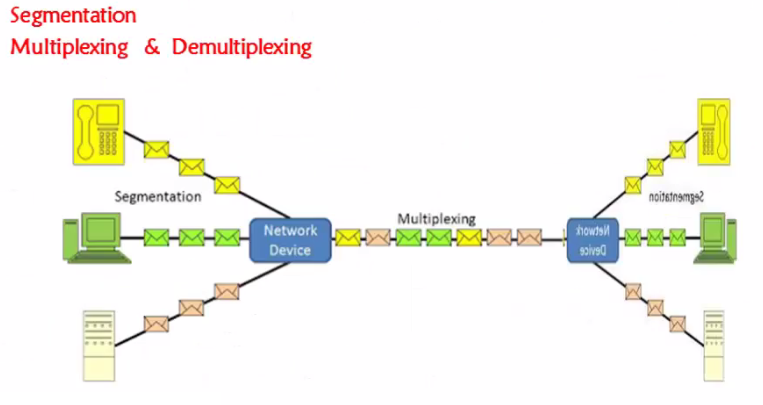


**ICMP -1** The Internet Control Message Protocol is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information .

**Multiplexing and DE multiplexing**

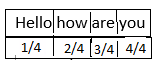
Different types of traffic is identified using different frequencies .FBD-TBD Frequency based division and Time based division

Data Traffic,Voice traffic,Verio traffic.

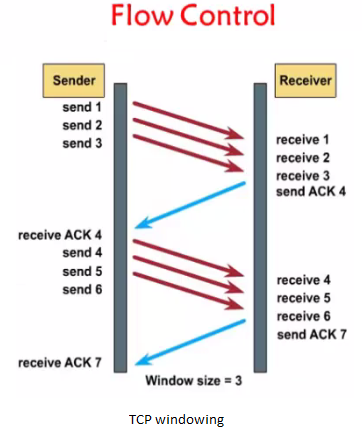


Sequencing and reassembling .

Hello how are you



Flow control – 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 .



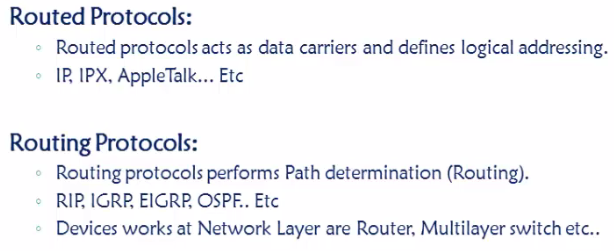
**Network Layer**

The **Network Layer** is the **3rd layer** in the **OSI (Open Systems Interconnection) model** , It is responsible for

1.Logical addressing – IP address

2.Path determination - Routing

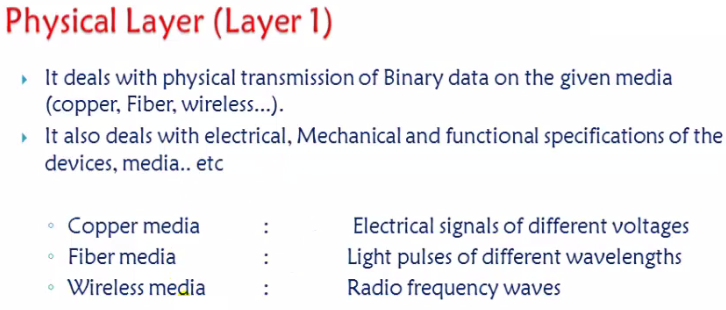
These are the two major functionalities of NL.



DATA laye

The **Data Layer** is the **6th layer** in the **OSI (Open Systems Interconnection) model** . It is responsible for “End to end delivery of data between the devices under a LAN network”

2 main functionalities.



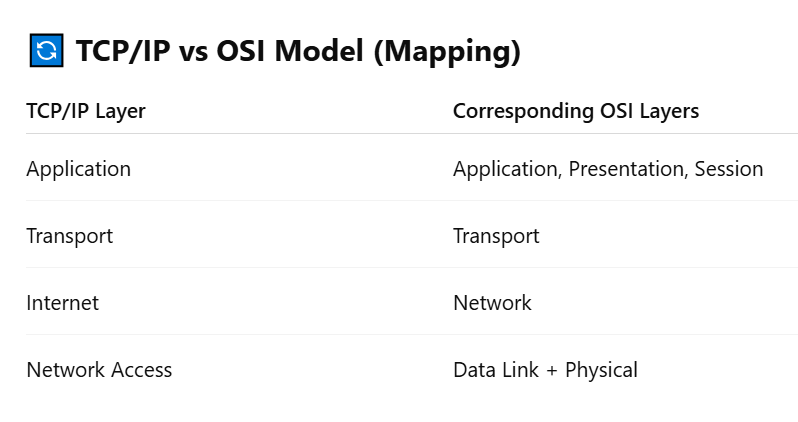
TCP / IP Model

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

Main goal of TCP / IP model

1.How to transmit data across the network

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



**NOTE:** Extra not in syllabus.

**Difference between KBps and Kbps (Kilo bytes/sec and Kilo bits/sec)**

**Measure of file size: KBps**  
File size i.e. how big the file or how much space a file occupies in the hard disk measured in terms of Kilo Bytes (KB upper case “K” and upper case “B”). In computing terms the upper case “K” stands for 1024. 1024 is computed from 210. (2 power 10). 2 denote the number of characters in the binary system which is used to store data in the disc (ones and zeroes).  
Other abbreviations like mega, giga and terra also use the base as 1024,

1KB (Kilo Byte) = 1024 Bytes (approximately 1000 Bytes)  
1MB (Mega Byte) = 1024 KB (approximately 1000 Kilo Bytes or 1 million Bytes)  
1GB (Gigabyte) = 1024 MB (approximately 1000 Mega Bytes or 1 billion Bytes)  
1TB (Terra Byte) = 1024 GB (approximately 1000 Gigabytes or 1 trillion Bytes)

**Measure of data transfer speeds: kbps**Data transfer speed over the networks (including the internet) is calculated in terms of bits per second: kilobits (kb small case “k” and small case “b”). The higher the kbps i.e. more the bits transferred per second, more the speed, faster the network/connection. Here k stands for 1000 (103 )

1 kbps (kilo bits per second) = 1000 bits per second  
1 Mbps (mega bits per second) = 1000 kilo bits per second.  
1 Gbps (giga bits per second) = 1,000 mega bits per second.

**ISP bandwidth and download speeds**  
The most common confusion caused by the similarity of KBps and kbps is when it comes to internet bandwidth and download speeds. People often complain that their ISP promised 512kbps connectivity but they are seldom able to download any file at 512 KBps. They fail to notice the difference in cases of the units and hence think their ISP is cheating them or offering them poor quality service. As mentioned earlier data transfer speeds are always calculated in terms of kilo bits per second (kbps) so an ISP connectivity of 512 kbps promises of transfer of at the max 512 kilo bits per second.

On the other hand, file size measure is always in Kilo Bytes and thus download speeds are always calculated based on how many Bytes per second are downloaded and hence Kilo Bytes per second (KBps). KBps and kbps are not interchangeable.

So an internet connectivity of say 512kbps can never achieve a download speed of 512 KBps. To calculate the maximum download speed of a “X kbps” connection, we need to use a simple formula as below.

Download KBPS speed = (Kbps value\*1000) /8)) / 1024.

I.e. For a connectivity of 512 kbps

kbps value \* 1000 = 512 \* 1000 = 512000

512000 / 8 = 64000

64000 / 1024 = 62.5 KBps

Therefore theoretically an internet connection of 512kbps bandwidth can download at a speed of 62.5 KBps.

If you don’t want to go through all the hassles of the above formula,**just multiply the kbps value with 0.1220703125 to get the KBps value.**

512 kbps \* 0.1220703125 = 62.5 KBps. Simple!

**Internet connectivity**

Download speed (approx) ( Marked in Italics)

256 kbps - 31.3 KBps

384 kbps - 46.9 KBps

512 kbps - 62.5 KBps

768 kbps - 93.8 KBps

1 mbps ~ 1000kbps - 122.1 KBps

I have mentioned download speed as approximate because they will vary (always reduce) by 15 – 20% due to network signal loss, computer hardware overheads etc. So for realistic, real world figures always reduce 15 – 20% from the computed KBPS download speeds  
Now I guess the confusion of kbps and KBps has cleared away. Just remember when you talk in terms of network it’s always bites per second (bps) and when you talk in terms of storage and files its always Bytes per second (Bps). And next time you won’t complain when your 512 kbps connection does not give you download speeds of 512KBps because now you know why .

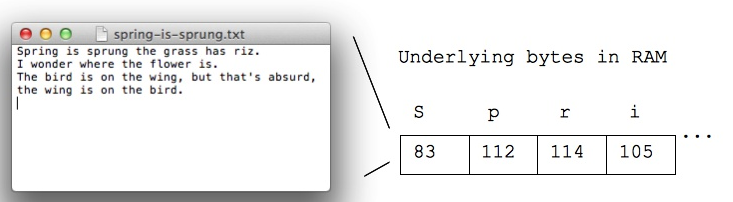
**Network Addressing Scheme**

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] .

**Types of various Units of Memory-**



* Bit – 0 1
* Byte – 8 bits
* Kilo Byte – 1024 bytes
* Mega Byte - 1024 KB
* Giga Byte - 1024 MB
* Tera Byte – 1024 GB
* Peta Byte
* Exa Byte
* Zetta Byte
* Yotta Byte

**DATA REPRESENTATION FORMATS**

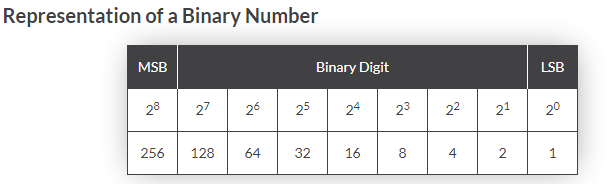
Binary - **Binary** is used for calculating **network** masks

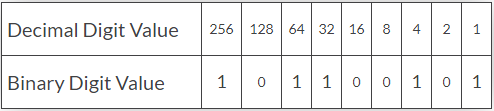
Decimal - **Decimal** is the human **numbering system** we display IPv4 addresses

Hexa decimal - **hexadecimal** is used to display Ethernet MAC addresses and IPv6 addresses

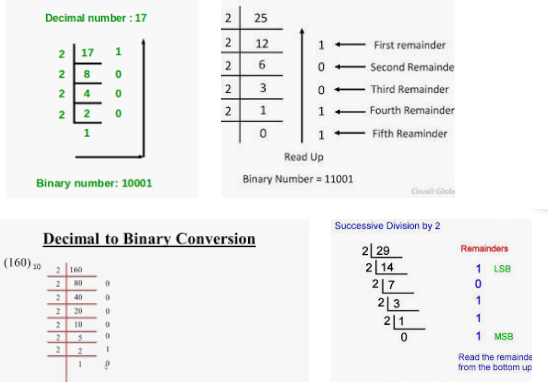
So expertize in converting of all these is very much required .

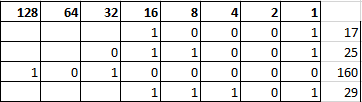
BINARY TO DECIMAL



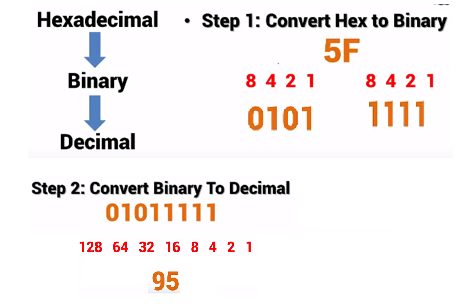


DECIMAL TO BINARY





Convert hex to binary and decimal



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

**IP addresses**

IP address is a logical address, It is a 32 bit binary number represented in decimal format.It is used to represent devices in a network to send and receive data between two devices.

****

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

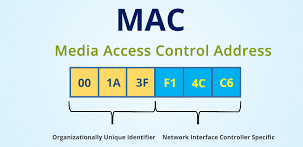
1.MAC address – Physical address.

2.IP address – Logical address.

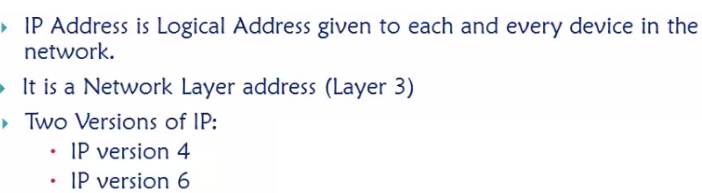
1. Mac address : A media access control **address** (**MAC address**) of a device is a unique identifier assigned to a network interface controller

It is a 48 bit binary number represented in hexa decimal format .

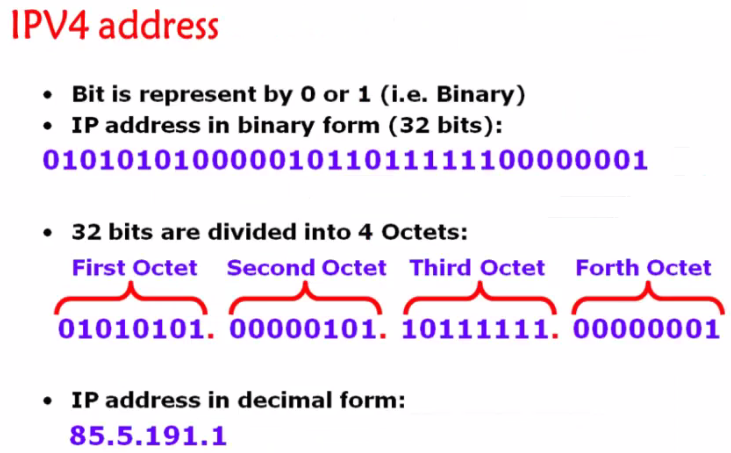
Mac / physical / Hardware / Burnt in address .

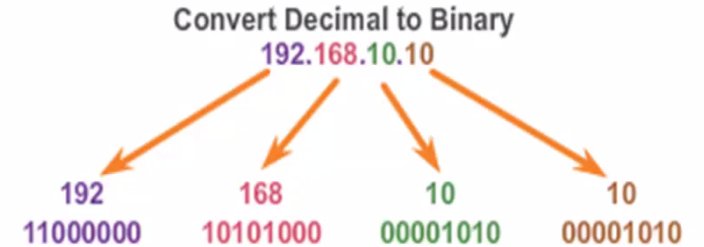


2.IP ADDRESS : IP addresses are 32 bit binary number represented in decimal format . AND DIVIDED in to 4 octet s .

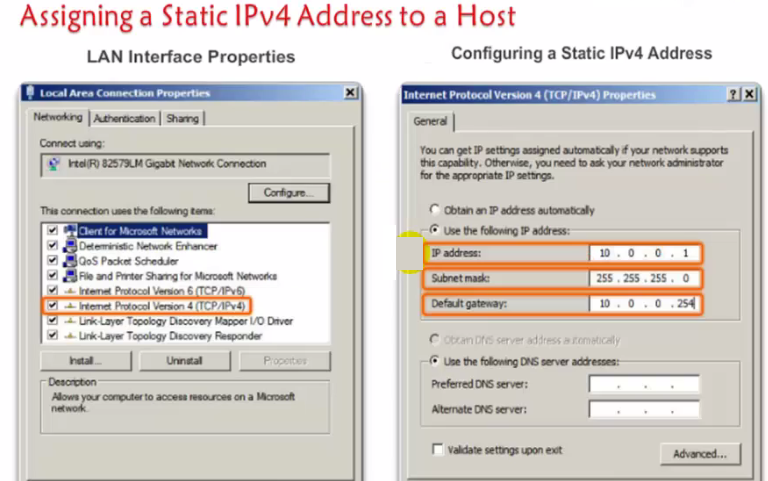


IP Address = 2 raise 32 ip address = 32billion – internet grew shortage IP address , To overcome the shortage of IPV4 , IPv6 128 bit

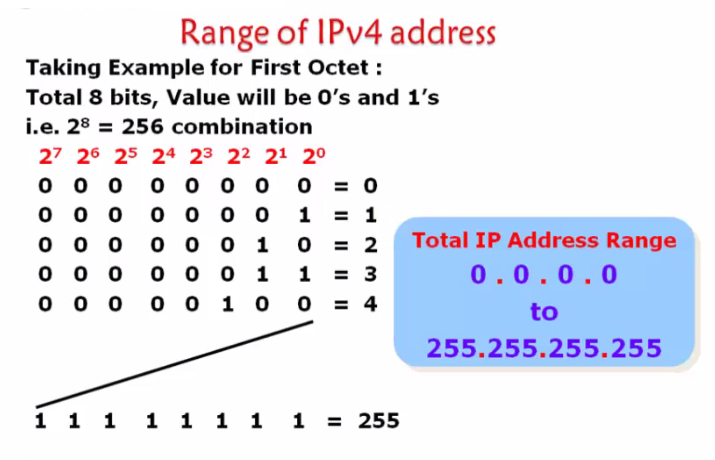
****

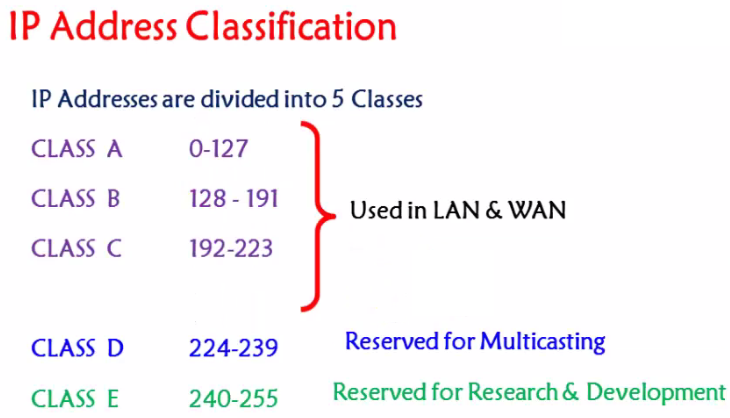
****

How to give IP address manually in your PC

****

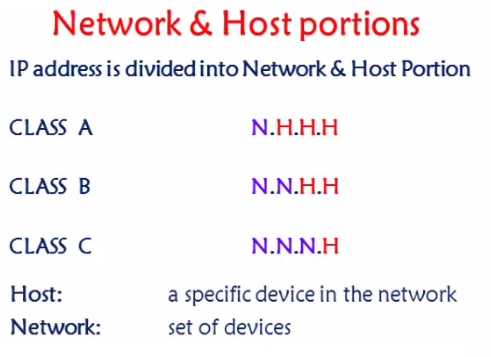
Control panel , Network and sharing . In real time – DHCP

****

****

169.254.0.0 to 169.254.255.255 – APIPA Ip addresses .

Unicast , Multicast and broadcast .

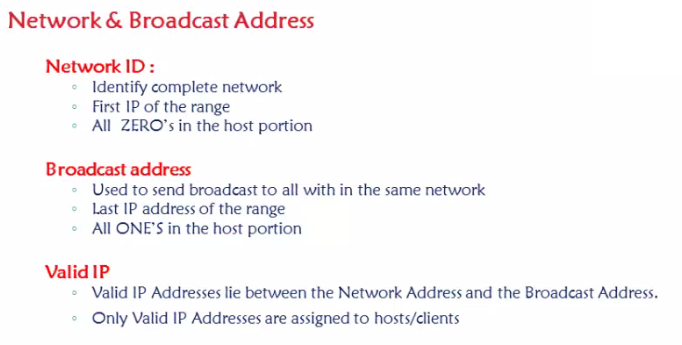
****

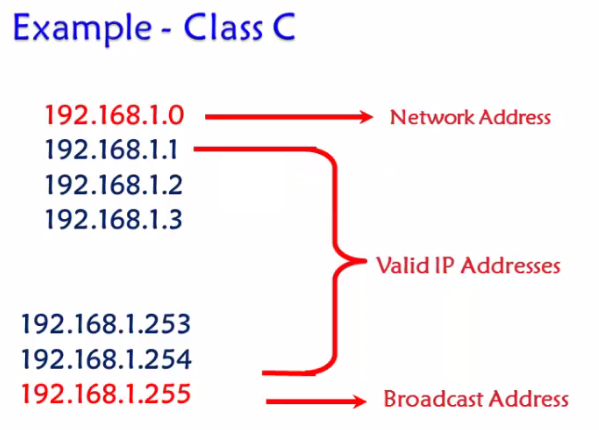
If two devices has to communicate then network part should be same .

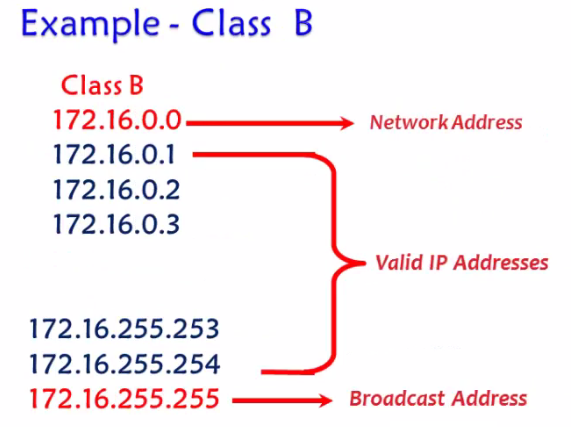
256 IP addresses

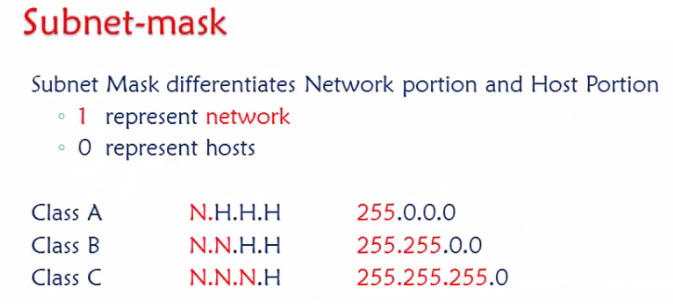
256 raise 2 = 65536

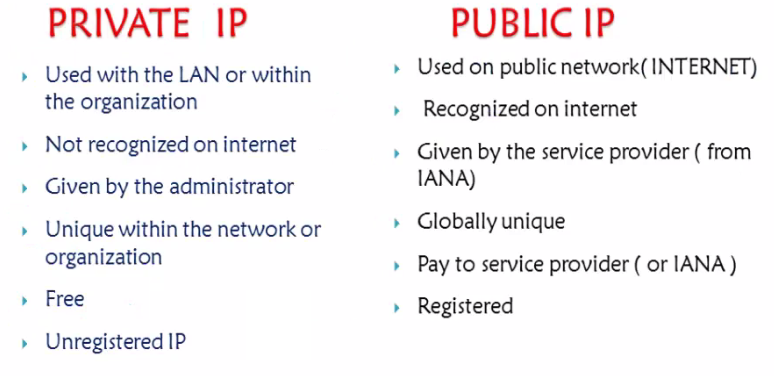
256 raise 3 = 16777212

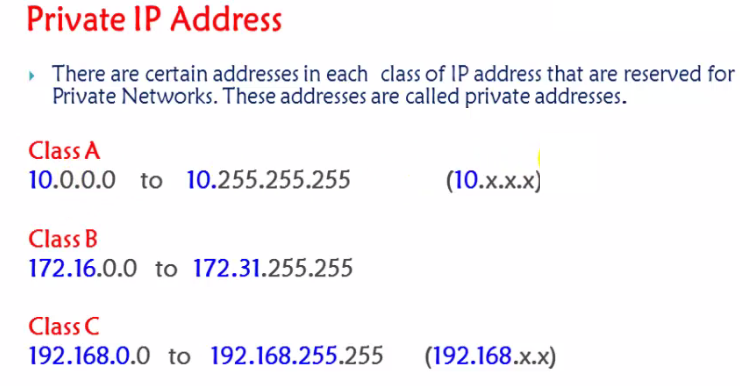
****

****

****

****

****

****



<https://www.iana.org/>

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

**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. **Efficient IP address Utilization**
2. **Ease administration**
3. **Better network performance**
4. **Simplifies Troubleshooting and management.**

**1.Network Scenario 1**

**216.21.5.0 – 5 Networks**

**1.Determine the number of NETWORKS and convert them to bits**

**128 64 32 16 8 4 2 1**

**0 0 0 0 0 1 0 1 - 00000111**

**2.REVERSE the bits (Entire host part) in subnet mask and find the INCREMENT**

**255.255.255.0**

**11111111.11111111.11111111.11100000**

**32**

**So the subnetworks subnet mask will be 255.255.255.224**

**3.Using the increment – find the SUBNETWORKS**

**216.21.5.0 - 216.21.5.31 – 1st Subnetwork**

**216.21.5.32 - 216.21.5.63 – 2nd Subnetwork**

**216.21.5.64 - 216.21.5.95 – 3rd Subnetwork**

**216.21.5.96 - 216.21.5.128 – 4th Subnetwork**

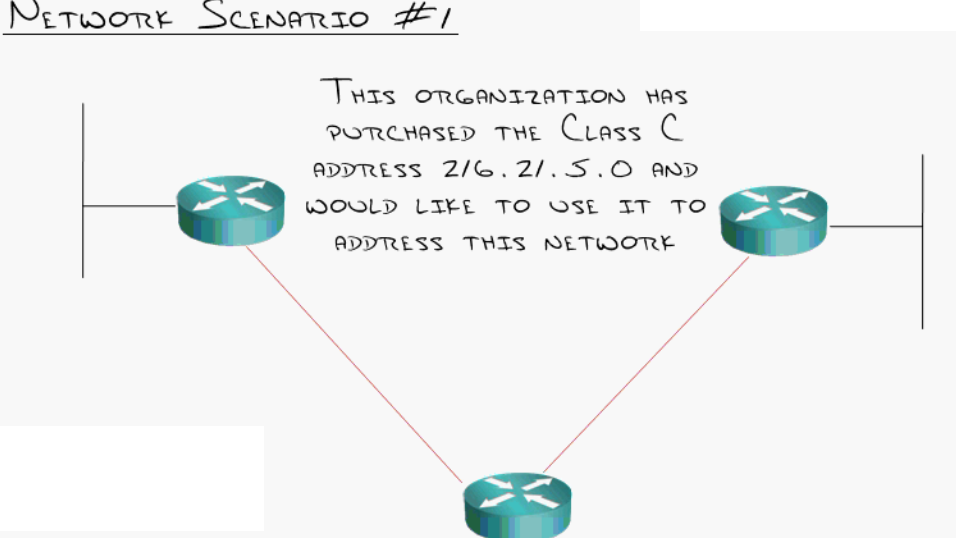
**216.21.5.128 - 216.21.5.159 – 5th Subnetwork**

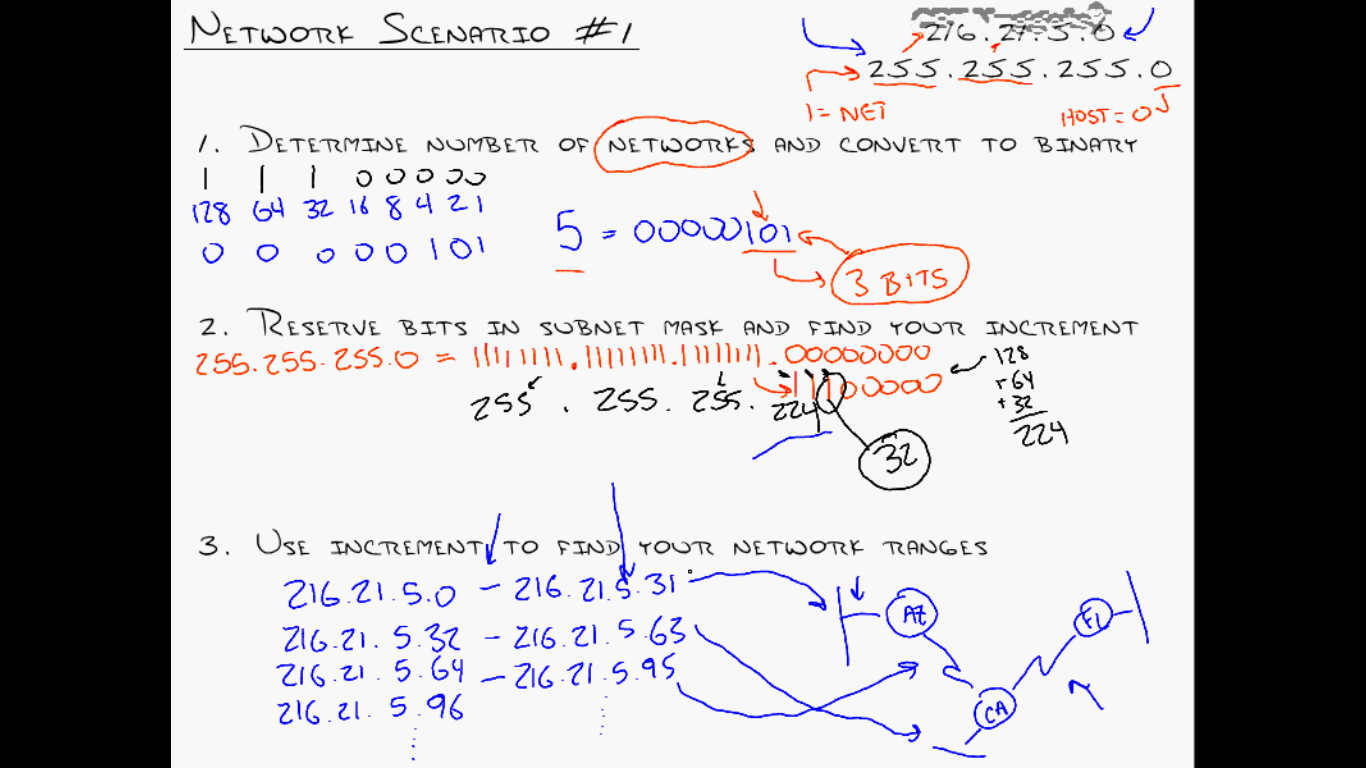
**216.21.5.160 - 216.21.5.191 – 6th Subnetwork**

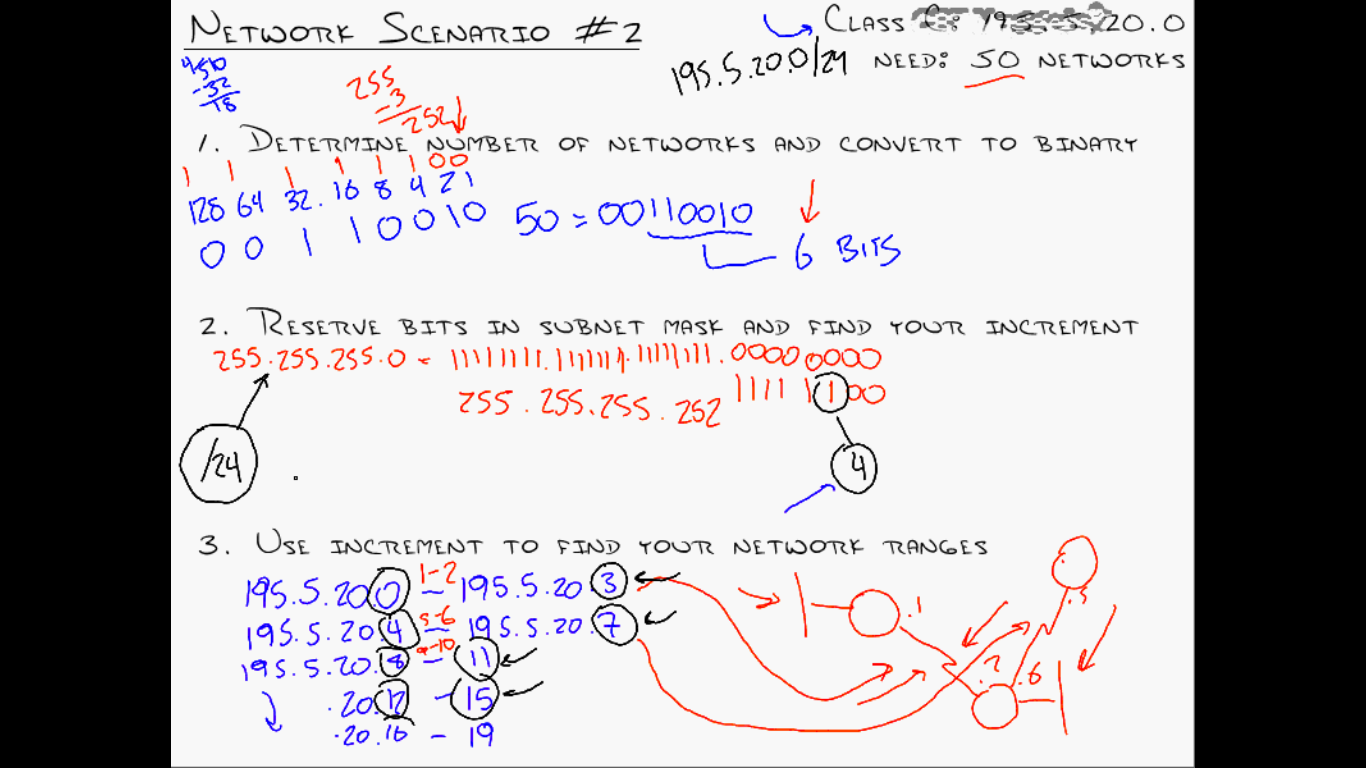
**216.21.5.192 - 216.21.5.223 – 7th Subnetwork**

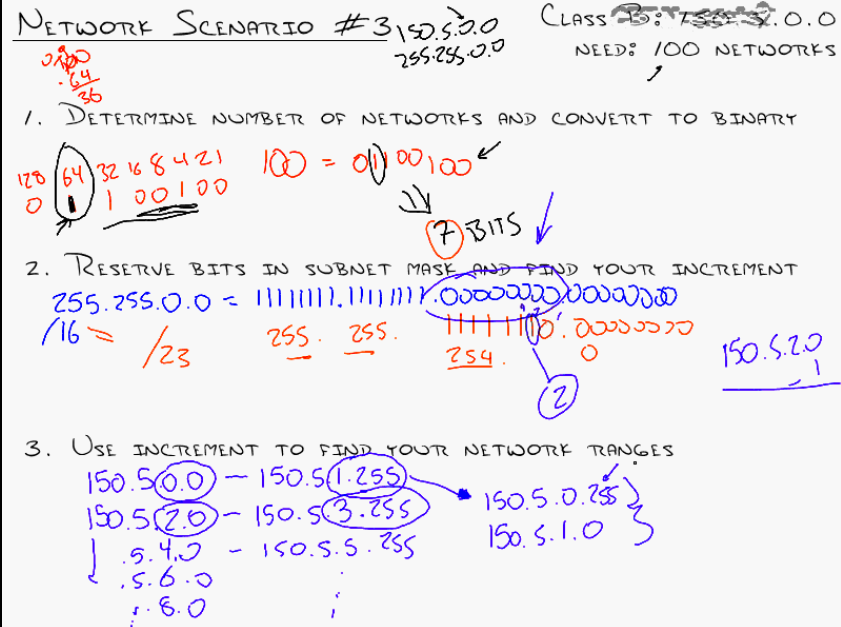
**216.21.5.224 - 216.21.5.255 – 8th Subnetwork**

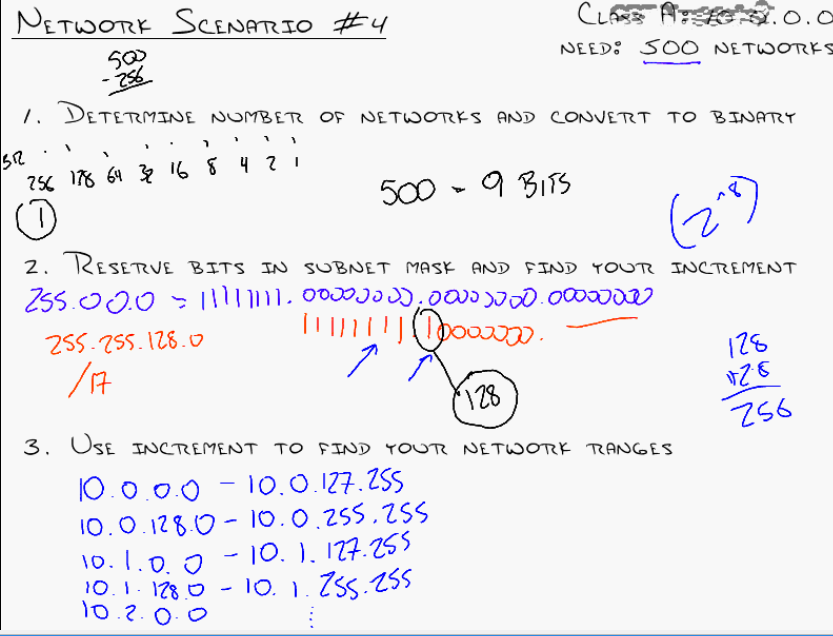
**Even though the required networks are 5 you will get 8 only.**

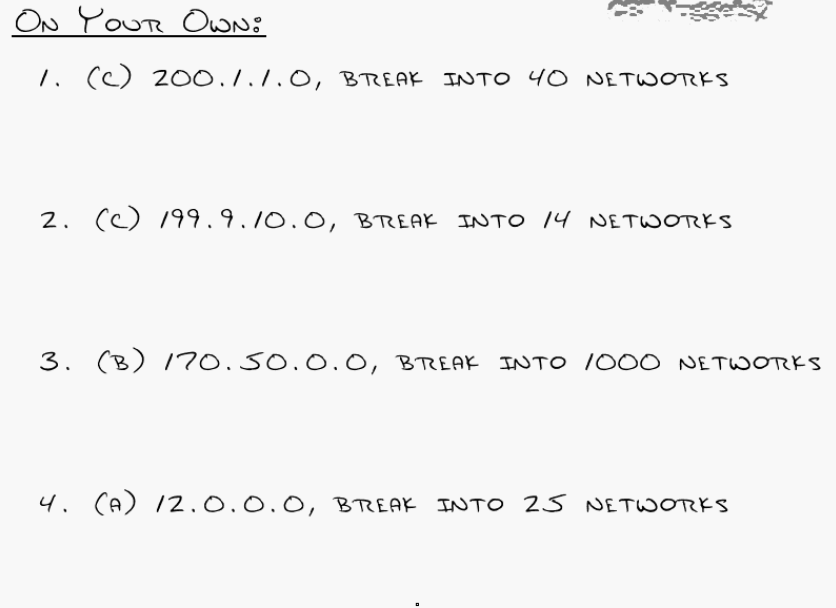
****



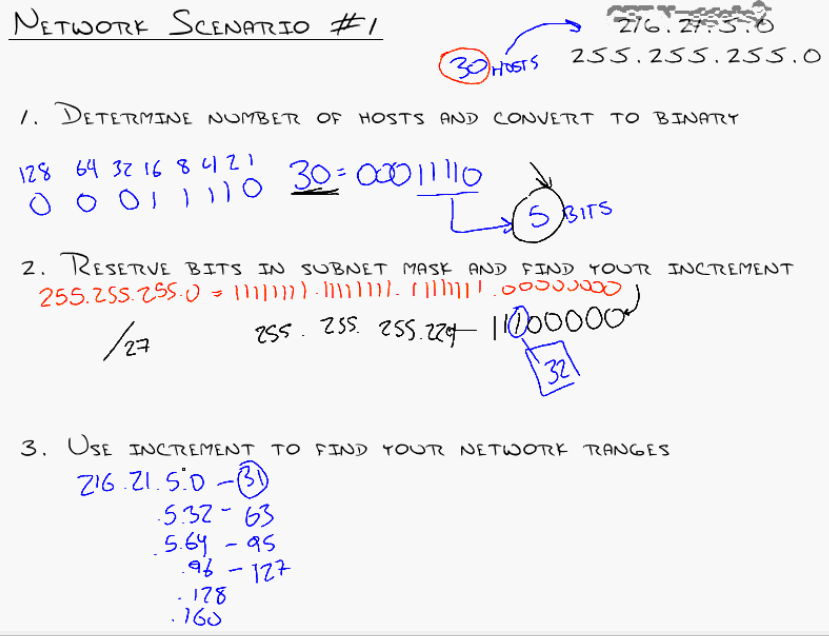




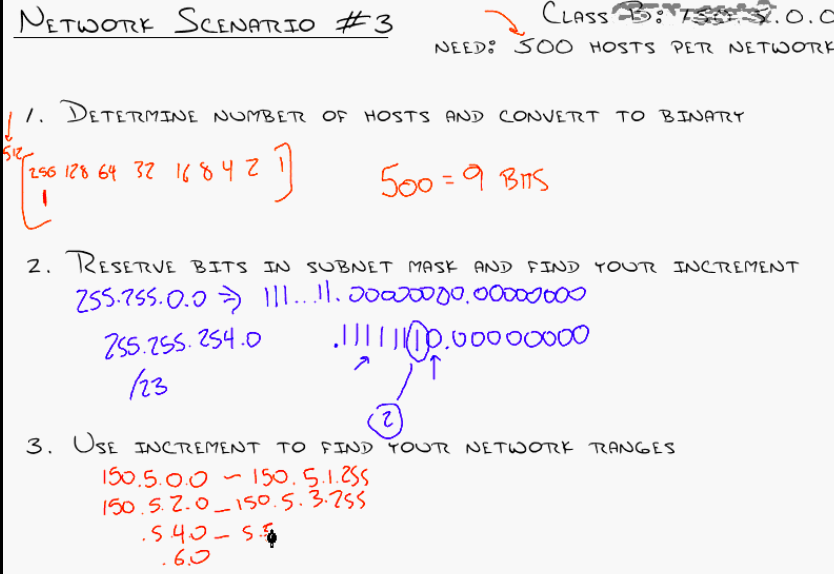




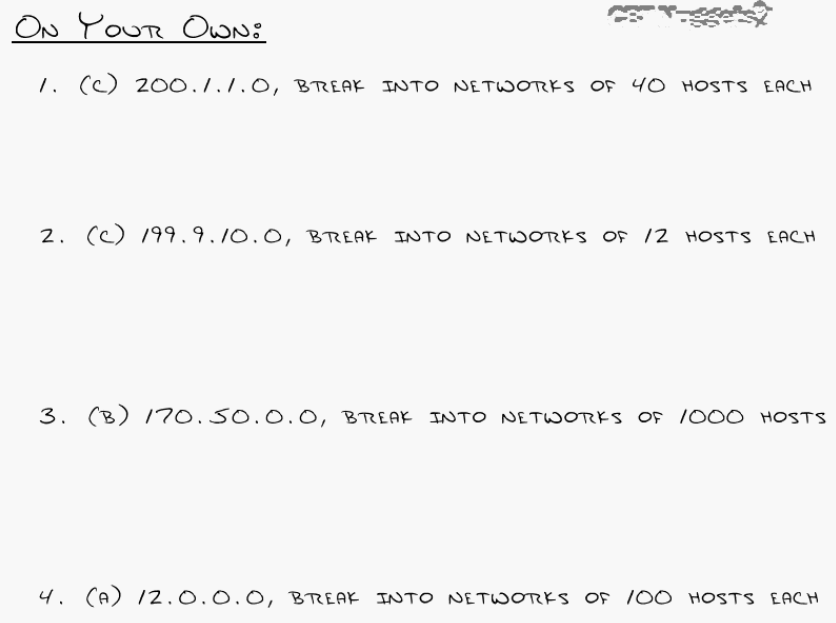
**SUBNETTING BASED ON HOSTS**





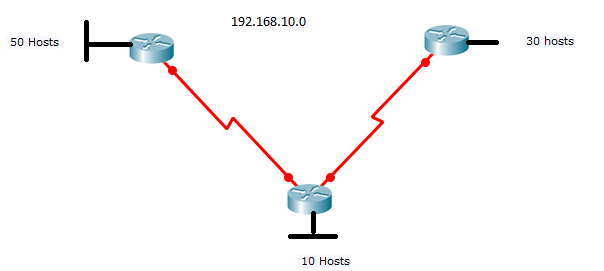






**VLSM**

Very important as it is used in real time



Finds lots of Sub netting Questions here:

http://www.subnettingquestions.com/

**Question:**What valid host range is the IP address172.18.229.223 255.255.255.128 a part of?

**Answer:**172.18.229.129 through to 172.18.229.254

**Question:**What is the last valid host on the subnetwork 172.24.52.0 255.255.255.0?

**Answer:**172.24.52.254

**Supernetting – will discuss after Routing.**

**“**What is Discontiguous vs. Contiguous?

### ****Contiguous vs. Discontiguous Networks**** (in networking)

This concept is mainly relevant to **IP subnetting** and **routing**,

### ****Contiguous Network****

* **Definition:** All subnets of a network are **logically connected** and fall under the **same major network (classful network)**.
* **Example:**

192.168.1.0/24

192.168.2.0/24

192.168.3.0/24

All are part of **192.168.0.0/16** – **Contiguous**.

### ****Discontiguous Network****

* **Definition:** Subnets **belong to the same major network** but are **separated by a different network** – **break in logical continuity**.
* **Example:**

Network A: 192.168.1.0/24

Network B: 10.0.0.0/8

Network C: 192.168.2.0/24

Here, **Network A and C** are from the same classful network (192.168.0.0/16), but separated by an unrelated **10.0.0.0** network – this is **Discontiguous**.

**”**

**What is Major Network Number?**

### 🔑 ****Major Network Number**** (also known as ****Classful Network Number****)

In traditional **classful addressing**, a **major network number** refers to the **original base network address** defined by IP address **classes (A, B, or C)**, before **subnetting** was introduced.

### 🧱 ****Classful IP Addressing Basics****

| **Class** | **Starting Bits** | **Default Subnet Mask** | **Address Range** | **Major Network Example** |
| --- | --- | --- | --- | --- |
| A | 0 | 255.0.0.0 (/8) | 1.0.0.0 to 126.0.0.0 | 10.0.0.0 |
| B | 10 | 255.255.0.0 (/16) | 128.0.0.0 to 191.255.0.0 | 172.16.0.0 |
| C | 110 | 255.255.255.0 (/24) | 192.0.0.0 to 223.255.255.0 | 192.168.1.0 |

* The **major network number** is the address defined **before any subnetting is done**.
* For example:
  + **192.168.1.0/24** → Major network is **192.168.1.0** (Class C)
  + **10.1.1.0/24** → Major network is **10.0.0.0** (Class A)

”

**Assigning IP address to a small network .**

