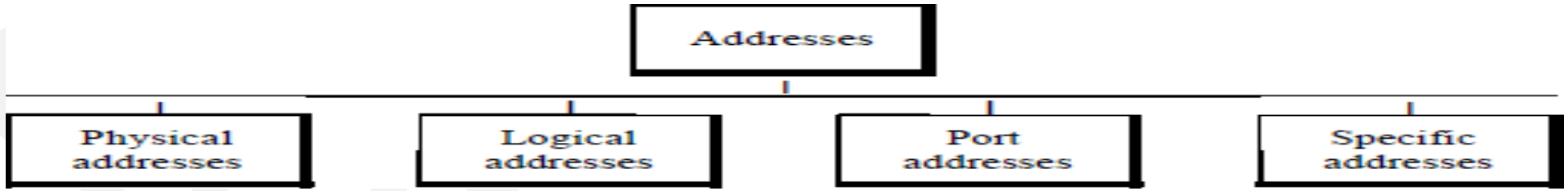
Data Communication & Network

Trainer : Sujata Mohite
Email: sujata.mohite@sunbeaminfo.com

Addressing

Addressing



Physical Address/ Link Address

- For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).

Logical Address

- logical address in the Internet is currently a **32-bit address** that can uniquely define a host connected to the Internet. IP address

Port Address

- computer A can communicate with computer C by using TELNET(login into a remote computer). At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP).

Specific Addresses

- Examples include the e-mail address and any Uniform Resource Locator (URL)

TELNET

- **A network protocol that allows a user on one computer to log into another computer that is part of the same network manage devices over a TCP/IP network**.
- A program that establishes a connection from one computer to another by means of telnet.
- A link established using a telnet program.
- Login into a remote computer using a telnet program.

- **File transfer protocol (FTP)** is an Internet tool provided by TCP/IP.
- It helps to transfer files from one computer to another by providing access to directories or folders on remote computers and allows software, data, text file to be transferred between different kinds of computers.

- **A Uniform Resource Locator (URL),** is a web address. It is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.

TELNET

- Telnet (short for Teletype Network) is a network protocol and command-line tool that allows a user to remotely access and manage devices over a TCP/IP network.
- Telnet is used to:
- 1. Remotely log in to a computer or network device
- 2. Execute commands on remote systems as if you're physically present
- 3. Perform basic troubleshooting and configuration (e.g., routers, switches)
- **How Telnet Works ?**
- 1. You open a Telnet client (like Command Prompt on Windows).
- 2. You connect to a remote server using its IP address or domain name and port (default is port 23).
- 3. After authentication (username/password), you can control the remote system via command line.

MAC Address / Physical Address/ Ethernet Address

- used on data link layer
- used to identify every NIC uniquely
- is burnt into the ROM part of NIC once written the MAC address can not be changed
- also known as read only address
- to find the MAC address of NIC
  - windows: ipconfig /all
  - linux/macOS: ifconfig
- e.g. 78 : 4f : 43 : 90 : 13 : d0
- size: 6 bytes = 8 x 6 = 48 bits
- Group of first three bytes(78 : 4f : 43) represent's manufacturer ID and last 3 bytes (90 : 13 : d0) represents NIC's unique address.
- to find the manufacturer, please visit https://hwaddress.com/

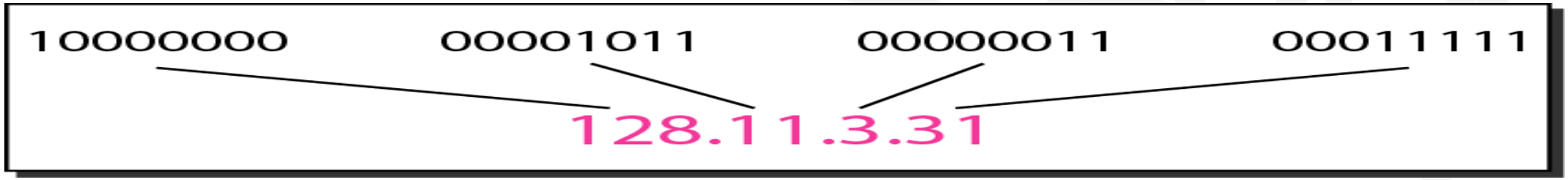
IP Address / Logical Address

- IP address to mean a logical address in the network layer of the TCP/IP protocol suite.
- Identify a machine / device uniquely.
- Size = 4 bytes = 32 bits
- to find the IP address of Machine
  - windows: ipconfig
  - linux/macOS: ifconfig
- IP Versions:
  - IPV4 (32 bits address length)
  - IPV6 (128 bits address length)
- IP addresses are made up of four sets of numbers called **“Octets”.**
- Types
  - Private : used to identify a machine on the LAN and can not be used to connect to internet
  - Public : used to connect to the internet
- e.g.
  - decimal: 192.168.1.6
  - binary : 11000000.10101000.00000001.00000110

IP Addressing Types

- Classful : IP Address is split into 5 classes
- Classless

  - IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or4,294,967,296 (more than 4 billion)
  - **There are two prevalent notations to show an IPv4 address:**
    - binary notation
    - dotted decimal notation



Example

- *Find the error, if any, in the following IPv4 addresses.*

a. 111.56.045.78
b. 221.34.7.8.20
c. 75.45.301.14
d. 11100010.23.14.67

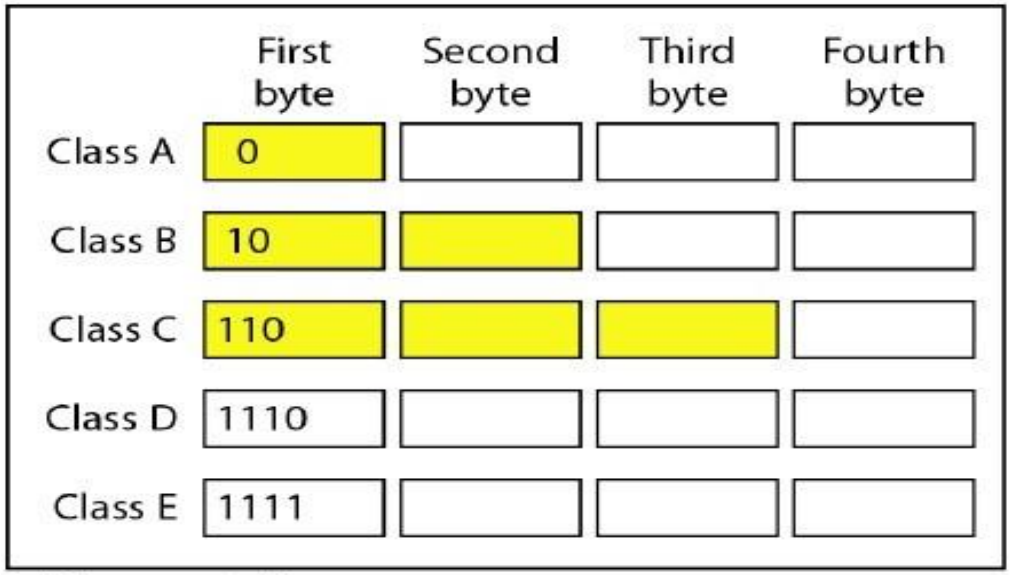
Solution

a. There must be no leading zero (045).
b. There can be no more than four numbers.
c. Each number needs to be less than or equal to 255.
d. A mixture of binary notation and dotted-decimal notation is not allowed.

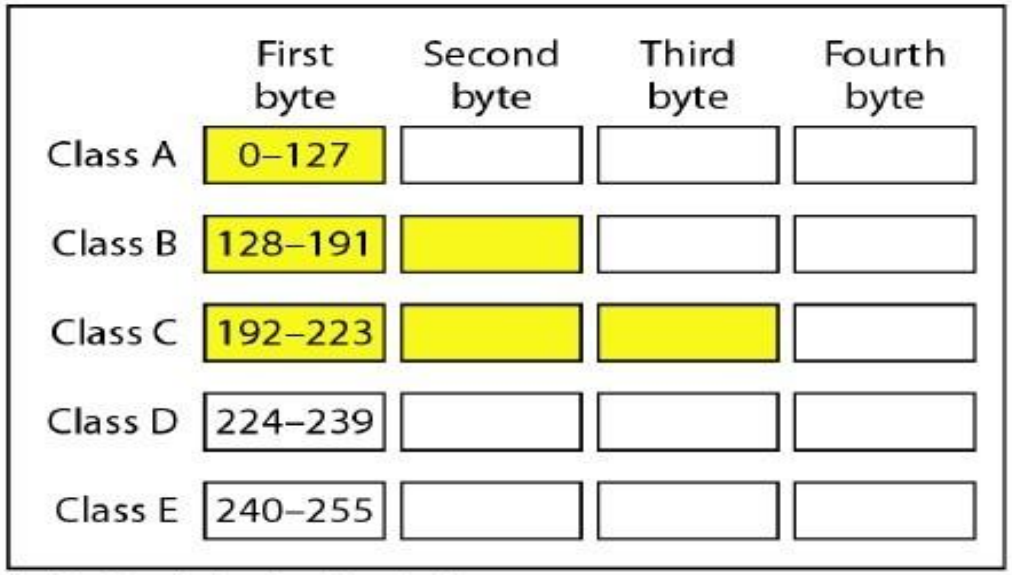
Classful Addressing

Classful Addressing

- IP is 32 bit means 2^{32} IP Addresses. (more than 4 billion , so many IP Addresses)
- We need to distribute those that's why we have classes.
- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.



a. Binary notation

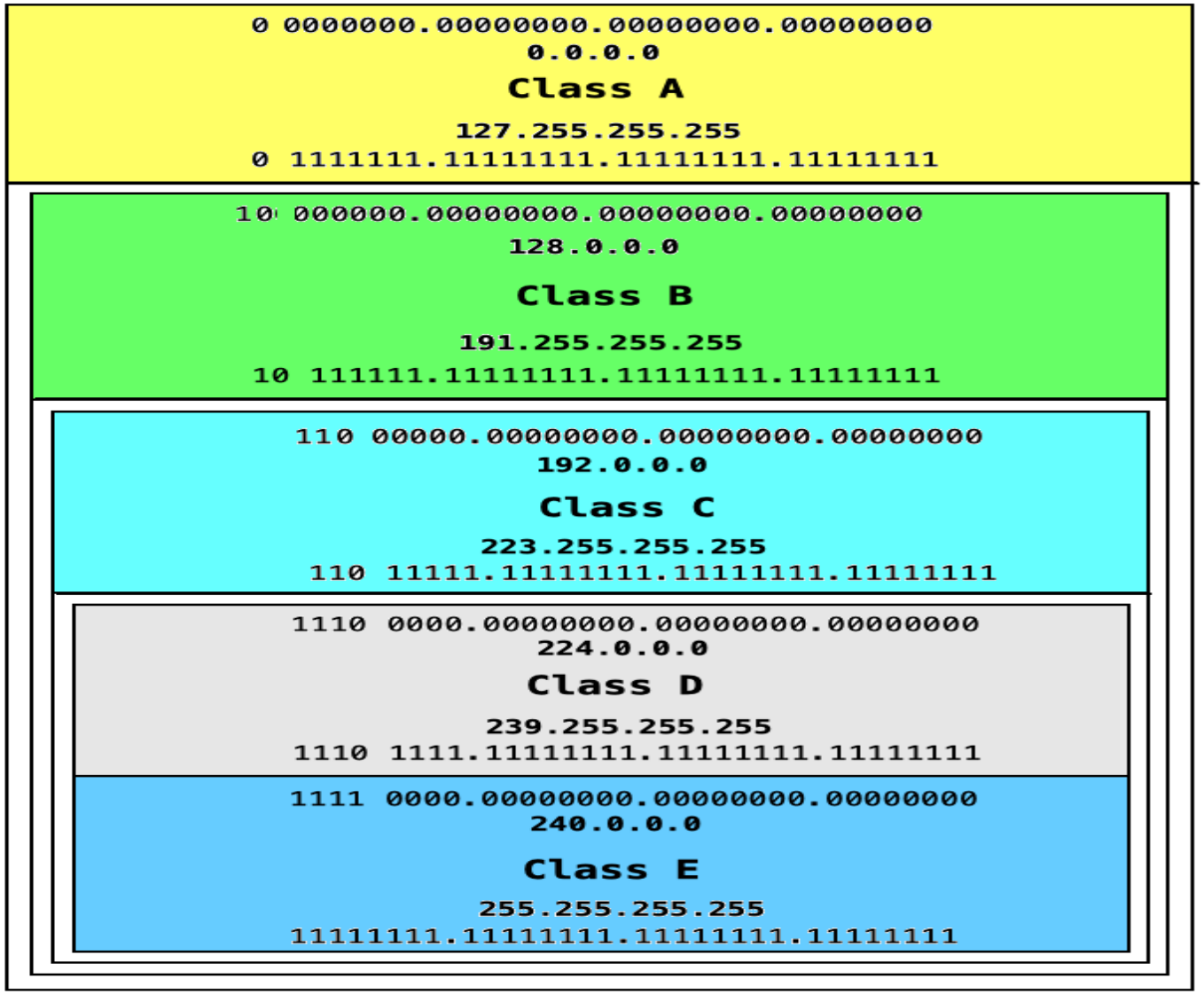


b. Dotted-decimal notation

How range of IP Address is defined

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
128	64	32	16	8	4	2	1		Range
0	x	x	x	x	x	x	x	Class A	0-127
1	0	x	x	x	x	x	x	Class B	128-191
1	1	0	x	x	x	x	x	Class C	192-223
1	1	1	0	x	x	x	x	Class D	224-239
1	1	1	1	x	x	x	x	Class E	240-255

IP Classful Addressing



- IP addresses starting with 0
- 0.0.0.0 – 127.255.255.255

- IP addresses starting with 10
- 128.0.0.0 – 191.255.255.255

- IP addresses starting with 110
- 192.0.0.0 – 223.255.255.255

- IP addresses starting with 1110
- 224.0.0.0 – 239.255.255.255

- IP addresses starting with 1111
- 240.0.0.0 – 255.255.255.255

Example

- Find the class of each address.

1. 00000001 00001011 00001011 11101111
2. 11000001 10000011 00011011 11111111
3. 14.23.120.8
4. 252.5.15.111

Solution-

1. The first bit is 0. This is a class A address.
2. The first 2 bits are 1; the third bit is 0. This is a class C address.
3. The first byte is 14 (between 0 and 127); the class is A.
4. The first byte is 252 (between 240 and 255); the class is E.

Points to be noted

- Any IP Address start with 127, That is : 127.x.x.x means its **a loop back series** that is used for **self testing**.
- E.g. Ping 127.0.0.1 (ping to yourself)
- That is 127.0.0.1 is **Universal IP** ,
- We can not configure **universal IP**. Its by default configured.
- PING (Packet Internet Groper) is a tool used to troubleshoot networking issues .

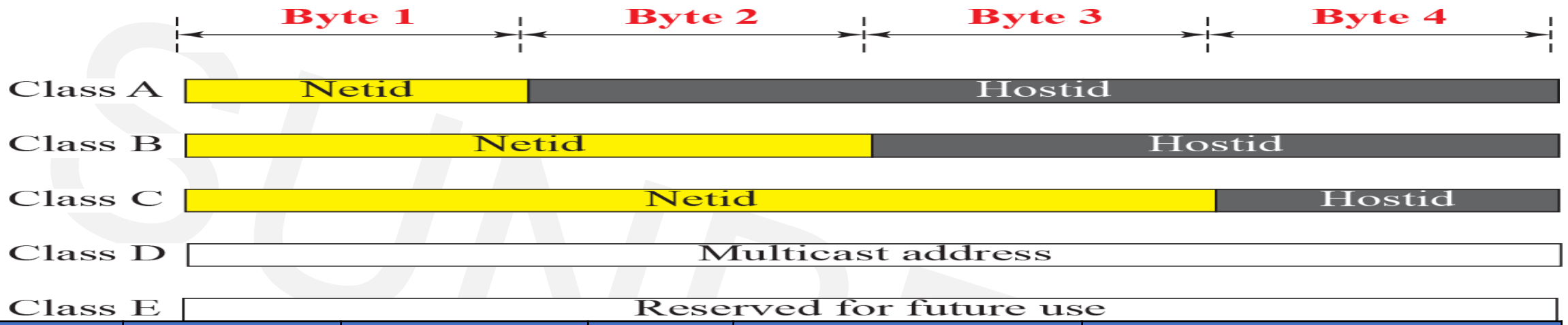
IANA(Inter Associated Number Association) manages private IP's.

Regular Private IP Addresses

Address Class	Reserved Private IP Addresses
Class A	10.0.0.0 - 10.255.255.255
Class B	172.16.0.0 - 172.31.255.255
Class C	192.168.0.0 - 192.168.255.255

Private network will have private IP's means devices that we connect to our router will get private IP addresses provided by IANA.

Netid and hostid of A, B, and C Classes



Class	Network bits	Networks	Host bits	Hosts Per Network	Suitable for
Class A	8	2^8=256	24	2^{24} - 2* =16,777,214 maximum hosts	For large organizations like Apple/Google/MS/Amazon
Class B	16	2^{16}=65536	16	2^{16} - 2* = 65,534 maximum hosts	for medium scaled organizations like Sunbeam
Class C	24	2^{24}=16million	8	2^8 - 2* = 254 maximum hosts	for small organizations/home network

**** Subtracting the network and broadcast address***

Example: What is the type of the given IP address

1. 11.34.56.66
2. 10.46.34.67
3. 156.46.36.46
4. 172.20.34.56
5. 172.45.66.77
6. 192.168.2.5
7. 192.169.34.6

1. 11.34.56.66 : public
2. 10.46.34.67 : private
3. 156.46.36.46 : public
4. 172.20.34.56 : private
5. 172.45.66.77 : public
6. 192.168.2.5 : private
7. 192.169.34.6 : public

Address Class	Reserved Private IP Addresses
Class A	10.0.0.0 - 10.255.255.255
Class B	172.16.0.0 - 172.31.255.255
Class C	192.168.0.0 - 192.168.255.255

Example (Solution): What is the type of the given IP address

1. 11.34.56.66 : public
2. 10.46.34.67 : private
3. 156.46.36.46 : public
4. 172.20.34.56 : private
5. 172.45.66.77 : public
6. 192.168.2.5 : private
7. 192.169.34.6 : public

Example : which class needs to be used for following number of Devices?

1. 200 devices
2. 3000 devices
3. 50000 devices
4. 200000 devices

1. 200 devices : class C
2. 3000 devices : class B
3. 50000 devices : class B
4. 200000 devices : class A

Example (Solution) : which class needs to be used for following number of Devices?

1. 200 devices : class C
2. 3000 devices : class B
3. 50000 devices : class B
4. 200000 devices : class A

An IP address represented in decimal

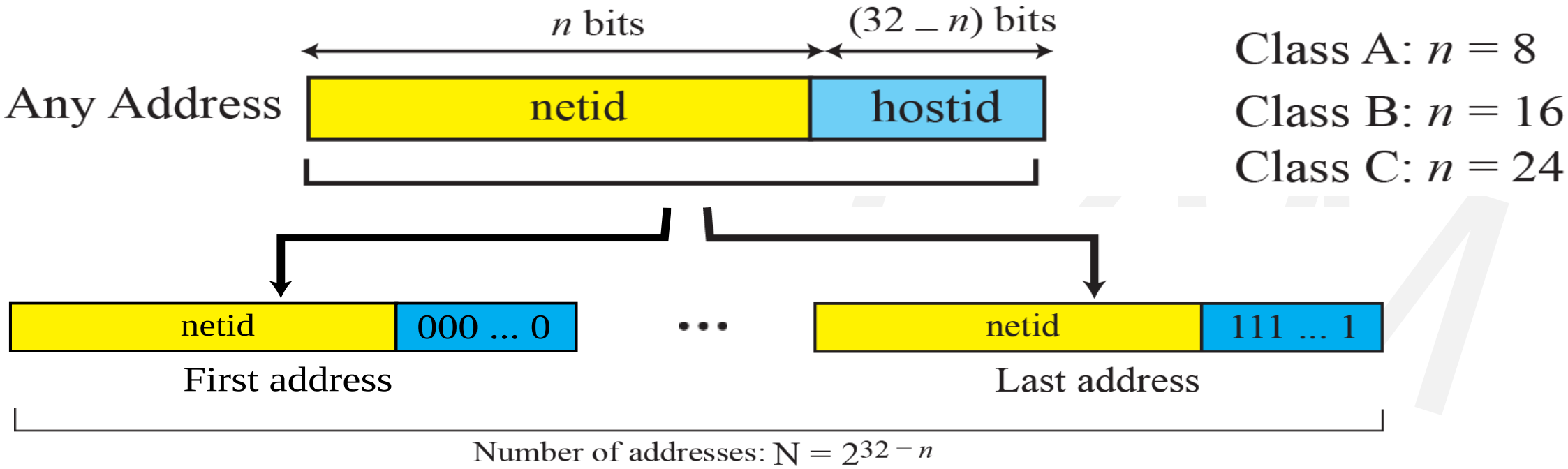
158.80.164.3

An IP address has four octets

: First Octet	Second Octet	Third Octet	Fourth Octet
158	80	164	3

Information Extraction in Classful Addressing

The number of addresses
The first address
The last address



Information Extraction in Classful Addressing

An address in a block is given as 73.22.17.25. Find the number of addresses in the block, the first address, and the last address

If we observe the given address it is of Class A (class A : n=8)
The **number of addresses** in this block is

$N = 2^{32-n} = 2^{24} = 16,777,216$

To find the **first address**, we keep the left most 8 bits and set the rightmost 24 bits all to 0s.
The first address is 73.0.0.0/8 in which 8 is the value of *n*.

To find the **last address**, we keep the leftmost 8 bits and set the rightmost 24 bits all to 1s.
The last address is 73.255.255.255

Decimal Equivalents of 8-Bit Patterns

128	64	32	16	8	4	2	1	
1	0	0	0	0	0	0	0	= 128
1	1	0	0	0	0	0	0	= 192
1	1	1	0	0	0	0	0	= 224
1	1	1	1	0	0	0	0	= 240
1	1	1	1	1	0	0	0	= 248
1	1	1	1	1	1	0	0	= 252
1	1	1	1	1	1	1	0	= 254
1	1	1	1	1	1	1	1	= 255

Finding Network Address

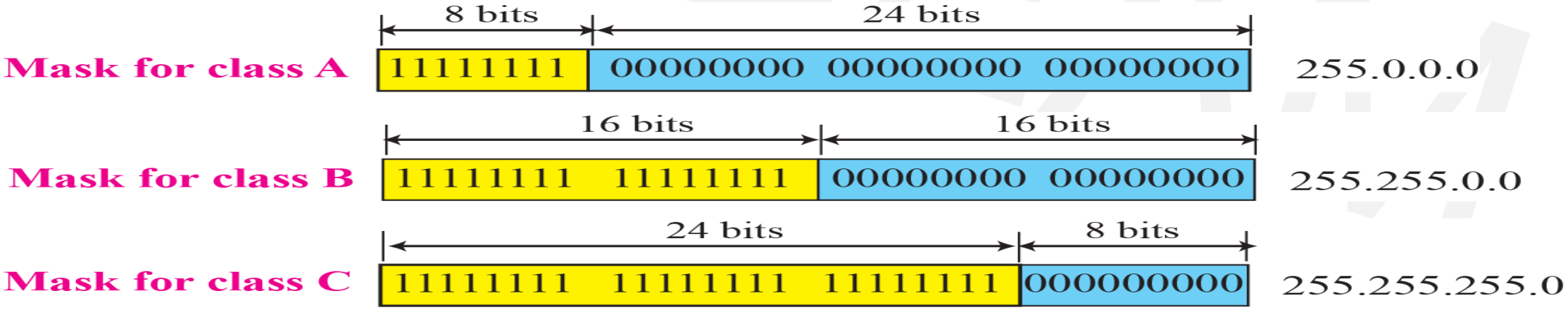
Network Mask/ Default Mask/ Subnet Mask

IP Address never comes alone , it comes with subnet mask.

Mask :

- 32-bit number of contiguous 1's followed by contiguous 0's.
- Mask Distinguishes which portion of the address identifies the network and which portion of the address identifies the node(host).

- Network Mask is used to extract the network address from the destination address of a packet called a default mask
- Classes D and E don't have default masks (they're for **multicast** and **future** use).



Network Mask/ Default Mask/ Subnet Mask

What is a Default Mask?

-A **default mask** (or **default subnet mask**) is the **standard subnet mask** assigned to an IP address **based on its class** in classful addressing.

-It tells you how many bits are used for the **network portion** of the IP address — the rest are used for hosts

eg: IP address: 192.168.1.25

First octet = 192 → **Class C**

Default subnet mask = 255.255.255.0

CIDR notation = /24

Network portion = First 24 bits

Host portion = Last 8 bits

- Classful addressing caused **waste of IP addresses**.
- A company needing 300 IPs would be forced to take a Class B (65,000+ IPs).
- There was **no flexibility** to allocate IPs based on exact need.
- So **CIDR (Classless Inter-Domain Routing)** was introduced in 1993 — to make IP allocation **more efficient and scalable**.

Example : Find Network Address

A router receives a packet with the destination address 132.24.67.32. How the router finds the network address of the packet.

Solution :-

Since the class of the address is B (128 to 191) , we assume that the router applies the default mask for class B, 255.255.0.0 to find the network address.

Destination address ->	**132**	**.**	**24**	**.**	**67**	**.**	**32**
Default mask ->	**255**	**.**	**255**	**.**	**0**	**.**	**0**
Network address ->	**132**	**.**	**24**	**.**	**0**	**.**	**0**

Example : Find Network Address

If IP is given as 192.168.1.10 , Find:
1) Class of IP
2) Subnet Mask
3) Network Address
4) Maximum Last Address

Example : Find Network Address

Class C				
IP	192	168	1	10
IP in binary	1100 0000	1010 1000	0000 0001	0000 1010
Subnet Mask	255	255	255	0
Subnet Mask in binary	1111 1111	1111 1111	1111 1111	0000 0000
Network Address	192	168	1	0
Maximum (Last Address)	192	168	1	255

Network Mask/ Default Mask/ Subnet Mask

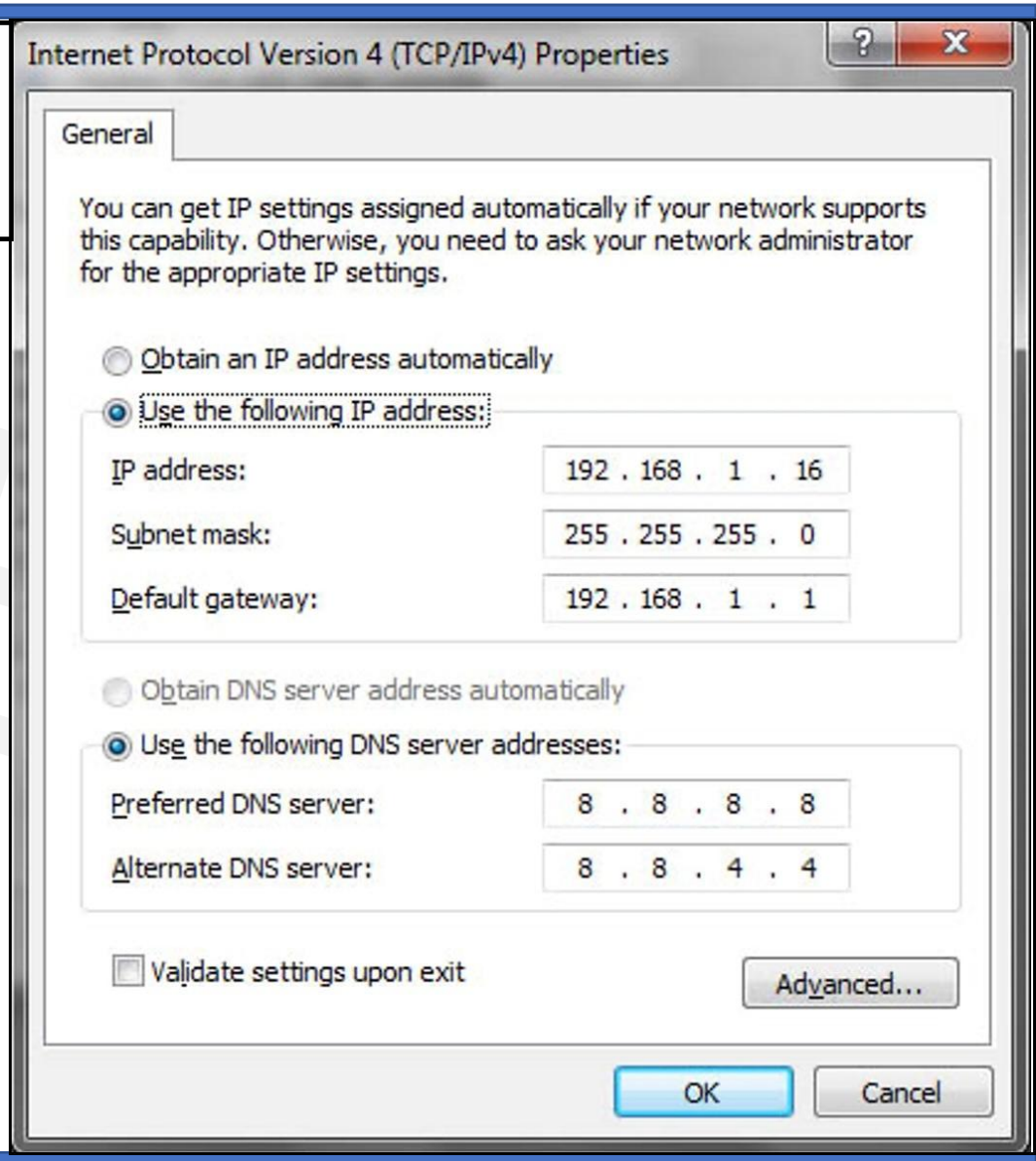
What is Subnet Masking?
Subnet masking is a technique used to **divide a network into smaller sub-networks (subnets)**.
A **subnet mask** determines **which part** of an IP address represents the **network** and which part represents the **host**.

- **Subnet masking** is a **technique** used **within** both classful and classless addressing.
- **Classless addressing** (CIDR) is a **modern approach** that **replaces classes** and allows for more **efficient IP allocation**.
- Subnetting is the process of creating new networks (or subnets) by stealing bits from the host portion of a subnet mask.
  Stealing bits from hosts creates more networks but fewer hosts per network.
  Consider the following Class C network: 192.168.254.0
  The default subnet mask for this network is 255.255.255.0.
  This single network can be segmented, or subnetted, into multiple networks.

Subnet Mask

IP ADDRESS: 192 . 168 . 1 . 16
SUBNET MASK: 255 . 255 . 255 . 0

- When a number in the subnet mask is a 255, the equivalent number above it in the IP address cannot change.
- When the number in a subnet mask is a zero, the equivalent number in the IP address can indeed change.
- The first three octets of the IP address – 192.168.1 cannot change, but the final number can be anything from 0 to 255.



Subnet Mask

CIDR	Subnet Mask	Host Bits	Hosts
/8	255.0.0.0	24	16,777,214
/16	255.255.0.0	16	65,534
/24	255.255.255.0	8	254
/25	255.255.255.128	7	126
/26	255.255.255.192	6	62
/27	255.255.255.224	5	30
/28	255.255.255.240	4	14
/29	255.255.255.248	3	6
/30	255.255.255.252	2	2

Number of hosts = 2^host_bits - 2 (subtract 2 for network + broadcast)

Subnet Mask

The Subnet Mask Part of an IP address identifies the network.
The other part of the address identifies the host.
A subnet mask is required to provide this distinction:
158.80.164.3 255.255.0.0
The above IP address has a subnet mask of 255.255.0.0.
The subnet mask follows two rules:
• If a binary bit is set to a 1 (or ON) in a subnet mask, the corresponding bit in the address identifies the network.
• If a binary bit is set to a 0 (or OFF) in a subnet mask, the corresponding bit in the address identifies the host.

the above address and subnet mask in binary:
IP Address: 10011110.01010000.10100100.00000011
Subnet Mask: 11111111.11111111.00000000.00000000
The first 16 bits of the subnet mask are set to 1. Thus, the first 16 bits of the address (158.80) identify the network.
The last 16 bits of the subnet mask are set to 0. Thus, the last 16 bits of the address (164.3) identify the unique host on that network.
The network portion of the subnet mask must be contiguous. For example, a subnet mask of 255.0.0.255 is not valid.

Subnet Mask

- Hosts on the same logical network will have identical network addresses, and can communicate freely.

  Eg: the following two hosts are on the same network:
  Host A: 158.80.164.100 255.255.0.0
  Host B: 158.80.164.101 255.255.0.0
  Both share the same network address (158.80), which is determined by the 255.255.0.0 subnet mask.
  Hosts that are on different networks cannot communicate without an intermediating device.

  Eg: : Host A: 158.80.164.100 255.255.0.0
  Host B: 158.85.164.101 255.255.0.0
  The subnet mask has remained the same, but the network addresses are now different (158.80 and 158.85 respectively).
  Thus, the two hosts are not on the same network, and cannot communicate without a router between them.
  Routing is the process of forwarding packets from one network to another.

Subnet Mask

- Host A: 158.80.1.1 255.248.0.0
  Host B: 158.79.1.1 255.248.0.0
  The specified subnet mask is now 255.248.0.0, which doesn't fall cleanly on an octet boundary.
  To determine if these hosts are on separate networks, first convert everything to binary:

  Host A Address: 10011110.01010000.00000001.00000001
  Host B Address: 10011110.01001111.00000001.00000001
  Subnet Mask: 11111111.11111000.00000000.00000000

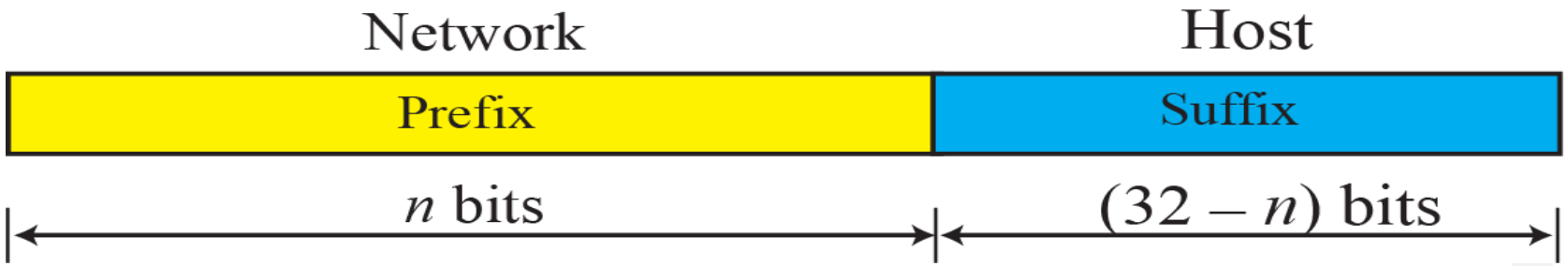
  Note: the 1 (or ON) bits in the subnet mask identify the network portion of the address.

  Here, the first 13 bits (the 8 bits of the first octet, and the first 5 bits of the second octet) identify the network.
  Looking at only the first 13 bits of each address:
  Host A Address: 10011110.01010
  Host B Address: 10011110.01001
  The network addresses are not identical. Thus, these two hosts are on separate networks, and require a router to communicate.

Classless Address (CIDR)

Prefix and Suffix

- Prefix : play the same role as the netid
- Suffix : play the same role as the hostid
- The prefix length in classless addressing can be 1 to 32



Classless Address (CIDR)

What is Classless Addressing (CIDR)?
CIDR = Classless Inter-Domain Routing
Introduced to replace the **old classful system** (Classes A, B, C).
Uses **slash notation** (e.g., /24) instead of fixed address classes.

CIDR notation: IP_address/prefix_length

192.168.1.10/24 → Same as subnet mask 255.255.255.0
The /24 means the **first 24 bits** are the **network part**.

In modern networking (CIDR), we **override the default mask** using custom subnet masks (e.g: /16,/24)

Classless Address (CIDR)

CIDR (Classless Inter-Domain Routing) is a simplified method of representing a subnet mask.
CIDR identifies the number of binary bits set to a 1 (or ON) in a subnet mask, preceded by a slash.
Eg: a subnet mask of 255.255.255.240
represented as follows in binary: 11111111.11111111.11111111.11110000
The first 28 bits of the above subnet mask are set to 1.

The CIDR notation for this subnet mask would thus be /28.
The CIDR mask is often appended to the IP address.

Eg: an IP address of 192.168.1.1 and
subnet mask of 255.255.255.0 would be represented as
using CIDR notation: 192.168.1.1 /24

Classless Address (CIDR)

- The first octet on an address dictates the class of that address
  • The subnet mask determines what part of an address identifies the network, and what part identifies the host.
  • Each class has a default subnet mask. A network using its default subnet mask is referred to as a classful network. Eg: 10.1.1.1 is a Class A address, and its default subnet mask is 255.0.0.0 (/8 in CIDR).

  It is entirely possible to use subnet masks other than the default.

  Eg: Class B subnet mask can be applied to a Class A address: 10.1.1.1 /16
  This does not change the class of the above address.
  It remains a Class A address, which has been subnetted using a Class B mask.

  The only thing that determines the class of an IP address is the first octet of that address.
  Similarly, the subnet mask is the only thing that determines what part of an address identifies the network, and what part identifies the host.

Classless Address (CIDR)

Eg: assume a minimum of 10 new networks are required.
Resolving this is possible using the following formula:
2^n where, 'n' identifies the number of bits to steal from the host portion of the subnet mask.
The default Class C mask (255.255.255.0)
in binary: 11111111.1111111.1111111.00000000
There are a total of 24 bits set to 1, which are used to identify the network.
There are a total of 8 bits set to 0, which are used to identify the host, and these host bits can be stolen.
Stealing bits essentially involves changing host bits (set to 0 or OFF) in the subnet mask to network bits (set to 1 or ON).
N Network bits in a subnet mask must always be contiguous - skipping bits is not allowed.
The result if three bits are stolen.
Using the above formula: 2^n = 2^3 = 8 . 8 new networks created
A total of 8 new networks does not meet the original requirement of at least 10 networks.
if four bits are stolen: 2^n = 2^4 = 16, 16 new networks created
A total of 16 new networks does meet the original requirement.
Stealing four host bits results in the new subnet mask:
11111111.11111111.11111111.11110000 = 255.255.255.240

Subnet Mask

CIDR → Subnet Mask:

Eg: 192.168.10.0/26

- /26 = 26 bits for network
- Subnet mask = 255.255.255.**192**
  The last octet has 2 bits for network: 11000000 = 192

Final subnet mask = 255.255.255.192

Subnet Mask → CIDR:

Given: 255.255.255.224

Convert each octet to binary:

255 = 11111111 (8 bits)
255 = 11111111 (8 bits)
255 = 11111111 (8 bits)
224 = 11100000 (3 bits)

Total network bits = 8 + 8 + 8 + 3 = /27

Subnet Mask

CIDR	Subnet Mask	Host Bits	Hosts
/8	255.0.0.0	24	16,777,214
/16	255.255.0.0	16	65,534
/24	255.255.255.0	8	254
/25	255.255.255.128	7	126
/26	255.255.255.192	6	62
/27	255.255.255.224	5	30
/28	255.255.255.240	4	14
/29	255.255.255.248	3	6
/30	255.255.255.252	2	2

Number of hosts = 2^host_bits - 2 (subtract 2 for network + broadcast)

What subnet mask can be used in scenario?

1. 100 devices
2. 50 devices
3. 1000 devices
4. 2000 devices
5. 10 devices

You need a subnet that provides at least 10 usable IP addresses.
2^3-2=6 (too few) & (2^4-2=14) (sufficient)
usable IP addresses (the network and broadcast addresses are reserved)
You need 4 host bits.
A standard IPv4 address has 32 bits, so 32 - 4 = 28 network bits, or a /28 CIDR notation.

Subnet Mask: is **255.255.255.240**.

Using the smallest possible subnet that fits your needs (Variable Length Subnet Masking or VLSM)
helps conserve IP addresses and reduce unnecessary broadcast traffic in the network.

What subnet mask can be used in scenario? (Solution)

1. 100 devices
   2^4=16
   2^5 :32
   2^6 : 64
   2^7 -2 : 126
   1111 1111. 1111 1111 . 1111 1111. 1000 0000
   255 .255. 255. 128

2. 50 devices : 255.255.255.192
   2^4=16
   2^5 :32
   2^6 -2 : 62
   1111 1111. 1111 1111 . 1111 1111. 1100 0000
   255 .255. 255. 192

3. 1000 devices
   2^7 = 128
   2^8 = 256
   2^9 = 512
   2^10 -2 = 1022
   11111111.11111111.11111100.00000000
   255.255.252.0

4. 2000 devices :
   2^11 -2 = 2046
   11111111.11111111.11111000.00000000
   255.255.248.0

IPv4 Header

The IPv4 header is comprised of 12 required fields and 1 optional field.
The minimum length of the header is 160 bits (20 bytes) and it can be **up to 60 bytes** if options are included.

Field	Size (bits)	Description
Version	4	IP version (4 for IPv4)
IHL (Header Length)	4	Length of the header in 32-bit words
Type of Service (ToS)	8	Priority and QoS settings
Total Length	16	Total size of the packet (header + data)
Identification	16	Unique ID for fragmenting packets
Flags	3	Control flags (e.g., "Don't Fragment")
Fragment Offset	13	Where this fragment belongs in the original packet
Time to Live (TTL)	8	Max hops (router limit) before discarding
Protocol	8	Protocol used (e.g., TCP=6, UDP=17)
Header Checksum	16	Error-checking of the header
Source IP Address	32	Sender’s IP address
Destination IP Address	32	Receiver’s IP address
Options (if any)	Variable	Rarely used, optional fields
Padding	Variable	To align the header to 32-bit boundaries

NAT — Network Address Translation

NAT (Network Address Translation) is a method used in networking to map private IP addresses to a public IP address so that multiple devices in a private network can access the internet using one public IP address.

Why is NAT Used?
IPv4 address shortage: Only ~4.3 billion IPv4 addresses exist.
NAT lets many private devices share a single public IP.
It adds a layer of security, hiding internal IP addresses from the public internet.

NAT is not required in IPv6 because there are enough IP addresses for every device to have its own unique public IP.
IPv6 was designed to eliminate the need for NAT and simplify end-to-end communication.

IPv6

- IPv6 is the modern version of IP addressing.
- IPv6 stands for Internet Protocol version 6. It is the newer version of the IP protocol, designed to replace IPv4 because IPv4 has a limited number of IP addresses (about 4.3 billion), which are now mostly used up.

Written in **hexadecimal** and separated by colons (:)
IPv6: **128-bit address**

2001:0db8:85a3:0000:0000:8a2e:0370:7334

You can **shorten** IPv6 addresses:
Remove leading zeros:
2001:db8:85a3:0:0:8a2e:370:7334

Use :: to represent a series of zero blocks (only once):
2001:db8:85a3::8a2e:370:7334

An IPv6 address consists of eight groups of four hexadecimal digits separated by ' : ' and each Hex digit representing four bits so the total length of IPv6 is 128 bits.

IPv6

Feature	IPv4	IPv6
Address Size	32 bits	128 bits
Address Format	Decimal (e.g. 192.168.1.1)	Hexadecimal (e.g. 2001:db8::1)
Address Space	~4.3 billion	~340 undecillion
Header Size	20 bytes	40 bytes
NAT (Network Address Translation)	Needed	Not needed (more IPs)
Security	Optional (IPSec)	Built-in (IPSec)
Broadcast	Yes	No (uses multicast)
Configuration	Manual or DHCP	Auto-config via SLAAC

IPv6

IPSec (Internet Protocol Security) is a suite of protocols used to secure IP communications by authenticating and encrypting each IP packet in a data stream. It is used in both IPv4 and IPv6, but in IPv6, IPSec is built-in and mandatory for implementation.

DHCP (Dynamic Host Configuration Protocol) is a network protocol used to automatically assign IP addresses and other network settings to devices on a network.

SLAAC (Stateless Address Autoconfiguration) is a method used in IPv6 that allows a device to automatically generate its own IP address without needing a DHCP server.

Types of IPv6 Address

"Different types help IPv6 serve different purposes, like broadcasting to many devices or communicating locally.

Unicast Addresses : Only one interface is specified by the unicast address. A packet moves from one host to the destination host when it is sent to a unicast address destination.

Multicast Addresses: It represents a group of IP devices and can only be used as the destination of a datagram.

Anycast Addresses: The multicast address and the anycast address are the same. The way the anycast address varies from other addresses is that it can deliver the same IP address to several servers or devices. The hosts do not receive the IP address.
Multiple interfaces or a collection of interfaces are assigned an anycast address.

IPv6 Address

Advantages :
IPv6 is the future of internet addressing.
It solves IPv4 exhaustion with **massive address space**.
It supports **faster routing**, **built-in security**, and **simplified network configuration**

Disadvantages
Conversion: Due to widespread present usage of IPv4 it will take a long period to completely shift to IPv6.
Communication: IPv4 and IPv6 machines cannot communicate directly with each other.
Not Going Backward Compatibility: IPv6 cannot be executed on IPv4-capable computers because it is not available on IPv4 systems.
Conversion Time: One significant drawback of IPv6 is its inability to uniquely identify each device on the network, which makes the conversion to IPV4 extremely time-consuming.

IPv6 Header Format

- **Fixed size**: **40 bytes**

Simpler and more efficient than IPv4 (no fragmentation or checksum)

Designed for **fast processing** by routers

Field	Size (bits)	Description
Version	4	Always 6 for IPv6
Traffic Class	8	Like IPv4's ToS (priority/QoS)
Flow Label	20	Identifies packet flows (e.g. VoIP streams)
Payload Length	16	Size of data after the header
Next Header	8	Identifies the next protocol (e.g. TCP=6, UDP=17)
Hop Limit	8	Like TTL in IPv4 (limits packet lifetime)
Source Address	128	Sender's IPv6 address
Destination Address	128	Receiver's IPv6 address

IPv4 Vs IPv6

Feature	IPv4	IPv6
Header Size	Variable (20–60 bytes)	Fixed (40 bytes)
Fragmentation	Handled in header	Handled via extension
Checksum	Present	Removed
NAT Use	Common	Not needed
Options	Built into header	Handled with extensions

Wireless LAN – IEEE 802.11

A Wireless LAN (WLAN) is a local area network that uses wireless communication instead of wired Ethernet connections. It enables devices like laptops, smartphones, and tablets to connect to the network and the internet without physical cables.

The standard that governs how wireless LANs operate is called IEEE 802.11, developed by the Institute of Electrical and Electronics Engineers (IEEE).

IEEE 802.11 is a family of standards that defines the protocols and rules for wireless networking. It specifies how data is transmitted over radio waves between wireless devices.

Often referred to as Wi-Fi, though “Wi-Fi” is the commercial name based on these IEEE standards.

Provide wireless connectivity within a local area (home, office, campus).

Allow users to access the internet and network resources without being tethered by cables. Support mobility, flexibility, and scalability.

Wireless LAN – IEEE 802.11

Station: Stations (STA) comprise all devices and equipment that are connected to the wireless LAN. It can be of two types:
Wireless Access Point (WAP): WAPs or simply access points (AP) are wireless routers that bridge connections for base stations.
Client: Examples include computers, laptops, printers, and smartphones.

Access Point: It is a device that can be classified as a station because of its functionalities and acts as a connection between wireless medium and distributed systems.

Distribution System: A system used to interconnect a set of BSSs and integrated LANs to create an ESS.

Frame: It is a MAC protocol data unit
SSID (Service Set Identifier): It's the network name for a particular WLAN. All-access points and devices on a specific WLAN must use the same SSID to communicate.

SDU: It is a data unit that acts as an input to each layer. These can be fragmented or aggregated to form a PDU.

PDU: It is a data unit projected as an output to communicate with the corresponding layer at the other end. They contain a header specific to the layer.

Network Interface Controller: It is also known as network interface card. It is a hardware component that connects devices to the network.

Portal: Serves as a gateway to other networks

Operating Modes in IEEE 802.11

1) Infrastructure Mode-
Requires a Wireless Access Point (AP).
Devices (stations/clients) communicate through the AP.
AP acts as a bridge to a wired network.
Centralized management, Scalable and secure, Can provide internet access
Eg: Laptop connects to a Wi-Fi router, which connects to the internet.
Most common mode used in homes, offices, schools, etc.

2) Basic Service Set (BSS)
Basic Service Set (BSS) A basic service set is a group of stations communicating at the physical layer level BSS can be of two categories depending upon the mode of operation
Infrastructure BSS - the devices communicate with other devices through access points.
Independent BSS - the devices communicate in a peer-to-peer basis in an ad hoc manner.

3) **Extended Service Set (ESS)** It is a set of all connected BSS.
4) **Distribution System (DS)** It connects access points in ESS.

IEEE 802.11 Frame Format

+---------- MAC Header ----------+----- Frame Body---+------ FCS ----------+

| FC | Dur | Addr1 | Addr2 | Addr3 | SC | [Addr4] | Payload/Data | CRC Error Check |

| 2 | 2 | 6 | 6 | 6 | 2 | [6] | (0 to 2312 bytes) | 4 bytes |

+----------

Frame Control-It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.
Duration(Dur)-It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.
Address fields There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.
Sequence control - It a 2 bytes field that stores the frame numbers.(sequence number of frame)
Used only in Wireless Distribution System (WDS/mesh)
Address 4 *(optional)* 6 bytes (Used only in Wireless Distribution System (WDS/mesh)
Data This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.
Check Sequence – Contains CRC values, It is a 4-byte field containing error detection information.

Quality of Service (QoS) in IEEE 802.11

•IEEE 802.11 Quality of Service (QoS) is a feature designed to improve the performance of delay-sensitive applications, such as voice, streaming multimedia, and online gaming, by allowing packets to belong to different traffic classes with different transmit priorities.
Wi-Fi puts data into 4 lanes:
Voice, Video, Best Effort (web browsing) , Background
The network gives faster access to the higher-priority lane
Voice & video = high priority (less delay).
File downloads or web browsing = medium priority.
Background tasks (like updates) = low priority.

IEEE 802.11 Security
Wi-Fi security is about keeping your wireless network safe from hackers and unauthorized users.
Main Security Types :
WEP – Like using a lock with a weak key. Easy to break.
WPA – A stronger lock but still not perfect.
WPA2 – Much better, uses strong encryption (AES). Most common.
WPA3 – The latest and strongest. Harder to hack and protects even if someone guesses your password.

HTTP Protocol

- What is HTTP?
- Web Server and Web Client
- Request Response Model
- Stateless Protocol

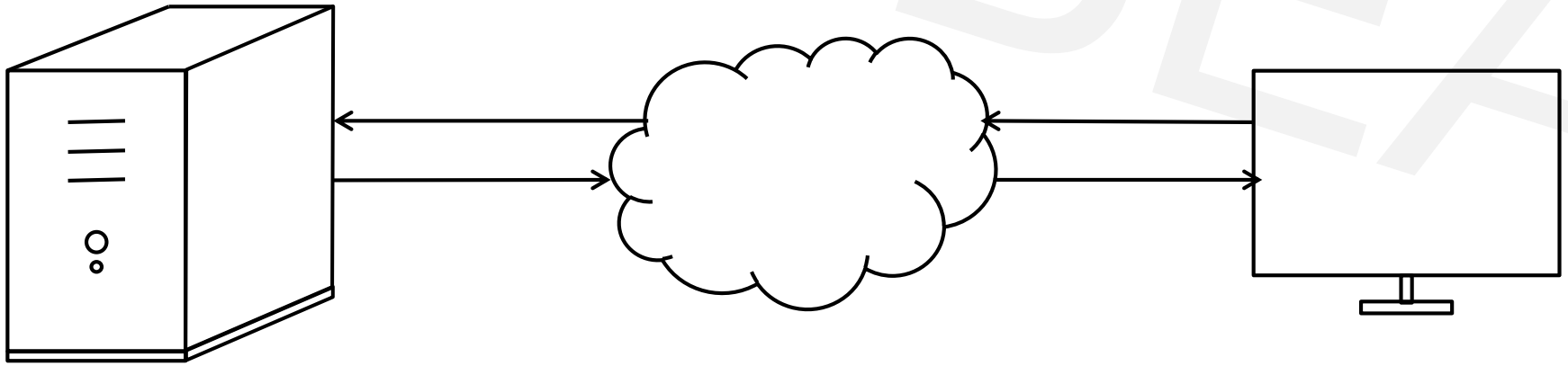
HTTP

- HTTP is HyperText Transfer Protocol.

  Access web pages over the network/internet.

  HTTP is application layer protocol.

  Based on TCP protocol in transport layer.



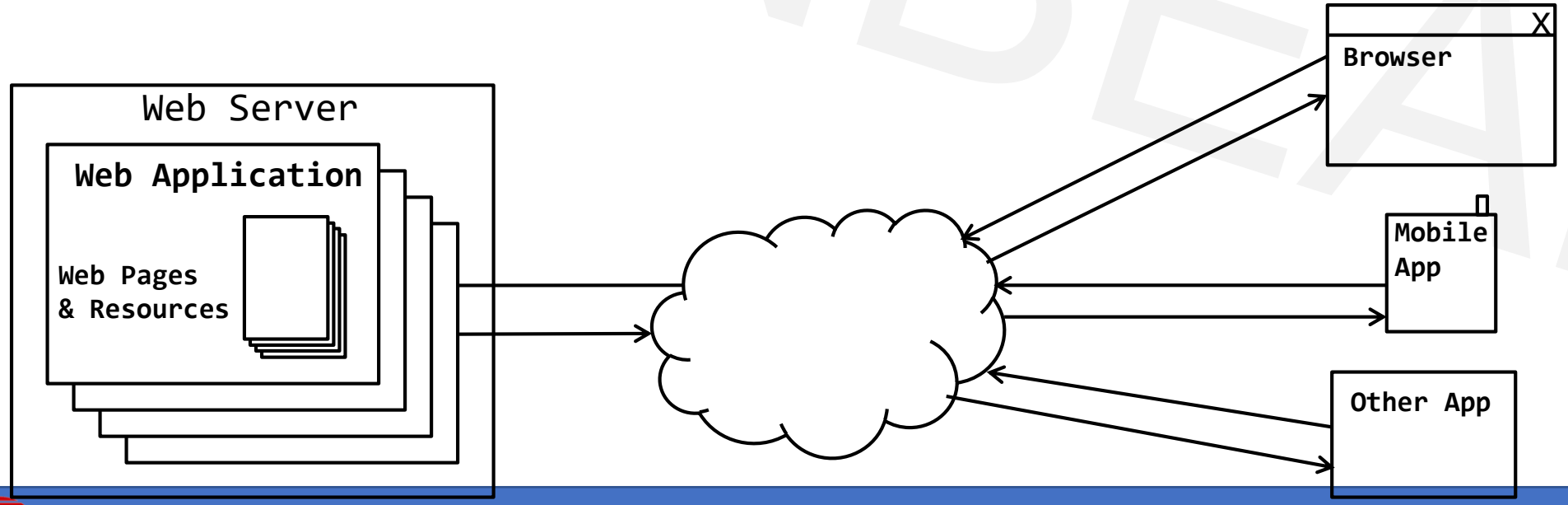
Web Server and Web Client

Server - Client

Server is a program that provides some service.
Client is a program that consumes the service.

Web Server - Web Client

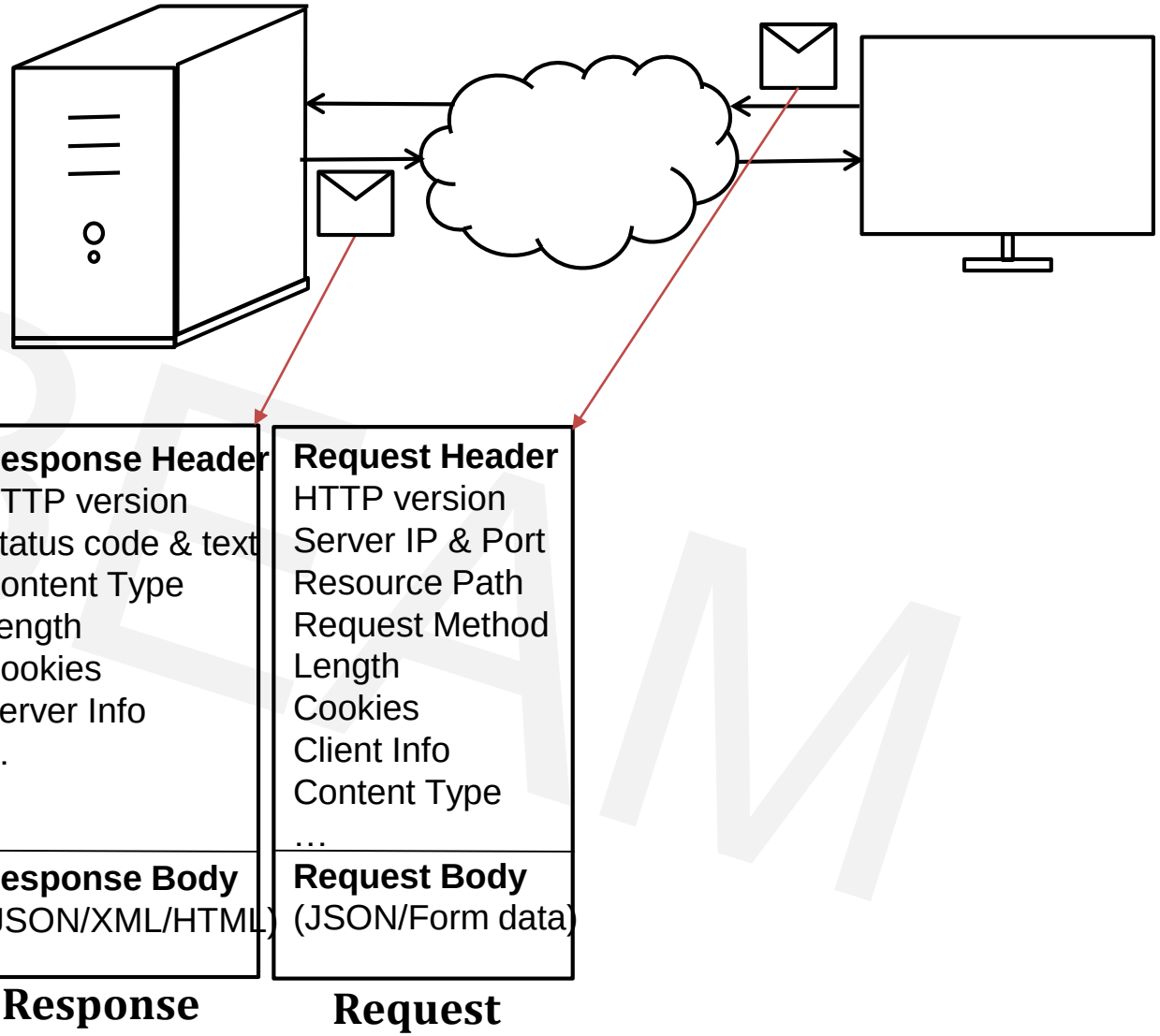
Web Server is a program that allows hosting multiple web applications in it.
Web application is set of web pages and resources. The web pages can be static or dynamic.
Java Web Server is web server that allow hosting multiple Java web apps.



Request Response Model

HTTP follows Request Response model.

Client sends request.
Server process the request.
Server sends response.



Request/Response contain header + body.

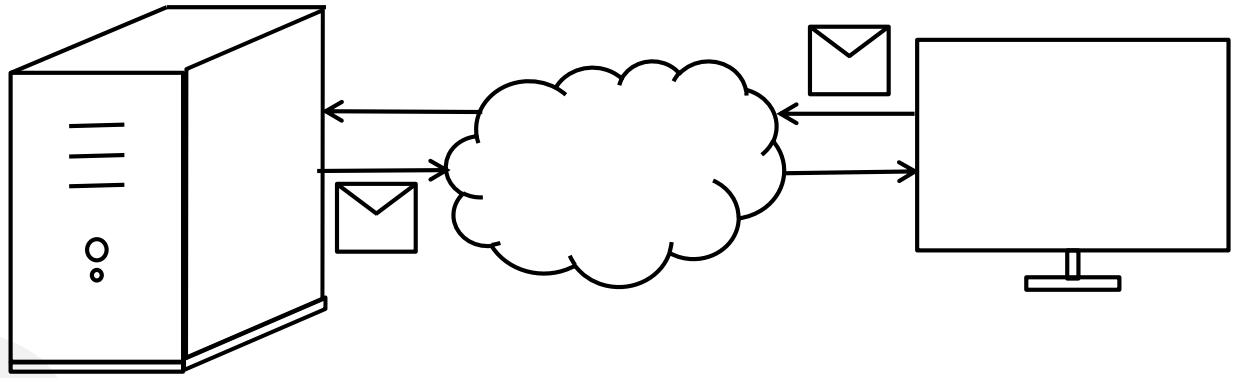
Request methods:
GET, POST, HEAD, PUT, DELETE, TRACE, OPTIONS, CONNECT, PATCH.

Request/Response content types:
text/html, text/xml, multipart/form-data, application/json, image/jpeg, video/mp4, …

Response status codes:
1xx (information), 2xx (success), 3xx (redirection), 4xx (client error), 5xx (server error)

Stateless protocol

HTTP is connection-less protocol.



For web server each request is a new request and produce response for it.

Web server doesn't maintain any information (state) about the client, so HTTP is stateless protocol.

For consistent user experience the client state should be maintained. This is referred as "state management".

Server side state management:

Session, Application, …

Client side state management:

Cookie, Hidden fields, Session storage, …

1. Open Developer Tools:

Right-click on the webpage and select "Inspect" or "Inspect Element".
OR
Chrome, Firefox, Edge: Ctrl + Shift + I (Windows/Linux) or Cmd + Option + I (Mac).

2. Navigate to the "Network" Tab:

In the panel that opens, find and click on the **"Network"** tab.

3. Perform an action to generate traffic:

The network tab usually starts recording automatically. If not, look for a red circle "Record" button and click it.
Now, refresh the page (F5 or the refresh button) or interact with the webpage (e.g., click a link, submit a form). You will see a list of requests populate in the left pane

conti…..

4. Inspect a specific request:

Click on a specific resource name (e.g., the main HTML document, a CSS file, an API call like users.json) from the list.

A side panel will open showing details of that single transaction.

Click the "Headers" sub-tab to see:

Request URL: The address being accessed.
Request Method: (GET, POST, PUT, etc.).
Status Code: (e.g., 200 OK, 404 Not Found, 301 Redirect).
Request Headers: Information sent from your browser to the server (e.g., User-Agent, Cookie).
Response Headers: Information sent back from the server (e.g., Content-Type, Set-Cookie).

Click the "Response" or "Preview" sub-tab to see the actual data payload that the server sent back (e.g., the HTML source code, the JSON data, the image file).

Thank You!!