IP Protocol

UNIT -4

Course Outcome:CompareIPv4 and IPv6 addressing scheme

What is protocol?

- ***A protocol is a set of rules that govern data communications. It defines what is communicated, how it is communicated, and when it is communicated.***
- Without a protocol ,two devices may be connected but can not communicate.
- Key elements of protocol
  - Syntax
  - Semantics
  - Timing
- ***Syntax*** **:** *refers to the* ***structure or format of the data, i.e the*** **order in which they are presented.**
- ***Semantics: the meaning of each section of bits.***
- ***Timing*** **:** *refers to when data should be sent* and how fast they can be sent

Internet Protocol(IP)

- IP is a **network layer** protocol.
- IP provides **unique addresses for devices**, enabling their identification and location on a network.
- The IP (Internet Protocol) is **responsible for communication between different devices on a network and across the internet**.
- It is primary network layer protocol in TCP/IP suit.

Why we need Internet Protocol?

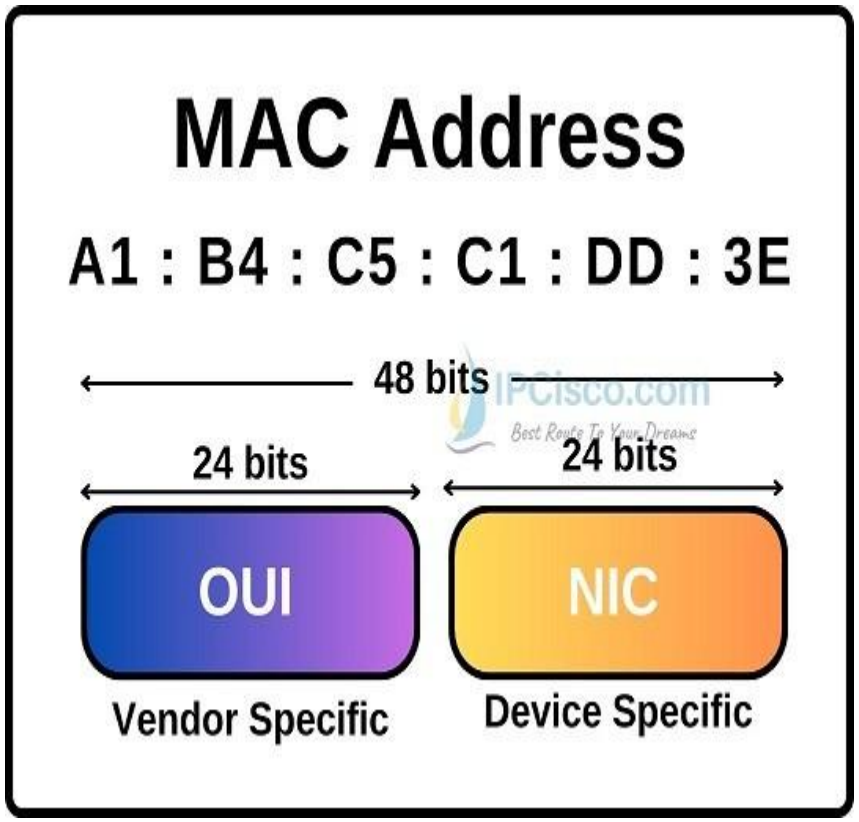
- IP (Internet Protocol) provides **unique addresses** for devices.
- Data traversing over internet is divided into smaller pieces called packets.
- IP allows **routing of data packets between networks**, ensuring that information **reaches its intended destination.**
- **IP enables internet connectivity.**
- It serves as the **foundation for end-to-end communication**, facilitating seamless data transmission between devices.

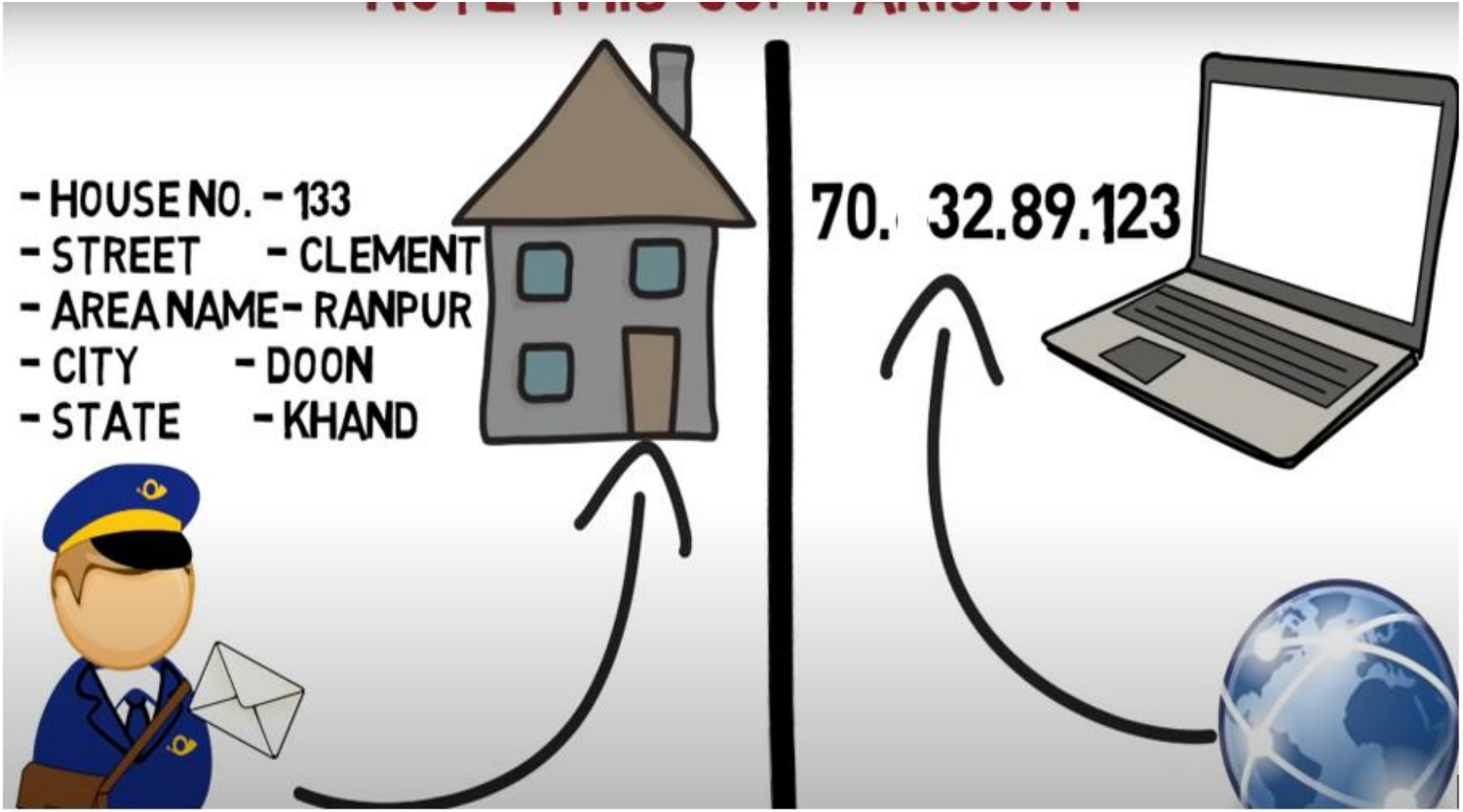
Types of IP address:

- There are two version of IP
  - (i) IPv4(Internet Protocol version 4)
  - (ii) IPv6 (Internet Protocol version 6)
- The network adapters has two types of address
  - MAC Addresses.
  - An IP addresses

Media Access Control address

- A MAC address is a 12-digit(48bit) hexadecimal number.
- It's usually represented as a string of 12 hexadecimal digits, often grouped into pairs separated by colons or dashes.
- The manufacturer inserts the MAC address into a device's network interface card (NIC) during production.
- A MAC address is used to identify a device on a network and to ensure its physical location.




- HOUSE NO. - 133
- STREET - CLEMENT
- AREA NAME - RANPUR
- CITY - DOON
- STATE - KHAND
70. 32.89.123

IPv4

- IPv4 is **32-bit address** used by the TCP/IP protocols to deliver a packet over the network.
- It is a **network layer** protocol.
- it is **unreliable and connectionless** datagram protocol
- it has **no error control or flow control.**
- IP uses **only error detection** mechanism and **discards the corrupted** packet.
- If **reliability is important, IPv4 must be paired with a reliable protocol such as TCP.**

Address Space

- Address space is **total number of addresses used by the protocol**.
- If a protocol uses N bits to define an address, the address space is 2^N because each bit can have two different values (0 or 1) and N bits can have 2^N values
- An **IPv4 address is 32 bit** unique address and its total address space is **2^32 i.e. 4,29,49,67,296** (more than four billion).

IP Address Notation

There are common 2 notations used to represent IPv4address.

1. **Dotted Decimal -128.0.0.0**
2. **Binary notation- 10000000 00000000 00000000 00000000**

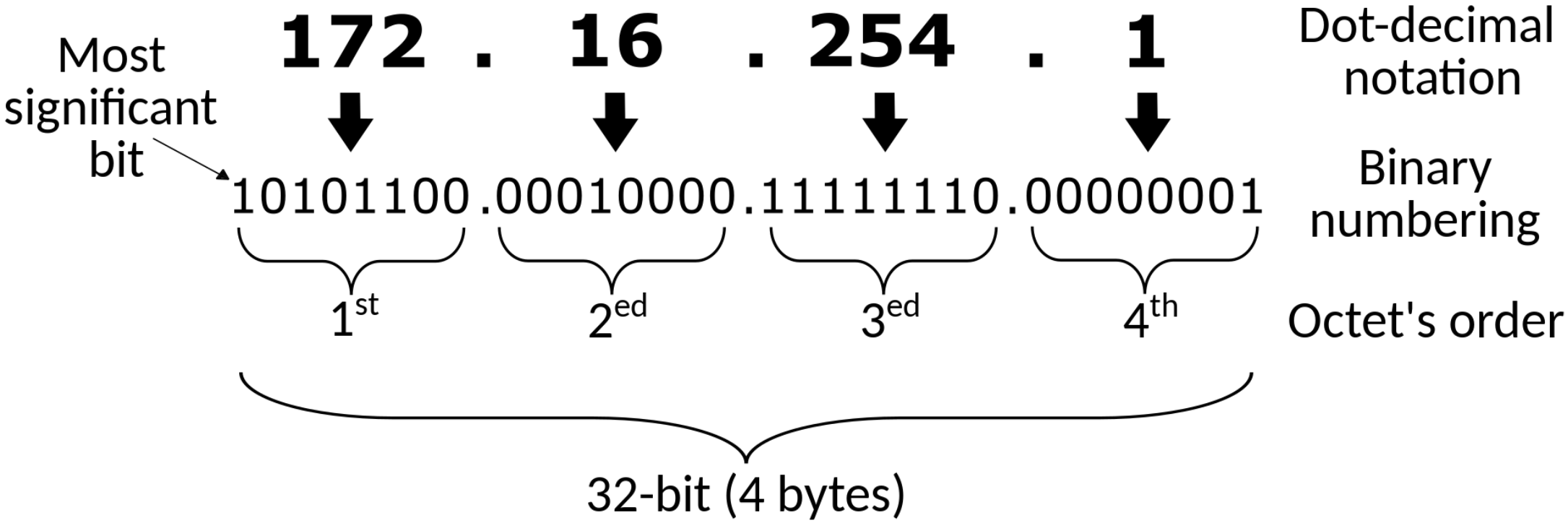
- **There are four octets in IPv4**

Dotted Decimal Notation

- The 32-bit IPv4 address is expressed **as four decimal numbers separated by periods (dots).**
- **Each decimal** number **represents** an **octet**, which is a **group of 8 bits**.
- The **range of each octet** is from **0 to 255**, as each octet can hold values from **00000000** to **11111111** in binary form.
  - i.e. **0.0.0.0 to 255.255.255.255**
- example of an IPv4 address in dotted decimal notation:

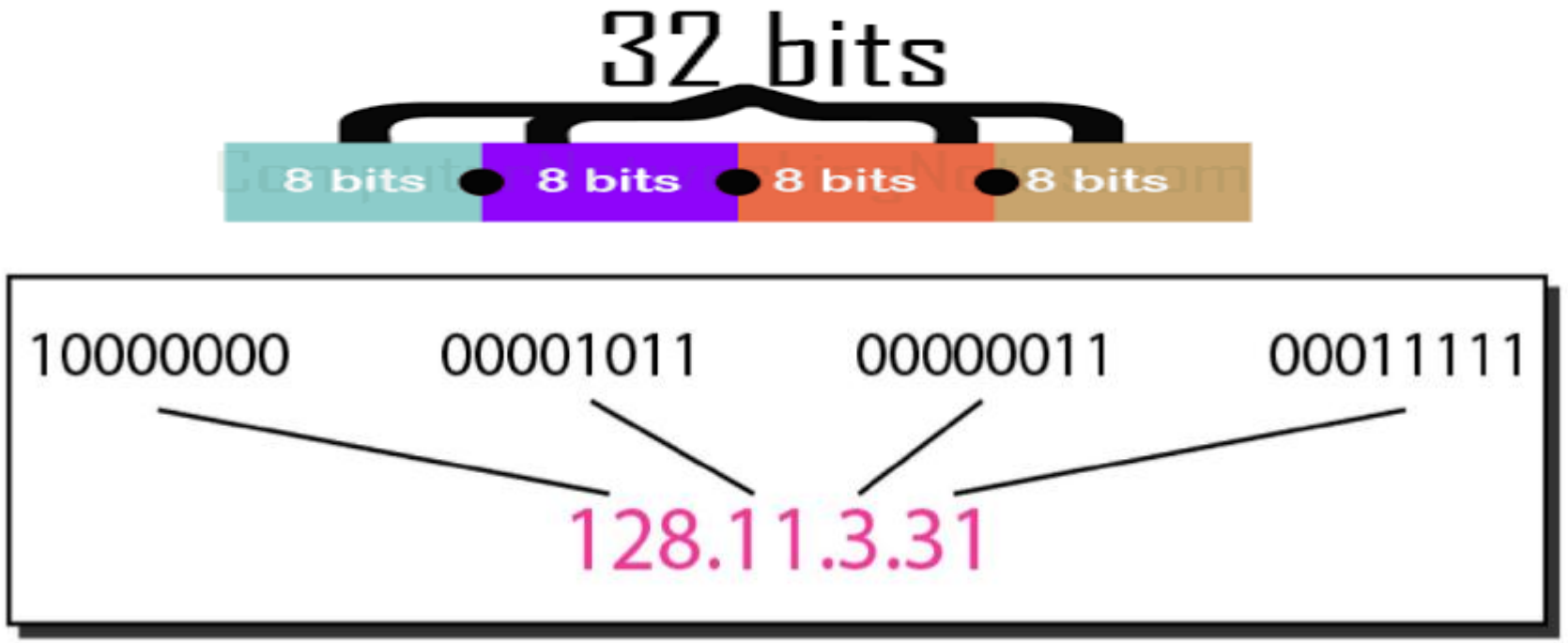
  192.168.0.1
- Each bit in the octet has binary weight (128,64,32,16,8,4,2,1).

Dotted decimal



Binary Notation

- In Binary notation **IPv4 address is displayed as 32-bits.**
- each **octet is expressed as a binary number consisting of 8 bits** i.e. of **1 byte.**



Binary to Decimal Conversion

Bit position:	7	6	5	4	3	2	1	0
Binary exponential:	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Value if bit = 1:	128	64	32	16	8	4	2	1

Figure 3-4 Components of a byte

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Exercise

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number (see Appendix B) and add dots for separation.

a. 129.11.11.239

b. 193.131.27.255

Exercise

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a. 111.56.45.78

b. 221.34.7.82

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

Exercise

Solution

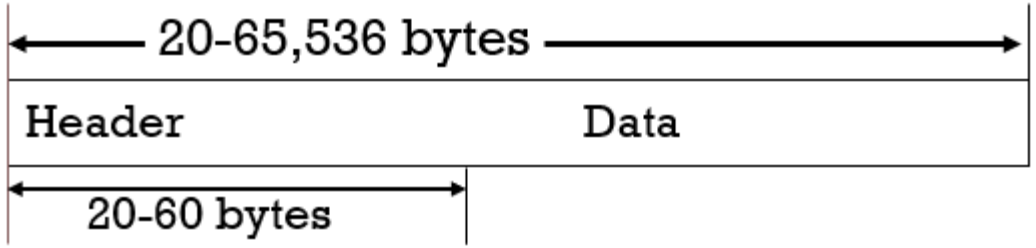
We replace each decimal number with its binary equivalent (see Appendix B).

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

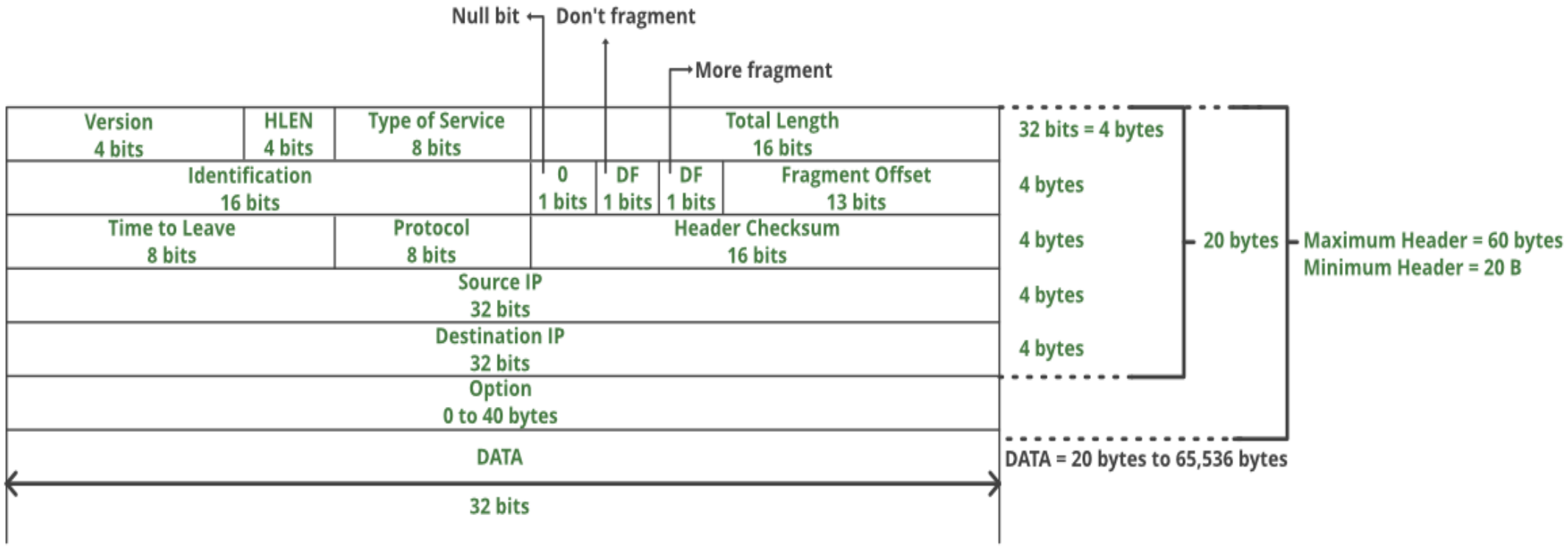
IPv4 Packet Structure

- Packet in IP layer is called datagram, as the IP is connection less protocol each datagram is handled independently.
- Each datagram can follow different route to the destination.
- A datagram is a variable-length packet consisting of two parts: header and data.
- **IPv4 header and Protocol Functions**
- IP datagram



- Header is 20 to 60 bytes in length and contains information required to routing and delivery of datagram.

FORMAT OF IPv4



ipv4

- **Version (VER).** This 4-bit field defines the version of the IPv4 protocol. In IPv4 the version is 4 so the value of this field is 0100.
- ***HLEN: Header length***

- This 4-bit field defines the total length of the datagram header in 4-bit words i.e. 32 bit. *The minimum value for this field is 5 and the maximum is 15.*
  - This field is needed because the length of the header is variable (between 20 and 60 bytes).
  - When there are no options, the header length is 20 bytes, and the value of this field is 5 (5 x 4 = 20 bytes). When the option field is at its maximum size, the value of this field is 15 (15 x 4 = 60 bytes).
  - This is required because if we know HLEN then and then only we know the size of the packet by subtracting it from total length.

ipv4

- ***Type of service:*** *Low Delay, High Throughput, Reliability (8 bits)*
- ***Total Length:*** This is a 16-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes.

Length of data =total length - header length

e.g. header length = 20 byte then

Length of data=65,535-20=65,515

Since the field length is 16 bits, the total length of the IPv4 datagram is limited to 65,535 (2^16 - 1) bytes, of which 20 to 60 bytes are the header and the rest is data from the upper layer.

ipv4

- **Identification:** identification field is used in fragmentation.
- A datagram when passing through different network may be divided into fragments to match the network frame size. So each frame is identified with a sequence number in this field.
- **Flags:** This is 3 bit field
- 3 flags of 1 bit each : **1st bit - reserved bit (must be zero)**, 2nd bit- do not fragment flag, 3rd bit- more fragments flag (same order)
  - **DF (Do not Fragment):** if it is 1, it is an instruction to routers not to fragment the datagram, as the destination is incapable of putting the pieces back together.
  - **MF (More Fragment):** if it is 1, it means this is not last fragment there are more fragments after this one. If value is 0 it means this is last on only one fragment.

ipv4

- **Fragment offset:** It tells the position of current fragment in the ongoing datagram transmission, with respect to the first fragment.

It is a **13 bits field = 8192 fragments per datagram**.

- ***Time to live:*** *Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the maximum number of Hops(routers) visited by a Packet before delivering to the Destination. After visiting each node its value is decreased and at some point when it is zero then this packet is discarded if not delivered to destination.*
- ***Protocol:*** *Name of the protocol to which the data is to be passed (8 bits)* i.e. TCP/UDP
- ***Header Checksum:*** *16 bits header checksum for checking errors in the datagram header*

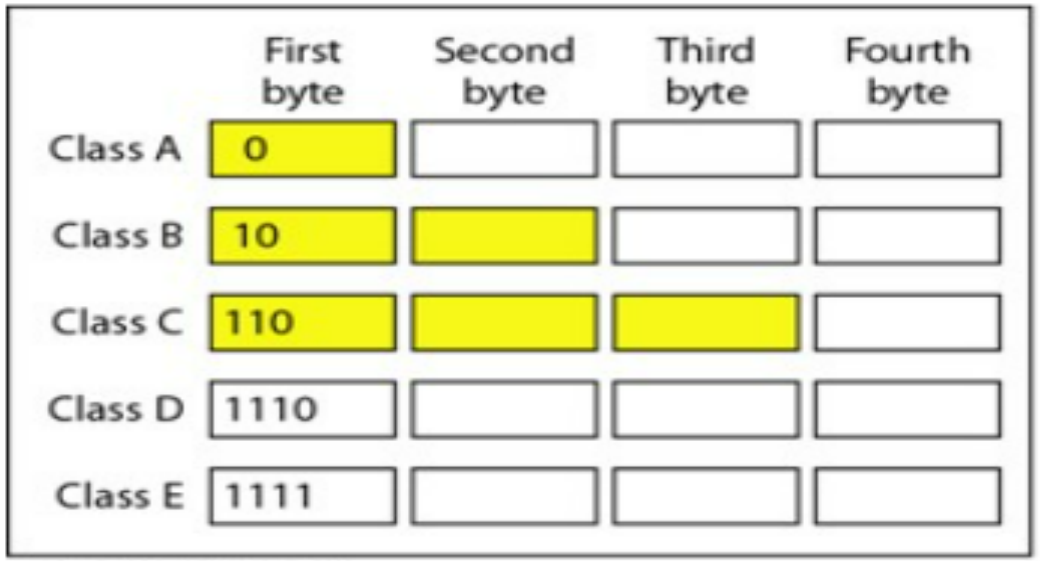
ipv4

- ***Source IP address:*** *32 bits IP address of the sender*
- ***Destination IP address:*** *32 bits IP address of the receiver*
- ***Option:*** *Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.*

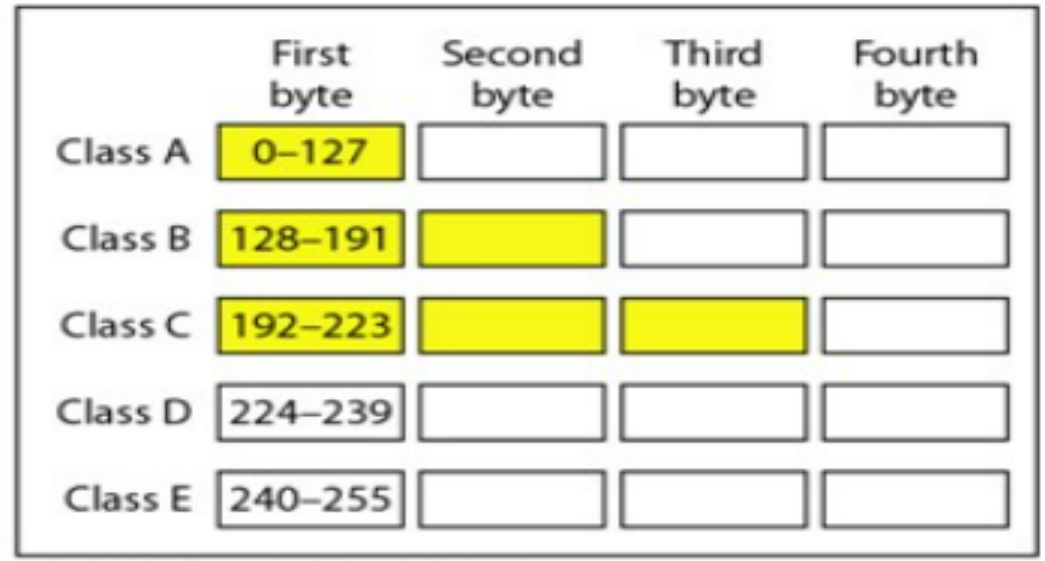
Classful Addressing

- In classful addressing, the address space is divided into five classes:
- A, B, C, D, and E.
- Each class occupies some part of the address space.
- If the address is given in binary notation, the first few bits can immediately tell us the class of the address.
- If the address is given in decimal-dotted notation, the first byte defines the class.

Finding the Classes in Binary and Dotted-Decimal Notation



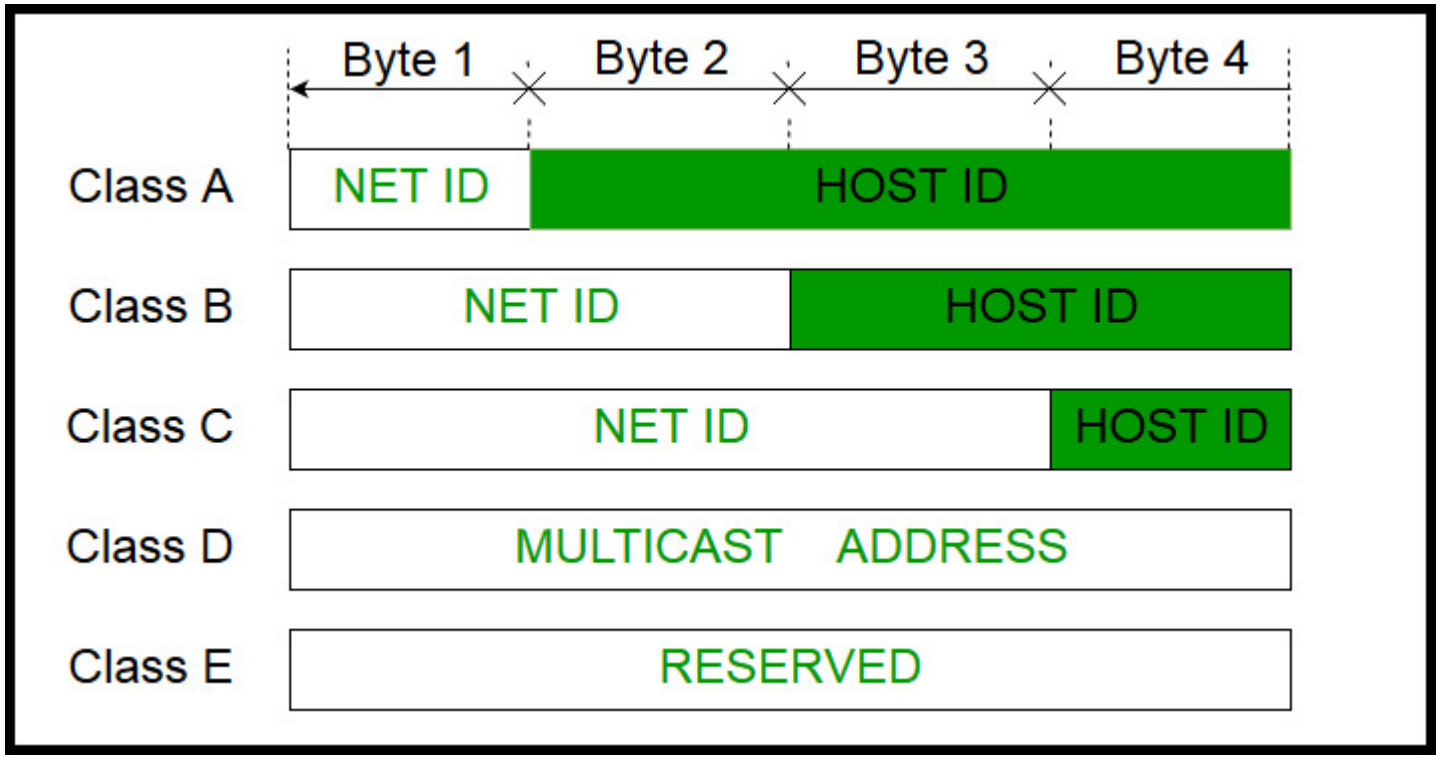
a. Binary notation



b. Dotted-decimal notation

Classful IP addresses

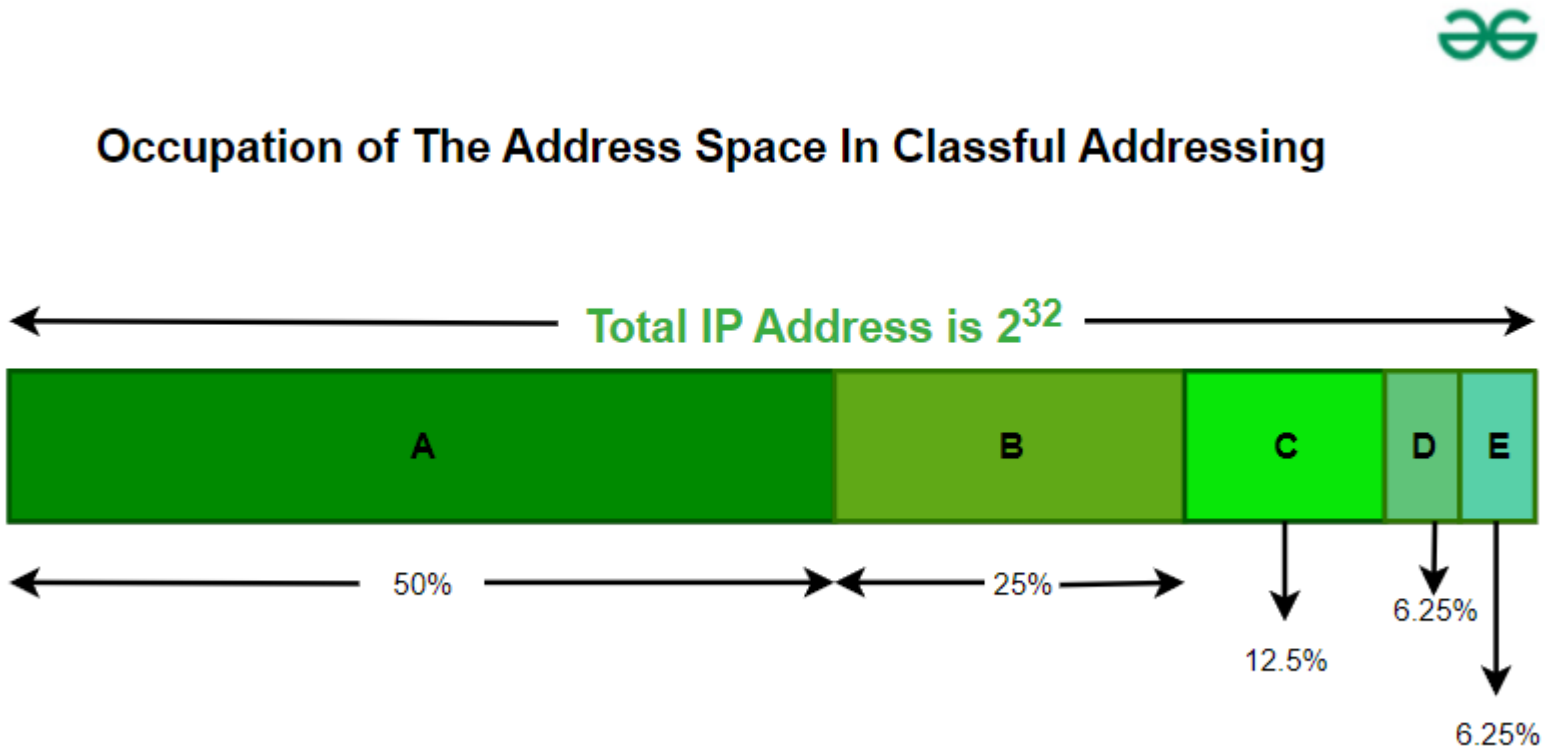
- The order of bits in the first octet determine the classes of IP address. IPv4 address is divided into two parts:
- **Network ID Host ID**
- **The class of IP address is used** to determine the **bits used for network ID and host ID and the number of total networks and hosts** possible in that particular class.
- Each ISP or network administrator assigns IP address to each device that is connected to its network.



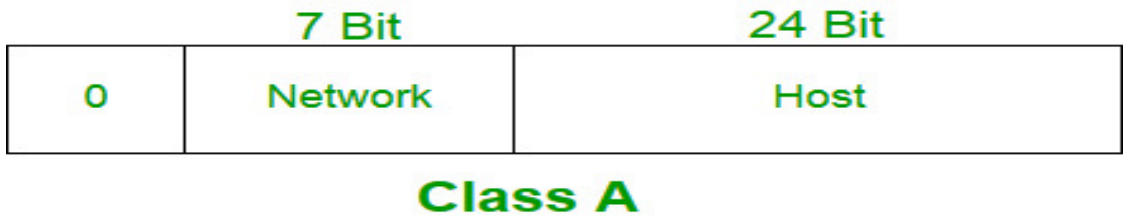
Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

IPv4 OCCUPATION

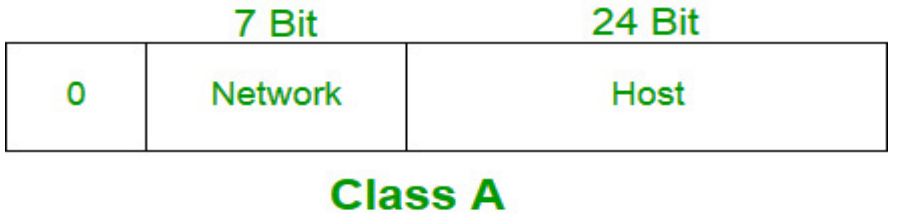


Class A address



- The network ID is 8 bits long.
- The host ID is 24 bits long.
- The network ID is 7 bits long,1st bit is reserved.
- The higher order bit of the first octet in class A is always set to 0.
- The remaining 7 bits in first octet are used to determine network ID.

Class A address

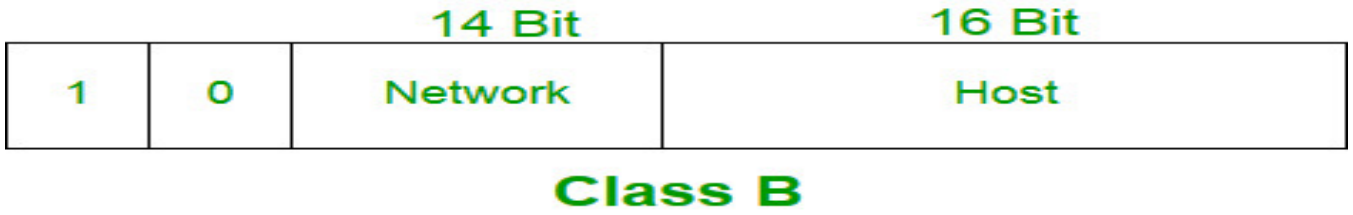


- The 24 bits of host ID are used to determine the host in any network.
- The default subnet mask for class A is 255.0.0.0. (11111111.0.0.0)
- **class A has a total of:**
- **2^7= 128 network ID**
- **2^{24} – 2 = 1,67,77,214 host ID**
- (Here 2 address is subtracted because 0.0.0.0 and 127.x.y.z are special address.)
- **IP address** belonging to **class A are assigned to** the **networks** that contain a **large number of hosts.**

summary

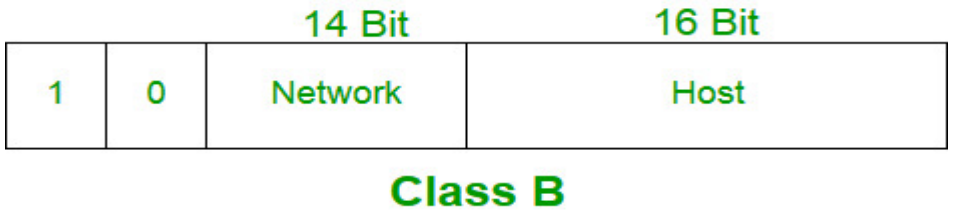
1. Class A addresses:
    1. Range: 1.0.0.0 to 126.0.0.0
    2. Subnet mask: 255.0.0.0
    3. EXAMPLE: 10.0.0.1
    4. Used for large networks with a large number of hosts.
    5. The first octet represents the network portion, and the remaining three octets represent the host portion.
    6. Addresses beginning with 01111111 or 127 are reserved for loop back e.g. your XAMMP local host address.

Class B



- In class B The network ID is 16 bits long.
- The host ID is 16 bits long.
- The higher order bits of the first octet of IP addresses of class B are always set to 10.
- The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.0.0.

Class B

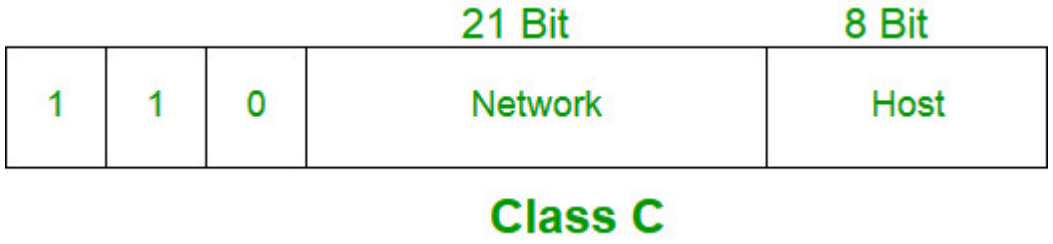


- Class B has a total of:
- 2^14 = 16384 network address
- 2^16 – 2 = 65534 host address
- IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.
- IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

summary

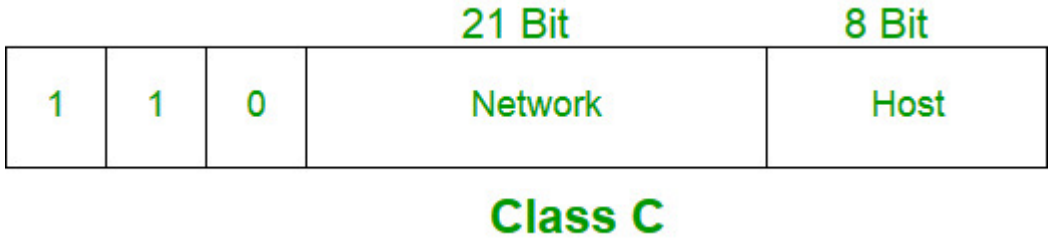
1. Class B addresses:
    1. Range: 128.0.0.0 to 191.255.0.0
    2. Subnet mask: 255.255.0.0
    3. Used for medium-sized networks.
    4. The first two octets represent the network portion, and the remaining two octets represent the host portion.

Class C



- IP address belonging to class C are assigned to small-sized networks.
  - The network ID is 24 bits long.
  - The **host ID is 8 bits long.**
- The higher order bits of the first octet of IP addresses of class C are always set to 110.
- The remaining 21 bits are used to determine network ID.
- The **8 bits of host ID is used to determine the host** in any network.

Class C



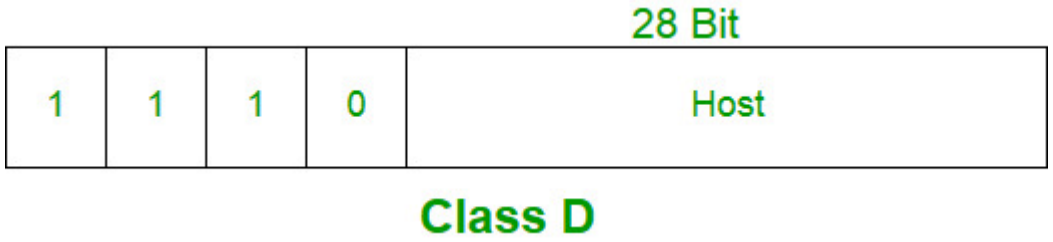
- The default sub-net mask for class C is 255.255.255.0 Class C has a total of:
  - 2^21 = 2097152 network address
  - **2^8 – 2 = 254 host address**
- IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.

summary

1. Class C addresses:
    1. Range: 192.0.0.0 to 223.255.255.0
    2. Subnet mask: 255.255.255.0
    3. Used for small networks.
    4. The first three octets represent the network portion, and the last octet represents the host portion.

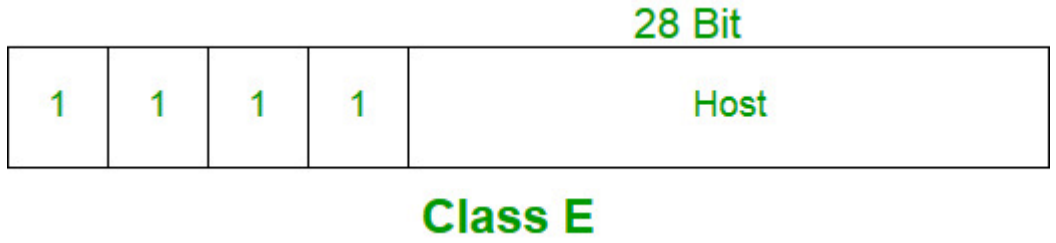
Class D

- IP address belonging to class D are **reserved for multi-casting.**
- The **higher order bits** of the first octet of IP addresses belonging to class D are always **set to 1110.**
- The remaining bits are for the address that interested hosts recognize.
- Class D **does not posses any sub-net mask.** IP addresses belonging to class D ranges from 224.0.0.0 – 239.255.255.255.



Class E

- IP addresses belonging to class E are reserved for experimental and research purposes.
- IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254.
- This class doesn’t have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



Addresses per Class

Class	*Number of Addresses*	*Percentage*	TOTAL RANGE 0- 255=256
A	$2^{31} = 2,147,483,648$	50%	0-127=128
B	$2^{30} = 1,073,741,824$	25%	128-191=64
C	$2^{29} = 536,870,912$	12.5%	192-223=32
D	$2^{28} = 268,435,456$	6.25%	224-239=16
E	$2^{28} = 268,435,456$	6.25%	239-240=16

Summary of class full addressing

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Task

1. Find the class of following IP addresses: (i) 237.14.2.1 (ii) 114.34.2.8

2.Identify the class of following IP addresses

(i) 121.23.19.222

(ii) 1100 0001 0000 1011 0000 1011 1110 1110

Task

- Write down class of a following IP addresses.

i) 227.12.14.87 ii) 14.23.120.8

iii) 1100 0001 1000 0011 0001 1011 1111 1111

iv) 1111 0011 1001 1011 1111 1011 0000 1111

Determine whether following IPv4 address are valid or invalid. If valid IPv4 addresses then find class, Network and Host ID of an IPv4 address. If invalid IPv4 address then write reason for the same.

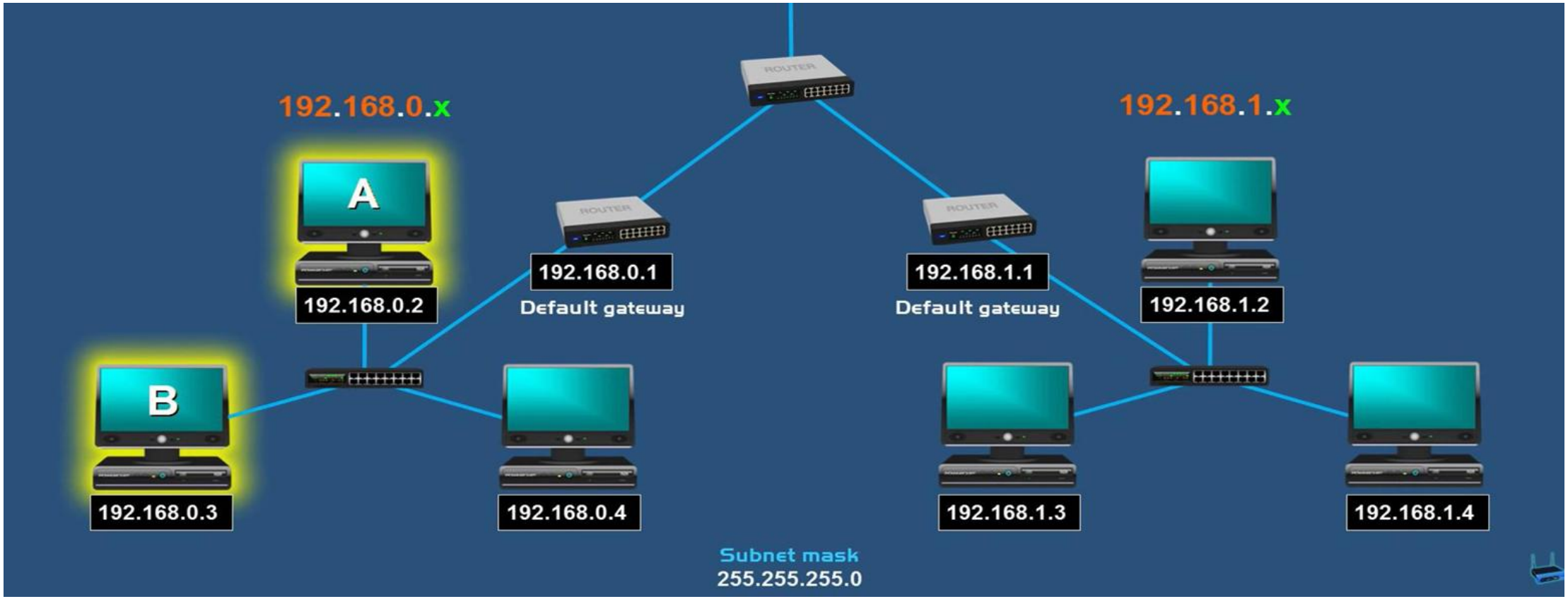
a) 1.4.5.5 b) 75.45.301.14 c) 111.56.088.78

d) 192.226.12.11 e) 130.45.151.154 f) 11100010.23.14.67

g) 221.34.7.8.20 h) 240.230.220.89

Task Solution

- Find the class of following IP addresses:(i) 237.14.2.1 – **class D** (ii) 114.34.2.8 – **class A**
- Identify the class of following IP addresses
- (i) 121.23.19.222- **class A**
- (ii) 11000001 00001011 00001011 11101110 - starts with 110 **= class C**
- Write down class of a following IP addresses.
- i) 227.12.14.87 **= class D** ii) 14.23.120.8 **class A**
- iii) 11000001 10000011 00011011 11111111 – **class C**
- iv) 11110011 10011011 11111011 00001111 – **class E**


192.168.0.x
192.168.1.x
ROUTER
ROUTER
ROUTER
A
B
192.168.0.2
192.168.0.1
Default gateway
192.168.1.1
Default gateway
192.168.1.2
192.168.0.3
192.168.0.4
192.168.1.3
192.168.1.4
Subnet mask
255.255.255.0

Subnet

- The process of dividing a given IP network into smaller subnetwork is called subnetting.
- Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets).
- Why we do Subnetting?
  - Different Technologies used in different network(e.g. ethernet, Ring etc.)
  - To solve Security Issues
  - To solve Maintenance issue
  - Control network traffic

Subnet

- Subnet bits are always borrowed from host id part
- Subnetting creates a three level of hierarchy.

NETWORK id	SUBNET ID	HOST ID

- Subnet
- Example(subnet example)

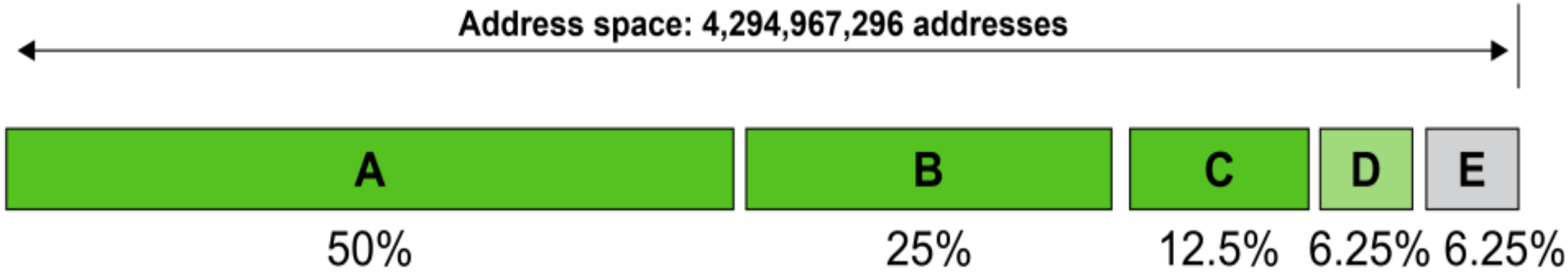
Subnet mask

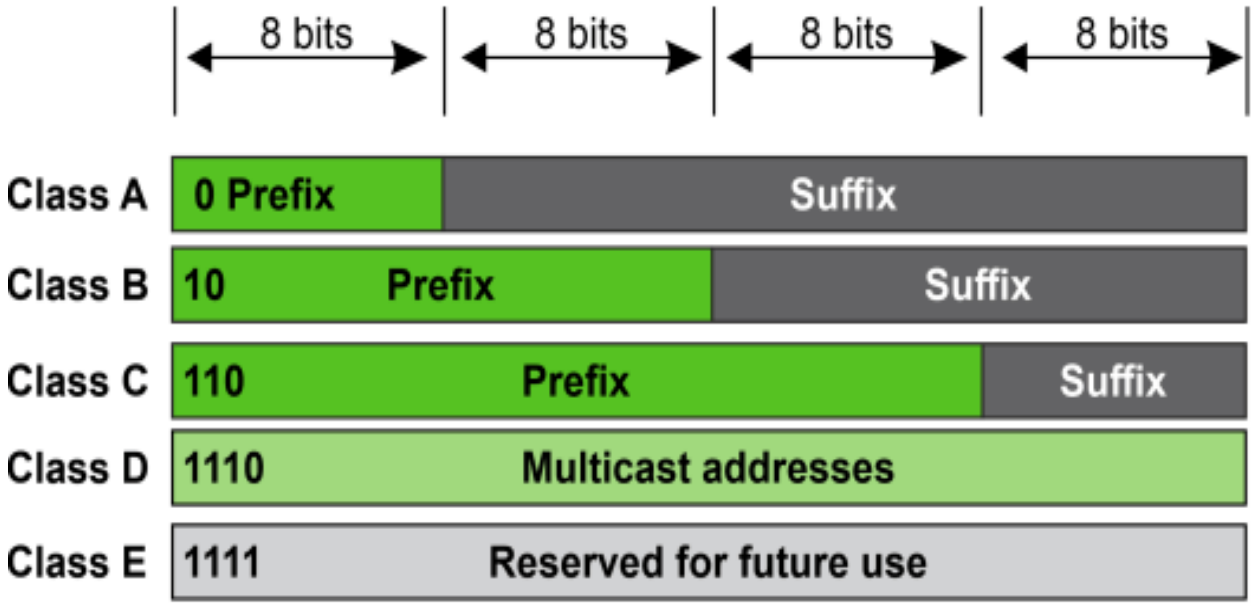
- When a router receiver a packet with a destination address, it needs to route the packet.
- The routing is based on the network address and sub network address.
- The router outside the organization (Network) route the packet based on the network address.
- The router inside the organization routes the packet based on the sub network address.

Masking

- How can a router find the network address or sub network address?
- A network administrator knows the network address and sub network addresses but router does not.
- **Router uses the masking process.**
- **A Masking is a process that extracts the address of the network from address. For that we have to set all network bits to 1 and host bits to 0**
- Masking can be done whether we have sub-netting or not.
- If we have sub-netted the network, masking extracts the network address from address.

Occupation of the address space in classful addressing





Classes	Prefixes	First Byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Type of IPv4

1. Public IP
2. Private IP

❑**A public IP :** address is **assigned to a device by an Internet Service Provider (ISP)** and is used to identify the device on the public internet.

- It **is unique globally** and can be **accessed from anywhere on the internet**.

❑**Private IP:** A private IP address is **used within a local network and is not routable on the public internet.**

- It **is assigned to devices within a private network, such as a home or office** network, to enable communication within the local network.

now Think????

- **Which IP address is show when we type ipconfig in cmd?**
- **How to know your public IP address?**

- Ipconfig give private IP of any host
- To know public ip goto:whatismyipaddress.com

Public vs Private IP ADDRESSES

192.168.0.4

192.168.0.2

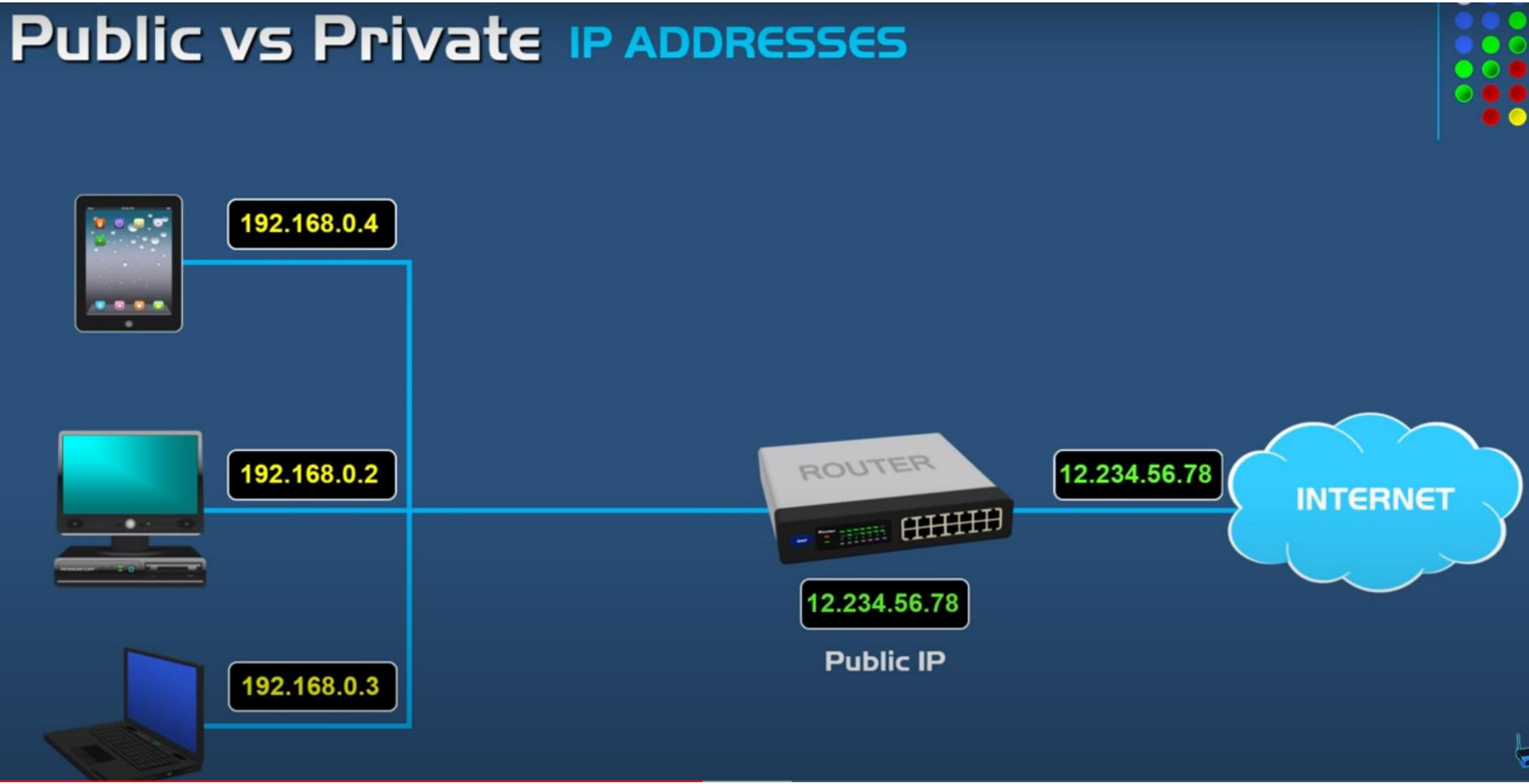
192.168.0.3

NAT (network address translation)
is what translates a set of IP addresses
to another set of IP addresses.

12.234.56.78

Public IP

Public vs Private IP ADDRESSES



Public IP

Unique

Publicly registered on the internet.

Used externally.

Assigned by an ISP.

Not free.

Not secure.

Private IP

Non-unique. Can be used on other private networks.

Not publicly registered.

Used internally.

Assigned by a router.

Free.

More secure.

PRIVATE IP ADDRESS

- The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets (local networks):

10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

PRIVATE IP ADDRESS

- Also, IP addresses in the range of **169.254.0.0 -169.254.255.255** are reserved for **Automatic Private IP Addressing**.
- These IP's should not be used on the Internet

PUBLIC IP ADDRESS

- The IP Address that you make known to others on the Internet is called your Public IP Address
- IP ADDRESS excluding private ip address range are used on internet

Reserved addresses in IPv4

- **IPv4, has several reserved addresses that used for specific purposes** and should **not be assigned to devices on a public network.**
- These reserved addresses **used for** functions, **such as private network addressing, loopback testing, and multicast communication.**

Private IPv4 Addresses:

- Private IPv4 Addresses:
  - 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 to 192.168.255.255
- **These address ranges are reserved for private networks** and are commonly **used in local area networks (LANs)** for internal communication

Loopback Address:

127.0.0.1 – 127.255.255.255

- The IP address range 127.0.0.0 - 127.255.255.255 is reserved for loopback,
- i.e. **a host's self- address, also known as localhost address.**
- This loopback IP address is managed entirely by and within the operating system.
- **Loopback addresses enable the Server and Client processes on a single system to communicate with each other.**
- When a process creates a packet with destination address as loopback address, the operating system loops it back to itself without the interference of NIC..

➢ **Lets check by typing in cmd : ping localhost -4**

IPv4

```
C:\Users\kirit>ping localhost -4

Pinging DESKTOP-TPU66TJ [127.0.0.1] with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\kirit>
```

Default it return IPv6

```
C:\Users\kirit>ping localhost

Pinging DESKTOP-TPU66TJ [::1] with 32 bytes of data:
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms
Reply from ::1: time<1ms

Ping statistics for ::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Link-local Address:

Range: 169.254.0.0 to 169.254.255.255

- **DHCP stands for Dynamic Host Configuration Protocol.** It is a network protocol **used to automatically assign IP addresses and network configuration settings to devices on a network.**
- **In case a host is not able to acquire an IP address from the DHCP server,** and it has not been assigned any IP address manually, the host can assign itself an IP address from a range of reserved Link-local addresses.

Multicast Addresses:

1. Range:
   224.0.0.0 to 239.255.255.255
2. Multicast addresses are used for one-to-many communication,
3. a single packet can be sent to multiple devices simultaneously.
4. They are reserved for specific multicast group communications.

Characteristics of IPv4

- The **length of an IPv4 address is 32 bits**.
- There are three types of addresses: **unicast, broadcast, and multicast**.
- The IPv4 address can be **represented in binary, dotted-decimal, or hexadecimal notation.**
- The **most commonly used** notation is the **dotted decimal format**.
- An IPv4 address is **classified into five classes** for classful addressing:

  Class A, Class B, Class C, Class D, and Class E.

Characteristics of IPv4

- In IPv4, **IP addresses are unique**, so two **devices on the same network cannot have the same** address.
- IPv4 addresses **consist of two parts** the **network part and the host part.**
- The **IPv4 packet header consists of 20 bytes** of **data and the number of the header field is 12.**
- IPv4 is a **connectionless protocol**.
- **IPv4** addresses can be **assigned manually or through DHCP** (Dynamic Host Configuration Protocol).

Advantages of IPv4:

1. **Simplicity:** IPv4 has a **straightforward and simple design,** making it **easier to implement and manage**.
2. **Wide support:** IPv4 is **supported by virtually all network devices, operating systems, and software applications**, ensuring compatibility.
3. **Established infrastructure:** IPv4 **has a well-established infrastructure** with **extensive routing capabilities, making it reliable and efficient.**

Disadvantages of IPv4:

1. **Address exhaustion:** IPv4 has a **limited address space**, leading to a **shortage** of available **unique IP addresses**.
   - Number of IPv4 **is 2^32** which is **not sufficient for today's world**
2. **NAT dependency:** Network Address Translation **(NAT)** is commonly used to **share a single public IPv4 address among multiple devices,** introducing **complex**ities and limitations.
3. **Security concerns:** IPv4 **lacks built-in features for network security, making it more vulnerable to attacks.**
4. **Lack of QoS support:** IPv4 does not provide native **support for Quality of Service (QoS), i**mpacting the prioritization of different types of network traffic.

CLASSLESS IP ADRESSINGIN IPV4

- **Classless Addressing** or **Classless Inter-Domain Routing** was introduced in 1993 to replace classful addressing.
- Classless Inter-Domain Routing (CIDR) is a method for efficiently allocating IP addresses and routing Internet Protocol (IP) packets.
- Unlike classful addressing, which divides IP addresses into fixed classes (A, B, C, etc.), CIDR allows for variable-length subnet masks (VLSM).
- This means that networks can be divided into smaller, more flexible subnets according to their specific needs, rather than being constrained by predefined class boundaries.

CIDR Notation

- In CIDR subnet masks are denoted by /X.
- For example a subnet of 255.255.255.0 would be denoted by /24.
- To work a subnet mask in CIDR, we have to first convert each octet into its respective binary value.
- For example, if the subnet is of 255.255.255.0.
- Therefore, in total there are 24 binary 1's, so the subnet mask is /24.
- While creating a network in CIDR, a person has to make sure that the masks are contiguous, i.e. a subnet mask like 10111111.X.X.X can't exist.

CIDR Notation

- With CIDR, we can create Variable Length Subnet Masks, leading to less wastage of IP addresses.
- It is not necessary that the divider between the network and the host portions is at an octet boundary.
- For example, in CIDR a subnet mask like 255.224.0.0 or 11111111.11100000.00000000.00000000 can exist.

Example

- An organization is granted the block 130.56.0.0/16. The administrator wants to create 1024 subnets. 1. Find the Network ID. 2. Find the subnet mask. 3. Find the number of addresses in each subnet.

solution

- Given:
  - Original block: 130.56.0.0/16
  - Number of subnets needed: 1024

Step 1: Find the Network ID

- The original network ID is already given as:
- Network ID = 130.56.0.0/16

Step 2: Find the Subnet Mask

- We need to divide the /16 network into 1024 subnets.

➤ How many bits are needed to create 1024 subnets?
  - $2^n = 1024 \Longrightarrow n = 10$
- So we borrow 10 bits from the host portion.

➤ New subnet prefix:
  - Original prefix: /16
  - Borrowed bits: 10
  - New prefix = 16 + 10 = /26
  - **Subnet Mask = /26 (11111111.11111111.11111111.1100000)**
    (Which is **255.255.255.192)**

Step 3: Find the number of addresses in each subnet

- A /26 prefix means 32 - 26 = 6 bits for host addresses.

  So each subnet has 2^6=64 addresses
- Out of which 2 addresses are reserved (Network & Broadcast)
  - Usable: 64−2=6264−2=62
- Addresses per subnet = 64
- Usable addresses per subnet = 62

Final Answers:

- Network ID: 130.56.0.0/16
- Subnet Mask: /26 or 255.255.255.192
- Addresses per Subnet: 64 (62 usable)

IPv6

- ***Despite all*** **short-term solutions, address depletion is still a long-term problem for the Internet.**
- IPv6 was **developed by Internet Engineering Task Force (IETF) to deal** with the problem of **IPv4 exhaustion**.
- **IPv6** is **next generation of IP** address. It is known as **IPng** (Internetworking Protocol, next generation), now a days it is a standard protocol widely used.

IPv6

- IPv6 is a **128-bit hexadecimal** address.
- **Hexa-decimal** uses **both numbers and alphabets**.
- An IPv6 address is made of **128 bits** divided into **eight 16-bits blocks**
- Each block is then converted into **4-digit Hexadecimal** numbers **separated by colon** symbols. **‘ : ’**
- IPv6 is capable of producing over **340 undecillion address**.

  i.e. **2^128=340,282,366,920,938,463,374,607,431,768,211,456** addresses.
- **Current population of world:8,061,876,001(source:https://datacommons.org)**

IPv6

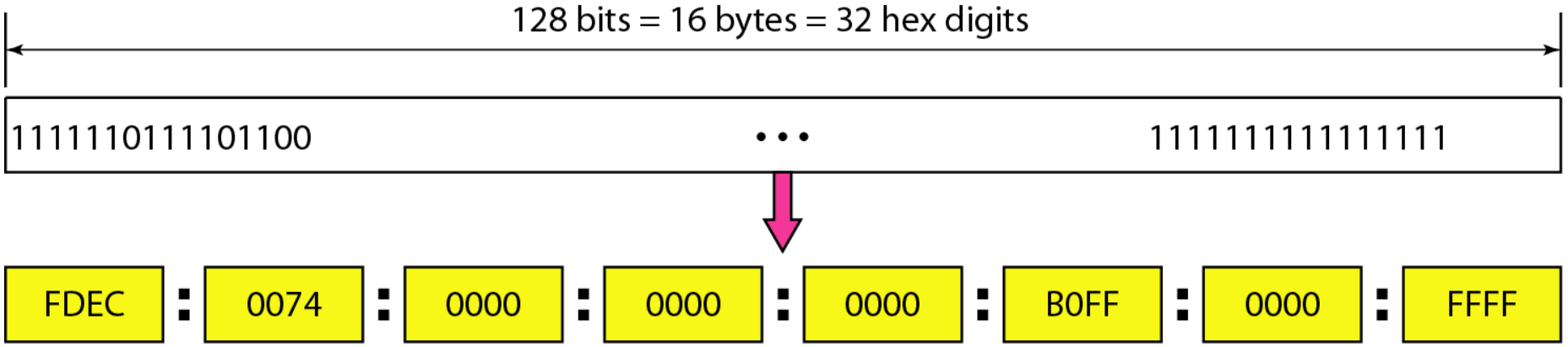
There are **8 groups(FIELDS)** and each group is of 16-bit i.e. 2 Bytes

3ffe:1900:4545:3:200:f8ff:fe21:67c

3ffe	1900	4545	3	200	f8ff	fe21	67cf
0011 1111 1111 1110	0001 1001 0000 0000	0100 0101 0100 0101	0000 0000 0000 0011	0000 0010 0000 0000	1111 1000 1111 1111	1111 1110 0010 0001	0110 0111 1100 1111
16-bit	16-bit	16-bit	16-bit	16-bit	16-bit	16-bit	16-bit

IPv6

•An IPv6 address is a string of 128 bits represented as 32 hexadecimal digits grouped in eight groups separated by colons.



IPv6 address in binary and hexadecimal colon notation

- Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:
- **Rule 1: Discard leading Zero (es):**
- In Block 2 , 0074, the leading two 0's can be omitted, such as (2^{nd} block): **fdec:0074:0000:0000:0000:b0ff:0000:ffff**

IP becomes : **fdec:74:0000:0000:0000:b0ff:0000:ffff**

- **Rule 2: If two or more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::,**

- such as (6th and 7th block):

- In Block 3, Block 4, Block 5, **fdec:74: :b0ff:0000:ffff**

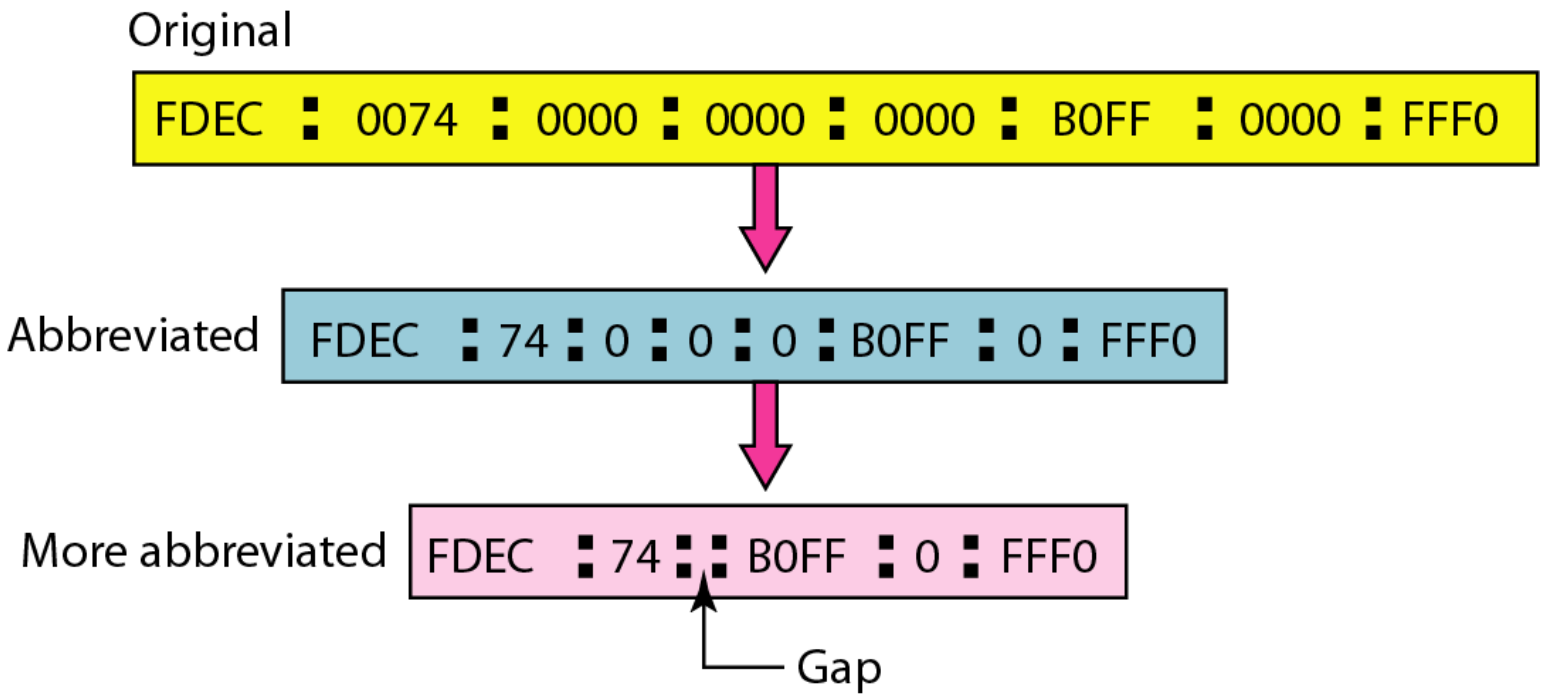
- A block of consecutive zeroes can only be replaced once by ::, so if there are still blocks of zeroes.

in the address, they can be shrunk down to a single zero, as shown in (7th block):

fdec:74: :b0ff:0:ffff

- We have 128 bits in IPv6 address but by looking at the first few bits we can identify what type of address it is.

Abbreviated IPv6 addresses



CASE 2:

- The IPv6 address is **128 bits** (i.e. 16 bytes) long and is written in **8 groups of 2 bytes** in hexadecimal numbers, separated by colons:
  - **fddd:f00d:cafe:0000:0000:0000:0000:0001**
- Leading zeros of each block can be omitted, the above address can be written like this:

  fddd:f00d:cafe:0:0:0:0:1
- We can abbreviate whole blocks of zeros with :: and write:

  fddd:f00d:cafe::1

CASE 3:

- IPv6: **00ff:0:0:0:1:0:0:1**

  Shortened: **ff:0:0:0:1:0:0:1**

  Further shorter form: **ff::1:0:0:1 (correct)**

  - ff::1::1 (ambiguous, wrong)
- ff:0:0:0:1::1 is **not correct because** the longest **group of concurrent zeroes must be shortened.**

TASK:

- WRITE FOLLOWING IN SHORTER FORM

1) 2041:0000:140F:0000:0000:0000:875B:131B
2) 2001:0001:0002:0003:0004:0005:0006:0007
3) 2001:4860:4860:0000:0000:0000:0000:8888

- WRITE IN EXPANDED FORM

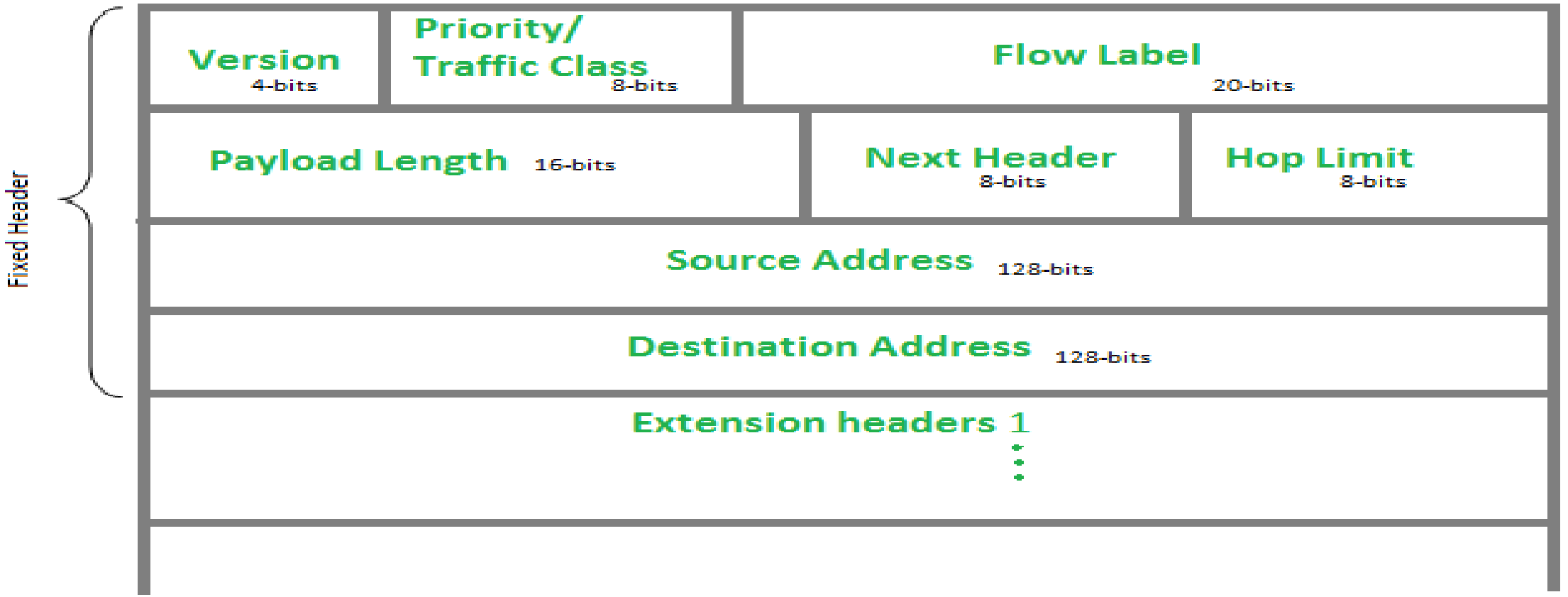
1)2001:db8::2:1

2)2002:7f00:001::

- **A)** 2041:0:140F::875B:131B
- B) Short: 2001:1:2:3:4:5:6:7
- C) 2001:4860:4860::8888

- EXPANDED
    1) 2001:0db8:0000:0000:0000:0000:0002:0001
    2) 2002:7f00:0001:0000:0000:0000:0000:0000

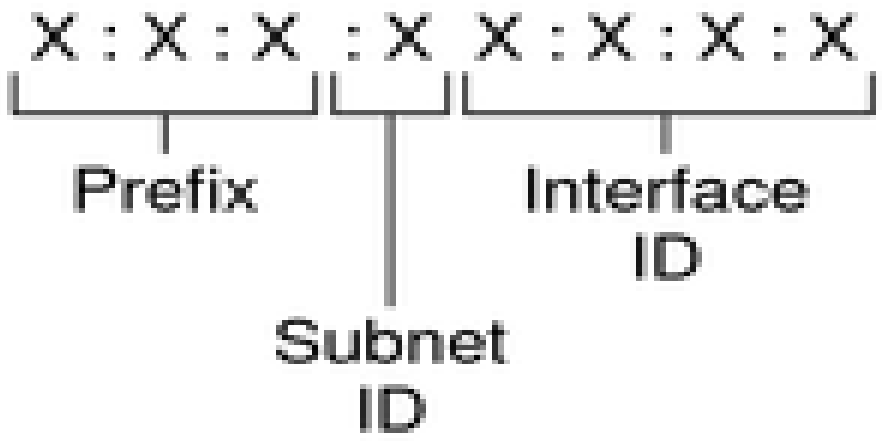
IPv6 header format



Version: This 4-bit field defines the version number of the IP. For IPv6, the value is 6(0110).

- **Priority:** The 4-bit priority field defines the priority of the packet with respect to traffic congestion.
- **Flow label.** The flow label is a 3-byte (20-bit) field that is designed to provide special handling for a particular flow of data.
- **Payload length**. The 2-byte payload length field defines the length of the IP datagram excluding the base header.
- **Next header**. The next header is an 8-bit field defining the header that follows the base header in the datagram.
- **Hop limit.** This 8-bit hop limit field serves the same purpose as the TTL field in IPv4.
- **Source address.** The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram.
- **Destination address.** The destination address field is a 16-byte (128-bit) Internet address that usually identifies the final destination of the datagram.

IPv6 addresses are divided into three main parts:



Example:

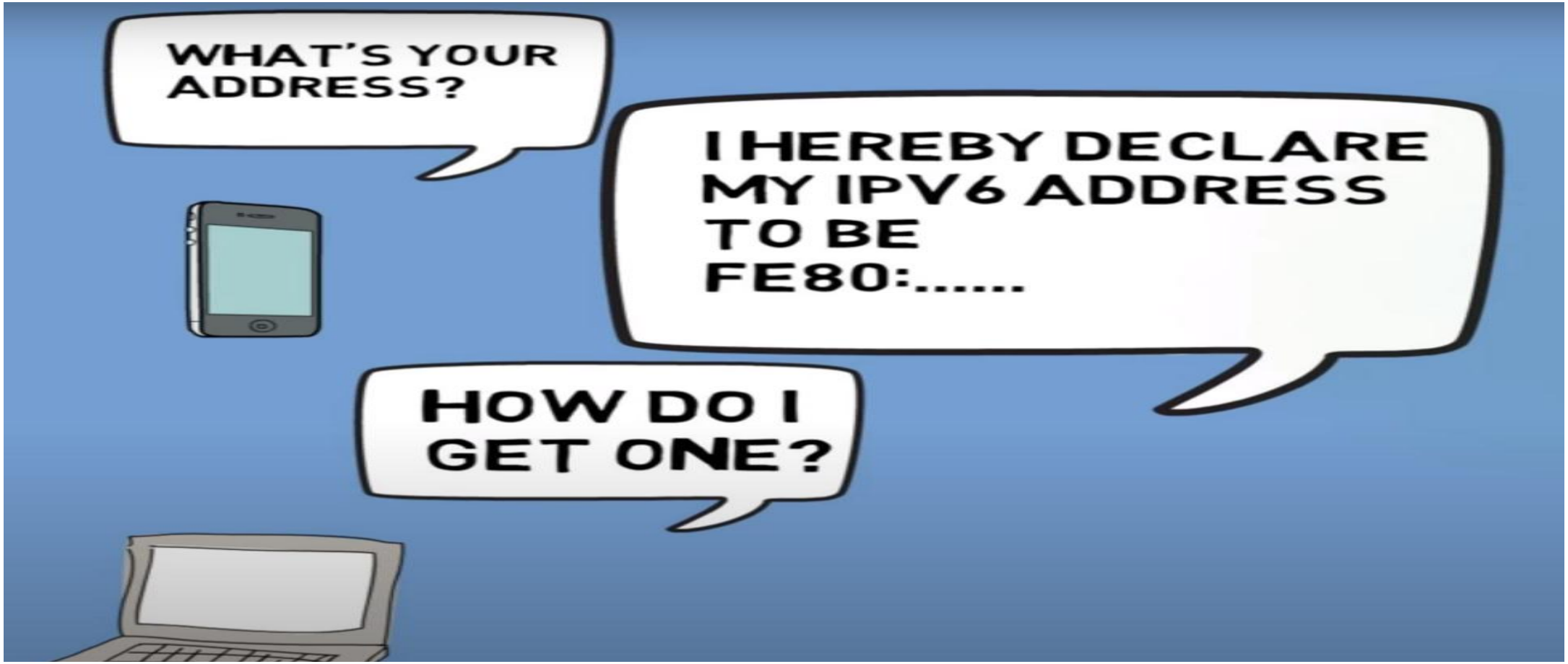
IPv6 addresses are divided into three main parts:

1. **Prefix**: The prefix specifies the **network portion of the address and is used for routing. It is typically assigned by an Internet Service Provider (ISP) or network administrator.** The length of the prefix is variable and denoted by a number following a slash (/). For example, in the address 2001:db8:85a3::/48, the prefix length is 48.
2. **Subnet ID**: **The subnet ID identifies a subnet within a larger network**. It is allocated by the network administrator. The **length of the subnet ID can vary** depending on the network's requirements.
3. **Interface ID**: The **interface ID identifies a specific interface or device within a subnet.** It is **typically assigned automatically or manually configured on each device. The length of the interface ID is 64 bits by default.**

PAPER STYLE

- CHAPTER 4 = 13 MARKS
- CHAPTER 5 = 7 MARKS
- 3,4,5,7

IPV6 is Stateless Address AutoConfiguration (SLAAC)

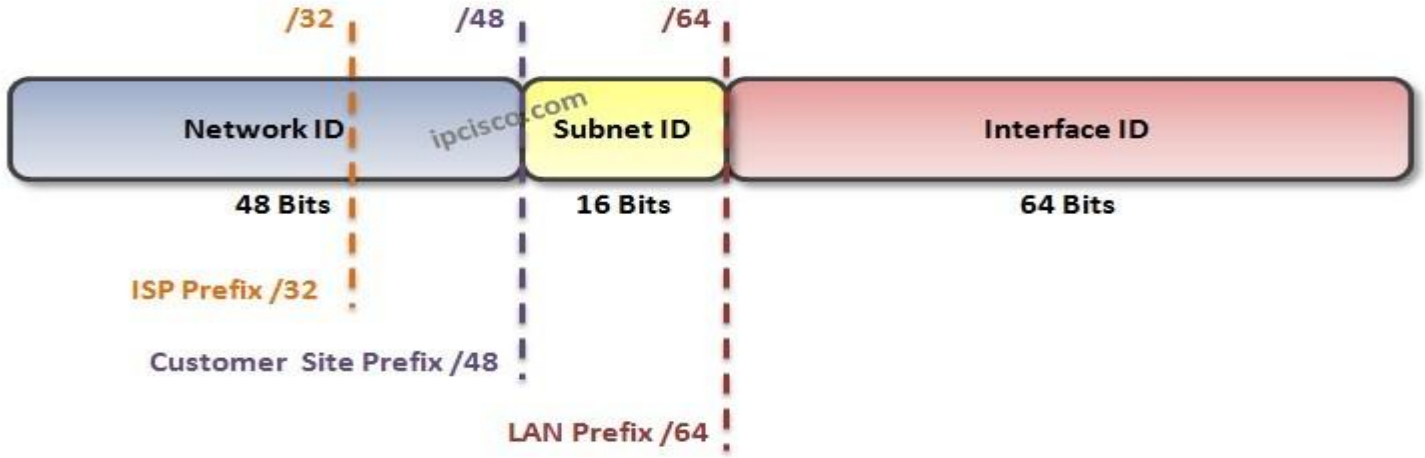


```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:4041:8e11:2f93:896b:277:5c26:f5c7
   Temporary IPv6 Address. . . . . . : 2409:4041:8e11:2f93:8078:86cb:6ee2:2f32
   Link-local IPv6 Address . . . . . : fe80::1258:fac7:55a1:6dd6%11
   IPv4 Address. . . . . . . . . . . : 192.168.186.33
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::68b6:feff:fe72:46c%11
                                       192.168.186.236

C:\Users\kirit>
```

IPv6 addresses are divided into three main parts:



- let's consider an IPv6 address within the "2000::/3" range: 2001:0db8:1234:5678::1.
- The first 3 bits of the address, "001," are part of the network prefix defined by the "/3" prefix length.
- The remaining 125 bits, from "2001" onwards, represent the interface identifier.
- 0010000000000001000011011011100000010010001101001010110011110000000000000000000000000000000000000000000000000001

IPv6 ADDRESSING MODES(TYPE)

- Within IPv6, there are a range of message options. **All of these message types have a single host transmitting the message and all delivery is handled by the switch or router:**

- **Unicast** is a message sent from a host to one receiver **(One to One),**
- **Multicast** is a message sent from a host to all subscribers of a Multicast group **(One to Specific**),
- **Anycast** is a message sent from a host to the fastest / nearest subscriber of a specific address (**One to Specific - Fastest Receiver / Nearest Node will receive).**

1. Unicast
   - Global Unicast
   - Unique Local
   - Link Local
2. Multicast
3. Anycast

Note:

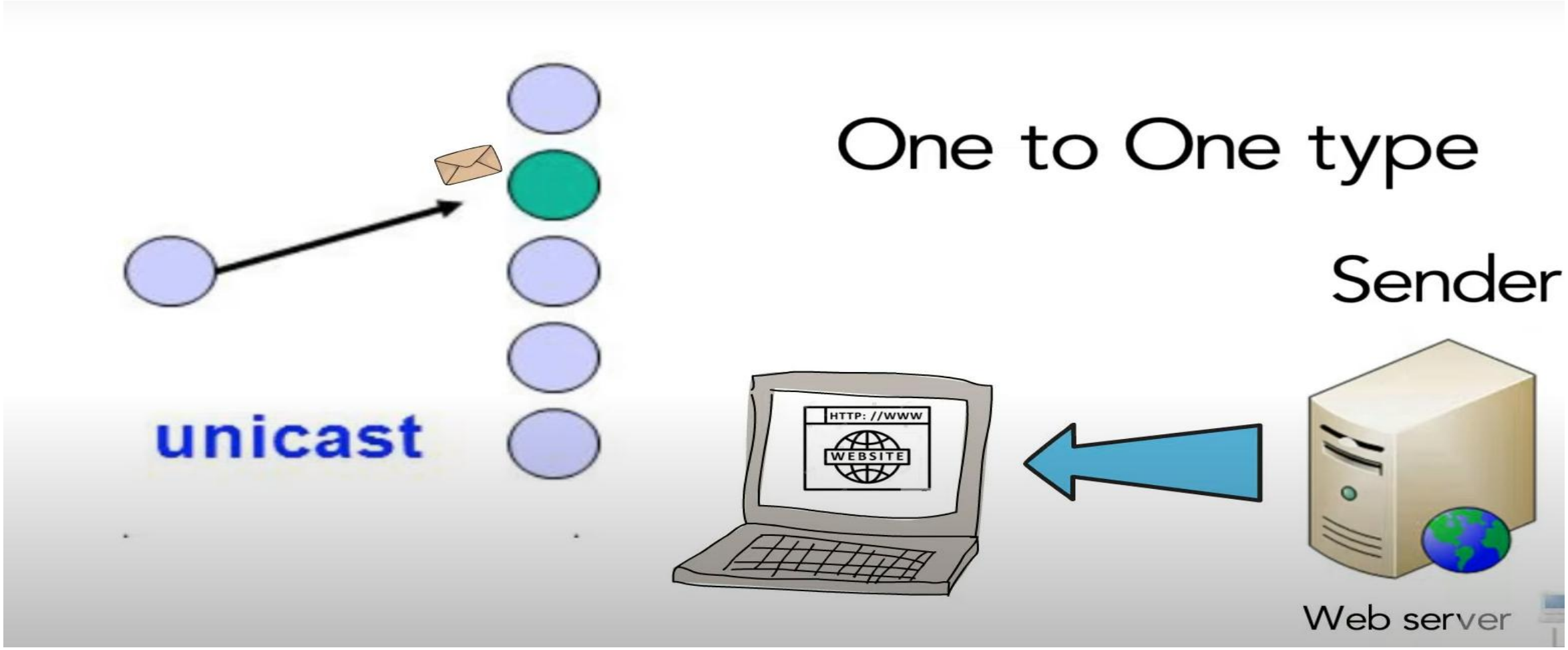
There is no broadcasting in IPv6.

UNICAST IPv6 Address Scopes

- **When working in the world of IPv6, our addresses can vary depending on our scope (i.e. what part of a network):**

- GLOBAL - Everything (i.e. the whole internet),
- UNIQUE LOCAL - Everything in our LAN (behind the internet gateway),
- LINK LOCAL - Everything within the same collision domain that will not be routed (i.e. **attached to the same switch**).

UNICAST ADDRESSES



GLOBAL UNICAST IPV6 ADDRESSES

- Used to identify a single interface on public network.

- They are standard globally unique unicast addresses.
  (like public IPv4 addresses)

- They are internet routable and start with 2.
  Example: 2001:db8:0:b::1A

GLOBAL UNICAST IPV6 ADDRESSES RANGE

- Since the leftmost three bits are reserved as "001" for Global unicast IPv6 addresses, the range of Global Unicast Addresses available now are from 2000 to 3FFF, as shown below:

Values for left most part Global Unicast Addresses	In Binaries	In Hexadecimals
Minimum possible	0010000000000000	2000
Maximum possible	0011111111111111	3FFF

IPv6 global unicast addresses

Similar to a public IPv4 address.

Globally unique

Internet routable

IANA 2000::/3

SITE/UNIQUE LOCAL IPV6 ADDRESS

- Used to identify a single interface on private network.
- These are local unique addresses. (like IPv4 private addresses)
- They are reserved with a range of FC00::/7
- IPv6 Unique Local addresses are not expected to be routable on the Internet, they are only routable inside of a company's multiple sites.
- Unique Local IPv6 addresses can be viewed as globally unique "private routable" IPv6 addresses, which are typically used inside an organization.

SITE/UNIQUE LOCAL IPV6 ADDRESS...

- A range of FC00::/7 means that IPv6 Unique Local addresses begin with 7 bits with exact binary pattern as 1111 110**0**
- So, we can have two Unique Local IPv6 Unicast Address prefixes.
- 1111 1100 (FC in hexadecimals) and 1111 1101 (FD in hexadecimals)

Unique / Site local

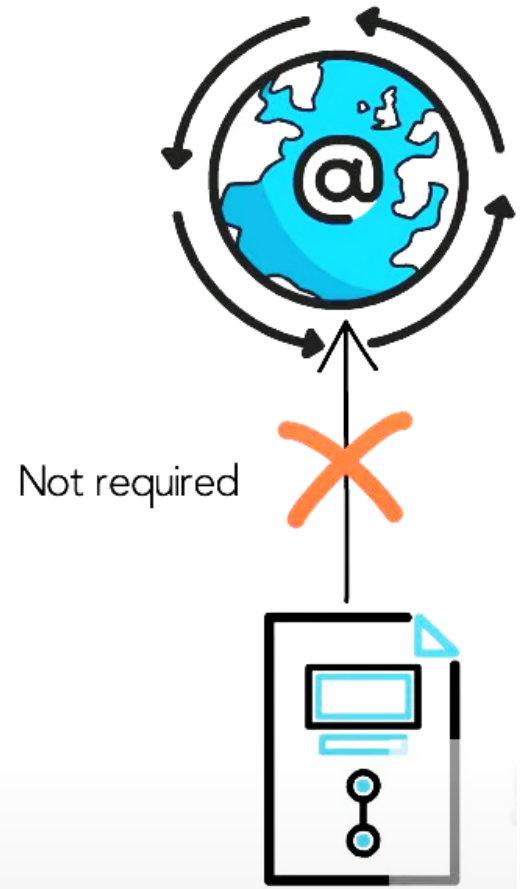
Private IPv6 addresses

Should not be routed in the global Internet.

Used in a limited area

Within a site

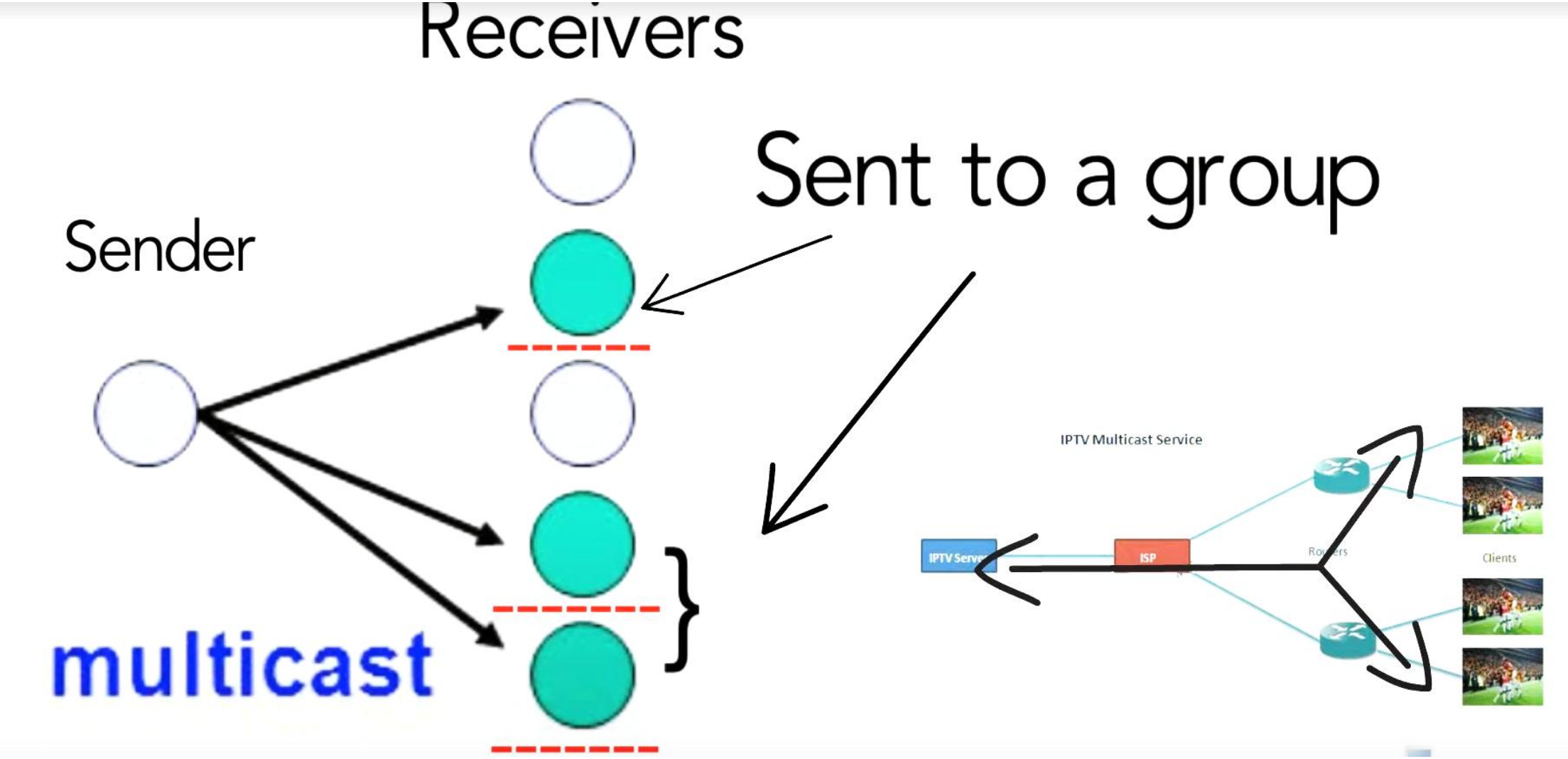
fc00::/7



LINK LOCAL IPV6 ADDRESSES

- Allow communications between devices on a local link.
- They start with FE80::/10
- These addresses are auto-configured (or auto-generated plug-and-play) addresses (Stateless addresses) similar to IPv4 APIPA address (169.254/16)
- Typically, getting an APIPA IPv4 address in an IPv4 network is because of some network error, but a Link local addresses are IPv6 addresses which can be used for local communication.

MULTICAST ADDRESSES



MULTICAST ADDRESS

- IPv6 multicast addresses Start with FF
- Following are the important IPv6 multicast addresses:

FF02::1 - All nodes on the local network segment

ROUTERS to HOST Multicast message

FF02::2 - All routers on the local network segment

Host to Routers Any one host want to send same message to multiple routers

Multicast Addresses

Similar to multicast addresses in IPv4.

Used to communicate with dynamic groupings of hosts.

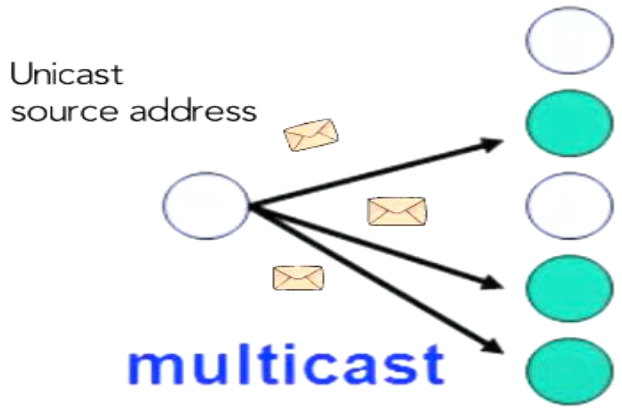
Multicast group.

ff00::/8 = 224.0.0.0/4

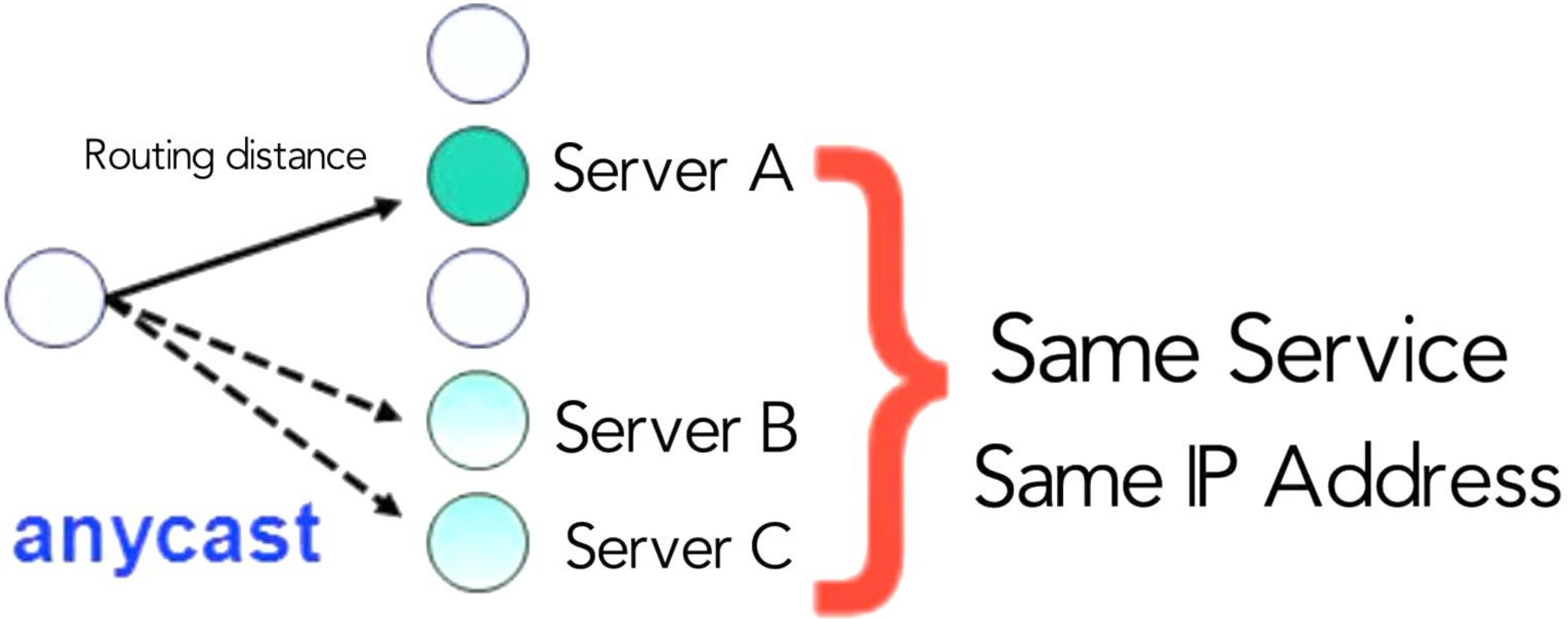
Well-Known Multicast Addresses

ff00::/12

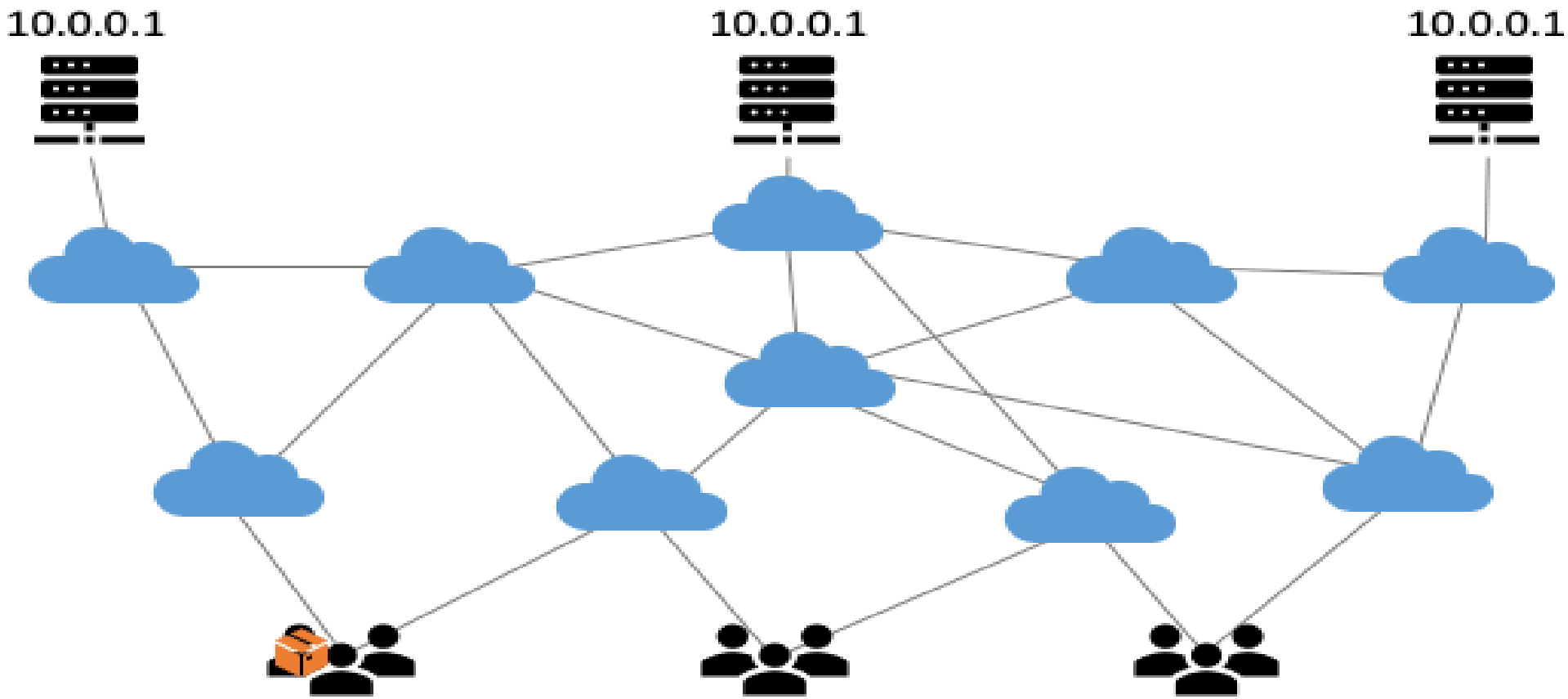
* ff02::1 All IPv6 devices
* ff02::2 All IPv6 routers
* ff02::5 All OSPFv3 routers
* ff02::a All EIGRP (IPv6) routers



ANYCAST ADDRESSES



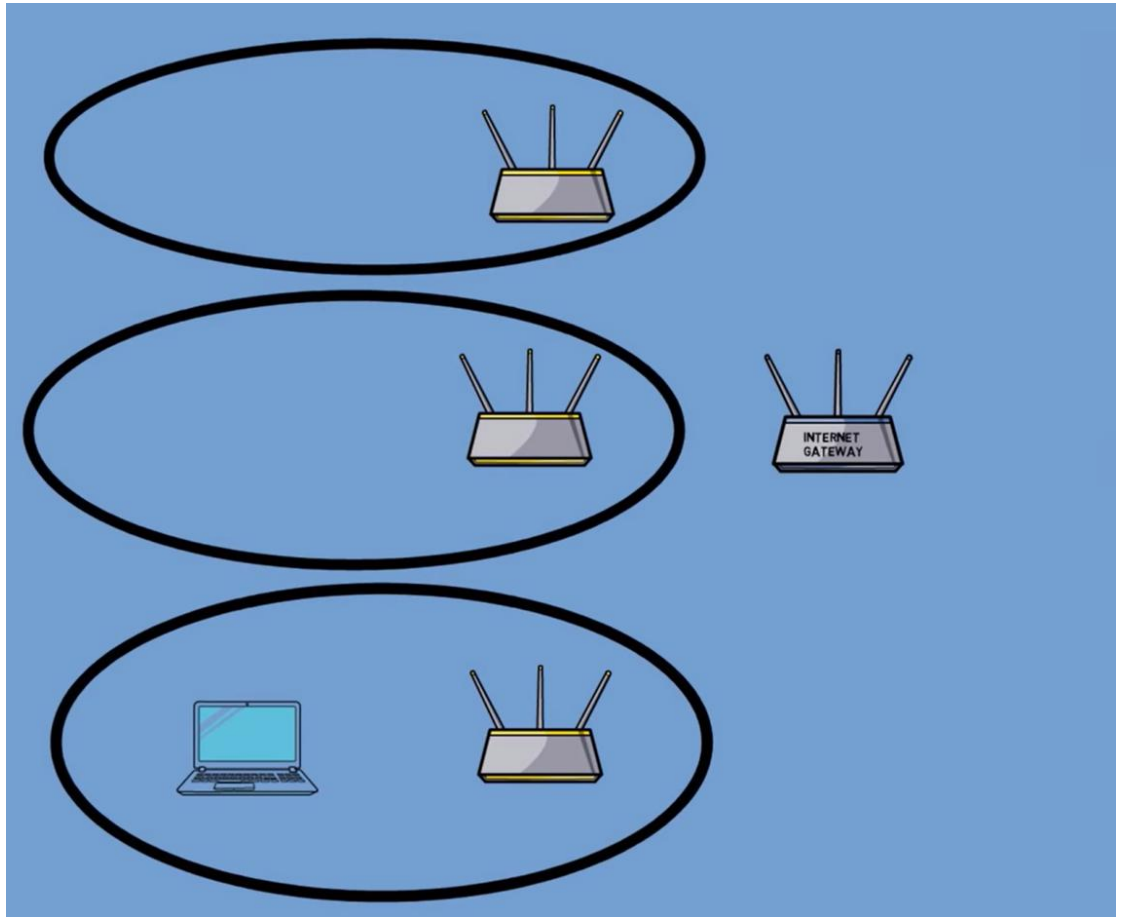
ANYCAST



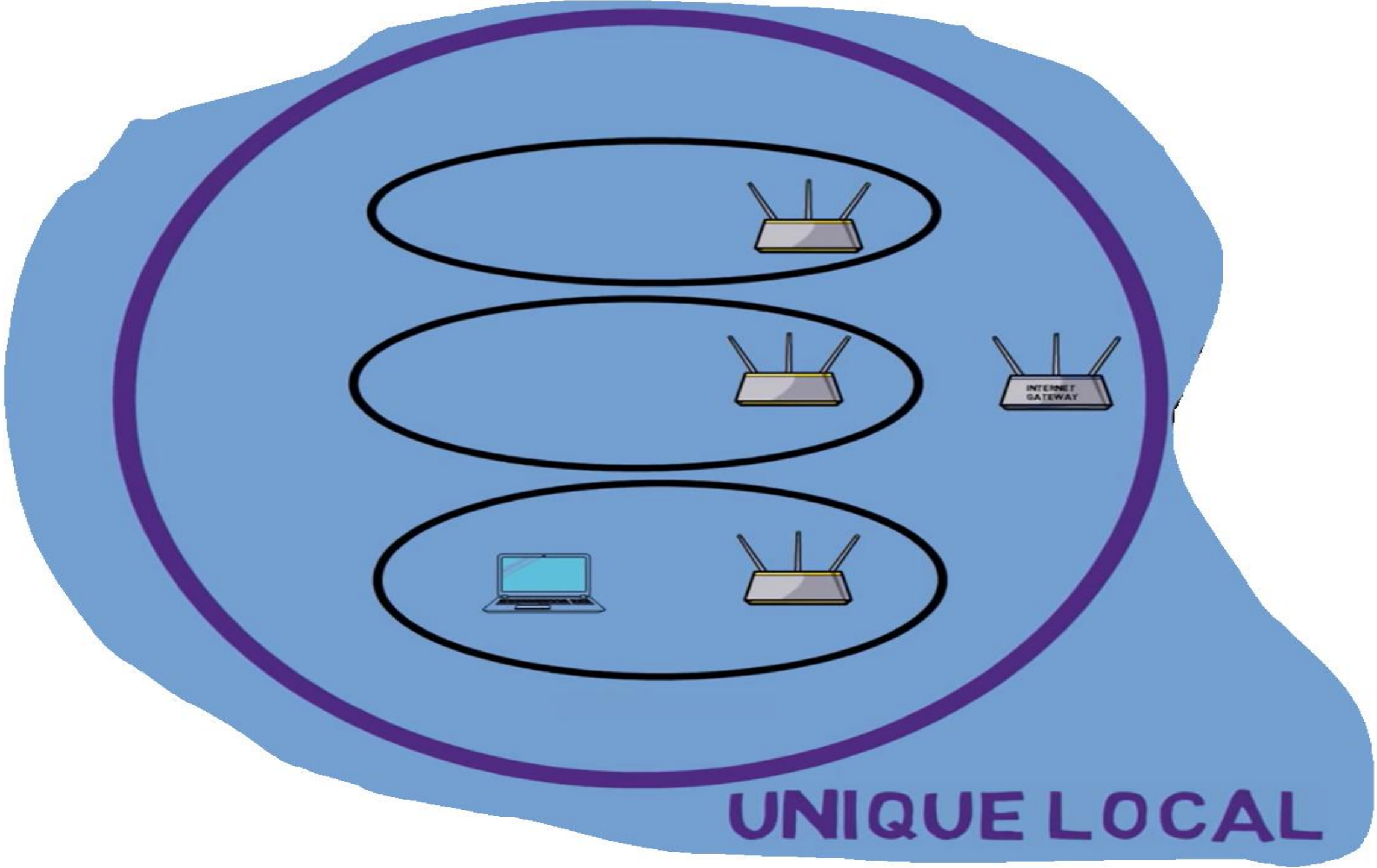
ANYCAST

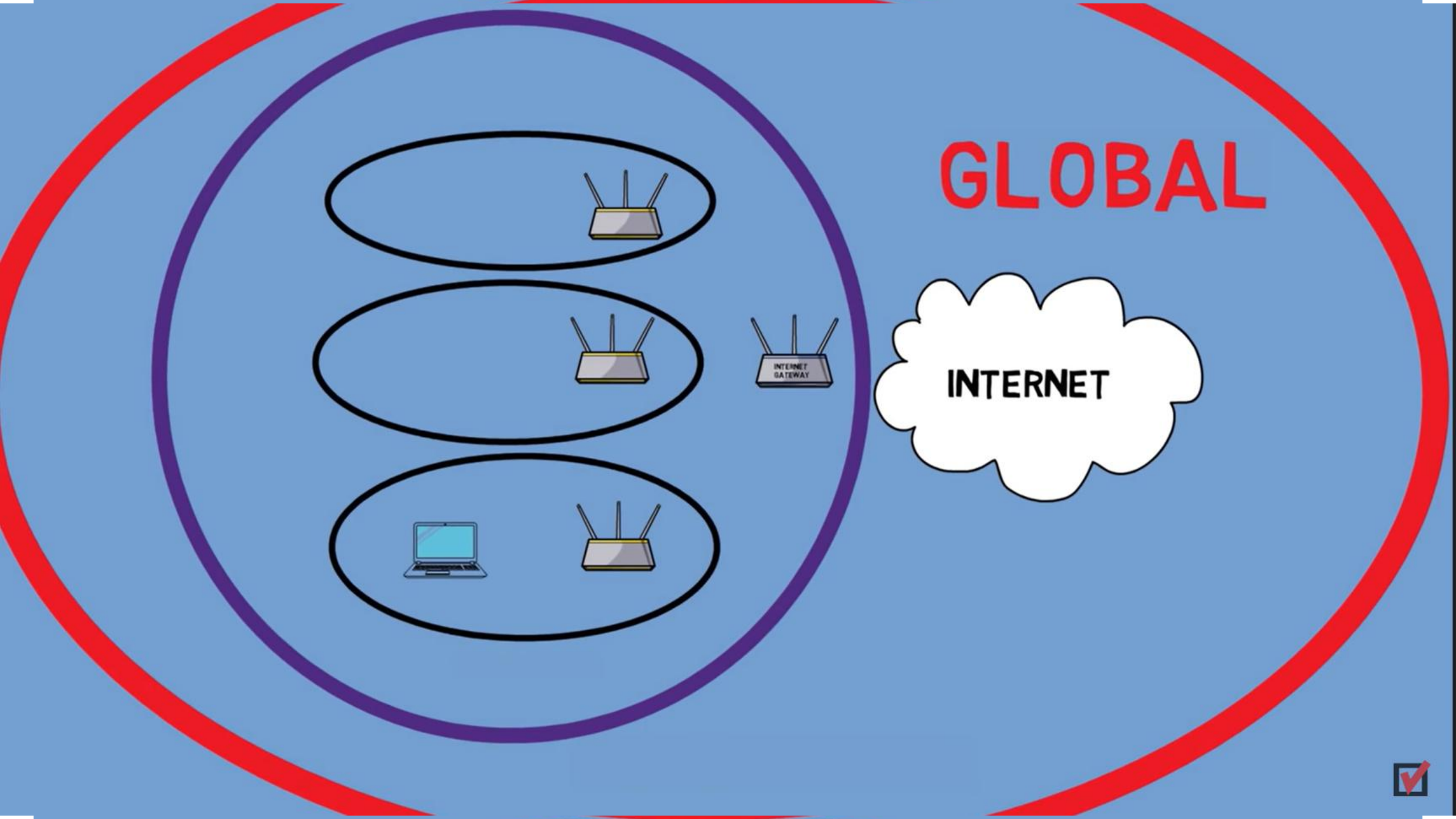
- Anycast addresses are similar to unicast addresses, but they are assigned to multiple interfaces in different locations.
- When a packet is sent to an anycast address, it is routed to the nearest interface that shares that address, based on the routing protocols and network topology.
- The Internet Assigned Numbers Authority (IANA) assigns specific IPv6 address blocks for anycast use.
- These address blocks are further allocated by the Regional Internet Registries (RIRs) to network operators.
- Here is an example of an IPv6 anycast address:
- 2001:db8::1

Scope of IPv6 address : Suppose we have 3 subnets



LINK LOCAL


INTERNET
GATEWAY
UNIQUE LOCAL


GLOBAL
INTERNET GATEWAY
INTERNET

Range	Purpose
::1/128	Loopback Address (localhost)
::/128	Unspecified Address
2000::/3	GLOBAL Unicast (Internet)
fc00::/7	Unique-Local (LAN)
fe80::/10	Link-Local Unicast (Same switch)

CHARACTERSTICS OF IPv6

- **Larger Address Space:** IPv6 uses 128-bit addresses, compared to the 32-bit addresses used in IPv4.
- **Address Autoconfiguration:** IPv6 supports stateless address autoconfiguration **(SLAAC)**, which enables devices to **automatically generate their own unique IPv6 addresses**
- **Simplified Header Format:** IPv6 has a simplified header format compared to IPv4.
- The **fixed-length 40-byte header in IPv6 reduces the processing overhead on routers** and improves overall network performance

CHARACTERSTICS OF IPv6

- **Enhanced Security: IPv6 incorporates IPsec (Internet Protocol Security) as a standard feature.** IPsec provides **authentication and encryption services at the network layer,** ensuring secure communication over IPv6 networks.
- **Quality of Service (QoS) Support:** IPv6 includes **built-in support for QoS,** enabling **the prioritization and differentiation of network traffic flows**.
- **Extension Headers:** IPv6 introduces the concept of **extension headers**, which are additional optional headers that can be added after the main IPv6 header. **Extension headers provide flexibility for the inclusion of additional information, such as routing, fragmentation, mobility, and authentication, without increasing the fixed header size.**

Ipv4 v/s Ipv6

SR NO.	IPv4	IPv6
1	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
2	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon(:).
3	Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal.
4	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
5	It generates 4 billion unique addresses. i.e. 2^32	It generates 340 undecillion unique addresses. i.e. 2^128.

Ipv4 v/s Ipv6

SR NO.	IPv4	IPv6
6	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC(protocol) is developed for security purposes.
7	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
8	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
9	The checksum field is available in IPv4.	The checksum field is not available in IPv6.

Ipv4 v/s Ipv6

SR NO.	IPv4	IPv6
10	It does not provide encryption and authentication.	It provides encryption and authentication.
11	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
12	Ex- 192.168.2.1	Ex: 3ffe:1900:4545:3:200:f8ff:fe21:67cf

SPECIAL ADDRESSES IN IPv6

- **Unspecified Address (::/128): 0.0.0.0.0.0.0.0/128**
- :: is shorthand for an IPv6 address that is all zeros.
- It is equivalent to **0000:0000:0000:0000:0000:0000:0000:0000**.
- The unspecified address is typically **used as a placeholder or to indicate an uninitialized or unknown address.**
- **/128 means the prefix length is 128 bits, which means all bits of the address are considered fixed.**
- Visit link to know all bout ipv6 http://www.gestioip.net/cgi-bin/subnet_calculator.cgi

SPECIAL ADDRESSES IN IPv6

- **Loopback Address (::1/128): 0:0:0:0:0:0:0:1**
- **0000:0000:0000:0000:0000:0000:0000:0001**
- The loopback address, represented as "::1", is equivalent to the IPv4 loopback address "127.0.0.1".
- IPv4=127.0.0.0 to 127.255.255.255, so 2^24 addresses are wasted.
- It is used to enable communication with the local host or to test network connectivity on a device.

- Unspecified address in IPv6 is the IPv6 address with all binary bits set to "0“

Address Type	IPv4	IPv6
Loopback Address	127.0.0.0/8	::1/128
Unspecified Address	0.0.0.0/0	::/0

SPECIAL ADDRESSES IN IPv6

- **Multicast Addresses (ff00::/8):**
- **Range:**

  ff00:0000:0000:0000:0000:0000:0000:0000–
  ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

- 11111111 00000000 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
- Multicast addresses in IPv6 are **used to send packets to multiple destinations simultaneously.**
- They are similar to IPv4 multicast addresses. Multicast addresses **start with the prefix "ff00::" followed by a group identifier.**

Range	Purpose
::1/128	Loopback Address (localhost)
::/128	Unspecified Address
2000::/3	GLOBAL Unicast (Internet)
fc00::/7	Unique-Local (LAN)
fe80::/10	Link-Local Unicast (Same switch)