Network Layer:

- Switching
- Logical addressing – IPV4, IPV6;
- Address mapping – ARP, RARP, BOOTP and DHCP
- Delivery, Forwarding and Unicast Routing protocols

Network Layer Services:

- Routing: When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.

- Logical Addressing: The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.

- Internetworking: This is the main role of the network layer that it provides the logical connection between different types of networks.

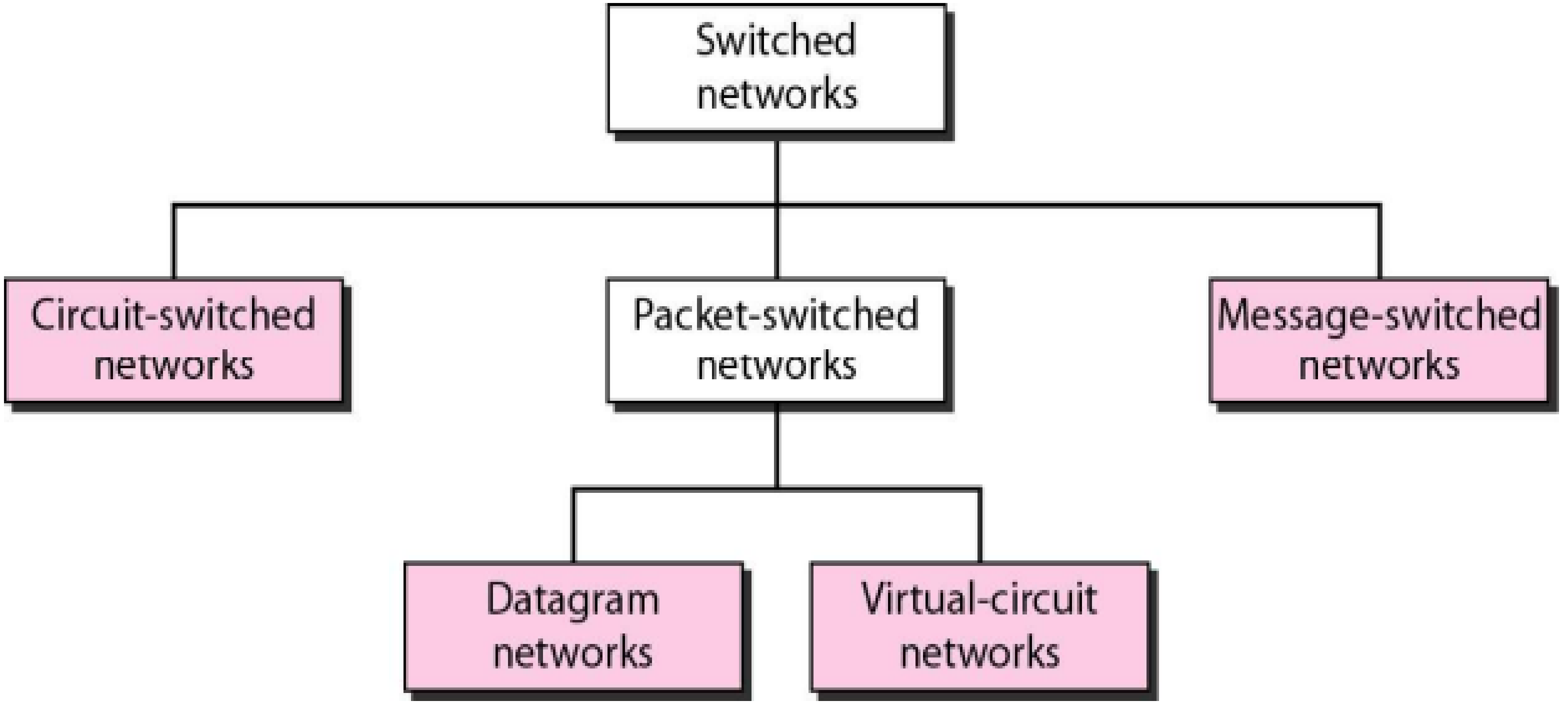
- Fragmentation: The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.

Switching

A network is a set of connected devices. Whenever we have multiple devices, we have the problem of how to connect them to make one-to-one communication possible. One solution is to make a point-to-point connection between each pair of devices (a mesh topology) or between a central device and every other device (a star topology). These methods, however, are impractical and wasteful when applied to very large networks. The number and length of the links require too much infrastructure to be cost-efficient, and the majority of those links would be idle most of the time.

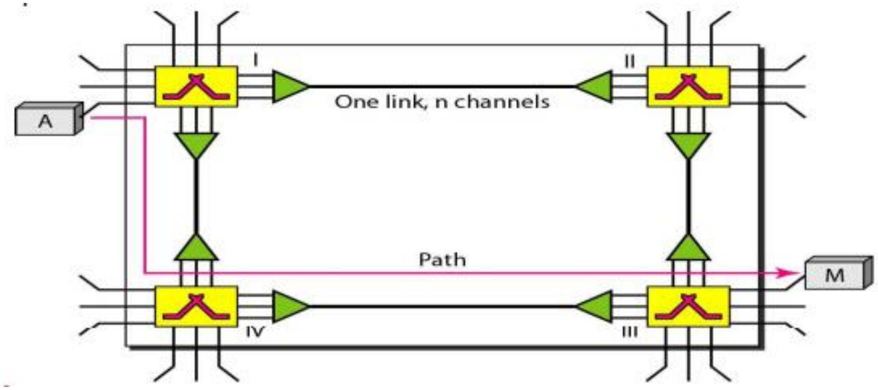
A better solution is switching. A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating **temporary connections** between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing.

The switching is classified as circuit switching, packet switching, and message switching. The first two are commonly used today. The third has been phased out in general communications but still has networking applications



CIRCUIT-SWITCHED NETWORKS

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link.



Three Phases of circuit switching :

The actual communication in a circuit-switched network requires three phases: connection setup

data transfer

connection teardown.

Setup Phase

Before the two parties can communicate, a dedicated circuit needs to be established. Connection setup means creating dedicated channels between the switches.

Data Transfer Phase

After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Efficiency

These are not as efficient as the other two types of networks because resources are allocated during the entire duration of the connection. These resources are unavailable to other connections.

Delay

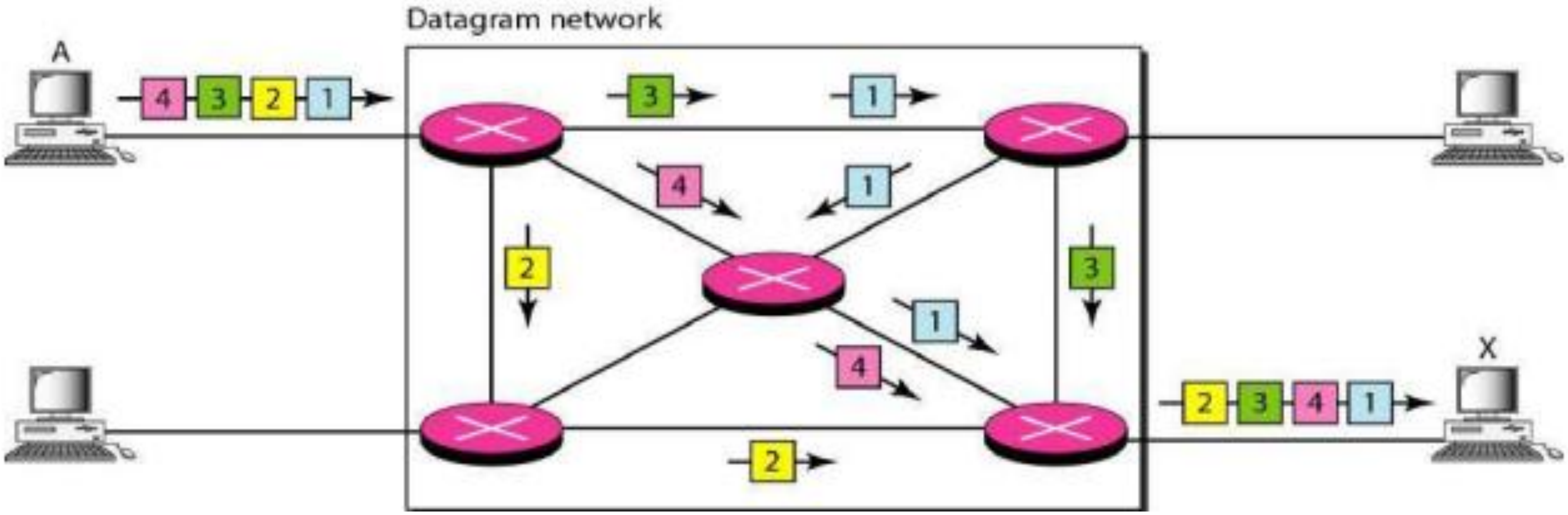
The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit.

Example :

Switching at the physical layer in the traditional telephone network uses the circuit-switching approach.

DATAGRAM NETWORKS

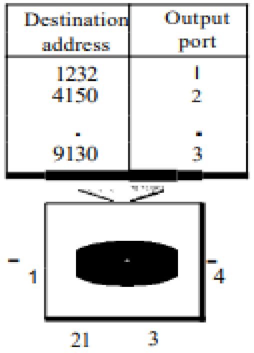
- In packet switching, there is **no resource allocation** for a packet. Resources are allocated on demand. The allocation is done on a firstcome, first-served basis. When a switch receives a packet, no matter what is the source or destination, the packet must wait if there are other packets being processed.
- Packets in this approach are referred to as **datagrams**. It is normally done at **network layer**.
- The datagram networks are sometimes referred to as **connectionless networks**. The term connectionless here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases.



Routing Table

In this type of network, each switch/router has a routing table which is based on the destination address. The routing tables are **dynamic and are updated periodically.**

The destination addresses and the corresponding forwarding recorded in the tables.



Destination address	Output port
1232	1
4150	2
.	.
9130	3

Efficiency

The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred.

Delay

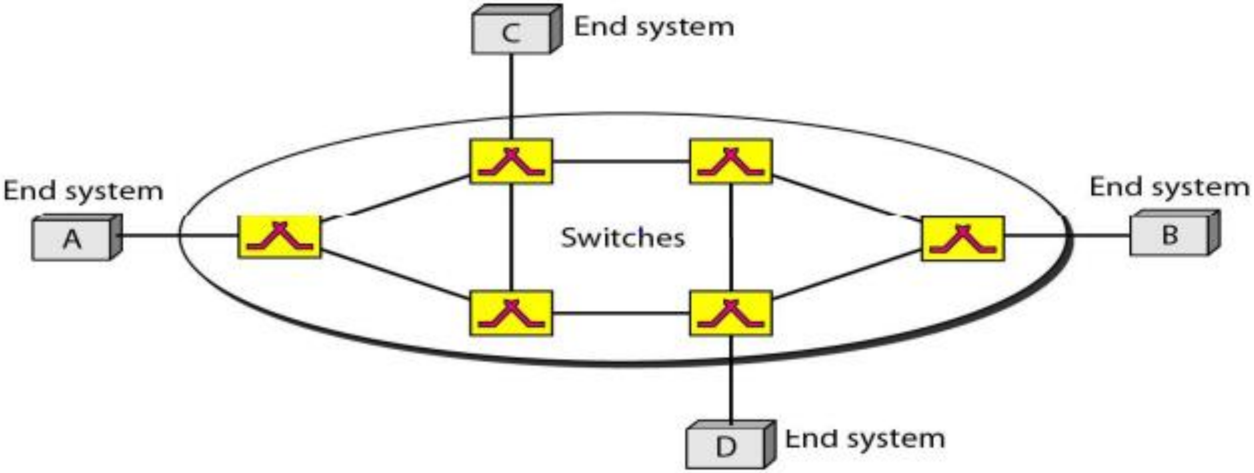
There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.

Example :

Switching in the Internet is done by using the datagram approach at network layer

VIRTUAL-CIRCUIT NETWORKS

A virtual-circuit network is a combination of circuit-switched network and a datagram network. It has characteristics of both



1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.

3. As in a datagram network, data are packetized and each packet carries an address in the header.

4. As in a circuit-switched network, all packets follow the same path established during the connection.

5. A virtual-circuit network is normally implemented in the data link layer

Addressing in Virtual Circuit

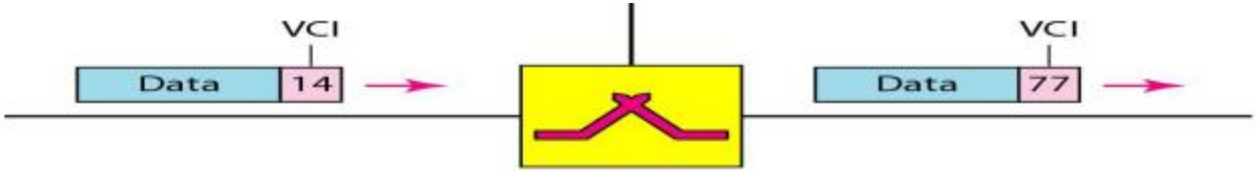
Two types of addressing are involved: global and local (virtual-circuit identifier).

Global Addressing

A source or a destination needs to have a global address-an address that can be unique in the scope of the network or internationally if the network is part of an international network.

Virtual-Circuit Identifier (Local addressing)

A virtual-circuit identifier (VCI), unlike a global address, is a small number that has only switch scope. It is used by a frame between two switches. When a frame arrives at a switch, it has a VCI.When it leaves, it has a different VCl.

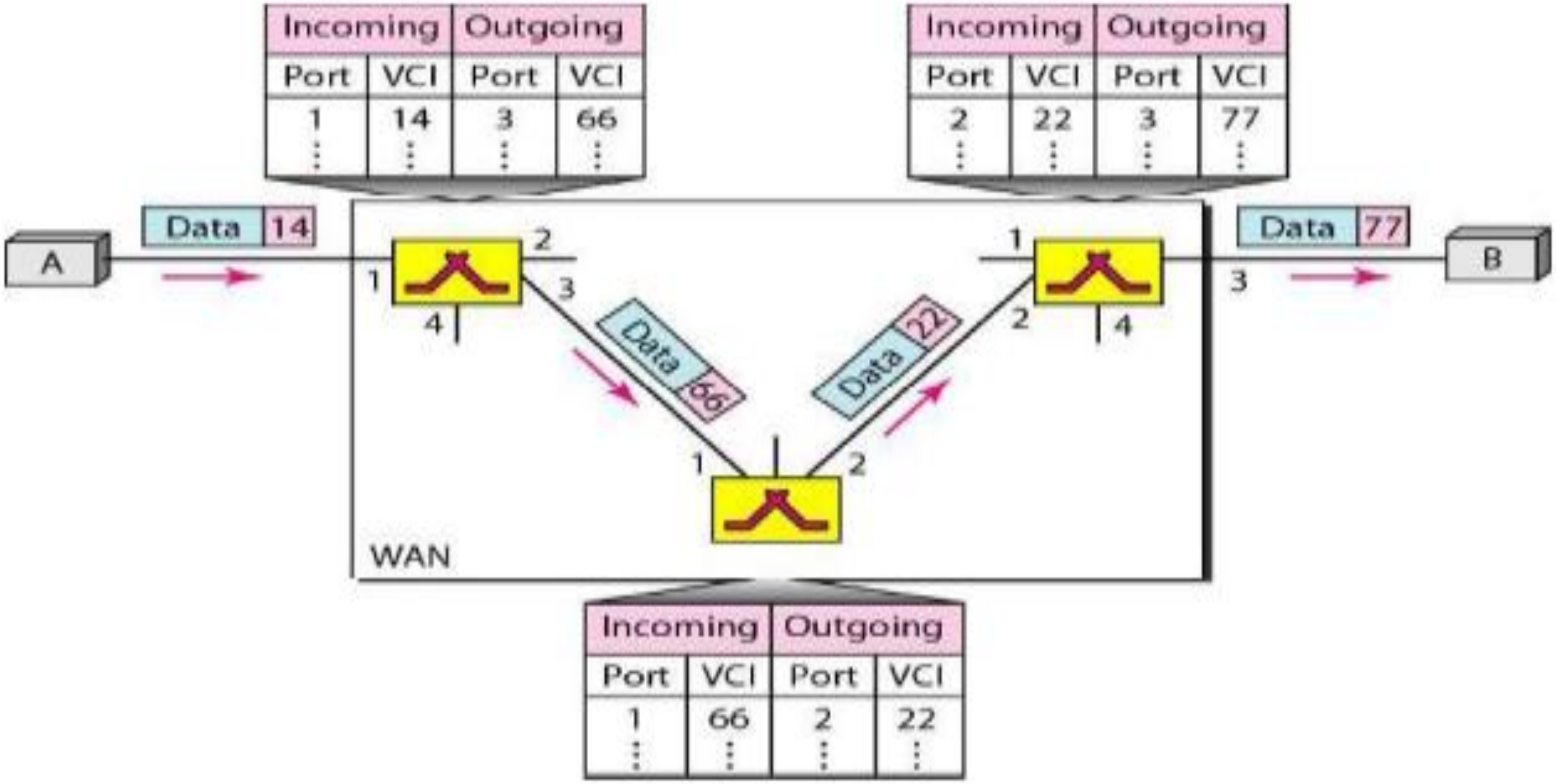


Three Phases

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network:

- setup
- data transfer
- teardown.

To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns.



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66
⋮	⋮	⋮	⋮

Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77
⋮	⋮	⋮	⋮

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22
⋮	⋮	⋮	⋮

The data transfer phase is active until the source sends all its frames to the destination. The procedure at the switch is the same for each frame of a message. The process creates a virtual circuit, not a real circuit, between the source and destination.

Logical Addressing

- The Internet addresses are 32 bits in length; this gives us a maximum of 2^32 addresses. These addresses are referred to as IPv4 (IP version 4) addresses or simply IP addresses.
- The need for more addresses, in addition to other concerns about the IP layer, motivated a new design of the IP layer called the new generation of IP or IPv6 (lP version 6).
- In this version, the Internet uses 128-bit addresses that give much greater flexibility in address allocation. These addresses are referred to as IPv6 (IP version 6) addresses.

Types Of IP Address

1.Static IP Address-

- Static IP Address is an IP Address that once assigned to a network element always remains the same.
- They are configured manually.

2. Dynamic IP Address-

- Dynamic IP Address is a temporarily assigned IP Address to a network element.
- It can be assigned to a different device if it is not in use.
- DHCP or PPPoE assigns dynamic IP addresses.
- Dynamic Host Configuration Protocol
- Point to point protocol over ethernet

IPv4 ADDRESSES

An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.

Address Space

A protocol such as IPv4 that defines addresses has an address space. An address space is the total number of addresses used by the protocol.

If a protocol uses N bits to define an address, the address space is 2^N.

The address space of IPv4 is 2^32 or 4,294,967,296.

Notations

There are two types of notations to show an IPv4 address: binary notation and dotted-decimal notation.

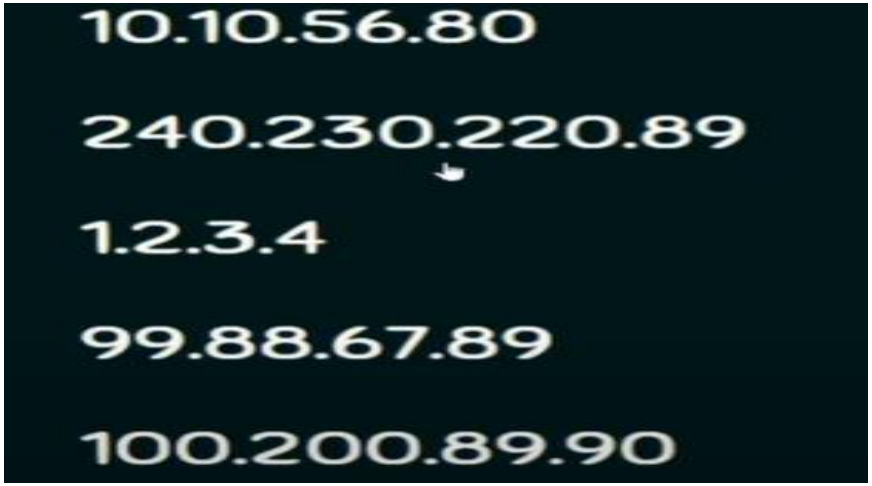
Binary Notation

In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. The following is an example of an IPv4 address in binary notation: 01110101 10010101 00011101 00000010

Dotted-Decimal Notation

To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted-decimal notation of the above address: 117.149.29.2

Valid and Invalid IP Addresses



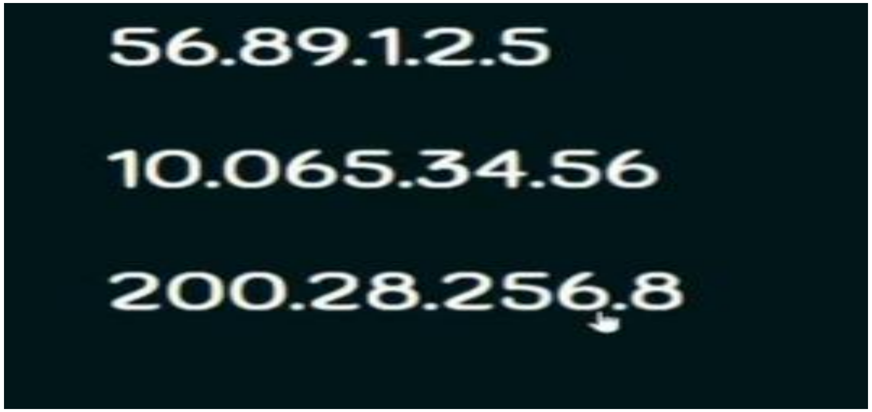
10.10.56.80

240.230.220.89

1.2.3.4

99.88.67.89

100.200.89.90

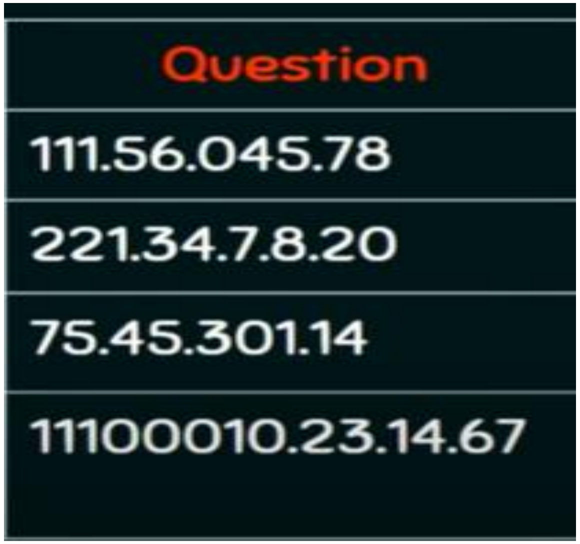


56.89.1.2.5

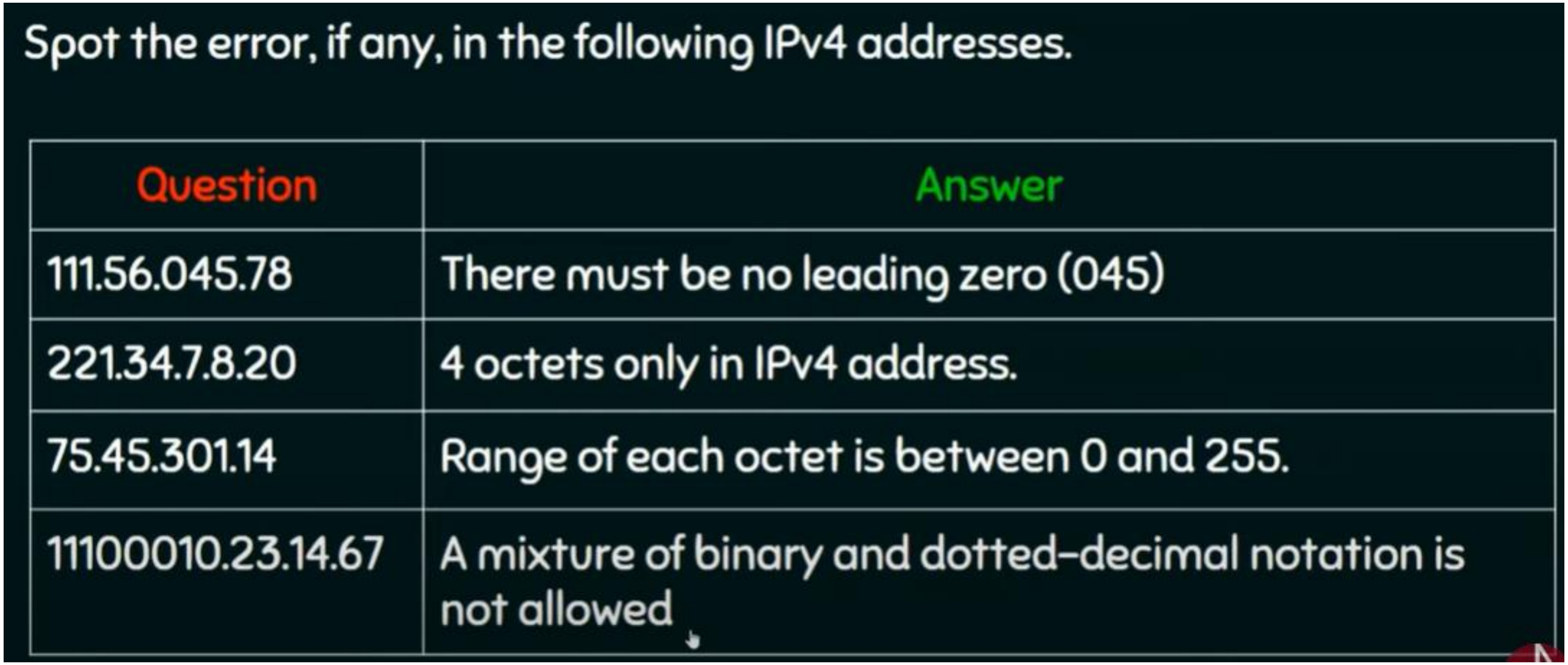
10.065.34.56

200.28.256.8

Spot the errors if any



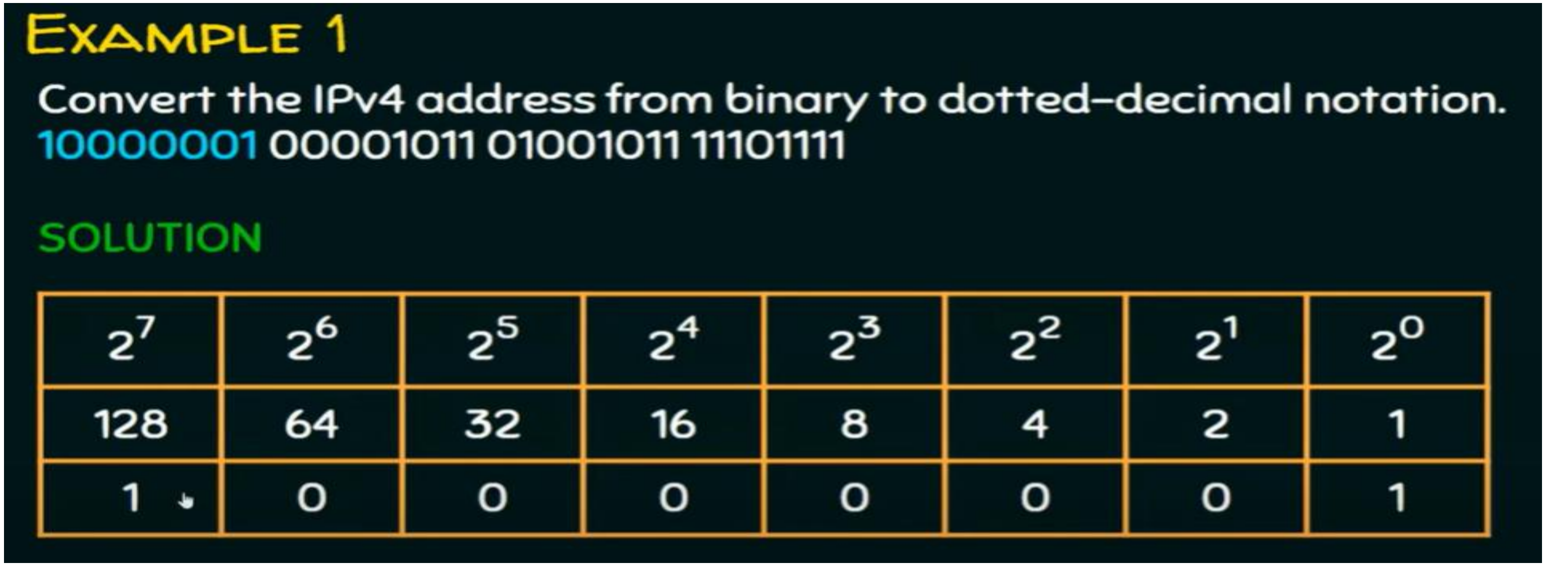
Question
111.56.045.78
221.34.7.8.20
75.45.301.14
11100010.23.14.67



Spot the error, if any, in the following IPv4 addresses.

Question	Answer
111.56.045.78	There must be no leading zero (045)
221.34.7.8.20	4 octets only in IPv4 address.
75.45.301.14	Range of each octet is between 0 and 255.
11100010.23.14.67	A mixture of binary and dotted-decimal notation is not allowed

Binary to Decimal



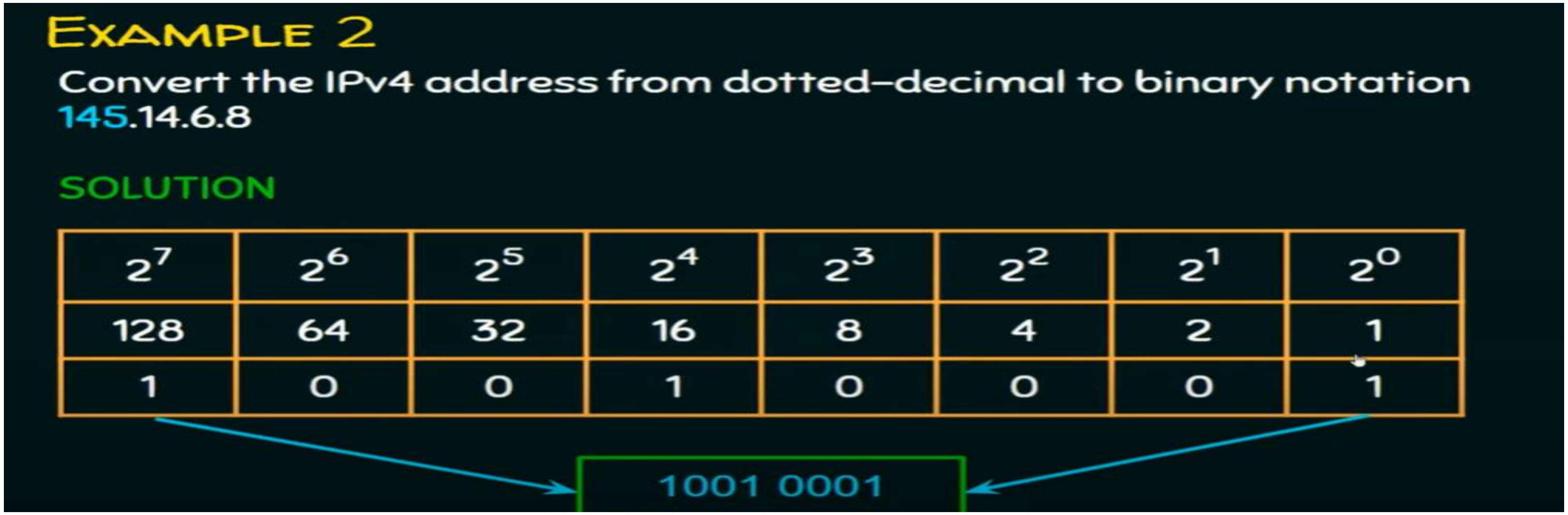
EXAMPLE 1

Convert the IPv4 address from binary to dotted-decimal notation.
10000001 00001011 01001011 11101111

SOLUTION

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

Decimal to Binary



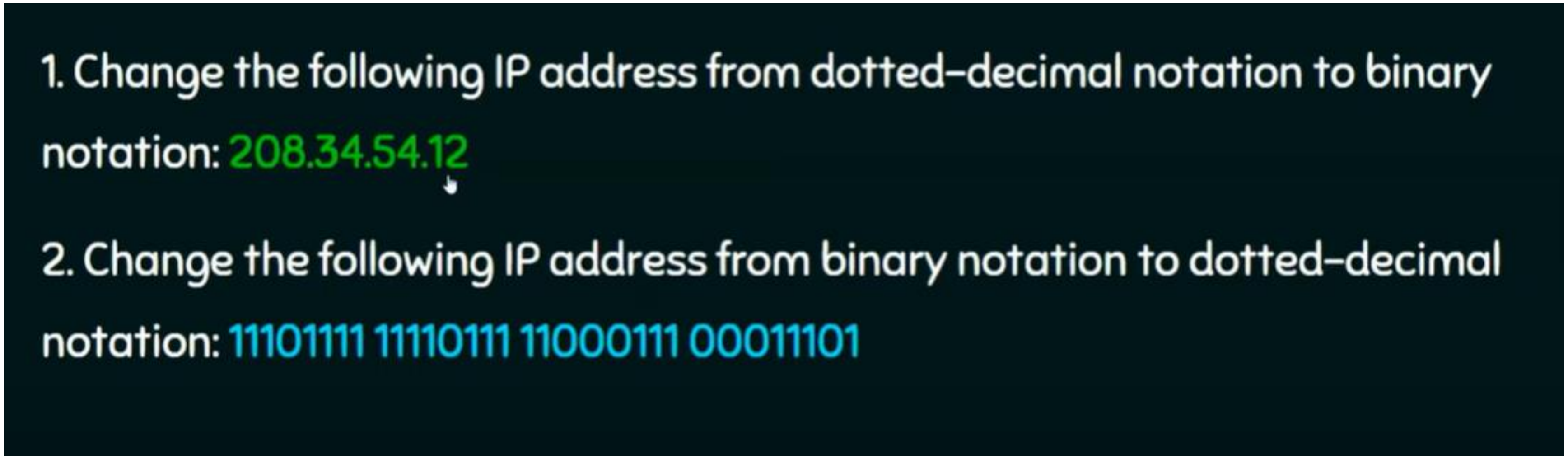
EXAMPLE 2

Convert the IPv4 address from dotted-decimal to binary notation
145.14.6.8

SOLUTION

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

1001 0001



1. Change the following IP address from dotted-decimal notation to binary notation: 208.34.54.12

2. Change the following IP address from binary notation to dotted-decimal notation: 11101111 11110111 11000111 00011101

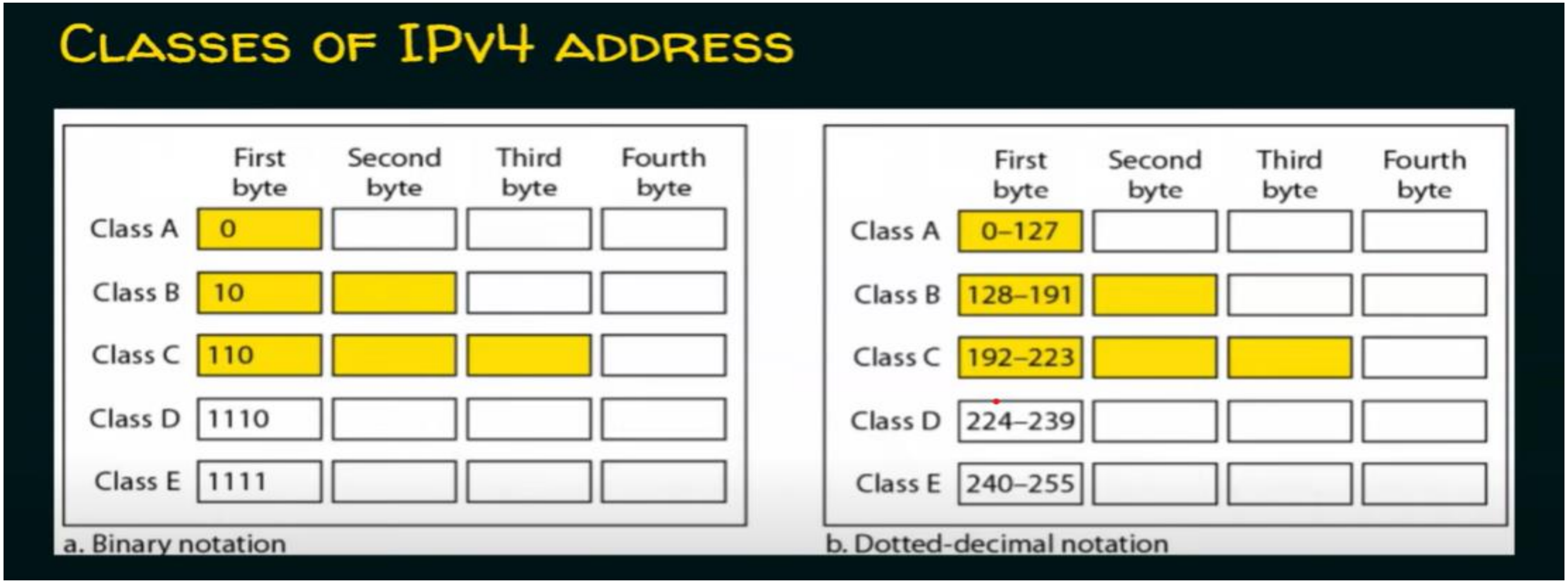
IP Addressing-

There are two systems in which IP Addresses are classified-

- Classful Addressing System
- Classless Addressing System/Classless Interdomain Routing(CIDR)

Classful Addressing System:

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 dotted-decimal notation, the first byte defines the class.



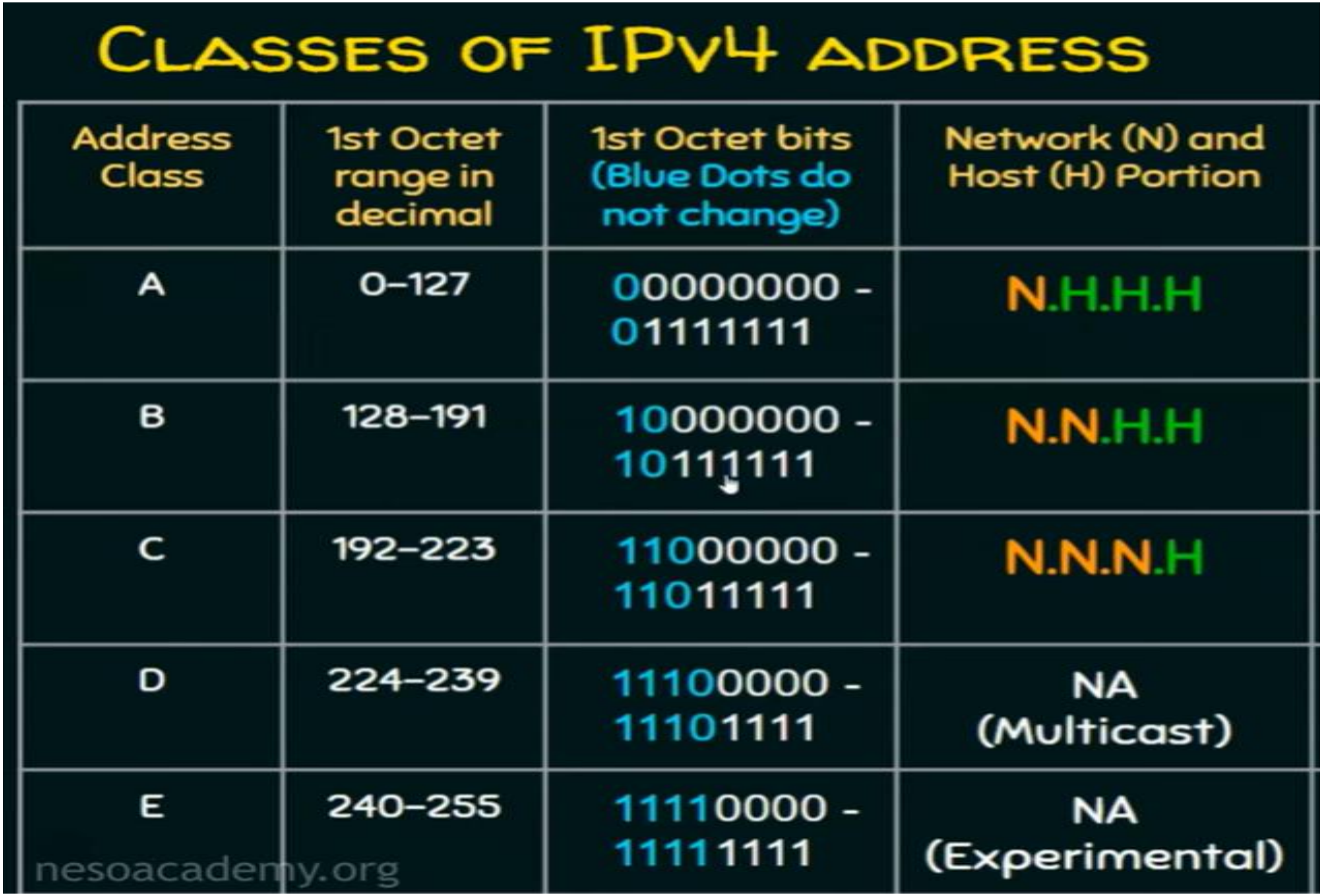
CLASSES OF IPV4 ADDRESS

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10	🟨		
Class C	110	🟨	🟨	
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191	🟨		
Class C	192–223	🟨	🟨	
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation



CLASSES OF IPV4 ADDRESS

Address Class	1st Octet range in decimal	1st Octet bits (Blue Dots do not change)	Network (N) and Host (H) Portion
A	0–127	00000000 - 01111111	N.H.H.H
B	128–191	10000000 - 10111111	N.N.H.H
C	192–223	11000000 - 11011111	N.N.N.H
D	224–239	11100000 - 11101111	NA (Multicast)
E	240–255	11110000 - 11111111	NA (Experimental)

Class A

Total Number Of IP Addresses

Total number of IP Addresses available in class A

= Numbers possible due to remaining available 31 bits

= 2^{31}

Total Number Of Networks

Total number of networks available in class A

= Numbers possible due to remaining available 7 bits in the Net ID – 2

= $2^7 - 2$ (**0 is reserved for the default network and 127 is reserved for loopback addresses.)**

= 126

Total Number Of Hosts

Total number of hosts that can be configured in class A

= Numbers possible due to available 24 bits in the Host ID – 2

= $2^{24} - 2$

(**Network Address: The first address (where all host bits are 0) represents the network itself and cannot be assigned to a host.**

Broadcast Address: The last address (where all host bits are 1) is used to broadcast messages to all hosts in the network and cannot be assigned to any single host.)

Class B:

Total Number Of IP Addresses

Total number of IP Addresses available in class B
= Numbers possible due to remaining available 30 bits
= 2^{30}

Total Number Of Networks

Total number of networks available in class B
= Numbers possible due to remaining available 14 bits in the Net ID
= 2^{14}

Total Number Of Hosts

Total number of hosts that can be configured in class B
= Numbers possible due to available 16 bits in the Host ID – 2
= $2^{16} – 2$

Class C

Total Number Of IP Addresses-

Total number of IP Addresses available in class C

= Numbers possible due to remaining available 29 bits

= 2^{29}

Total Number Of Networks-

Total number of networks available in class C

= Numbers possible due to remaining available 21 bits in the Net ID

= 2^{21}

Total Number Of Hosts-

Total number of hosts that can be configured in class C

= Numbers possible due to available 8 bits in the Host ID – 2

= $2^8 – 2$

Class D

Total Number Of IP Addresses

Total number of IP Addresses available in class D

= Numbers possible due to remaining available 28 bits

= 2^{28}

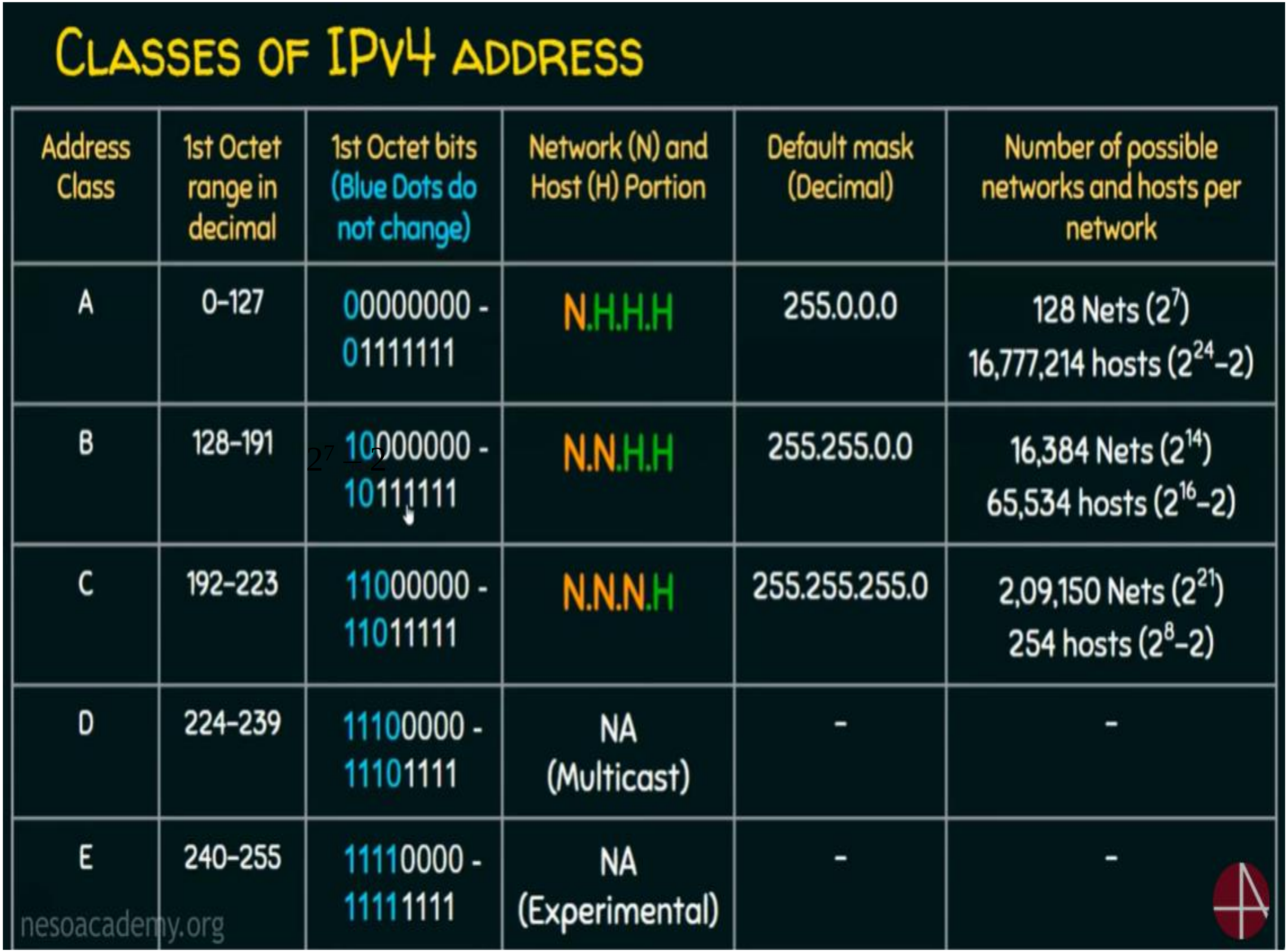
Class E

Total Number Of IP Addresses

Total number of IP Addresses available in class E

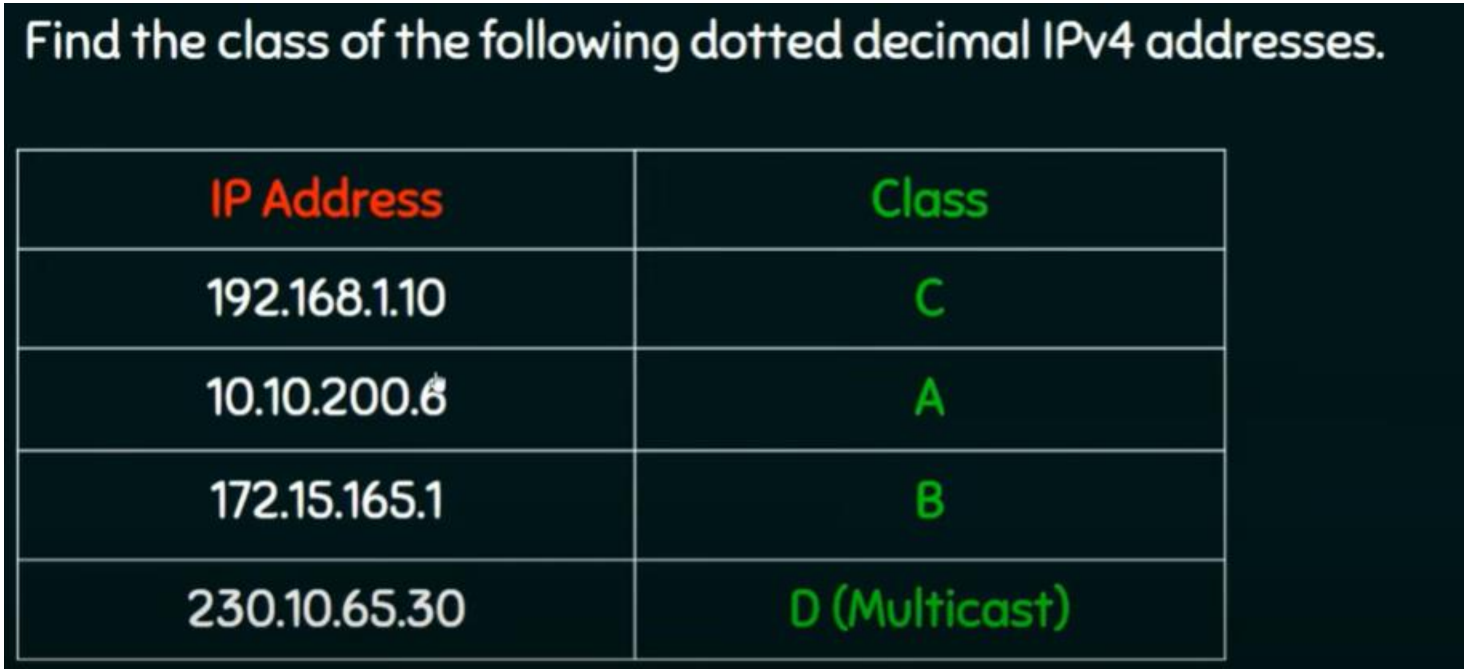
= Numbers possible due to remaining available 28 bits

= 2^{28}



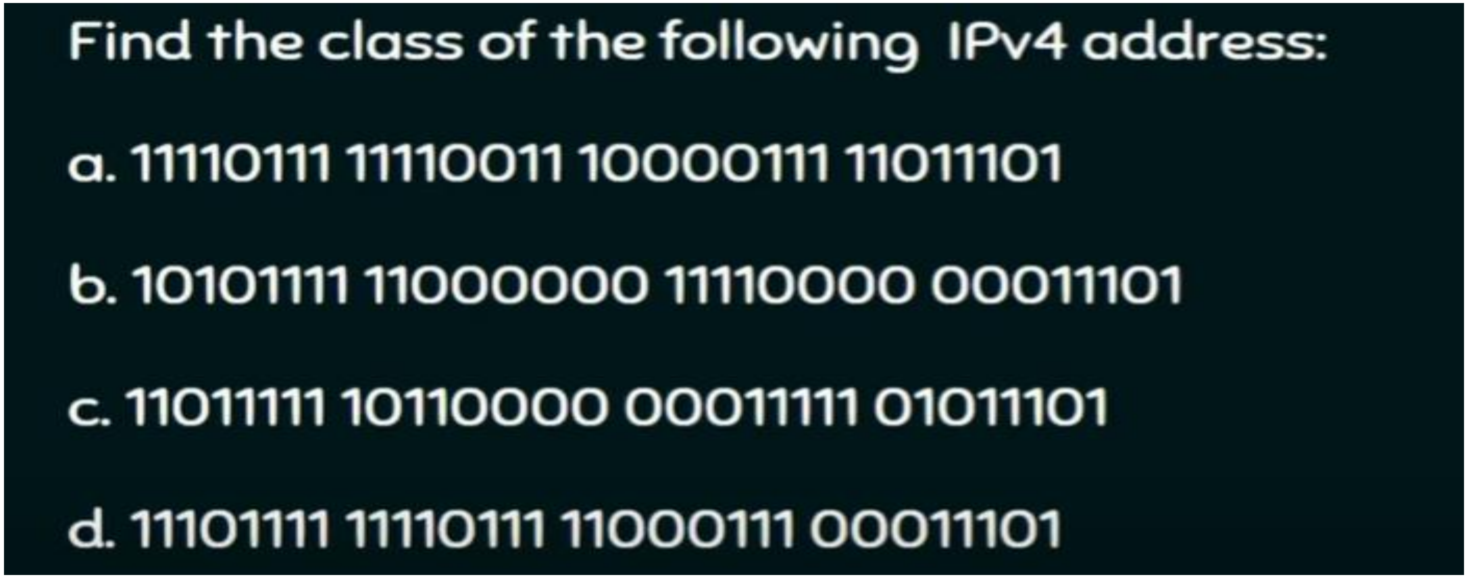
Classes of IPv4 address

Address Class	1st Octet range in decimal	1st Octet bits (Blue Dots do not change)	Network (N) and Host (H) Portion	Default mask (Decimal)	Number of possible networks and hosts per network
A	0–127	00000000 - 01111111	N.H.H.H	255.0.0.0	128 Nets (2^7) 16,777,214 hosts (2^{24}–2)
B	128–191	$2^7 - 2$ 10000000 - 10111111	N.N.H.H	255.255.0.0	16,384 Nets (2^{14}) 65,534 hosts (2^{16}–2)
C	192–223	11000000 - 11011111	N.N.N.H	255.255.255.0	2,09,150 Nets (2^{21}) 254 hosts (2^8–2)
D	224–239	11100000 - 11101111	NA (Multicast)	-	-
E	240–255	11110000 - 11111111	NA (Experimental)	-	-



Find the class of the following dotted decimal IPv4 addresses.

IP Address	Class
192.168.1.10	C
10.10.200.6	A
172.15.165.1	B
230.10.65.30	D (Multicast)



Find the class of the following IPv4 address:

a. 11110111 11110011 10000111 11011101

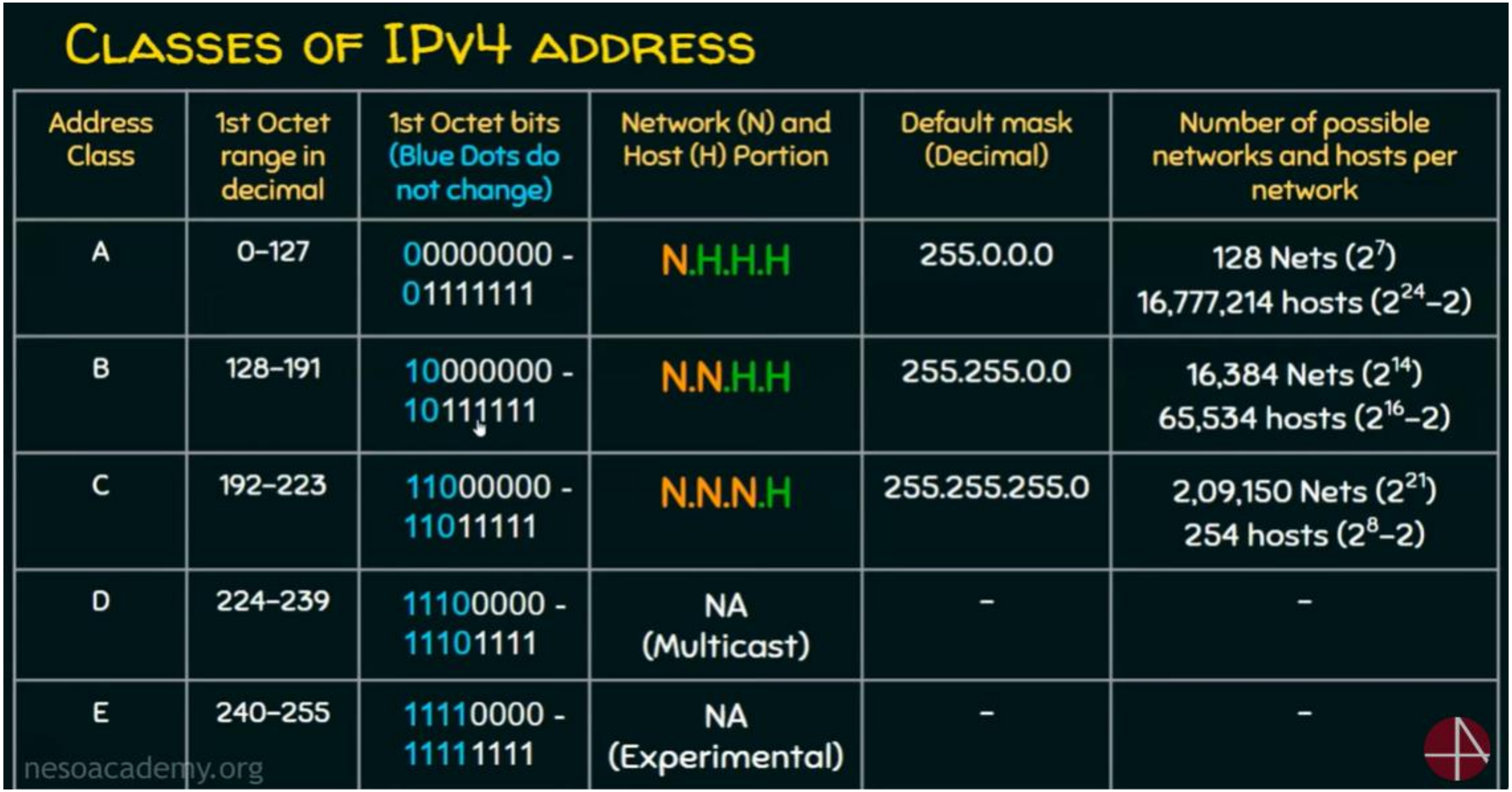
b. 10101111 11000000 11110000 00011101

c. 11011111 10110000 00011111 01011101

d. 11101111 11110111 11000111 00011101

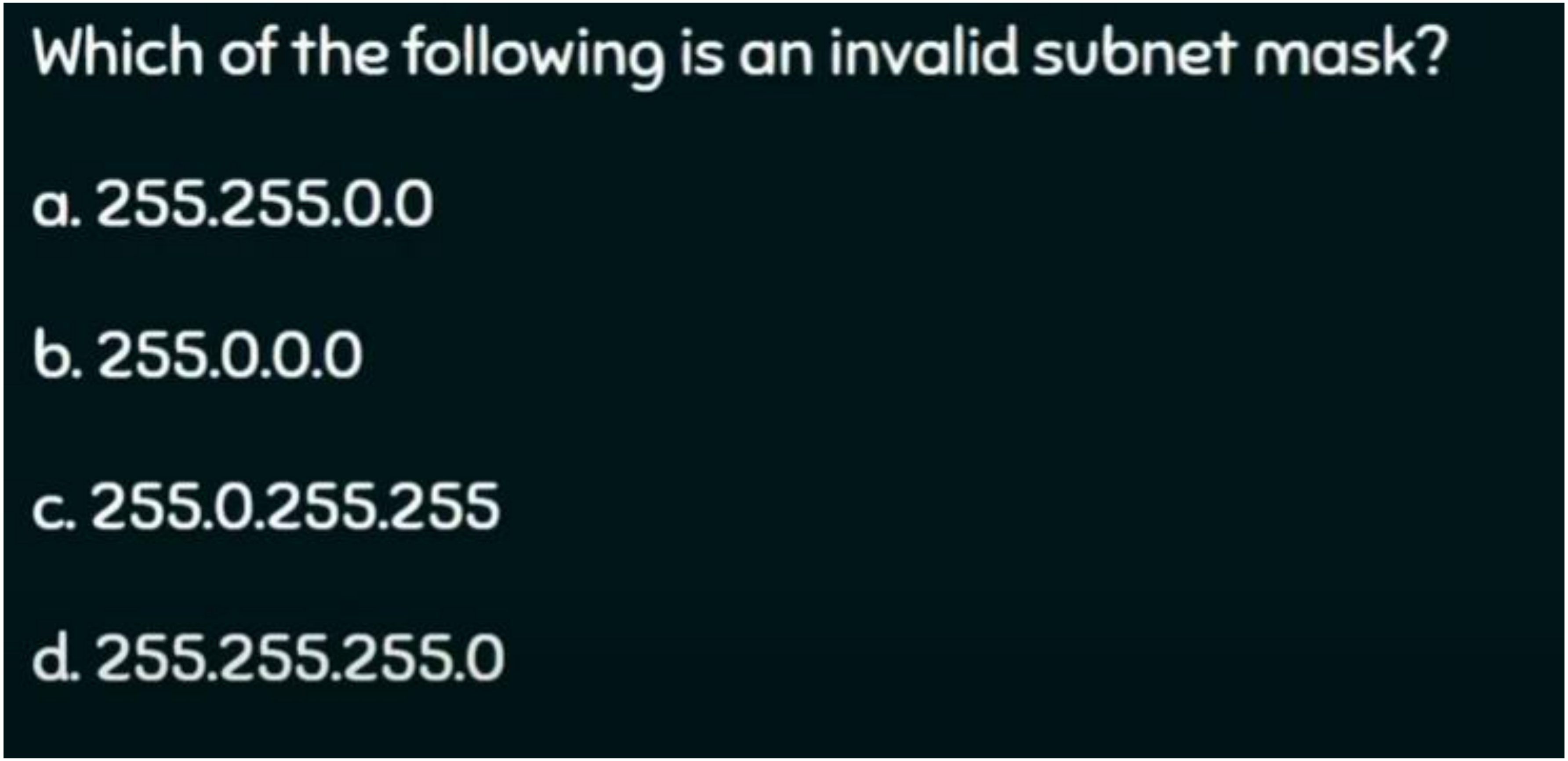
Subnet Mask

A 32-bit address that distinguishes the network address from the host address is called subnet mask. This indicates which part of the IP address belongs in the host section and which part belongs in the network section.



CLASSES OF IPV4 ADDRESS

Address Class	1st Octet range in decimal	1st Octet bits (Blue Dots do not change)	Network (N) and Host (H) Portion	Default mask (Decimal)	Number of possible networks and hosts per network
A	0–127	00000000 - 01111111	N.H.H.H	255.0.0.0	128 Nets (2^7) 16,777,214 hosts (2^{24}–2)
B	128–191	10000000 - 10111111	N.N.H.H	255.255.0.0	16,384 Nets (2^{14}) 65,534 hosts (2^{16}–2)
C	192–223	11000000 - 11011111	N.N.N.H	255.255.255.0	2,09,150 Nets (2^{21}) 254 hosts (2^8–2)
D	224–239	11100000 - 11101111	NA (Multicast)	–	–
E	240–255	11110000 - 11111111	NA (Experimental)	–	–



Which of the following is an invalid subnet mask?

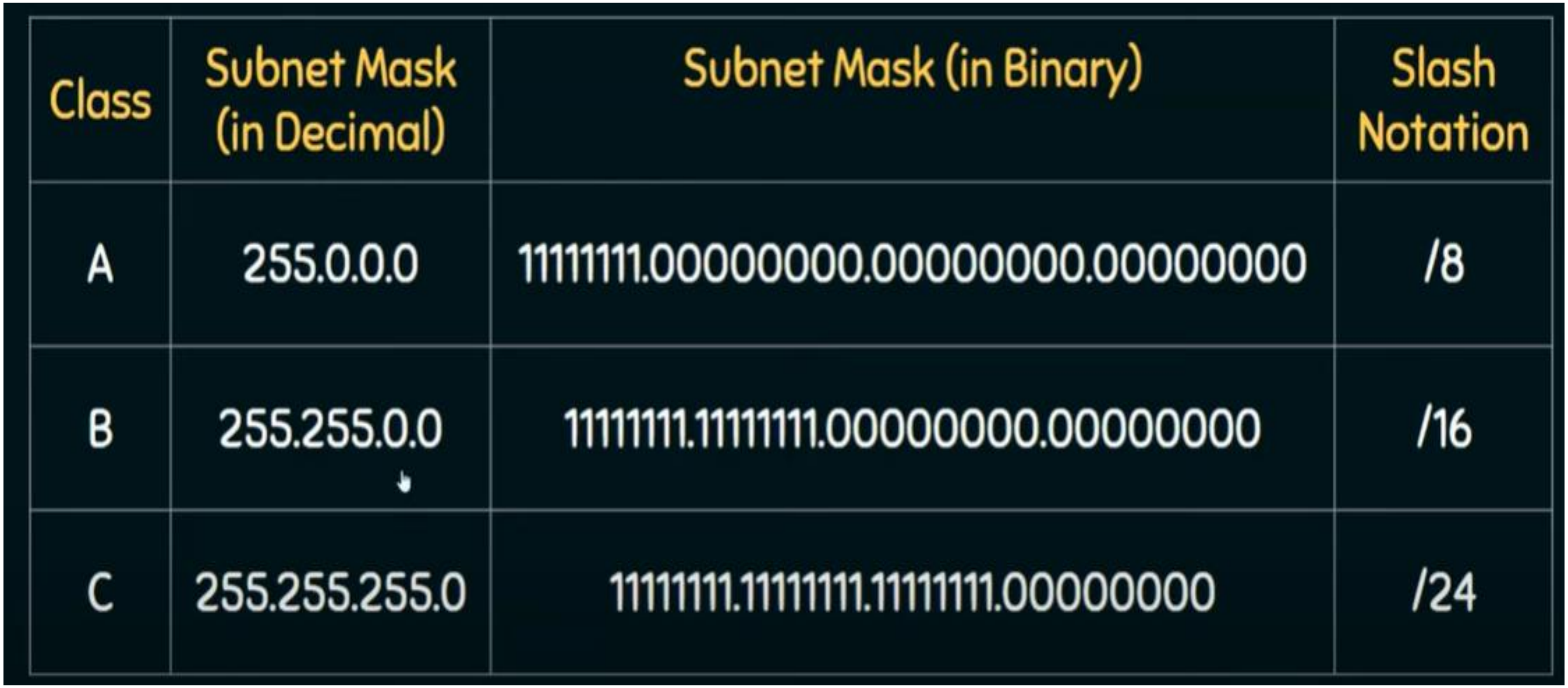
a. 255.255.0.0

b. 255.0.0.0

c. 255.0.255.255

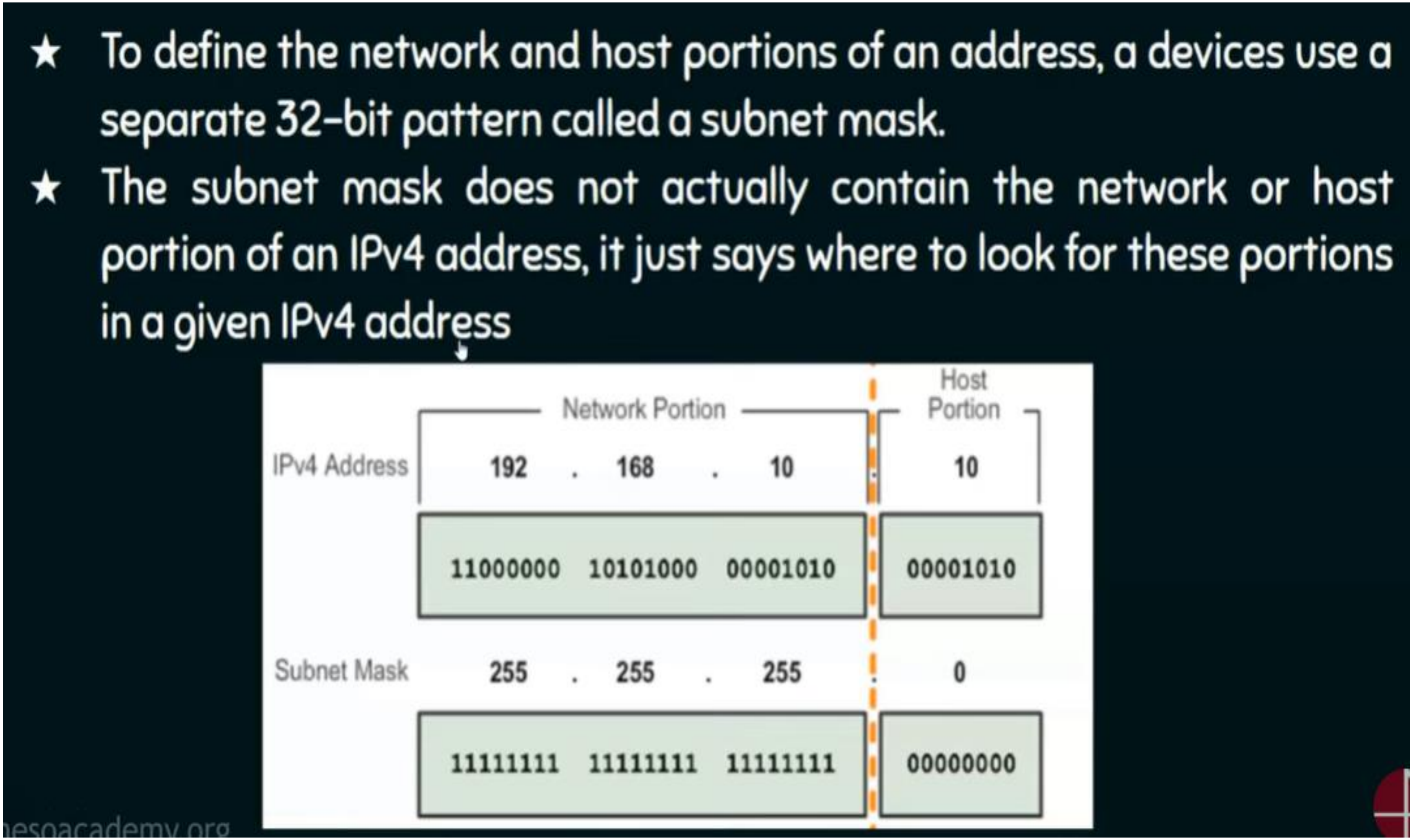
d. 255.255.255.0

Slash Notation/ CIDR Notation



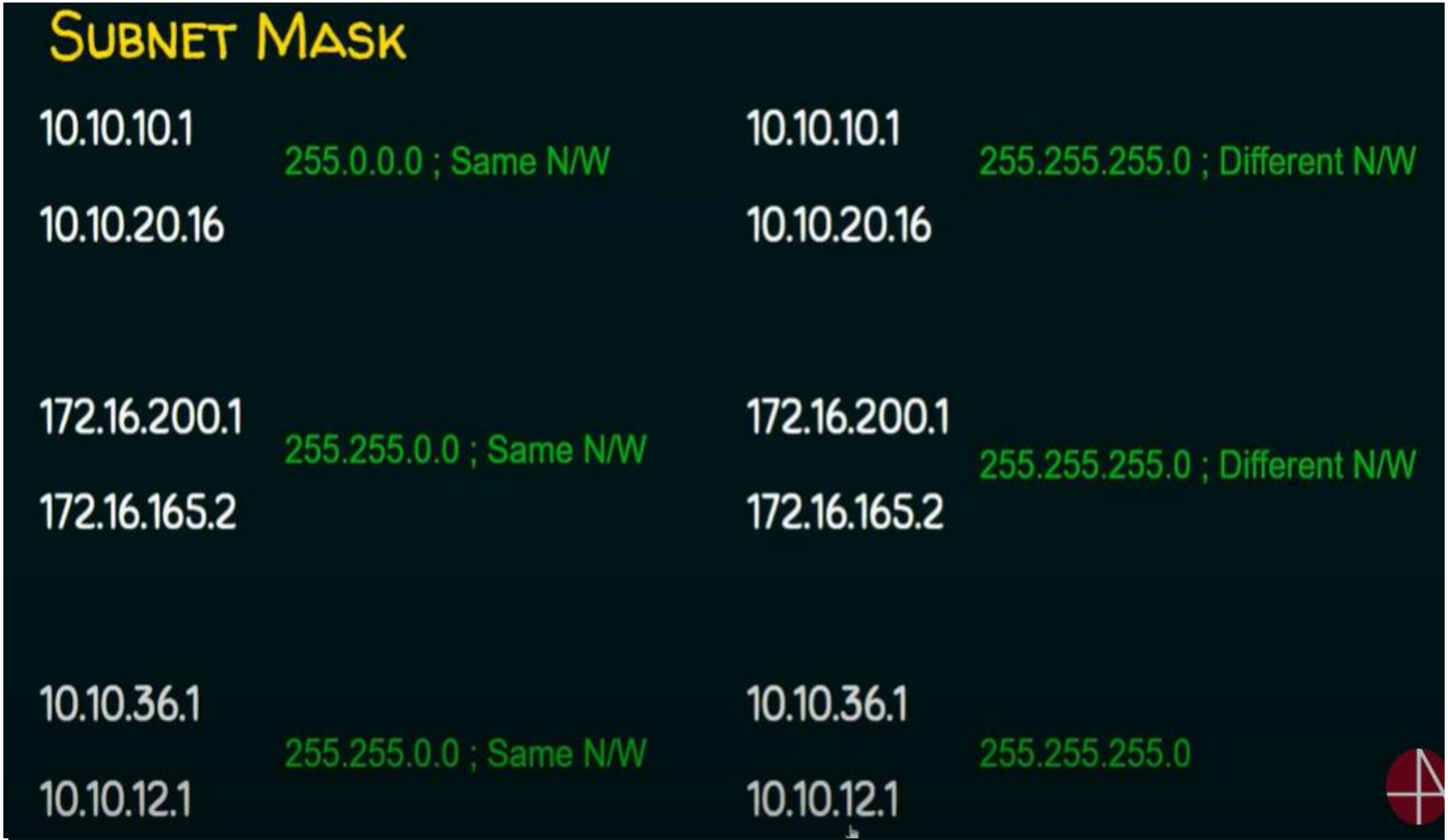
Class	Subnet Mask (in Decimal)	Subnet Mask (in Binary)	Slash Notation
A	255.0.0.0	11111111.00000000.00000000.00000000	/8
B	255.255.0.0	11111111.11111111.00000000.00000000	/16
C	255.255.255.0	11111111.11111111.11111111.00000000	/24

The mask in the form **/n** where n can be 8, 16, or 24 in classful addressing. This notation is also called slash notation or Classless Interdomain Routing (CIDR) notation. The notation is used in classless addressing.



- ★ To define the network and host portions of an address, a devices use a separate 32-bit pattern called a subnet mask.
- ★ The subnet mask does not actually contain the network or host portion of an IPv4 address, it just says where to look for these portions in a given IPv4 address

	Network Portion			Host Portion
IPv4 Address	192 .	168 .	10	10
	11000000	10101000	00001010	00001010
Subnet Mask	255 .	255 .	255	0
	11111111	11111111	11111111	00000000



Subnet Mask

10.10.10.1
10.10.20.16
255.0.0.0 ; Same N/W

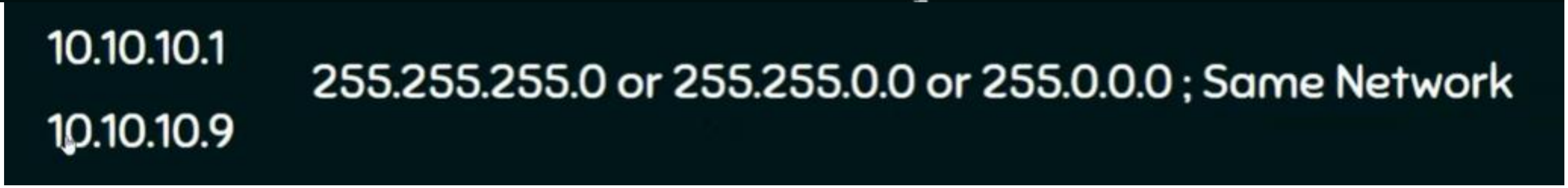
10.10.10.1
10.10.20.16
255.255.255.0 ; Different N/W

172.16.200.1
172.16.165.2
255.255.0.0 ; Same N/W

172.16.200.1
172.16.165.2
255.255.255.0 ; Different N/W

10.10.36.1
10.10.12.1
255.255.0.0 ; Same N/W

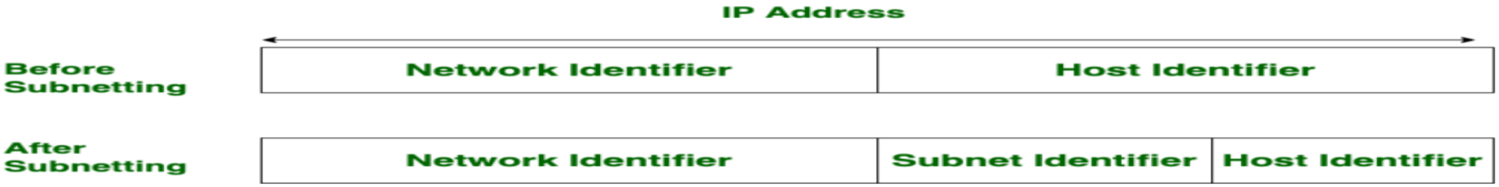
10.10.36.1
10.10.12.1
255.255.255.0

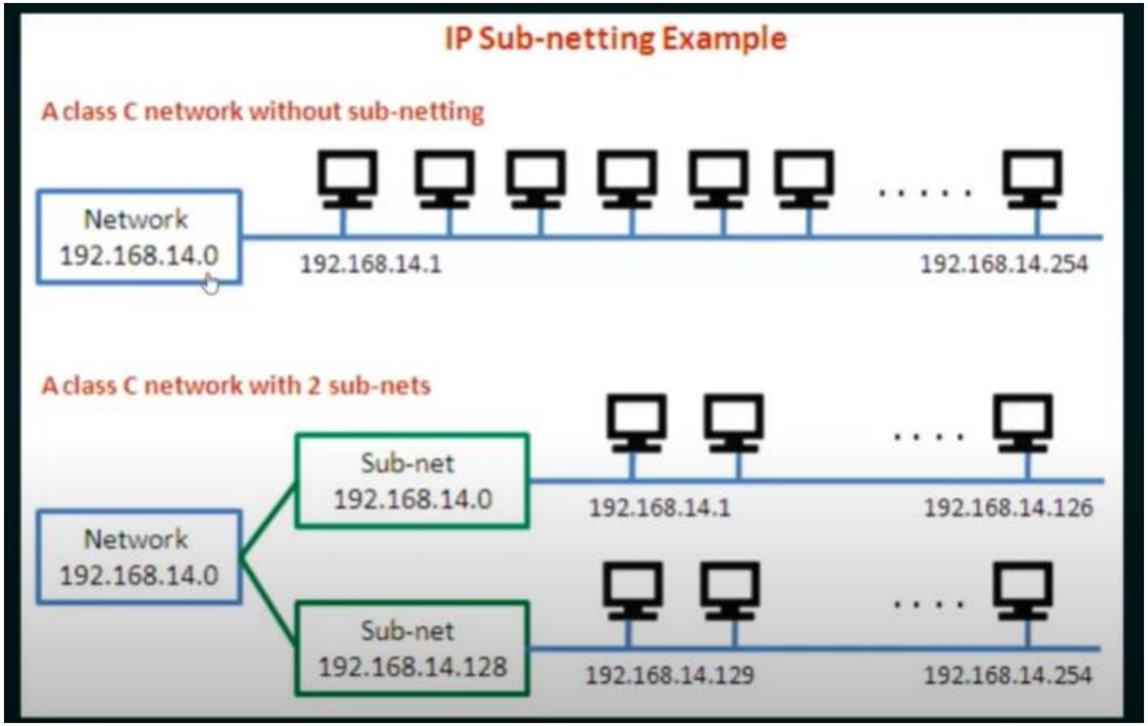


10.10.10.1
10.10.10.9
255.255.255.0 or 255.255.0.0 or 255.0.0.0 ; Same Network

Subnetting

It is the procedure to divide the network into sub-networks or small networks, these smaller networks are known as subnets. In a subnet, a few bits from the host portion are used to design small-sized subnetworks from the original network.



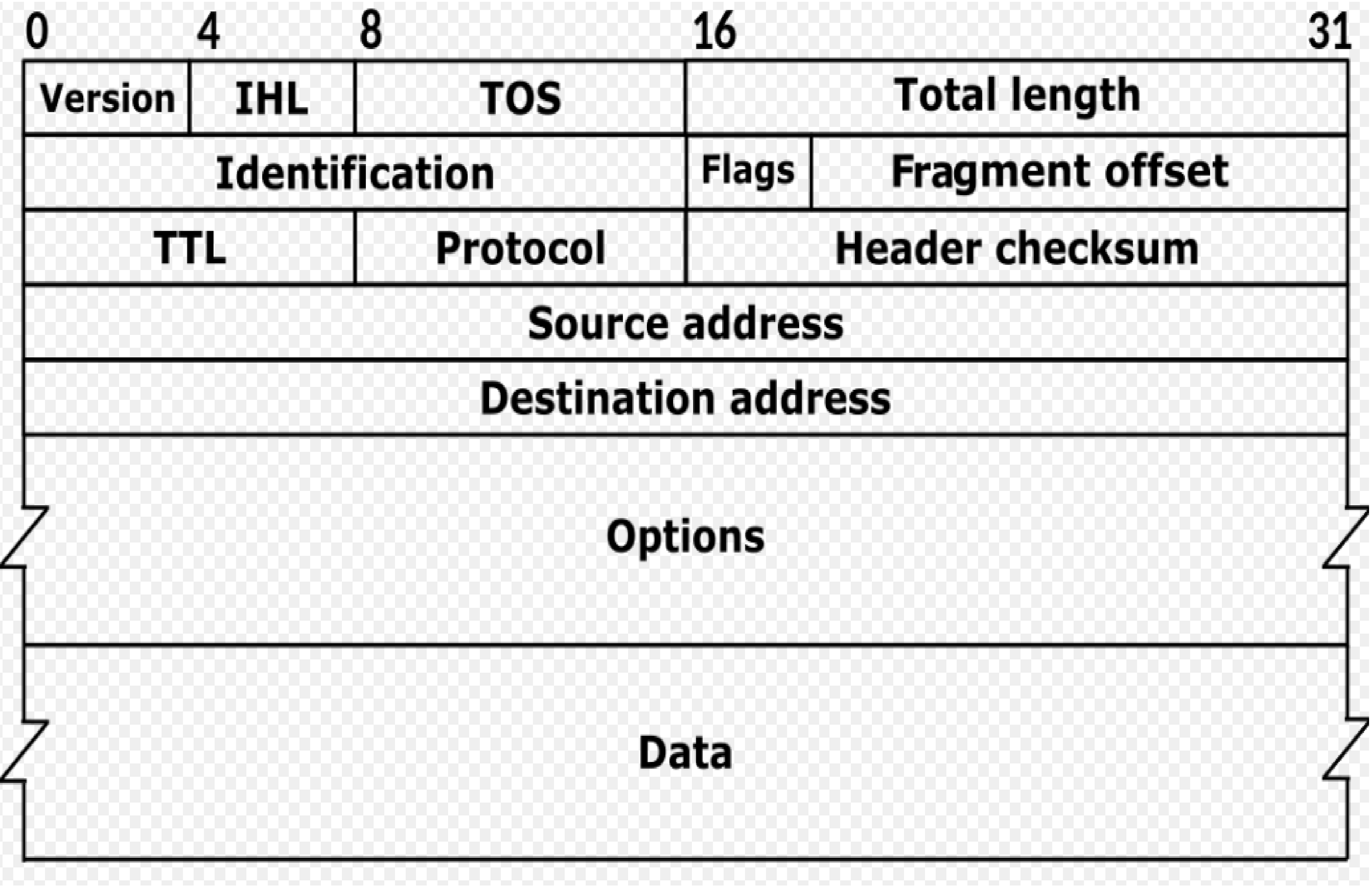


subnets are an area of the network, while subnet masks help devices determine the network area to which they belong.

Supernetting

- It is the procedure to combine small networks into larger spaces. In subnetting, Network addresses' bits are increased. on the other hand, in supernetting, Host addresses' bits are increased.

IPV4 Header Format



VERSION: Version of the IP protocol (4 bits), which is 4 for IPv4

HLEN: IP header length (4 bits),

Type of service: Low Delay, High Throughput, Reliability (8 bits)

Total Length: Length of header + Data

Identification: Unique Packet Id

Flags: 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)

Fragment Offset: Represents the number of Data Bytes ahead of the particular fragment

Time to live: Datagram’s lifetime (8 bits),

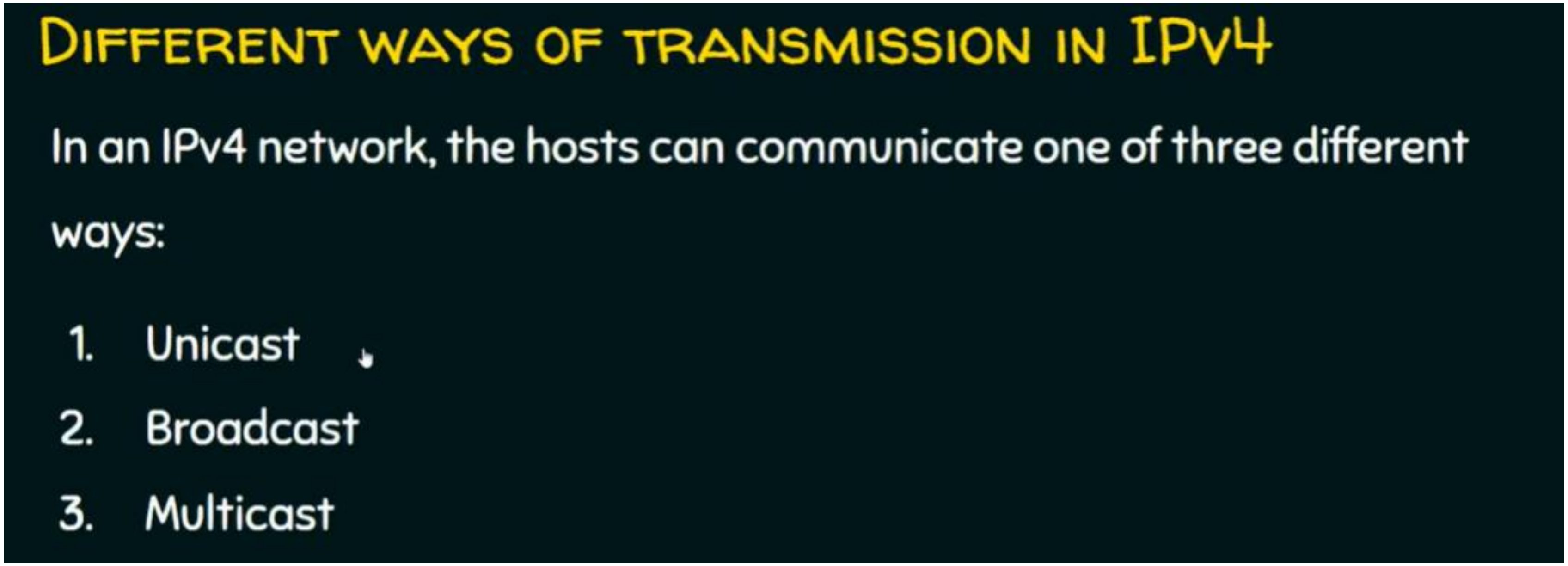
Protocol: Name of the protocol to which the data is to be passed (8 bits)

Header Checksum: 16 bits header checksum for checking errors in the datagram header

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.



DIFFERENT WAYS OF TRANSMISSION IN IPv4

In an IPv4 network, the hosts can communicate one of three different ways:

1. Unicast
2. Broadcast
3. Multicast

Unicast transmission

The process of sending a packet from one host to an individual host.

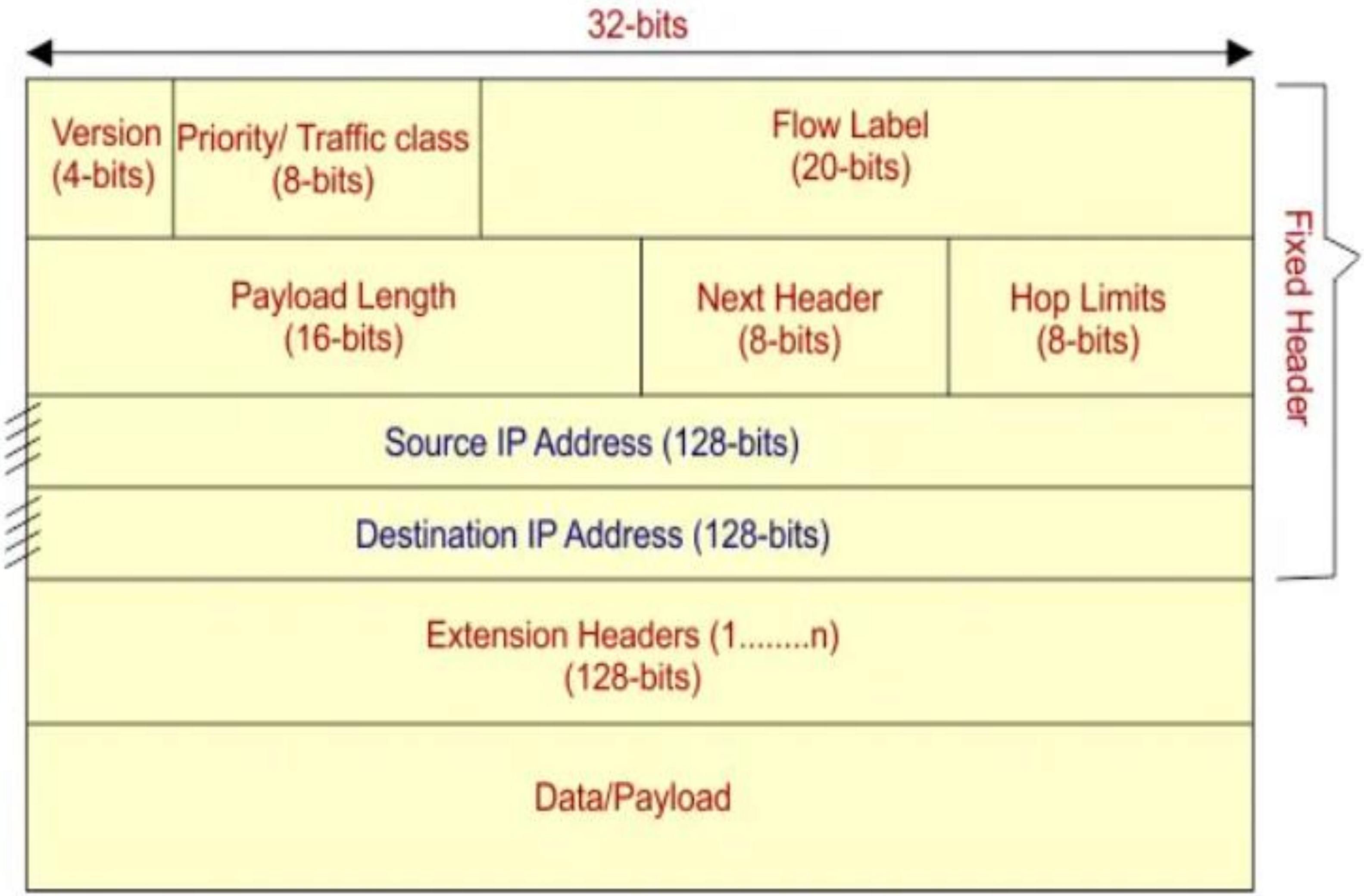
Broadcast transmission

The process of sending a packet from one host to all host in the network

Multicast Transmission

The process of sending a packet from one host to a selected group of host possibly in different networks.

IPV6



32-bits

Version (4-bits)

Priority/ Traffic class (8-bits)

Flow Label (20-bits)

Payload Length (16-bits)

Next Header (8-bits)

Hop Limits (8-bits)

Source IP Address (128-bits)

Destination IP Address (128-bits)

Extension Headers (1........n) (128-bits)

Data/Payload

Fixed Header

Version (4-bits): Indicates version of Internet Protocol

Traffic Class (8-bits): The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded.

Flow Label (20-bits): Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers.

Payload Length (16-bits): It is a 16-bit field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers(if any) and an upper-layer packet.

Next Header (8-bits): Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.

Hop Limit (8-bits): Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0.

Source Address (128-bits): Source Address is the 128-bit IPv6 address of the original source of the packet.

Destination Address (128-bits): The destination Address field indicates the IPv6 address of the final destination(in most cases).

Extension Headers: IPv6 extension headers contains supplementary information used by network devices (such as routers, switches, and endpoint hosts) to decide how to direct or process an IPv6 packet.

Address Mapping :

Address Resolution Protocol(IP to MAC)

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

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

Mapping Physical to Logical Address: RARP, BOOTP, and DHCP

RARP:

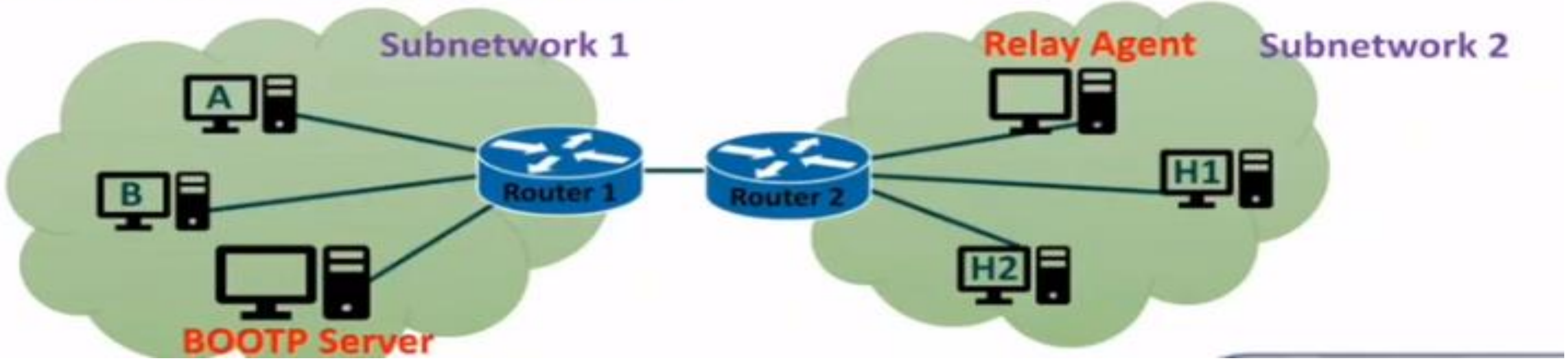
- RARP stands for Reverse Address Resolution Protocol.
- If the host wants to know its IP address, then it broadcast the RARP query packet that contains its physical address to the entire network. A RARP server on the network recognizes the RARP packet and responds back with the host IP address.
- The protocol which is used to obtain the IP address from a server is known as Reverse Address Resolution Protocol.
- The message format of the RARP protocol is similar to the ARP protocol.
- Like ARP frame, RARP frame is sent from one machine to another encapsulated in the data portion of a frame.

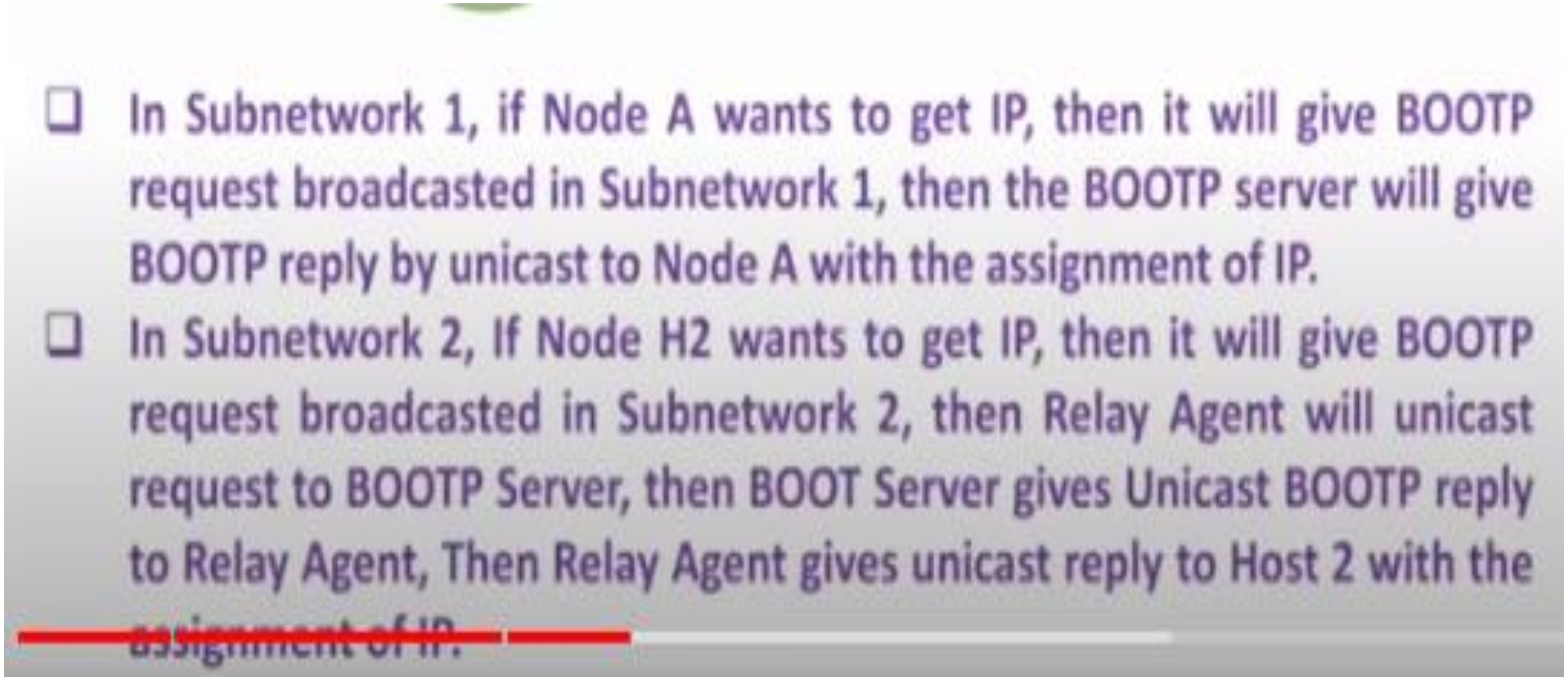
Drawback of RARP: If an administrator has several networks or several subnets, it needs to assign a RARP server for each network or subnet. This is the reason that RARP is almost obsolete.

Two protocols, BOOTP and DHCP, are replacing RARP.

Bootstrap protocol and Dynamic host configuration protocol

❖ Working of BOOTP Protocol

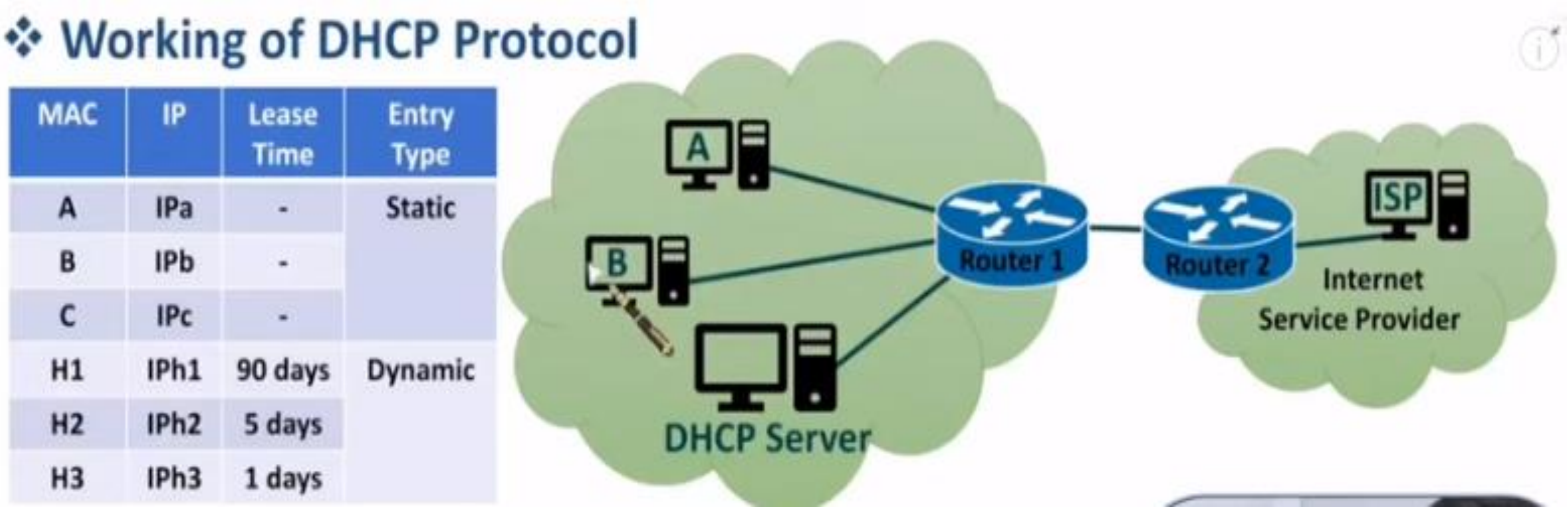




- ❑ In Subnetwork 1, if Node A wants to get IP, then it will give BOOTP request broadcasted in Subnetwork 1, then the BOOTP server will give BOOTP reply by unicast to Node A with the assignment of IP.
- ❑ In Subnetwork 2, If Node H2 wants to get IP, then it will give BOOTP request broadcasted in Subnetwork 2, then Relay Agent will unicast request to BOOTP Server, then BOOT Server gives Unicast BOOTP reply to Relay Agent, Then Relay Agent gives unicast reply to Host 2 with the assignment of IP.

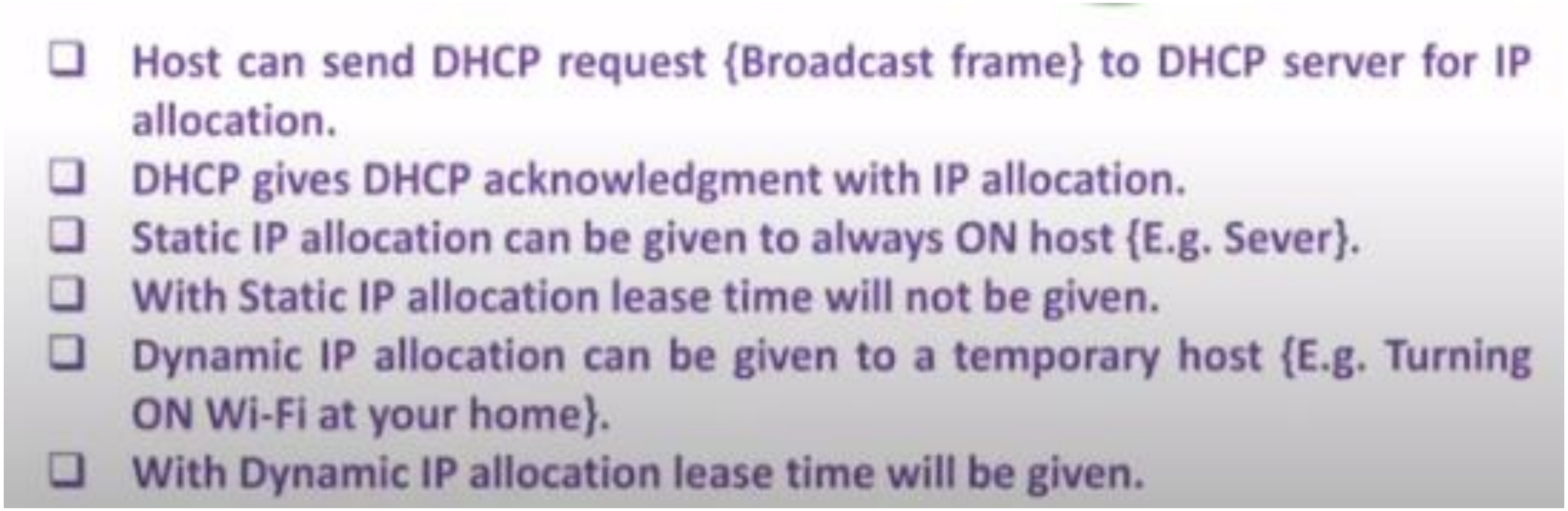
Limitations

BOOTP server uses a static table for IP assignments. Even if a user is not using the network, IP s are occupied by all the hosts , which leads to the shortage of IPs in computer networks.



❖ Working of DHCP Protocol

MAC	IP	Lease Time	Entry Type
A	IPa	-	Static
B	IPb	-	
C	IPc	-	
H1	IPh1	90 days	Dynamic
H2	IPh2	5 days	
H3	IPh3	1 days	



□ Host can send DHCP request {Broadcast frame} to DHCP server for IP allocation.

□ DHCP gives DHCP acknowledgment with IP allocation.

□ Static IP allocation can be given to always ON host {E.g. Sever}.

□ With Static IP allocation lease time will not be given.

□ Dynamic IP allocation can be given to a temporary host {E.g. Turning ON Wi-Fi at your home}.

□ With Dynamic IP allocation lease time will be given.

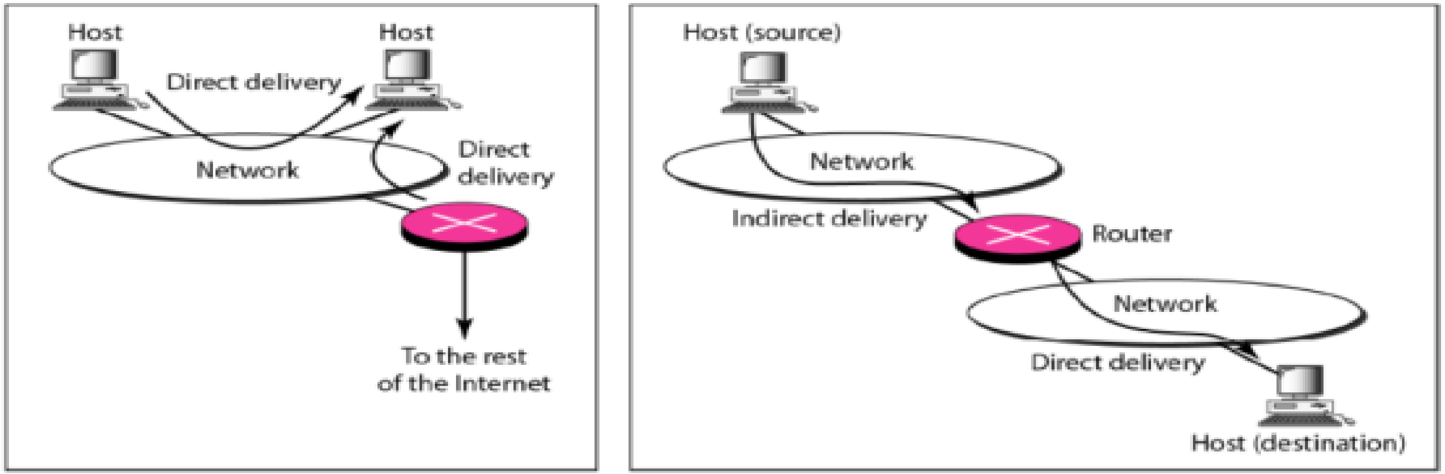
Delivery, Forwarding and Unicast Routing protocols

Delivery:

The network layer supervises the handling of the packets by the underlying physical networks. We define this handling as the delivery of a packet.

□ The delivery of a packet is called direct if the deliverer (host or router) and the destination are on the same network.

□The delivery of a packet is called indirect if the deliverer (host or router) and the destination are on different network.



a. Direct delivery

b. Indirect and direct delivery

Forwarding:

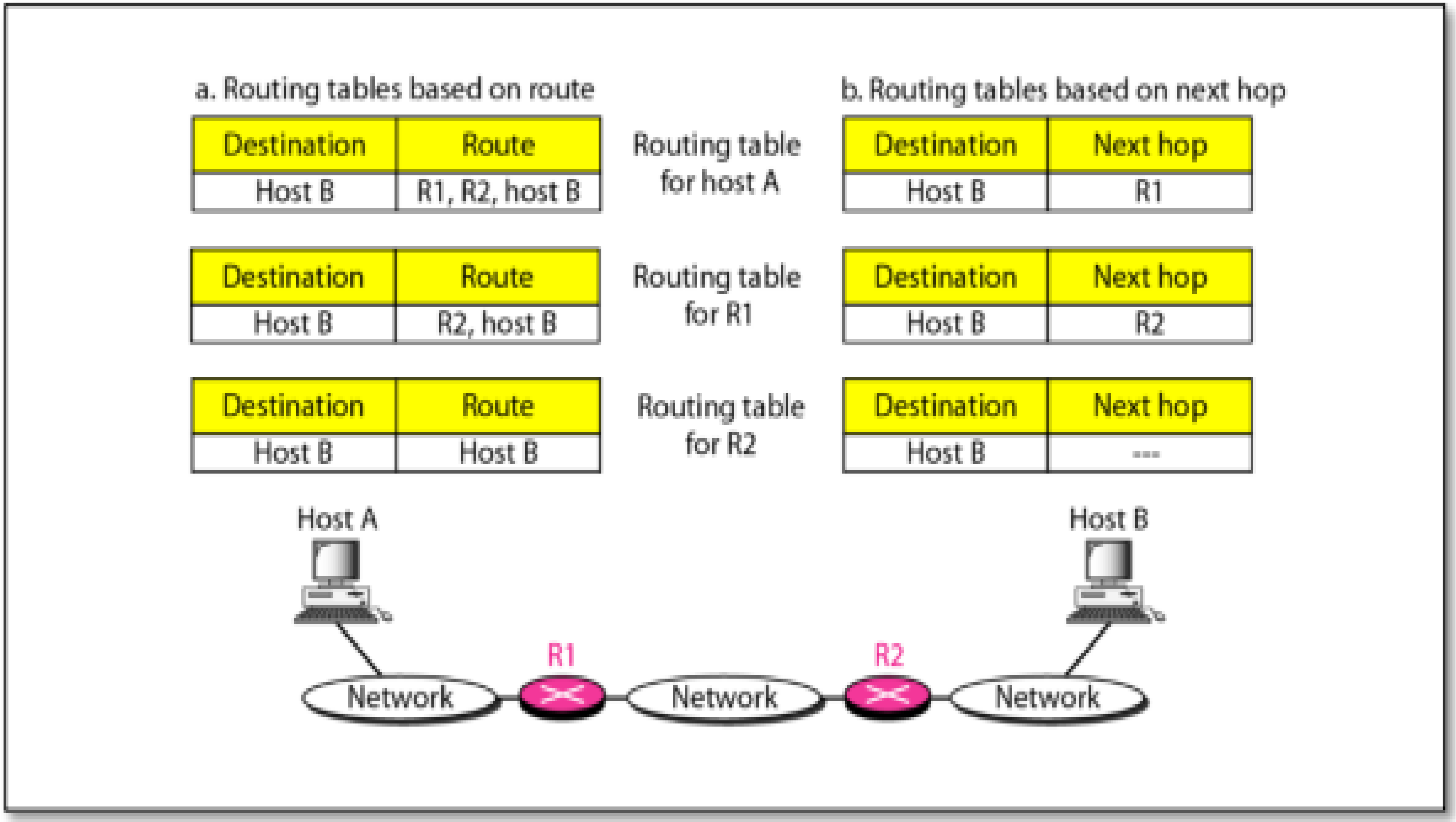
Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.

(i)Forwarding Techniques:

Several techniques can make the size of the routing table manageable and also handle issues such as security. We briefly discuss these methods here.

Next-Hop Method Versus Route Method

One technique to reduce the contents of a routing table is called the next-hop method. In this technique, the routing table holds only the address of the next hop instead of information about the complete route (route method). The entries of a routing table must be consistent with one another.



a. Routing tables based on route

b. Routing tables based on next hop

Routing table for host A

Destination	Route
Host B	R1, R2, host B

Destination	Next hop
Host B	R1

Routing table for R1

Destination	Route
Host B	R2, host B

Destination	Next hop
Host B	R2

Routing table for R2

Destination	Route
Host B	Host B

Destination	Next hop
Host B	---

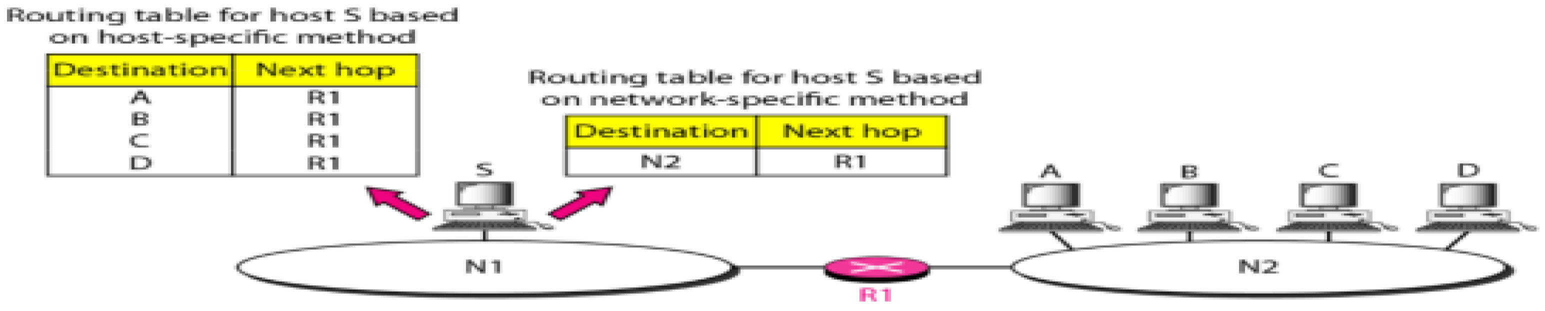
Figure 22.2 Route method versus next-hop method

Network-Specific Method Versus Host-Specific Method:

A second technique to reduce the routing table and simplify the searching process is called the network-specific method.

Here, instead of having an entry for every destination host connected to the same physical network (hostspecific method), we have only one entry that defines the address of the destination network itself. In other words, we treat all hosts connected to the same network as one single entity. For example, if 1000 hosts are attached to the same network, only one entry exists in the routing table instead of 1000.

Figure 22.3 *Host-specific versus network-specific method*



Routing table for host S based on host-specific method

Destination	Next hop
A	R1
B	R1
C	R1
D	R1

Routing table for host S based on network-specific method

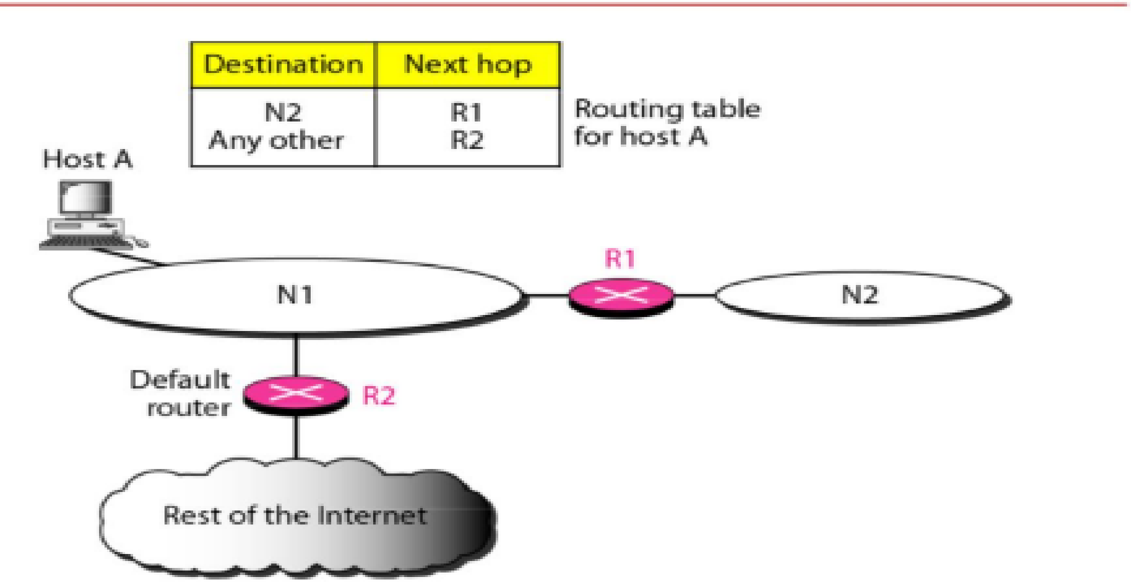
Destination	Next hop
N2	R1

Figure 22.3 Host-specific versus network-specific method

Default Method:

Another technique to simplify routing is called the default method. In the below Figure host A is connected to a network with two routers. Router Rl routes the packets to hosts connected to network N2. However, for the rest of the Internet, router R2 is used. So instead of listing all networks in the entire Internet, host A can just have one entry called the default (normally defined as network address 0.0.0.0).

Figure 22.4 *Default method*



Destination	Next hop
N2	R1
Any other	R2

Routing table for host A

(ii)Forwarding Process:

When a packet arrives at a router’s input link, the router must move the packet to the appropriate output link.

(iii)Routing Table

A host or a router has a routing table with an entry for each destination, or a combination of destinations, to route IP packets.

The routing table can be :

1.Static

2.Dynamic

Static Routing Table: A static routing table contains information entered manually. The administrator enters the route for each destination into the table. When a table is created, it cannot update automatically when there is a change in the Internet. The table must be manually altered by the administrator.

Dynamic Routing Table:

- A dynamic routing table is updated periodically by using one of the dynamic routing protocols such as RIP, OSPF, or BGP.

Routing information protocol

Open Shortest Path First Protocol

Border Gateway Protocol

- **Format:** A routing table for classless addressing has a minimum of four columns. However, some of today's routers have even more columns.

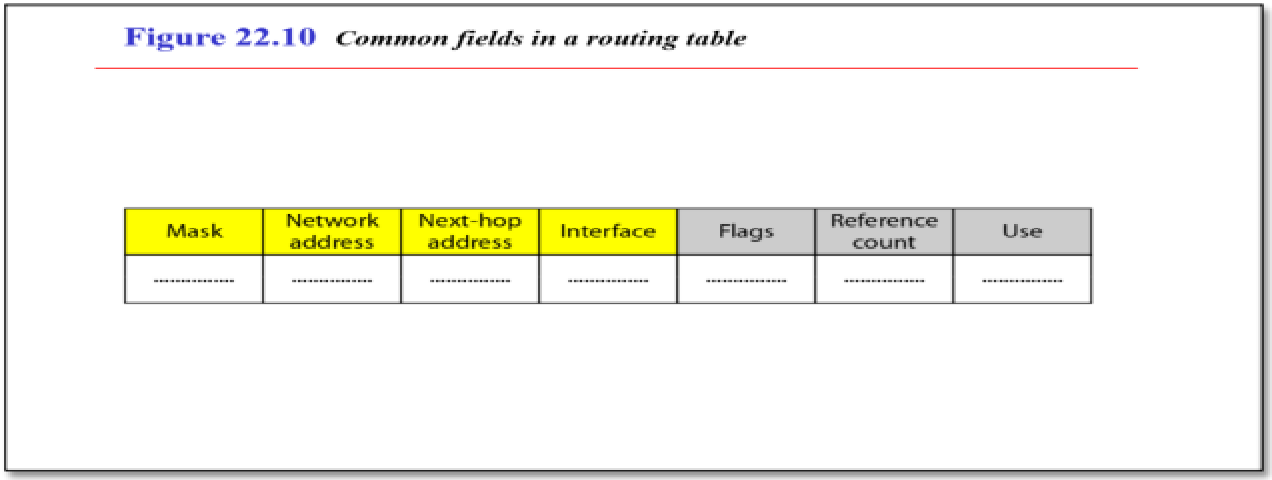


Figure 22.10 *Common fields in a routing table*

Mask	Network address	Next-hop address	Interface	Flags	Reference count	Use
....	....	....	....	....	....	....

Mask: This field defines the mask applied for the entry.

Network address: This field defines the network address to which the packet is finally delivered.

Next-hop address: This field defines the address of the next-hop router to which the packet is delivered.

Interface: This field shows the name of the interface.

Flags: This field defines up to five flags. Flags are on/off switches that signify either presence or absence. The five flags are U (up), G (gateway), H (hostspecific), D (added by redirection), and M (modified by redirection).

a. U (up). The U flag indicates the router is up and running. If this flag is not present, it means that the router is down. The packet cannot be forwarded and is discarded.

b. G (gateway). The G flag means that the destination is in another network. The packet is delivered to the next-hop router for delivery (indirect delivery). When this flag is missing, it means the destination is in this network (direct delivery).

a. H (host-specific). The H flag indicates that the entry in the network address field is a host-specific address. When it is missing, it means that the address is only the network address of the destination.

b. D (added by redirection). The D flag indicates that routing information for this destination has been added to the host routing table by a redirection message from ICMP(Internet Control Message Protocol).

c. M (modified by redirection). The M flag indicates that the routing information for this destination has been modified by a redirection message from ICMP.

Reference count: This field gives the number of users of this route at the moment. For example, if five people at the same time are connecting to the same host from this router, the value of this column is 5.

Use: This field shows the number of packets transmitted through this router for the corresponding destination

UNICAST ROUTING PROTOCOLS:

A routing protocol is a combination of rules and procedures that lets routers in the internet inform each other of changes. It allows routers to share whatever they know about the internet or their neighbourhood. The routing protocols also include procedures for combining information received from other routers.

Intra- and Interdomain Routing:

Routing inside an autonomous system is referred to as intradomain routing.

An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing between autonomous systems is referred to as interdomain routing. Each autonomous system can choose one or more intradomain routing protocols to handle routing inside the autonomous system. However, only one interdomain routing protocol handles routing between autonomous systems

Absentees:

71,81,8,93,9,B3,5,C2,Le-8,13