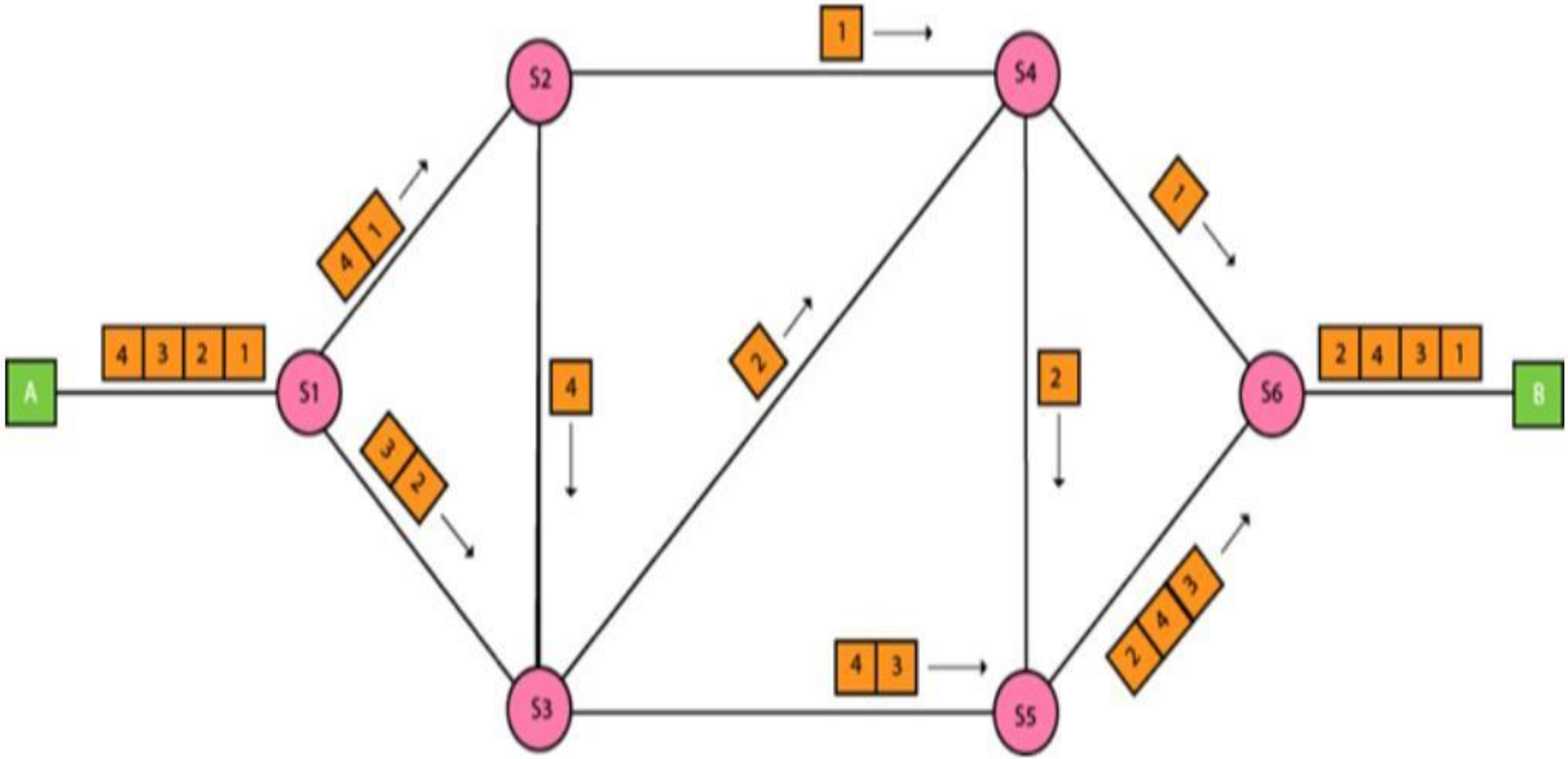
UNIT 4

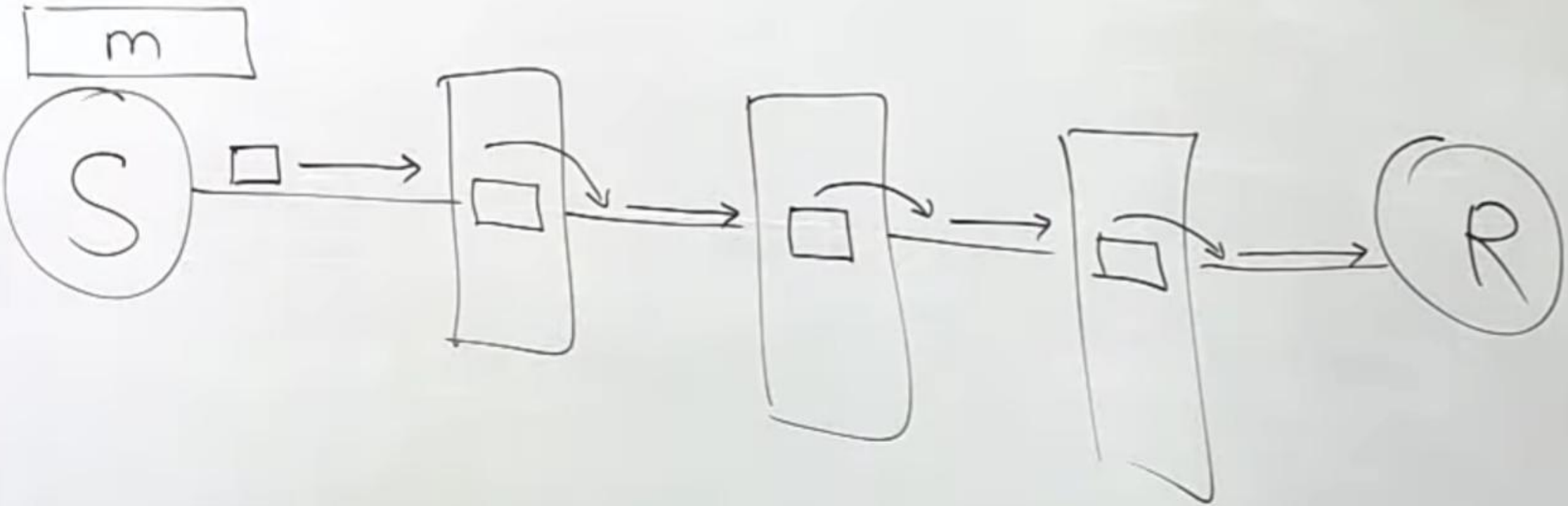
Network Link Layer part I – IP Addressing

- **Network Layer services**

- Store & foreword packet switching
- Services provide to transport layer
- Implementation of Connctionless services
- Implementation of connection oriented services

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.


A
4 3 2 1
S1
4 1
3 2
S2
4
1
S3
2
S4
4 3
2
S5
1
2 4 3
S6
2 4 3 1
B


m
S
R

Services provided to the transport layer

The services provided to the transport layer are as follows –

- **Logical Addressing** – Network layer adds header to incoming packet which includes logical address to identify sender and receiver.
- **Routing** – It is the mechanism provided by Network Layer for routing the packets to the final destination in the fastest possible and efficient way.
- **Flow control** – This layer routes the packet to another way, If too many packets are present at the same time preventing bottlenecks and congestion.
- **Breaks Large Packets** – Breaks larger packets into small packets.

followed by the users of connection oriented service. These are:

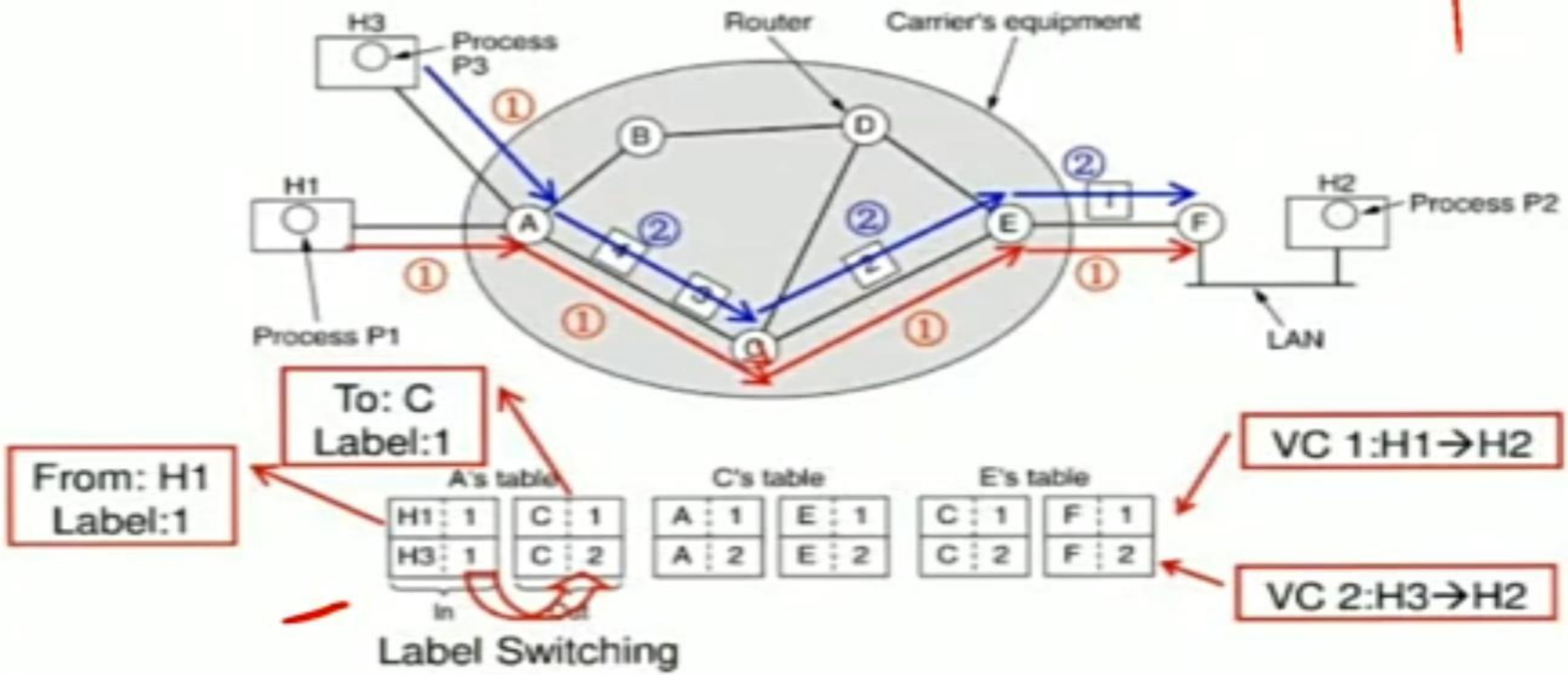
1. Connection is established.
2. Information is sent.
3. Connection is released.

In connection oriented service we have to establish a connection before starting the communication. When connection is established, we send the message or the information and then we release the connection.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

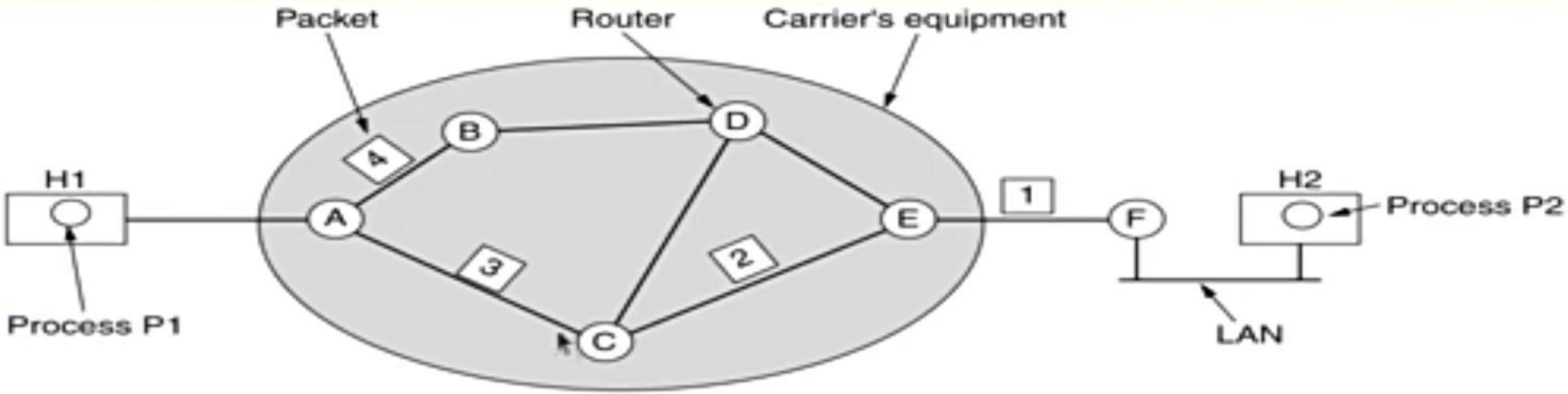
S.NO	Connection-oriented Service	Connection-less Service
1.	Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
2.	Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
3.	Connection-oriented Service is necessary.	Connection-less Service is not compulsory.
4.	Connection-oriented Service is feasible.	Connection-less Service is not feasible.
5.	In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
6.	Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give a guarantee of reliability.

Implementation of Connection-Oriented Service



Routing within a virtual-circuit subnet.

Implementation of Connectionless Service



A's table

Dest.	Line (initially)
A	–
B	B
C	C
D	B
E	C
F	C

Dest.	Line (later)
A	–
B	B
C	C
D	B
E	B
F	B

C's table

Dest.	Line
A	A
B	A
C	–
D	D
E	E
F	E

E's table

Dest.	Line
A	C
B	D
C	C
D	D
E	–
F	F

Routing within a diagram subnet.

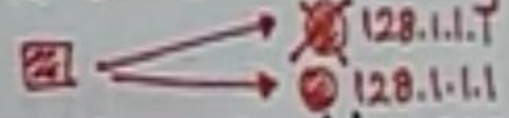
Comparison of datagram and virtual-circuit subnets

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Network Layer: Logical Addressing [IPV4 Addresses]

An IPV_4 is a 32-bit address that uniquely and universally defines the connection of a device to the Internet.

[Two device on the Internet can never have the same address at the same time.]



IMP. TERMS:

(i) Address Space: It is the total no. of addresses used by the protocol.

'n' bits in a add.

↳ n = 32

↳ 2^n addresses.

Add. space (IPv4) : 2^{32}

= 4,294,967,296.

(ii) Notations:

↳ (a) Binary Notation: In this IPV_4 is displayed as 32 bits or 4 byte.

01110101 10010101 00011101 11101010

↳ (b) Dotted-Decimal Notation: Used to make IPV_4 more compact and easier to read.

10000000 00001011 00000011 00011111

↳ 128. 11. 3. 31

↳ (c) Hexadecimal Notation: Each Hexadecimal digit is equivalent to four bits. This means that 32-bit address has 8 hexa-decimal digits.

Classful Addressing: In this the address space is divided into 5 classes

- Class A
- class B
- class C
- Class D
- class E

IMP..

How to Find Class of an Address:-

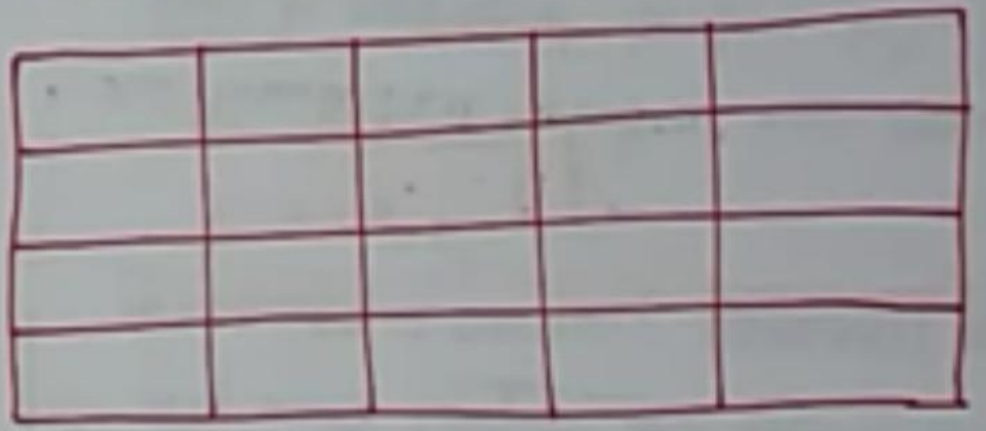
Binary Notation

	First Byte
class A	0....
class B	10....
class C	110....
class D	1110....
class E	1111....

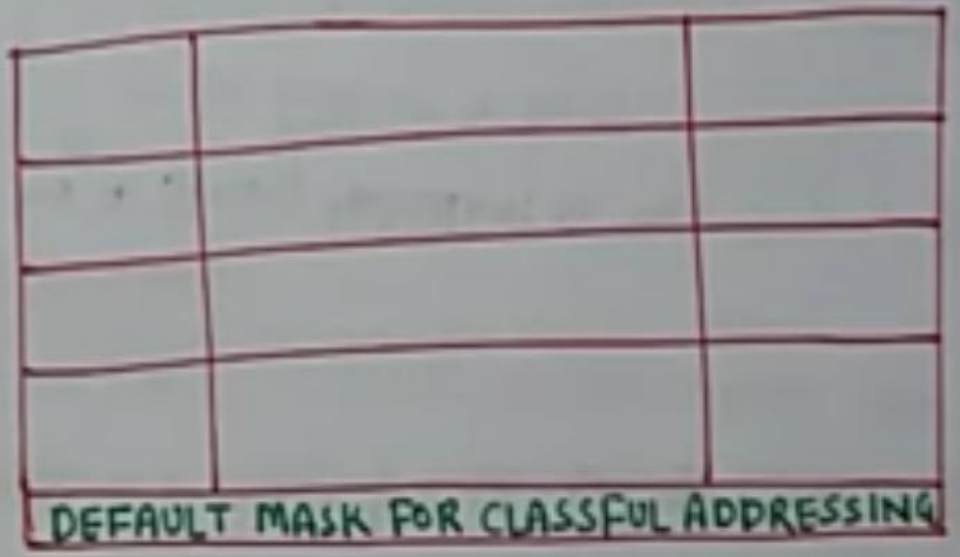
IMP: Dotted-Decimal

	First Byte
Class A	0-127
class B	128-191
class C	192-223
class D	224-239
class E	240-255

Netid and Hostid: Only class A, B or C is divided into netid and hostid.



Mask: It helps to find netid and hostid.



(Decimal Dotted)

Ques1.) Find the Class of each Address:-

Byte1

a.) 227.12.14.87 ⇒ Class D

b.) 193.14.56.22 ⇒ class C

c.) 14.23.120.8 ⇒ class A

d.) 252.5.15.111 ⇒ Class E

Classful Addressing: In this the address spac

is divided into 5 classes

- Class A
- class B
- class C
- class D
- class E

IMP..

How to Find Class of an Address:-

Binary Notation

	First Byte
class A	0....
class B	10....
class C	110....
class D	1110....
class E	1111....

IMP.. Dotted-Decimal

	First Byte
Class A	0-127
class B	128-191
class C	192-223
class D	224-239
Class E	240-255

Ques 2.) Find the class of each Address:-

Binary Notation.

a.) 00000001 → Byte1 00. . . . . → class A

b.) 11000001 → 100 . . . . . → class C

c.) 10100111 → 11D . . . . . → class B

d.) 11110011 → 100 . . . . . → class E

0
10-
110-
1110-
1111-

is divided into 5 classes

- Class A
- Class B
- Class C
- Class D
- Class E

IMP.:

How to Find Class of an Address:-

Binary Notation

	First Byte
class A	0....
class B	10....
class C	110....
class D	1110....
class E	1111....

IMP.: Dotted-Decimal

	First Byte
Class A	0-127
Class B	128-191
Class C	192-223
Class D	224-239
Class E	240-255

into netid and hostid.

class	Byte1	Byte2	Byte3	Byte 4
classA	NetId	HostId	HostId	HostId
ClassB	NetId	NetId	HostId	HostId
Class C	NetId	NetId	NetId	HostId

n bits = 1

(32-n) = 0

A: n = 8

B = n = 16

C = n = 24

Mask: It helps to find netid and hostid.

class	Binary (Mask)	Decimal
classA	11111111 00....	255.0.0.0
classB	11111111 11111111 00....	255.255.0.0
classC	11111111 11111111 11111111 0...	255.255.255.0

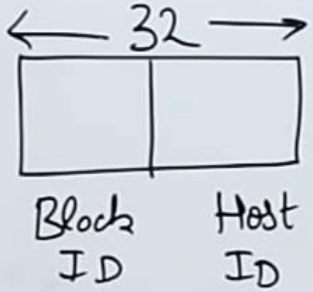
DEFAULT MASK FOR CLASSFUL ADDRESSING

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

"Classless Addressing" (1993)

→ No classes

→ Only blocks



→ Notation

x.y.z.w/n ← mask 1111
n → no. of bits represent block/network

200.10.20.40/28

Rules

→ Addresses should be Contiguous

→ No. of addresses in a block must be in Power of 2.

→ First address of every block must be evenly divisible with size of block.

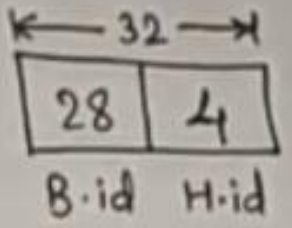
let's say 200.10.20.40/28

192.168.1 .1 /24

Network Host Subnet Mask

CIDR (Classless Addressing)

- Blocks, instead of specific classes.
- a.b.c.d /n



eg - 200.10.20.40 / 28

Mask - 28 → 11111111.11111111.11111111.11110000

Bits in block id - 28

Bits in host id - 4

Total no. of blocks - 2^{28}

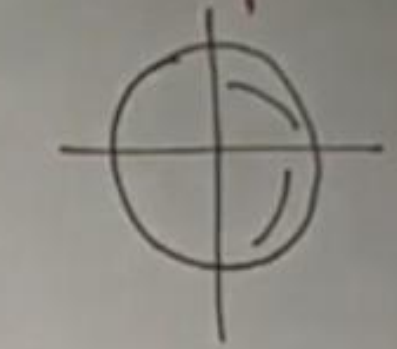
Total no. of hosts - 2^4

Network id / Block id -

200.10.20.40

255.255.255.240

200.10.20.32



classful → a.b.c.d

classless → a.b.c.d

```
1111 0000
0010 1000
---------
00100000
```

25

tive. The special blocks of addresses are listed below:

1. All Zeros Address
2. All Ones Address
3. Loopback Addresses
4. Private Addresses

IP Address = 32 bit

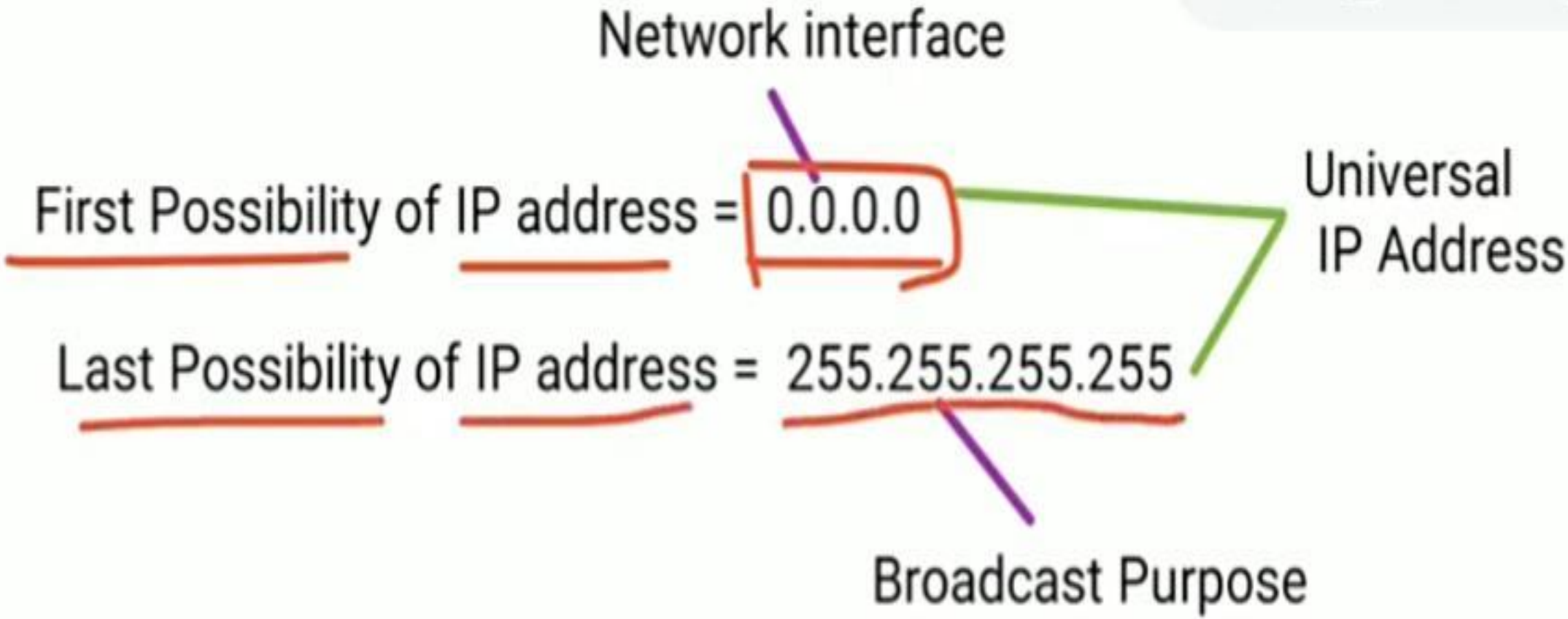
8 bit . 8 bit . 8 bit . 8 bit

00000000 = 0

11111111 = 255

(0-255).(0-255).(0-255).(0-255)

0.0.0.0


Network interface
First Possibility of IP address = 0.0.0.0
Universal
IP Address
Last Possibility of IP address = 255.255.255.255
Broadcast Purpose

SPECIAL ADDRESSES

Source IP

0.0.0.0/32

Loopback Address

127.0.0.0/8

Destination IP

255.255.255.255/32

Private Addresses

10.0.0.0/8

172.16.0.0/12

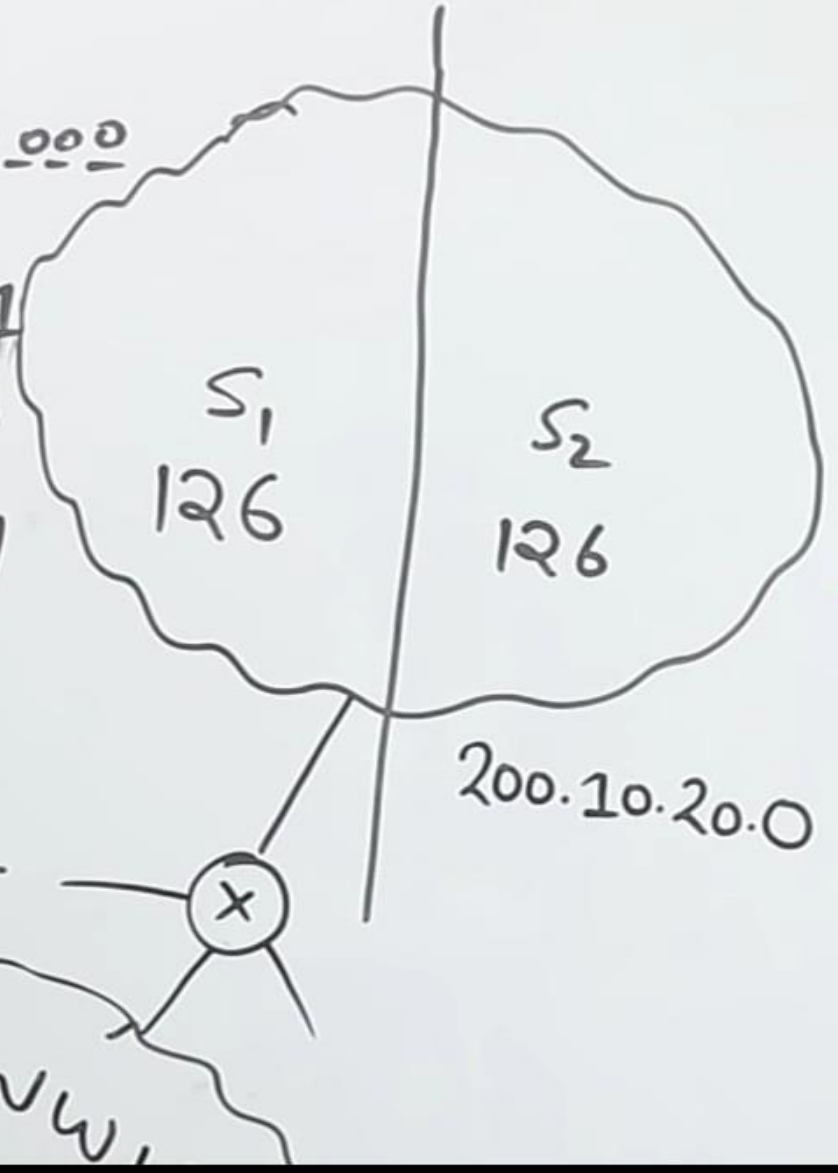
Subnetting

Dividing the network into smaller contiguous networks or subnets is called subnetting.

Why subnetting?

Suppose we take a network of class A. So, in class A, we have 2^{24} hosts. So to manage such a large number of hosts is tedious. So if we divide this large network into the smaller network then maintaining each network would be easy.

Subnetting ⇒ Dividing the big network into small networks



200.10.20.00000000

200.10.20.00000001

⋮

200.10.20.01111111

200.10.20.0 ⌣

to

200.10.20.127 ⌣

256

0
255] 254 (252)

200.10.20.10000000

200.10.20.10000001

200.10.20.10000010

⋮

200.10.20.11111111

200.10.20.128 ⌣

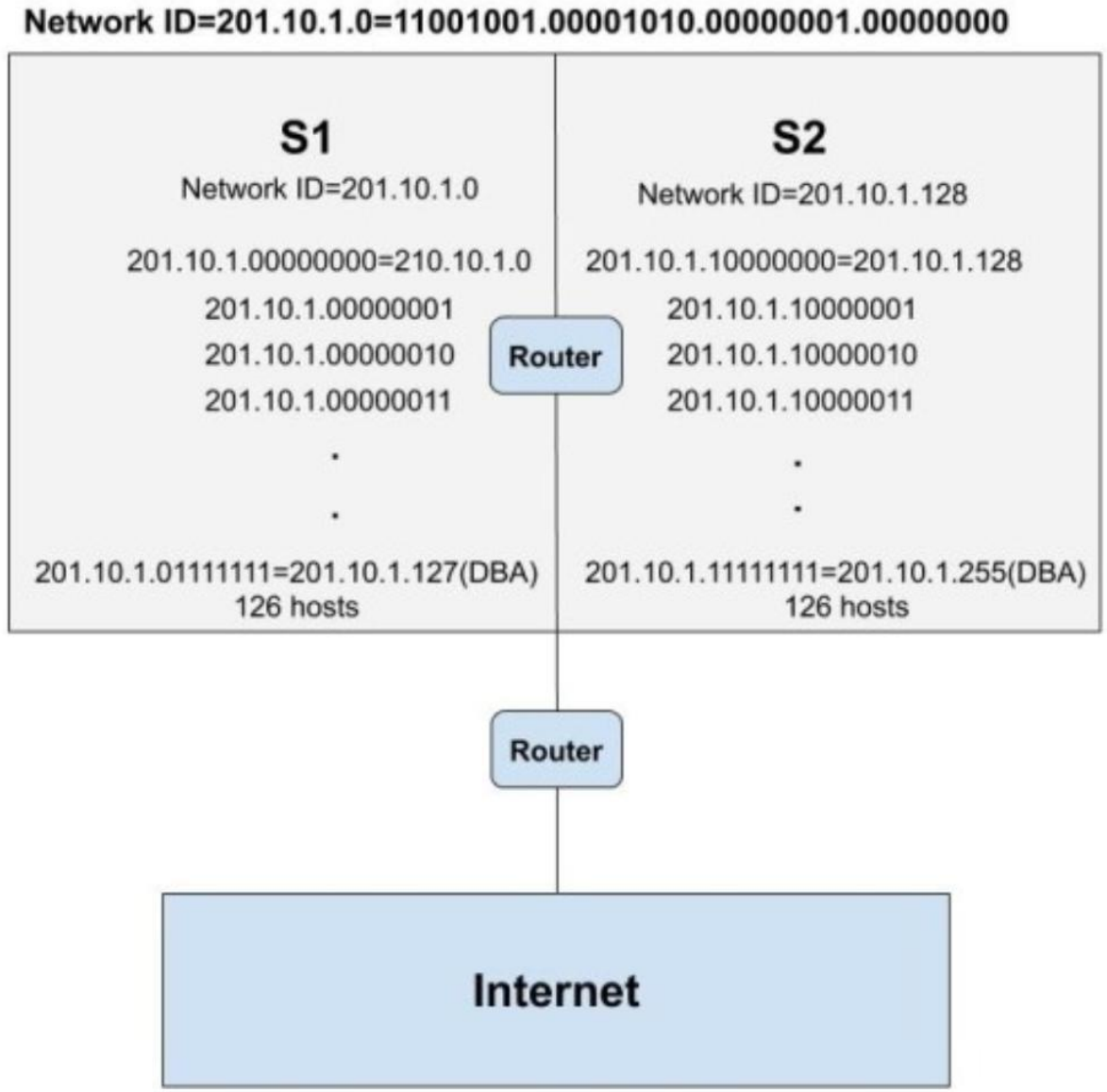
to

200.10.20.255 ⌣

How does subnetting work?

Suppose we have a class C network having network ID as 201.10.1.0(**range of class C 192–223**). So the total number of hosts is 256(for class C host is defined by last octet i.e. 2^8). But, the total usable host is 254. This is because the first IP address is for the **network ID** and the last IP address is **Direct Broadcast Address(**for sending any packet from one network to all other hosts of another network**).**

So, in subnetting we will divide these 254 hosts logically into two networks. In the above class C network, we have 24 bits for Network ID and the last 8 bits for the Host ID. We are going to borrow the **left-most bit** of the **host address** and declare for identifying the subnet. If the leftmost bit of the host address is 0 then it is the **1st subnet network** and if the leftmost bit is 1 then it would be **2nd subnet network**. Using 1 bit we can divide it into 2 networks i.e. 2^1. If we want to divide it into four networks then we need 2 bits(2^2=4 networks). The range of IP address which is in **1st subnet** network is from **201.10.1.0 to 201.10.1.127**. The range of IP address that lies in the **2nd subnet network** is from **201.10.1.128 to 201.10.1.255**.


Network ID=201.10.1.0=11001001.00001010.00000001.00000000
S1
Network ID=201.10.1.0
201.10.1.00000000=210.10.1.0
201.10.1.00000001
201.10.1.00000010
201.10.1.00000011
201.10.1.01111111=201.10.1.127(DBA)
126 hosts
S2
Network ID=201.10.1.128
201.10.1.10000000=201.10.1.128
201.10.1.10000001
201.10.1.10000010
201.10.1.10000011
201.10.1.11111111=201.10.1.255(DBA)
126 hosts
Router
Router
Internet

The subnet mask is represented as 11111111.11111111.11111111.10000000 i.e. 255.255.255.128 for the above network.

Sunny Subnetting Table

Subnet	1	2	4	8	16	32	64	128	256
Host	256	128	64	32	16	8	4	2	1
Subnet Mask	/24	/25	/26	/27	/28	/29	/30	/31	/32

Supernetting or Aggregation

It is the opposite of Subnetting. In this multiple smaller networks are combined together to form a large network.

How does supernetting work?

All the networks are not suitable for aggregation. There are some rules according to which the network can be aggregated. For any network to be aggregated it should follow three rules.

1. **Contiguous**: All the networks should be contiguous.
2. **Same size:** All the networks should be of the same size and also a power of 2 i.e. 2^n.
3. **Divisibility:** The first network ID should be divisible by the size of the block.

eg: 200·1·0·0/24 ✓

200·1·1·0/24 ✓

200·1·2·0/24 ✓

200·1·3·0/24

Replace 1 for fixed
0 for variable

255·255·11111100·00000000

255·255·252·0

→ Size of network = 4×2^8

$= 2^{10}$ → IP address

→ 200·1·00000000·00000000

200·1·0·0

255·255·252·0

200·1·0·0

↳ Supernet ID

* Supernet Mask:

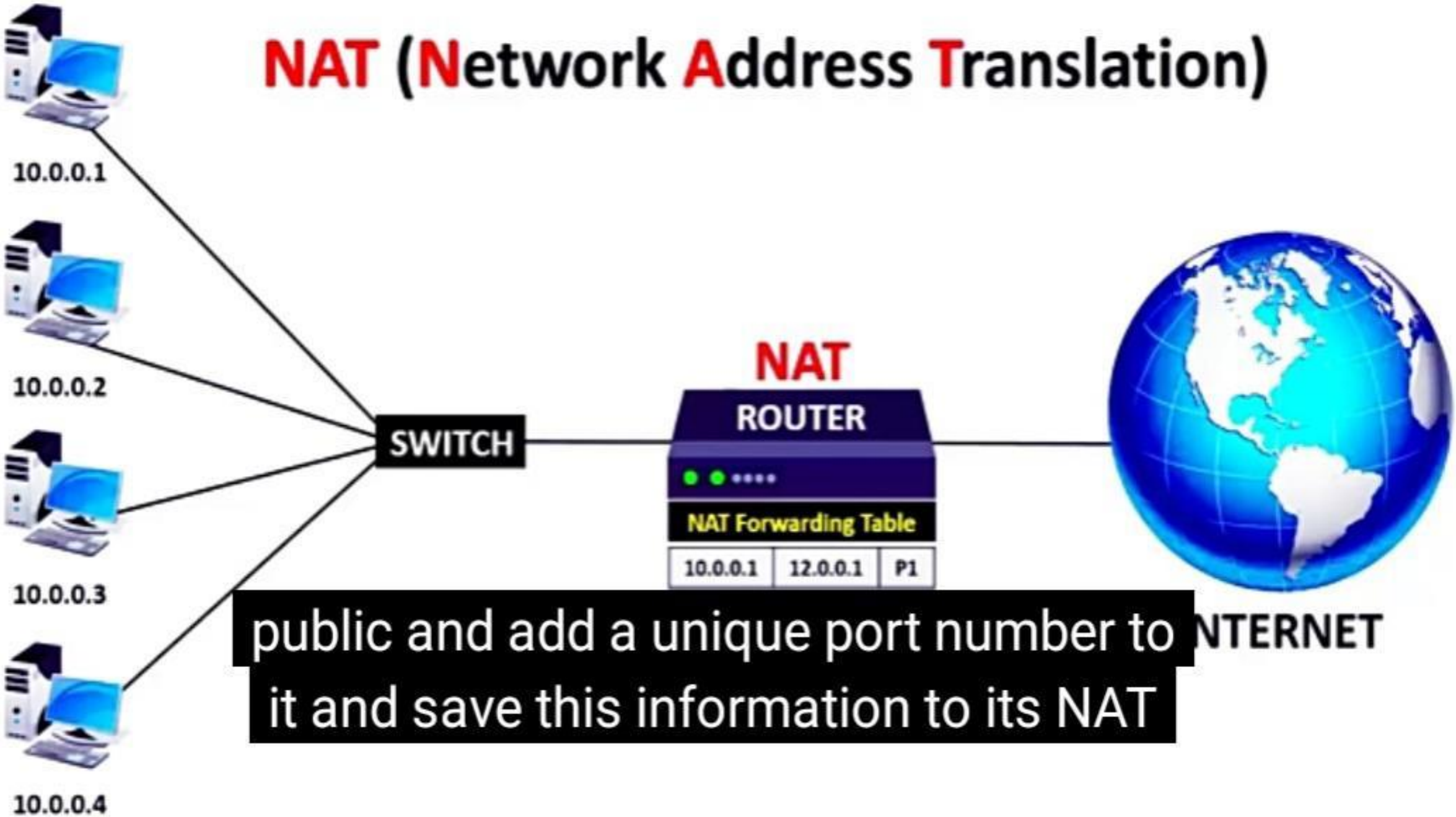
200·1·00000000·00000000

200·1·00000001·00000000

200·1·00000010·00000000

200·1·00000011·00000000

NAT (Network Address Translation)



public and add a unique port number to it and save this information to its NAT

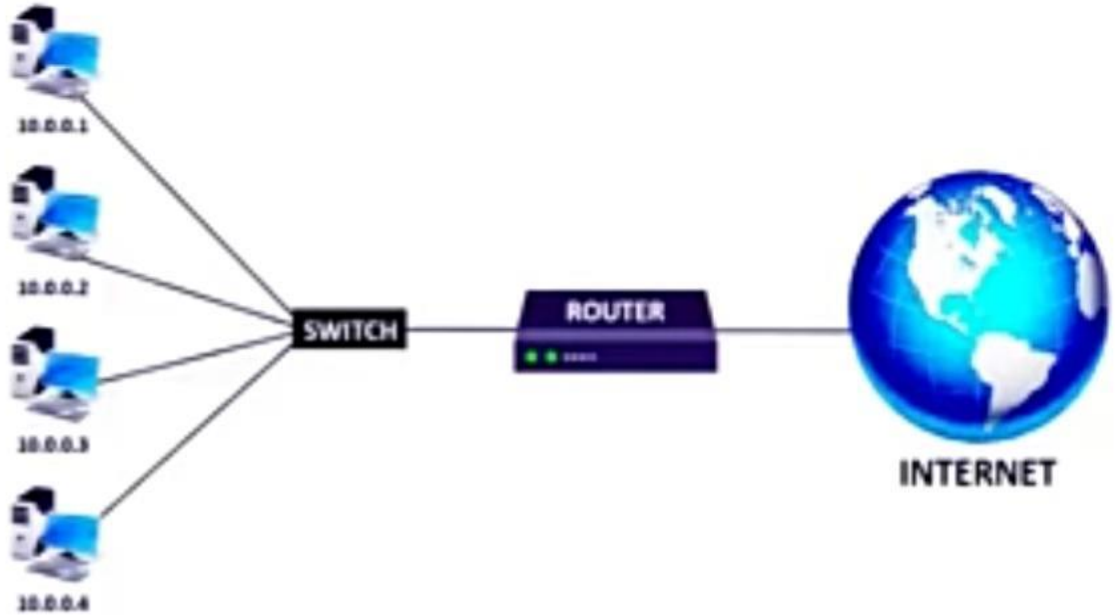
NAT Table

Private IP Address	Public IP Address
192.168.1.2	122.168.165.190
192.168.1.3	122.168.165.191
192.168.1.4	122.168.165.192
192.168.1.5	122.168.165.193


10.0.0.1
10.0.0.2
10.0.0.3
10.0.0.4
Costly
Needless
Waste
Internet
Agent
ISP


250.60.45.32
Costly
Needless
Waste
Internet
Agent
ISP

NAT (Network Address Translation)



Advantages of NAT

- It hide the real IP address of your internal network from the public network and act as a firewall.
- It allows unlimited number of private addresses to access the single internet connection.
- Hence, it allows multiple devices to access single internet connection. It helps you to save money from buying multiple internet connection for multiple devices.

Disadvantages of NAT

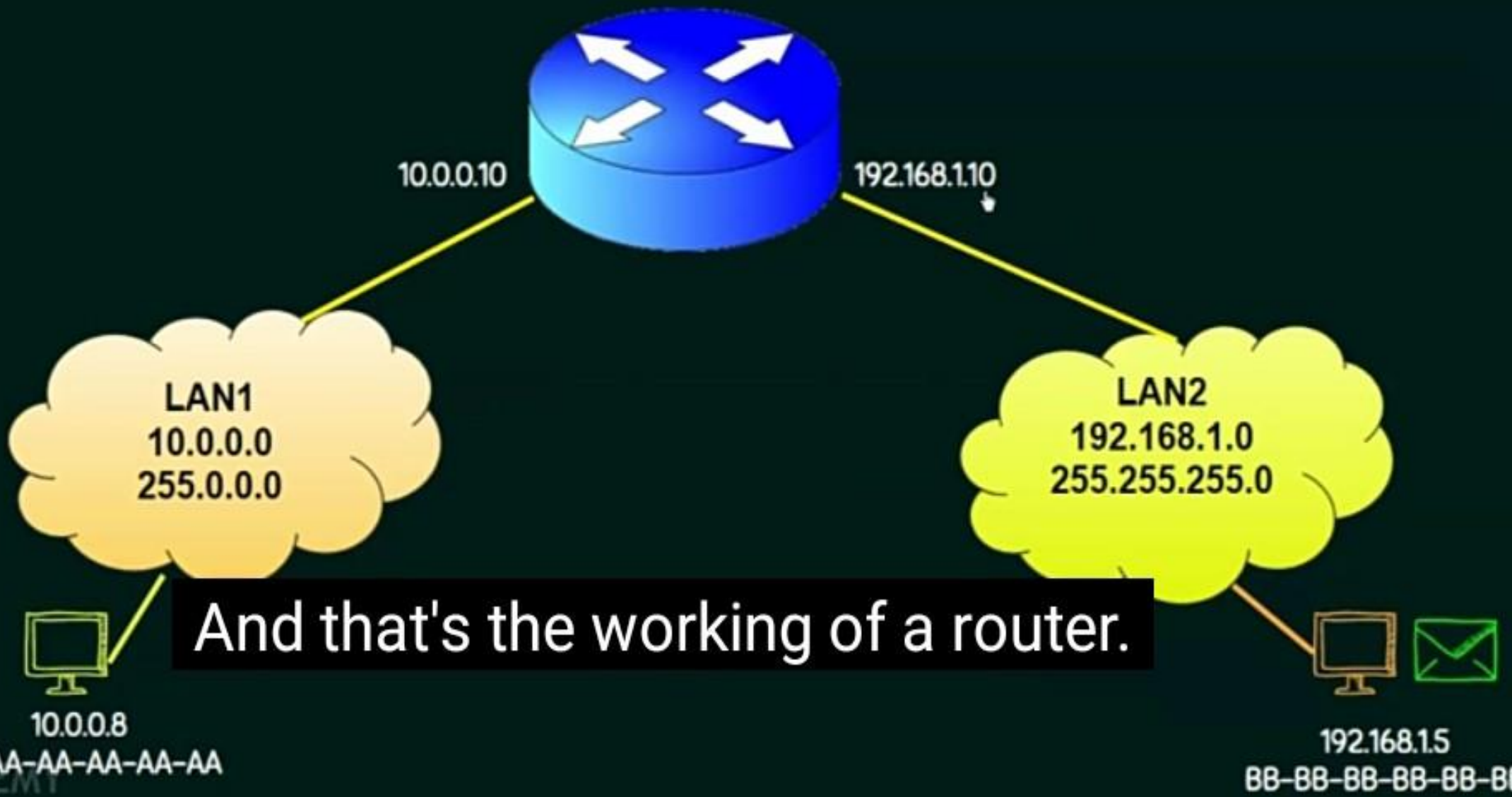
- If you change the IP Address, the troubleshooting may become more complex.
- It blocks some incoming connection.
- Some TCP/IP applications like peer to peer application, end to end IPsec, multicast routing protocol do not work well with NAT.

Router

- ★ A router is a networking device that forwards data packets between computer networks.
- ★ A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network.
- ★ It is a layer 3 (Network layer) device.
- ★ Stores routing table.

Let's see the working of a router now.

Working of Router



And that's the working of a router.

IP PACKET

WHAT IS AN IP PACKET?

- Each block of data is known as an IP packet.
- Each IP packet contains an HEADER(source,dest) and DATA.
- The HEADER includes the IP addresses of the source and destination.
- The DATA is the actual content,such as a string of letters or part of a webpage.

Delivery

- The network layer supervises the handling of the packets by the underlying physical networks.
- This handling is known as the delivery of a packet.

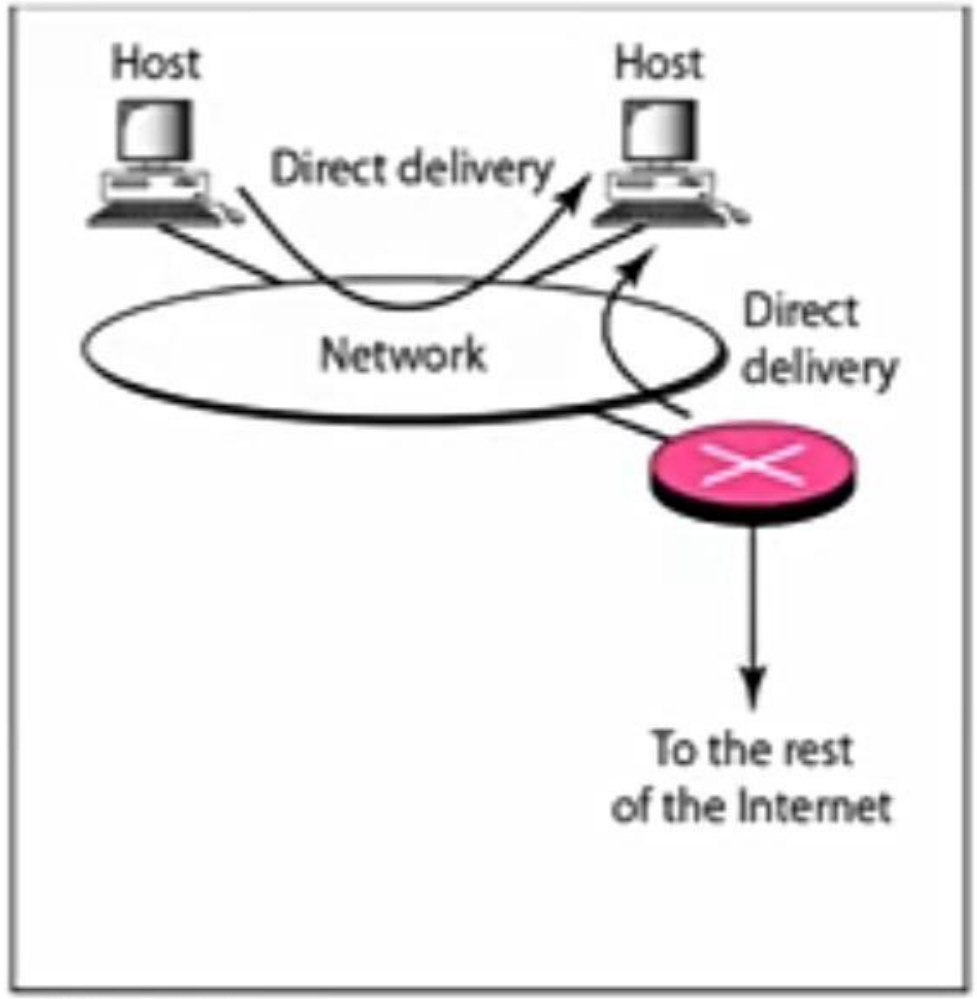
Types of Delivery

- The delivery of a packet to its final destination is accomplished by using two different methods :

1. Direct Delivery
2. Indirect Delivery

Direct delivery

- ***Direct delivery occurs when the source and destination of the packet are located on the same physical network or when the delivery is between the last router and the destination host***

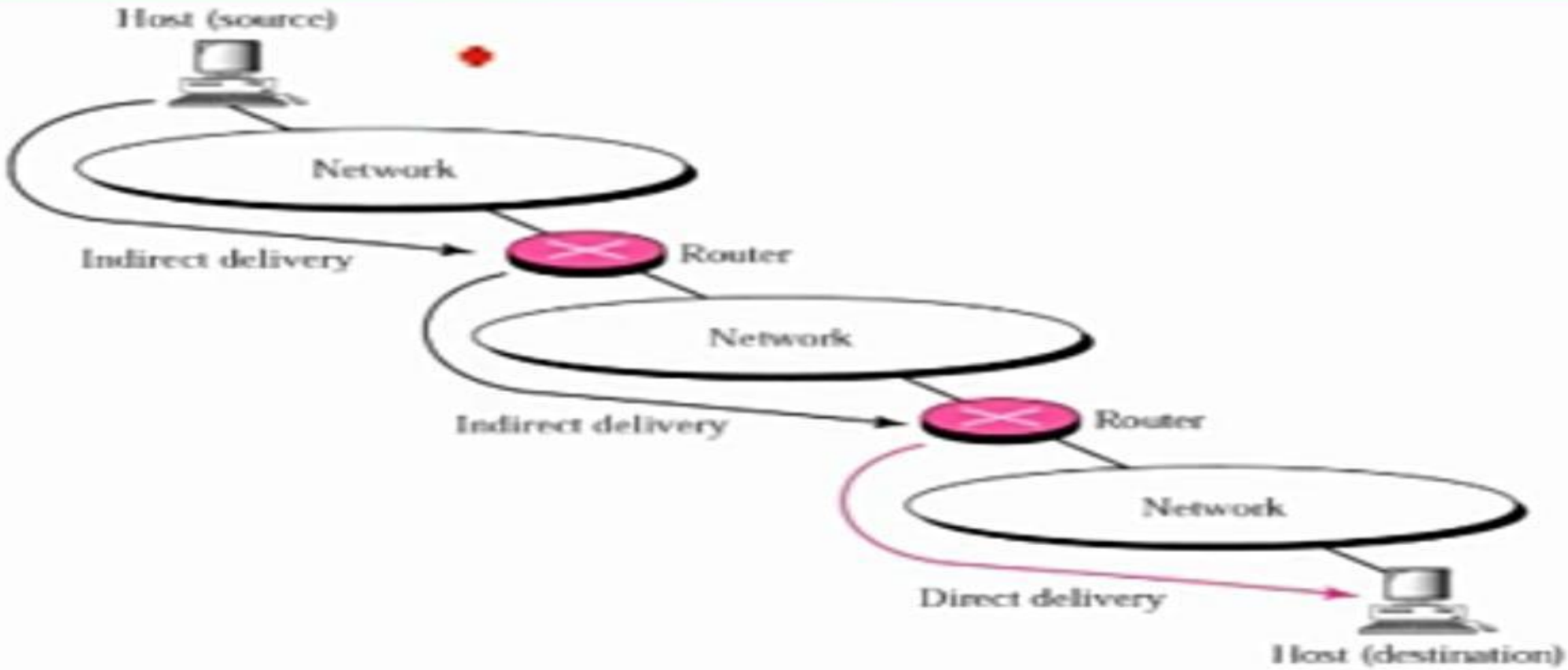


a. Direct delivery

Indirect delivery

- *If the destination host is not on the same network as the deliverer, the packet is delivered indirectly.*
- *In an indirect delivery, the packet goes from router to router until it reaches the one connected to the same physical network as its final destination.*

Indirect Delivery



22-2 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.***

A → R1 → R2 → R3 → B

Types of forwarding techniques:

1. Next hop versus route method.
2. Network specific versus host specific method.
3. Default method.

Forwarding techniques

1. Next-Hop method :

- This technique is used to reduce the contents of a routing table.
- The routing table hold only the address of the next hop instead of information about the complete route

Route method versus next-hop method

a. Routing tables based on route

Destination	Route
Host B	R1, R2, host B

Routing table for host A

Destination	Route
Host B	R2, host B

Routing table for R1

Destination	Route
Host B	Host B

Routing table for R2

b. Routing tables based on next hop

Destination	Next hop
Host B	R1

Destination	Next hop
Host B	R2

Destination	Next hop
Host B	---

2. Network specific versus host specific method.

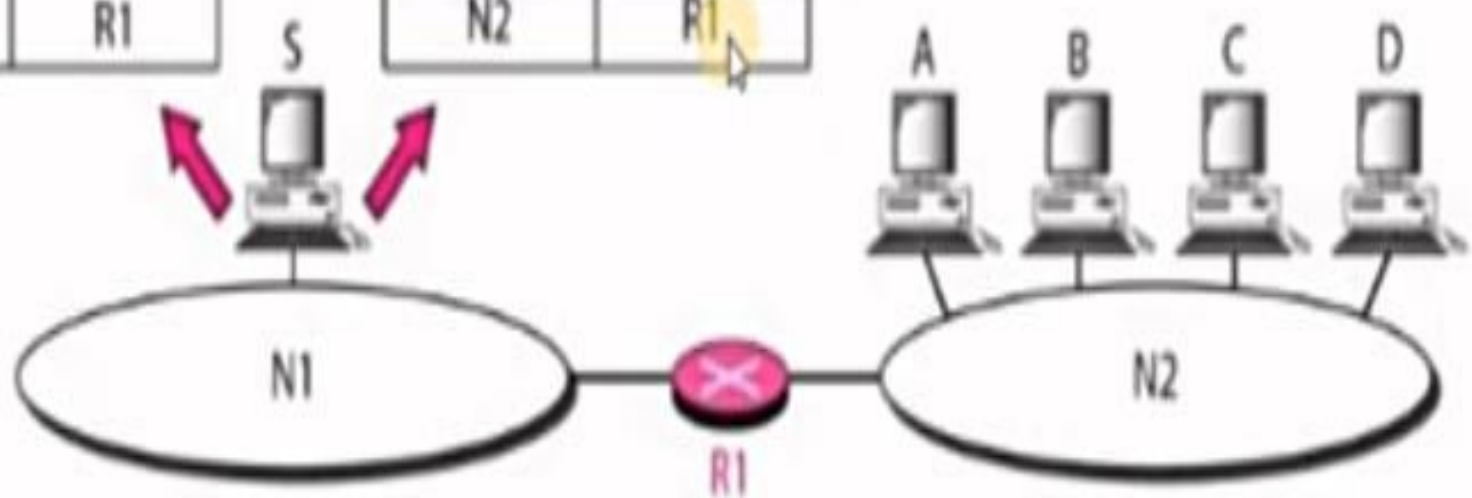
- A second technique to reduce the routing table and simplify the searching process is called the network-specific method.
- In the network-specific method, the routing table holds only one entry that defines the address of the destination network instead of all hosts on that network
- Host-specific routing is used for purposes such as checking the route or providing security measures

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



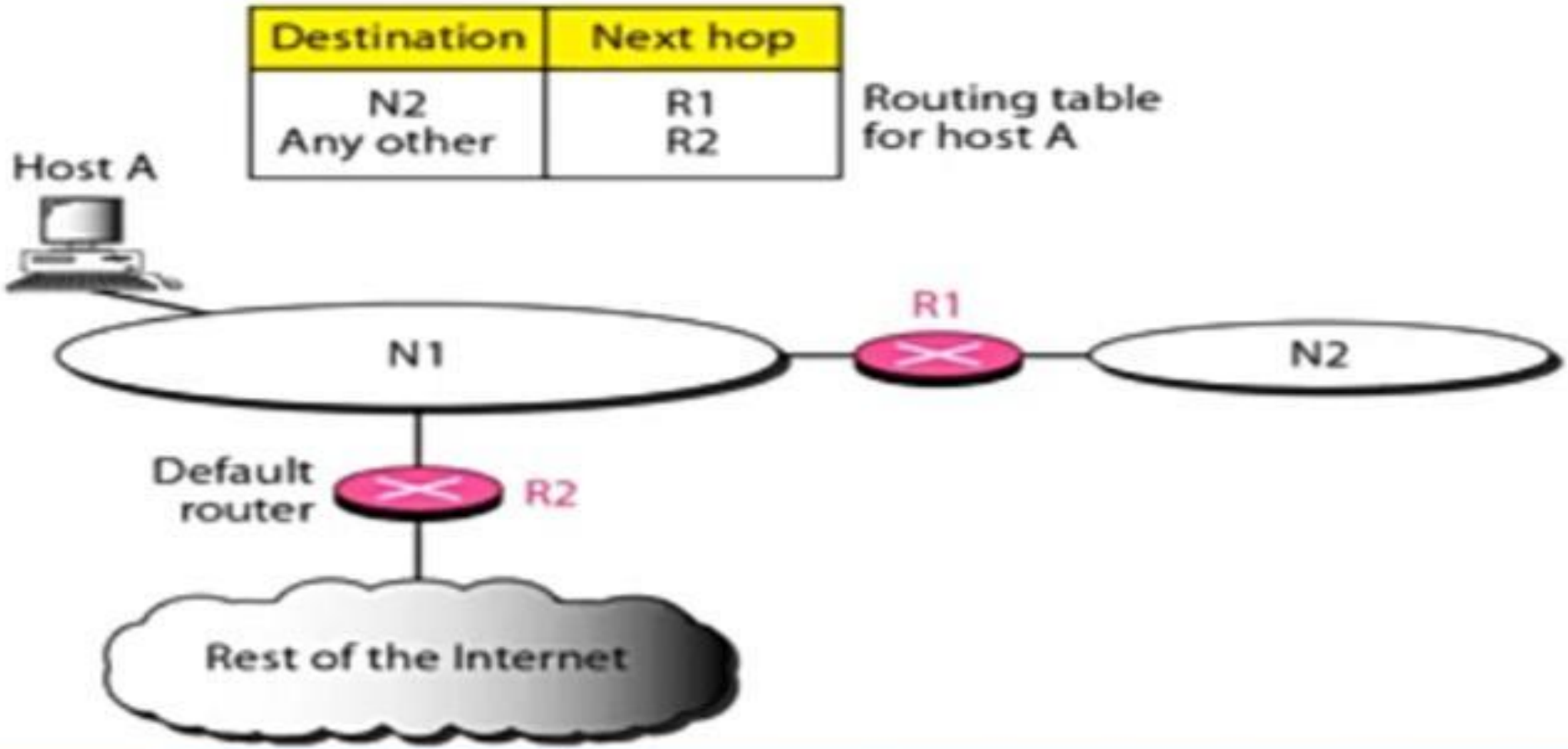
3. Default method

Another technique to simplify routing is called the default method. Host A is connected to a network with two routers.

Router R1 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).

Default method



IPv4 address

- IPv4 is 32 bit numeric address divided into four parts.
- Each 8 bit is known as a block, and it produces 0-255 numbers.
- The IP version 4 can produce 4 billion ($4x\ 10^9$) unique addresses.
- Example – 192 . 34 . 244 . 1

Conversion

The picture shown below illustrates the format of IPv4.

8 Bits . 8 Bits . 8 Bits . 8 Bits

When all the 8 bits are set to value 1, we get the sum 255 as shown below.

11111111 . 11111111 . 11111111 . 11111111

$2^7+2^6+2^5+2^4+2^3+2^2+2^1+2^0$

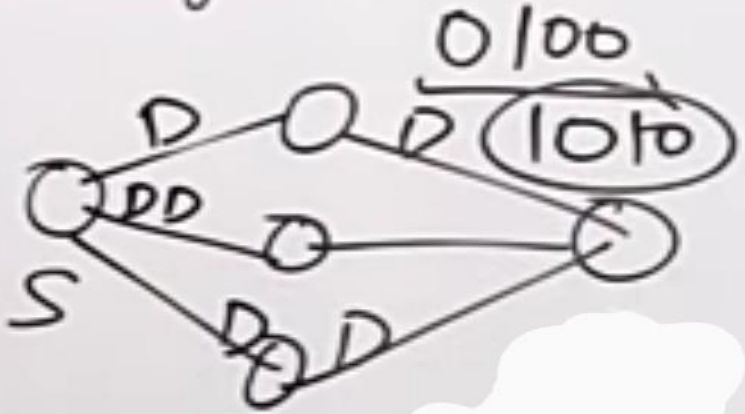
$= 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0$

$= 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = \mathbf{255}$

"IPv4 Header"

→ Connection less

→ Datagram Service



0100
0101

VER 4	HLEN 4	Type of Service (DSCP) 8	Total Length 16
Identification bits 16		Flag 3	Fragment offset 13
Time to LIVE TTL 8	Protocol 8	Header checksum 16	
Source IP Address 32 bits			
Destination IP Address 32 bits			
→ Options & Padding			

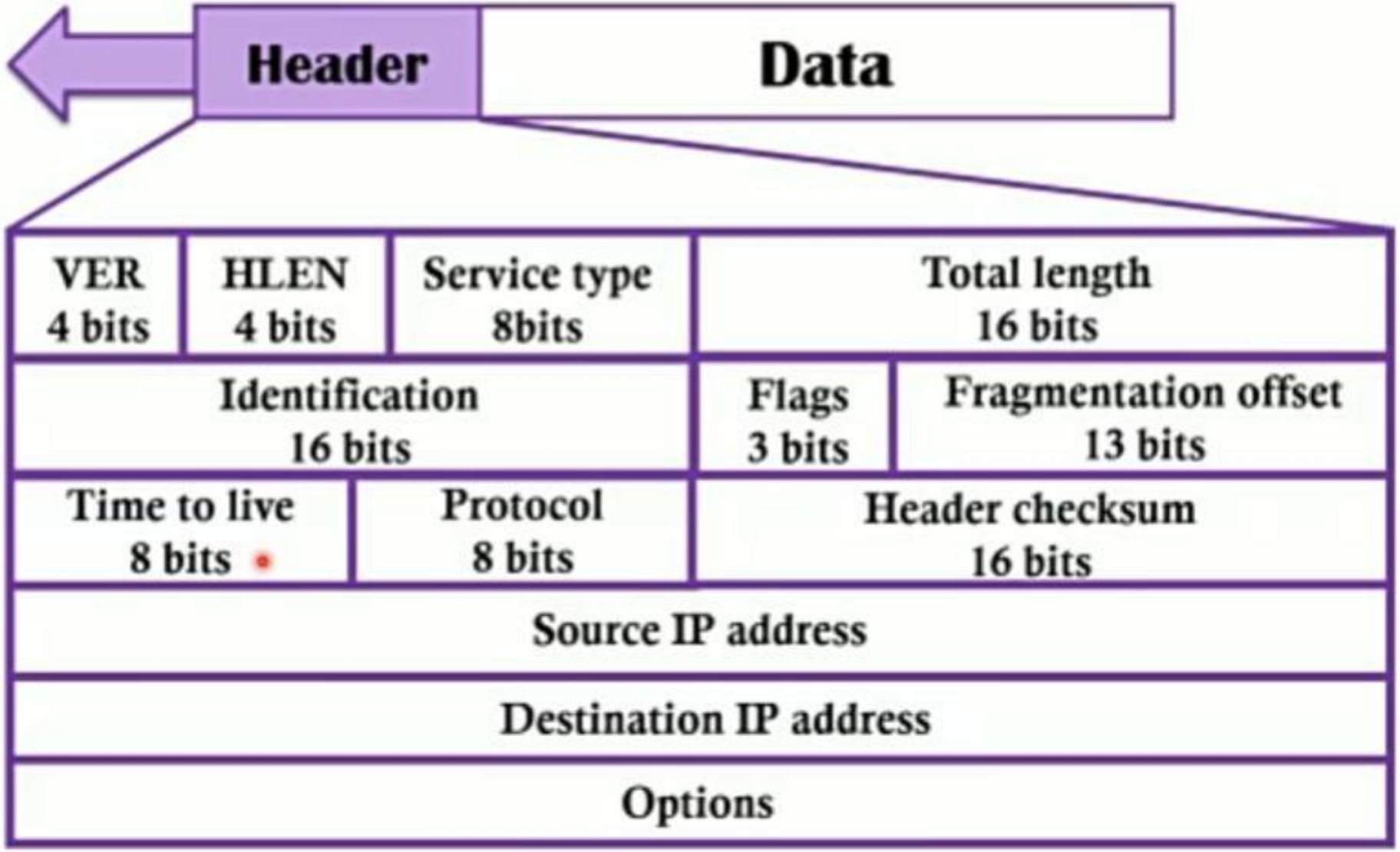
Datagram ⇐ Header Size = 20-60 Bytes 160 bits

"IPv4 Header"

Differentiated Services Code Point (DSCP)

VER 4	HLEN 4	Type of Service (DSCP) 8	Total Length 16
Identification bits 16		Flag 3	Fragment offset 13
Time to LIVE TTL 8	Protocol 8	Header checksum 16	
Source IP Address 32 bits			
Destination IP Address 32 bits			
→ Options & Padding			

IPv4 Datagram



IPv4 Limitations

- Limited numbers of IP addresses.
- No provision for authentication.
- Security issues.
- No provisions for routing.

IPv6 Addresses:- It is of 128 bits or 16 bytes.

↳ Length is (4) times the length address of IPv4.

Notations:-

(i) Dotted-Decimal:- It is used for IPv4 Compa-tibility. 221.14.65.11.105.45.170.34.12.234.18.0.14.0.115.255](16)

IMP (ii) Colon Hexadecimal:- It is used to make the address more readable. In this notation, the 128 bits are divided into 8 sections, each of 2 bytes in length. [Two bytes in Hexadecimal req. 4 Hexadecimal digits].

FDEC: BA98: 7654: 3210: ADBF: BBFF:

2922: FFFF

Abbreviation:- It is a technique to reduce the length of IPv6 address. It is done by omitting/removing the leading zeros of a section.

[NOTE:- Only the leading Zeros can be dropped]

[Zero-Compression]

FDEC:0074:0000:0000:0000:B0FF:0000:FFF0

omitting these Zeros

FDEC:74:0:0:0:B0FF:0:FFF0 } Abbreviated Address

↓

FDEC:74::B0FF:0:FFF0

↳ GAP.

IPv6 Address Types

IPv6 has three types of addresses:

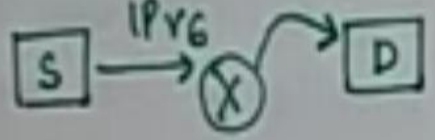
1. Unicast—For a single interface.

2. Multicast—For a set of interfaces on the same physical medium. A packet is sent to all interfaces associated with the address.

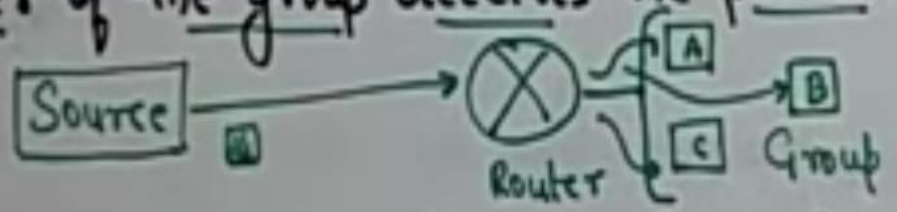
3. Anycast—For a set of interfaces on different physical media. A packet is sent to only one of the interfaces associated with this address, not to all the interfaces.

Types of Address Space in IPv6:-

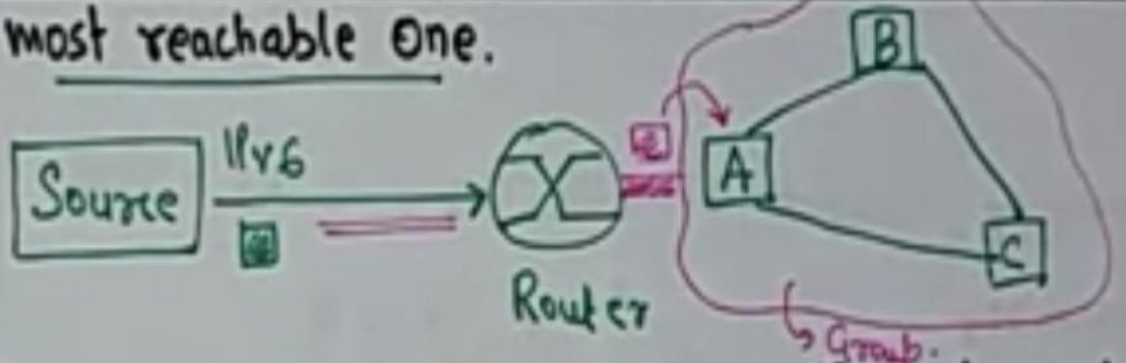
(i) Unicast Addresses:- It defines single interface or Computer. The packet Sent to a unicast address will be routed to the intended PC or recipient.



(ii) Multicast Addresses:- These are used to define a group of Computers/hosts. In this, each member of the group receives the packet.



(iii) Anycast Addresses:- Defines group of nodes or Computers that all share a single address. A packet with anycast address is delivered to most reachable one.



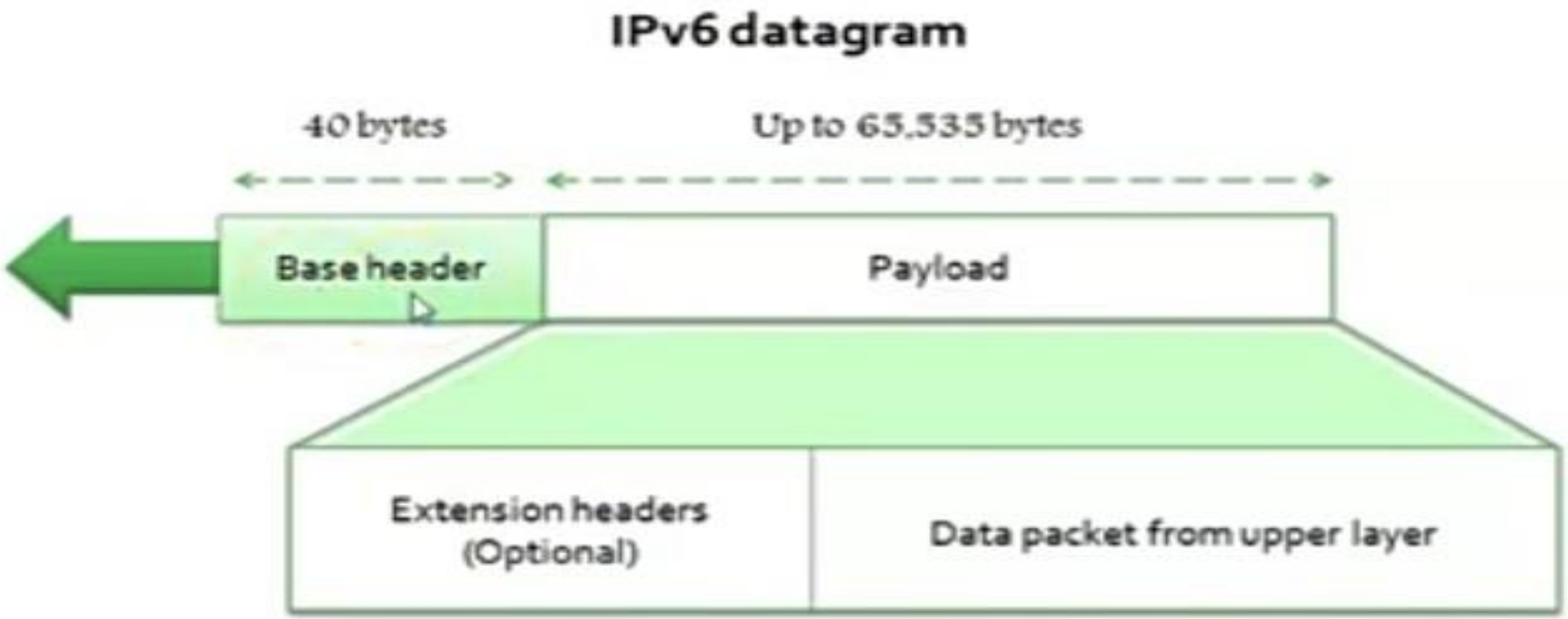
(iv) Broadcasting and Multicasting:- IPv6 doesnot define broadcasting and Considered it as a special Case of multicasting.

Reserved Addresses:-

↳ Starts with 8 0's

IPv6 Packet format

Each packet is consist of a mandatory base header succeeded by the payload. The payload includes two parts namely optional extension headers and data from an upper layer. The base header consumes 40 bytes, inversely the extension headers and data from the top layer usually hold up to 65,535 bytes of information.



"IPv6 Header"

128

32

2^{32}

0110

65535 B

2^{128}

Virtual circuit

VERSION (4)	Priority (8) Traffic type	Flow Label (20)
Payload Length (16)	Next Header (8)	Hop Limit (8)
Source Address (128)		
Destination Address (128)		

Base Header = 40 Bytes (320 bits) Fixed

Base Header	Extension Header 1	.....	Extension Header N	Data

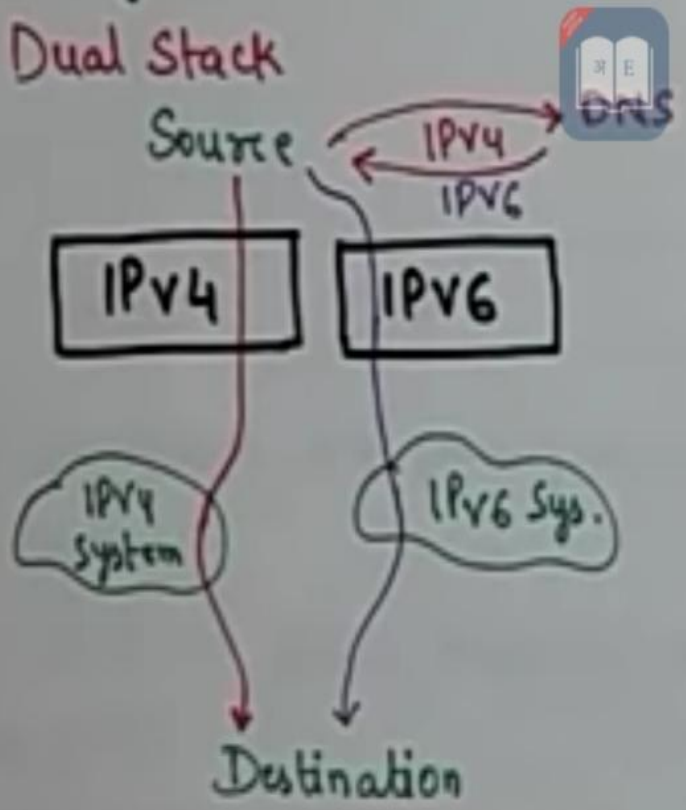
40 B

Extension Headers:

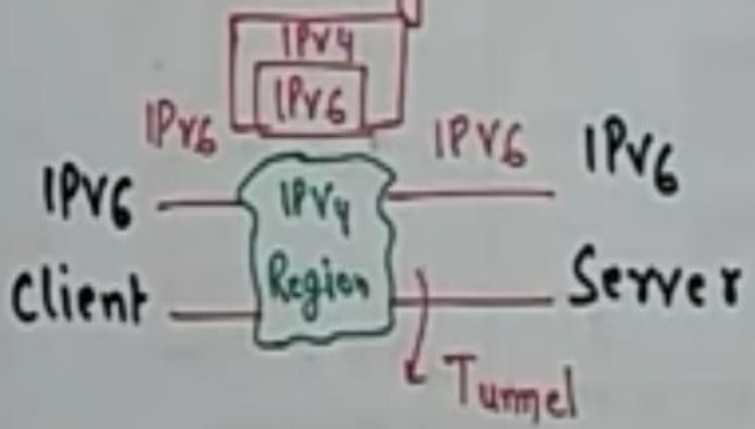
1) Routing Header (43)
2) Hop by Hop option (0)
3) Fragment Header (44)
4) Authentication Header (51)
5) Destination Options (60)
6) Encapsulating Security Payload (50)

Transition from IPv4 to IPv6:- There are three transition Strategies.

Dual Stack



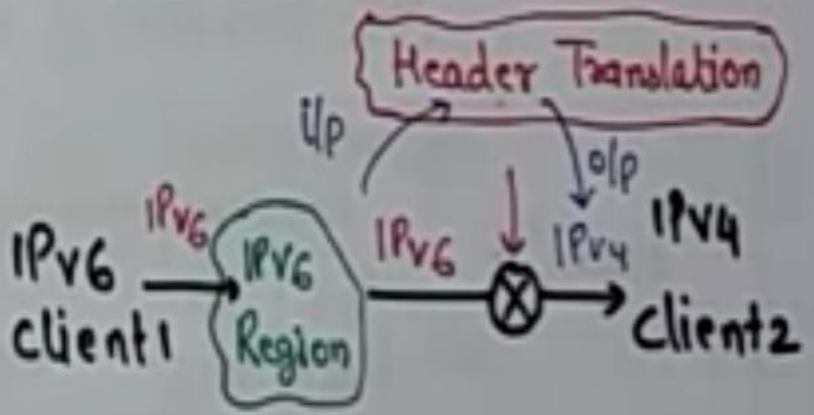
Tunneling



IPv6 Packet is encapsulated in an IPv4 Packet when it enters the IPv4 Region.

Header Translation

When most of system are on IPv6 but some still uses IPv4.



Difference Between IPv4 and IPv6 IMP..

IPv4	IPv6
1.) Length of Address: 32 Bit	i) Length of Address: 128 Bit
2.) Represent in Decimal notation	ii) Represented in Hexadecimal notation
3.) IPsec Support: Optional	3.) IPsec Support: Inbuilt
4.) Packet Flow Indication: NONE	4.) Packet Flow: YES → FLOW Label field
5.) checksum field: YES	5.) checksum field: NONE
6) option field: YES	6) options field: NONE, IPv6 Extension Header ✓
7.) Address(IP) to MAC = (ARP)	7.) Replaced By: Neighbour Discovery (NDP) Protocol
8) Broadcast Message: YES	8) Broadcast Message: Special type of Multicast Addr
9.) Total No. of Addresses: 2^{32}	9.) Total No. of Addresses: 2^{128}