SRM INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University

18CSS202J - COMPUTER COMMUNICATIONS

Semester 4 – Academic Year 2021-2022 (Even)

Course Objective:

The purpose of learning this course is to

- Understand the basic services and concepts related to Internetwork
- Understand the layered network architecture
- Acquire knowledge in IP addressing
- Exploring the services and techniques in physical layer
- Understand the functions of Data Link layer
- Implement and analyze the different Routing Protocols

Course Outcomes (CO):

At the end of this course, learners will be able to

1. Apply the knowledge of communication
2. Identify and design the network topologies
3. Design the network using addressing schemes
4. Identify and correct the errors in transmission
5. Identify the guided and unguided transmission media
6. Implement the various Routing Protocols

UNIT –II Contents

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- IPv4 Addressing, Address space
- Dotted Decimal Notation
- ClassfulAddressing
- Subnet Mask
- Subnetting
- Special Addresses
- Classless Addressing
- Private Address, NAT, Supernetting
- Hub, Repeaters, Switch, Bridge
- Structure of Router

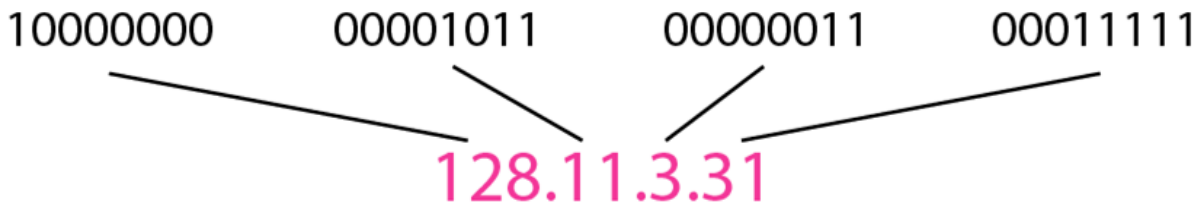
Session 1

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

IPv4 Addressing, Address space
Dotted Decimal Notation
Classful Addressing
Subnet Mask
Subnetting

IPv4 Address ,address space

- The IPv4 addresses are unique and universal.
- An IPv4 address is 32 bits long.
  - The address space of IPv4 is 2^{32} (4,294,967,296)
  - Notation.
    - Binary notation
    - Dotted-decimal notation



IPv4

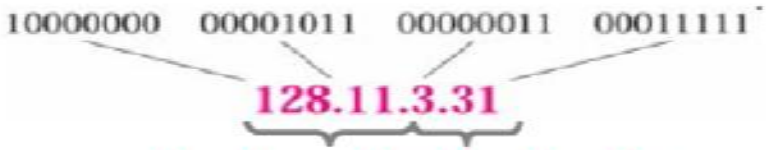
- 32 bits long
  - An **IPv4 address is a 32-bit address that *uniquely and universally defines the connection*** of a device (for example, a computer or a router) to the Internet.
- Unique and Universal.
  - Two devices on the Internet can never have the same address at the same time
  - Addressing system must be accepted by any host that wants to be connected to the Internet.

IPV4 NOTATIONS

IP Address: Binary Notation – 32-bit / 4-byte representation with a space inserted between each octet (byte)

IP Address: Decimal Notation – 4-number decimal representation with a decimal dot separating the numbers

- each decimal number corresponds to a byte
  ⇒ each decimal number ∈ [0, 255]



IP address = network part + host part

assigned by global authority (ICANN) to organization

assigned by local authority to particular machine

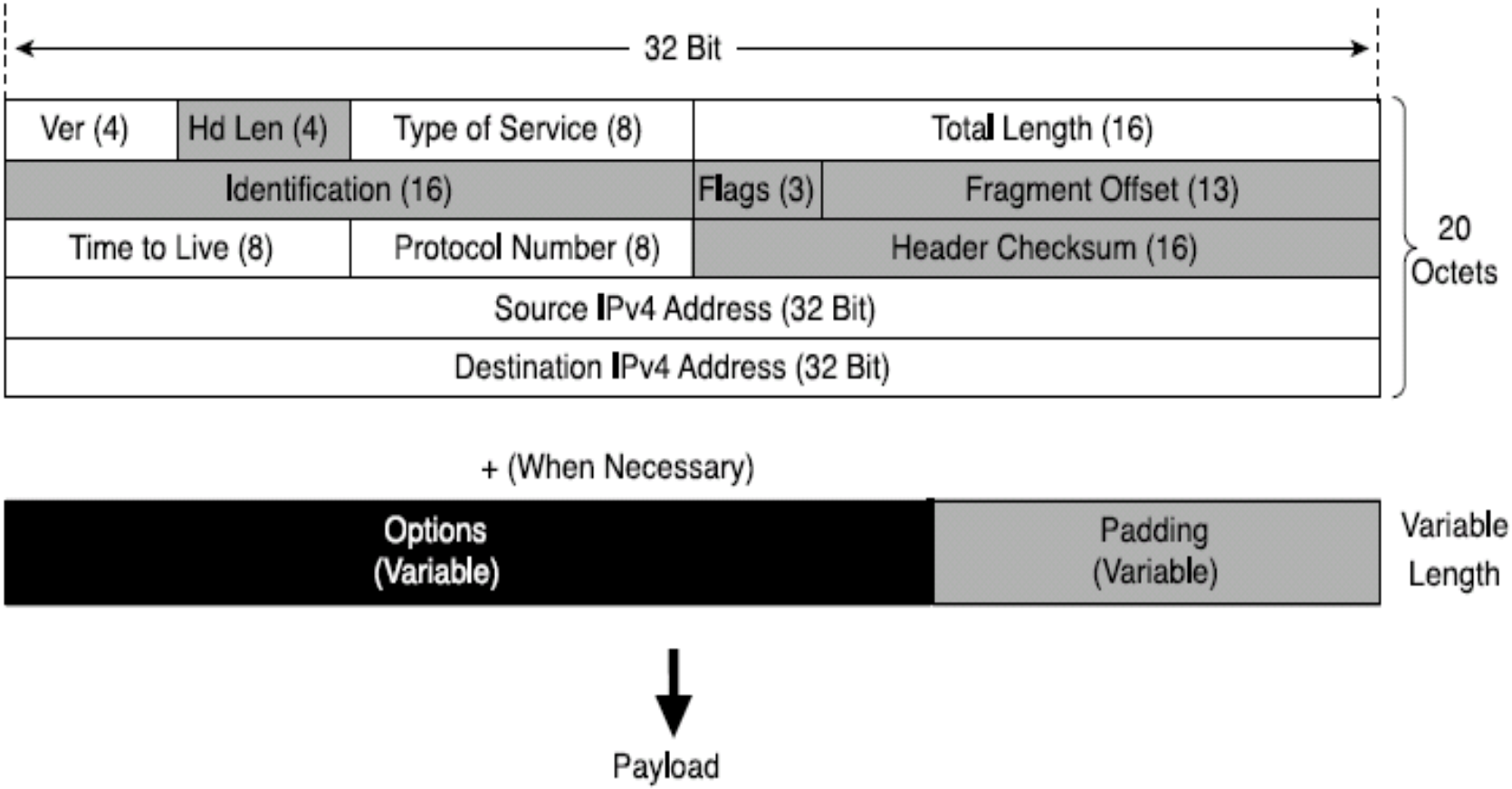
Example [IP Address Conversion]

Change the following IP addresses from binary to dotted decimal notation.

(a) 10000001 00001011 00001011 11101111 ⇒ 129.11.11.239
(b) 11111001 10011011 11111011 00001111 ⇒ 249.155.251.15

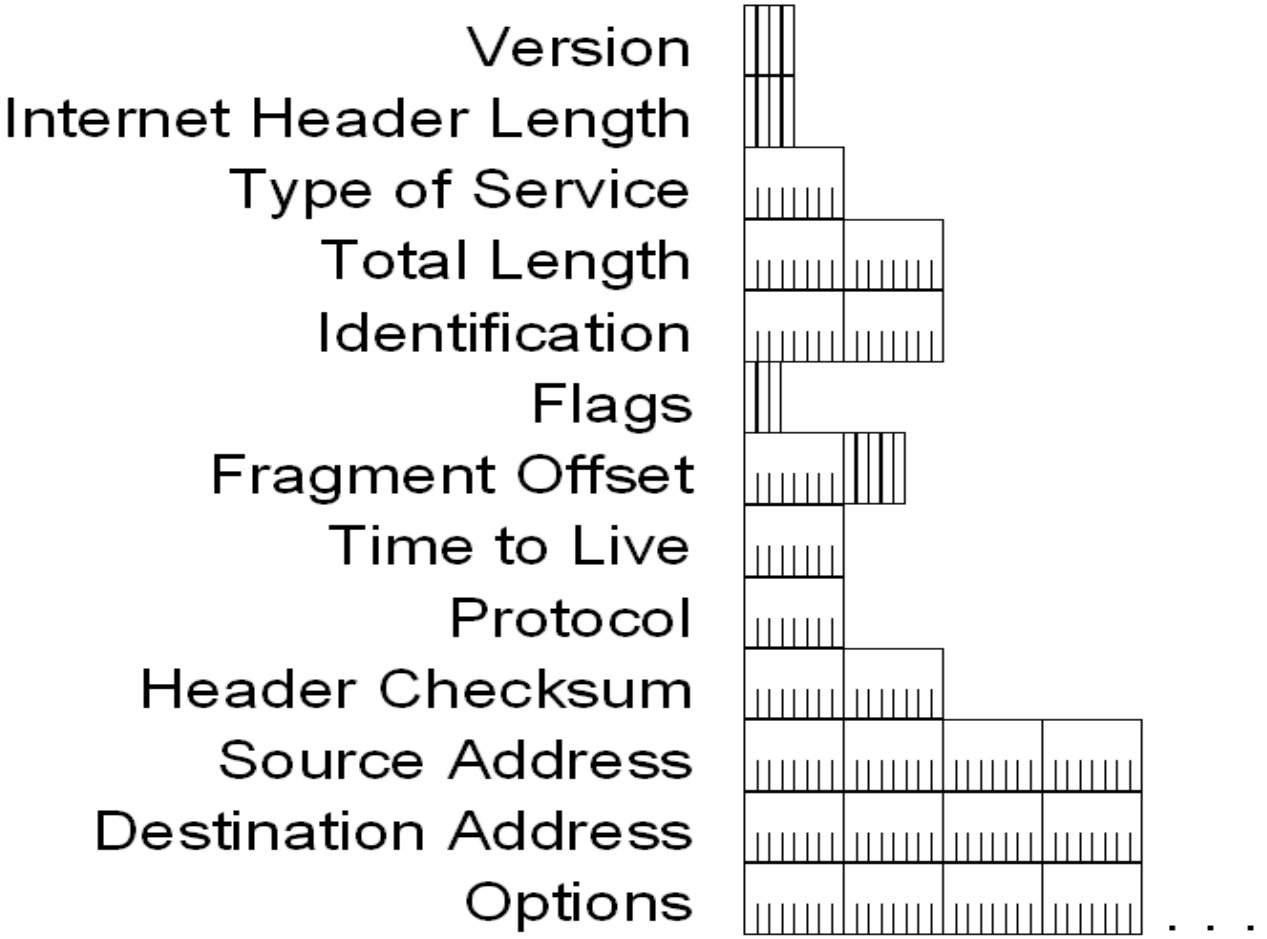
- An easier way to remember IP addresses is by assigning to them a name.
- (e.g., www.google.com), which is resolver through the Domain Name System (DNS).
- Strictly speaking, an IP address identifies an **interface that is capable of sending and** receiving IP datagrams.
- One system can have multiple such interfaces.
- Usually, hosts have only one interface (thus, one IP address), whereas routers have many interfaces (thus, many IP addresses).

IPv4 Header Structure



- basic IPv4 header contains 12 fields.
- each field of the IPv4 header has a specific use.
- Shaded field are removed in IPv6.

IPv4 Header - Review



IPv4 Header - Review

- **Version (4 bits)**
  - Indicates the version of IP and is set to 4.
- **Internet Header Length (4 bits)**
  - Indicates the number of 4-byte blocks in the IPv4 header.
  - Because an IPv4 header is a minimum of 20 bytes in size, the smallest value of the Internet Header Length (IHL) field is 5.
- **Type of Service (4 bits)**
  - Indicates the desired service expected by this packet for delivery through routers across the IPv4 internetwork.

IPv4 Header - Review

- **Total Length (16 bits)**
  - Indicates the total length of the IPv4 packet (IPv4 header + IPv4 payload) and does not include link layer framing.
- **Identification (16 bits)**
  - Identifies this specific IPv4 packet.
  - The Identification field is selected by the originating source of the IPv4 packet. If the IPv4 packet is fragmented, all of the fragments retain the Identification field value so that the destination node can group the fragments for reassembly.
- **Flags (3 bits)**
  - Identifies flags for the fragmentation process.
  - There are two flags—one to indicate whether the IPv4 packet might be fragmented and another to indicate whether more fragments follow the current fragment.
- **Fragment Offset (13 bits)**
  - Indicates the position of the fragment relative to the original IPv4 payload.

IPv4 Header - Review

- **Time to Live (8 bits)**
  - Indicate the maximum number of links on which an IPv4 packet can travel before being discarded.
  - Originally used as a time count with which an IPv4 router determined the length of time required (in seconds) to forward the IPv4 packet, decrementing the TTL accordingly. When the TTL equals 0,an ICMP Time Expired-TTL Expired in Transit message is sent to the source IPv4 address and the packet is discarded.
- **Protocol (8 bits)**
  - Identifies the upper layer protocol.
  - For example, TCP uses a Protocol of 6, UDP uses a Protocol of 17, and ICMP uses a Protocol of 1.
  - The Protocol field is used to demultiplex an IPv4 packet to the upper layer protocol.

IPv4 Header - Review

- **Header Checksum (16 Bits)**
  - Provides a checksum on the IPv4 header only.
  - The IPv4 payload is not included in the checksum calculation as the IPv4 payload and usually contains its own checksum..
- **Source Address (32 bits)**
  - Stores the IPv4 address of the originating host.
- **Destination Address (32 bits)**
  - Stores the IPv4 address of the destination host.
- **Options (multiple of 32 bits)**
  - Stores one or more IPv4 options.

Session 2

Subnet Mask
Subnetting

Types of addressing

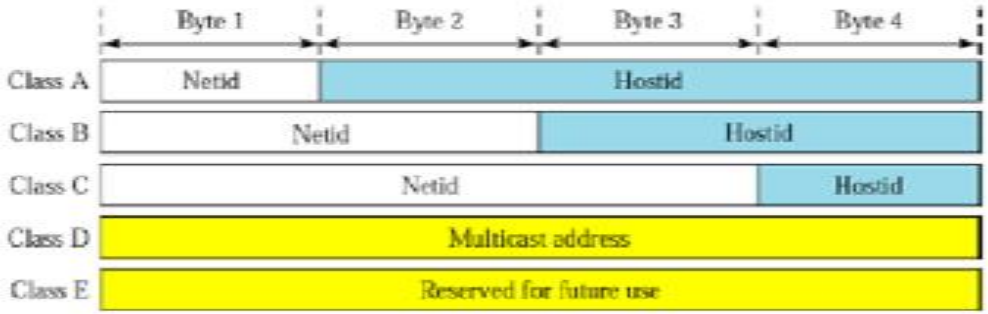
- Classful Addressing
- Classless Addressing

Classful Addressing and Problem solving

Classful IP Addressing

Classful IP Addressing – supports addressing of different size networks by dividing address space into 5 classes: A, B, C, D, E

- an IP address in classes A, B, and C is divided into **Netid** and **Hostid**
- **class A addresses** (**1-byte Netid**): get assigned to organizations with a large number of hosts or routers – there are only 126 class A networks with up to 16 million hosts in each
- **class B addresses** (**2-byte Netid**): allow around 16,000 networks and around 64,000 hosts per each network
- **class C addresses** (**3-byte Netid**): allow around 2 million networks and around 254 hosts per each network

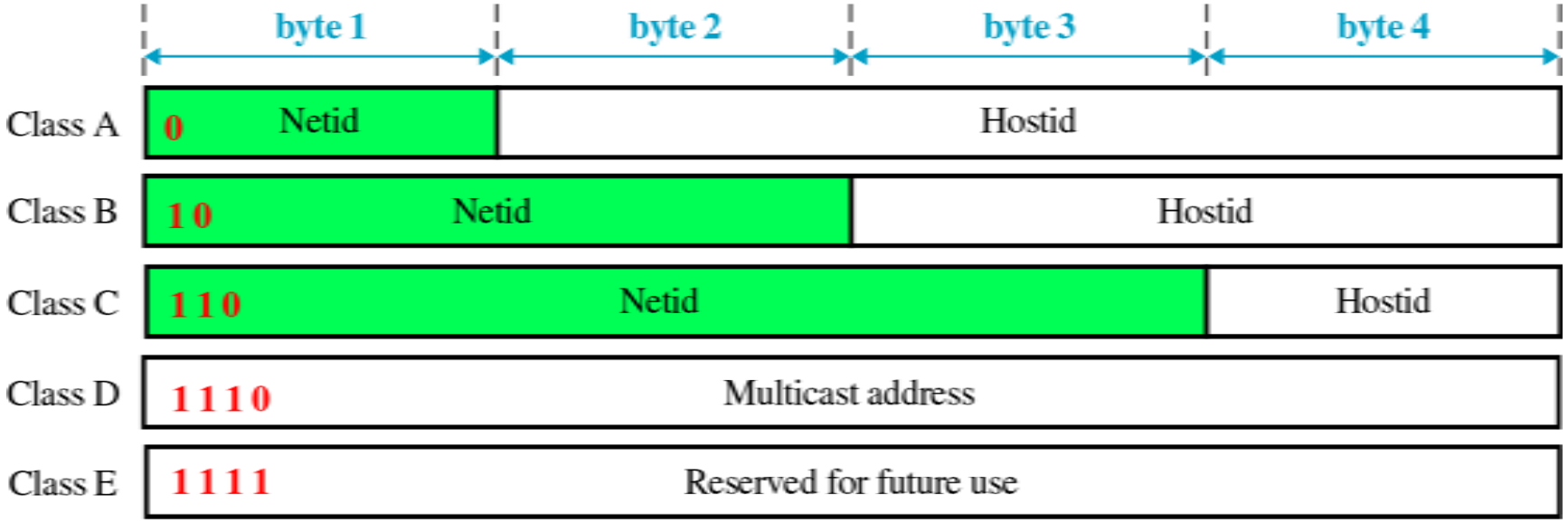


While many class A and B addresses are wasted, the number of addresses in class C is smaller than the needs of most organizations.

How do we know if an IP address is a class-A / B or C!?

Classful Addressing

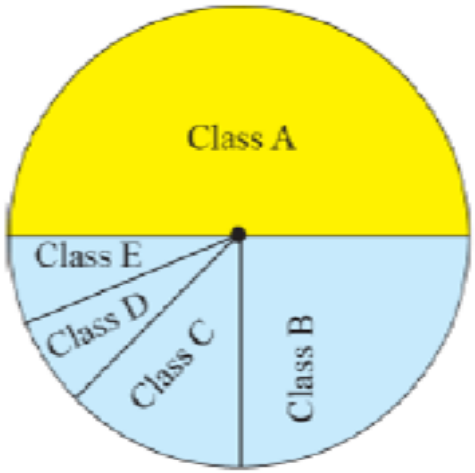
- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

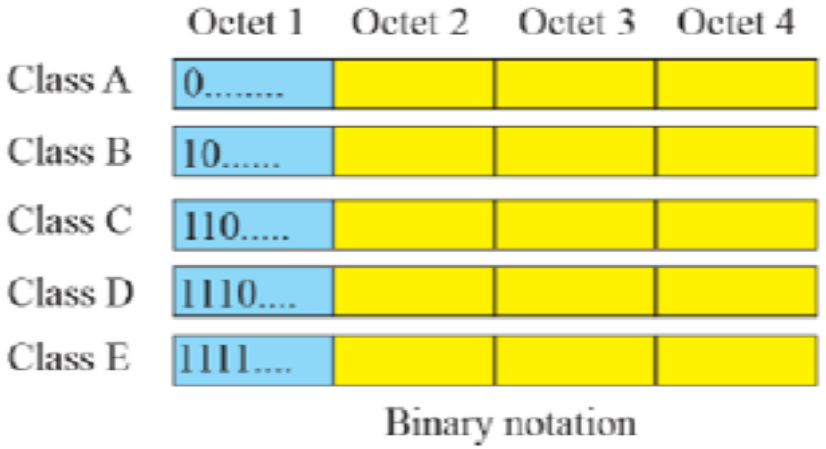


Classful Addressing

SRM INSTITUTE OF SCIENCE & TECHNOLOGY (Deemed to be University u/s 3 of UGC Act, 1956)

Occupation of Address Space by Class





Binary notation

Class A: 2^{31} = 2,147,483,648 addresses, 50%

Class B: 2^{30} = 1,073,741,824 addresses, 25%

Class C: 2^{29} = 536,870,912 addresses, 12.5%

Class D: 2^{28} = 268,435,456 addresses, 6.25%

Class E: 2^{28} = 268,435,456 addresses, 6.25%

Classful Addressing – Class Range

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

Example 1

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

Example 2

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

a. 111.56.45.78

b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

Example 3

Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

Solution

a. The first bit is 0. This is a class A address.

b. The first 2 bits are 1; the third bit is 0. This is a class C address.

c. The first byte is 14; the class is A.

d. The first byte is 252; the class is E.

Table 1 *Number of blocks and block size in classful IPv4 addressing*

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Note

In classful addressing, a large part of the available addresses were wasted.

Table 2 ***Default masks for classful addressing***

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Note

Classful addressing, which is almost obsolete, is replaced with classless addressing.

Note

In IPv4 addressing, a block of addresses can be defined as x.y.z.t /*n* in which x.y.z.t defines one of the addresses and the /*n* defines the mask.

Note

The first address in the block can be found by setting the rightmost $32 - n$ bits to 0s.

Example 4

A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first address in the block?

Solution

The binary representation of the given address is

11001101 00010000 00100101 00100111

If we set 32−28 rightmost bits to 0, we get

11001101 00010000 00100101 0010000

or

205.16.37.32.

Note

The last address in the block can be found by setting the rightmost $32 - n$ bits to 1s.

Example 5

Find the last address for the block in 205.16.37.39/28.

Solution

The binary representation of the given address is

11001101 00010000 00100101 00100111

If we set 32 − 28 rightmost bits to 1, we get

11001101 00010000 00100101 00101111

or

205.16.37.47

Note

The number of addresses in the block can be found by using the formula 2^{32-n}.

Example 6

Find the number of addresses in 205.16.37.39/28.

Solution

The value of n is 28, which means that number of addresses is 2^{32-28} *or 16.*

Example 7

Another way to find the first address, the last address, and the number of addresses is to represent the mask as a 32-bit binary (or 8-digit hexadecimal) number. This is particularly useful when we are writing a program to find these pieces of information. In Example 19.5 the /28 can be represented as

11111111 11111111 11111111 11110000

(twenty-eight 1s and four 0s).

Find

a. The first address

b. The last address

c. The number of addresses.

Example 7 (continued)

Solution

a. The first address can be found by ANDing the given addresses with the mask. ANDing here is done bit by bit. The result of ANDing 2 bits is 1 if both bits are 1s; the result is 0 otherwise.

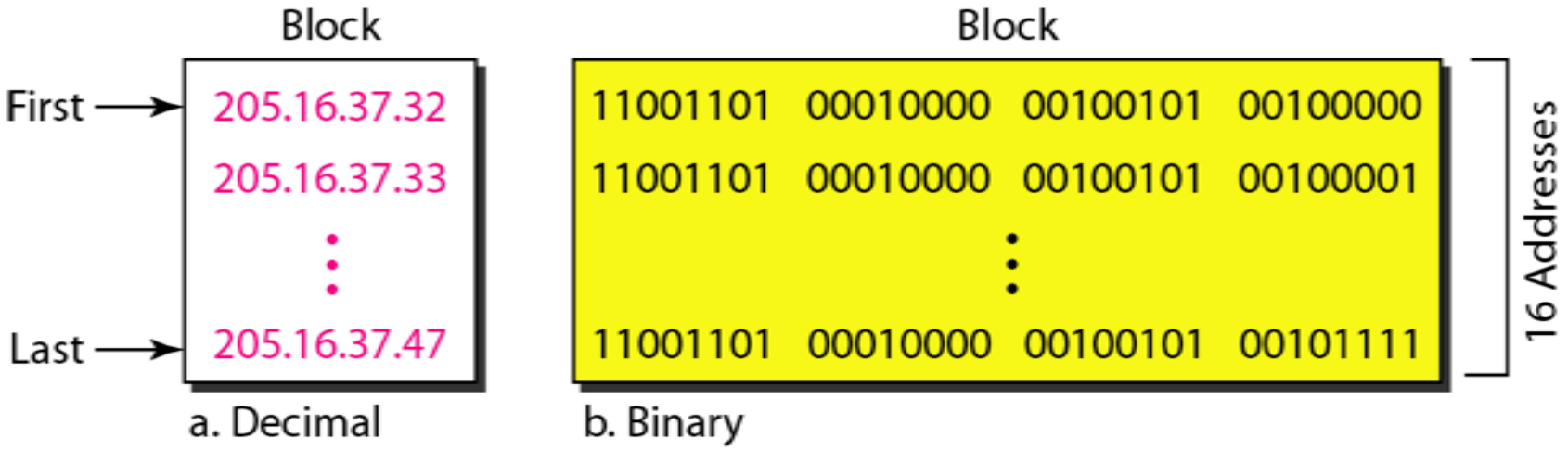
Address:	11001101	00010000	00100101	00100111
Mask:	**11111111**	**11111111**	**11111111**	**11110000**
First address:	11001101	00010000	00100101	00100000

Example 7 (continued)

b. The last address can be found by ORing the given addresses with the complement of the mask. ORing here is done bit by bit. The result of ORing 2 bits is 0 if both bits are 0s; the result is 1 otherwise. The complement of a number is found by changing each 1 to 0 and each 0 to 1.

Address:	11001101	00010000	00100101	00100111
Mask complement:	**00000000**	**00000000**	**00000000**	**00001111**
Last address:	11001101	00010000	00100101	00101111

Figure 1 *A network configuration for the block 205.16.37.32/28*



Note

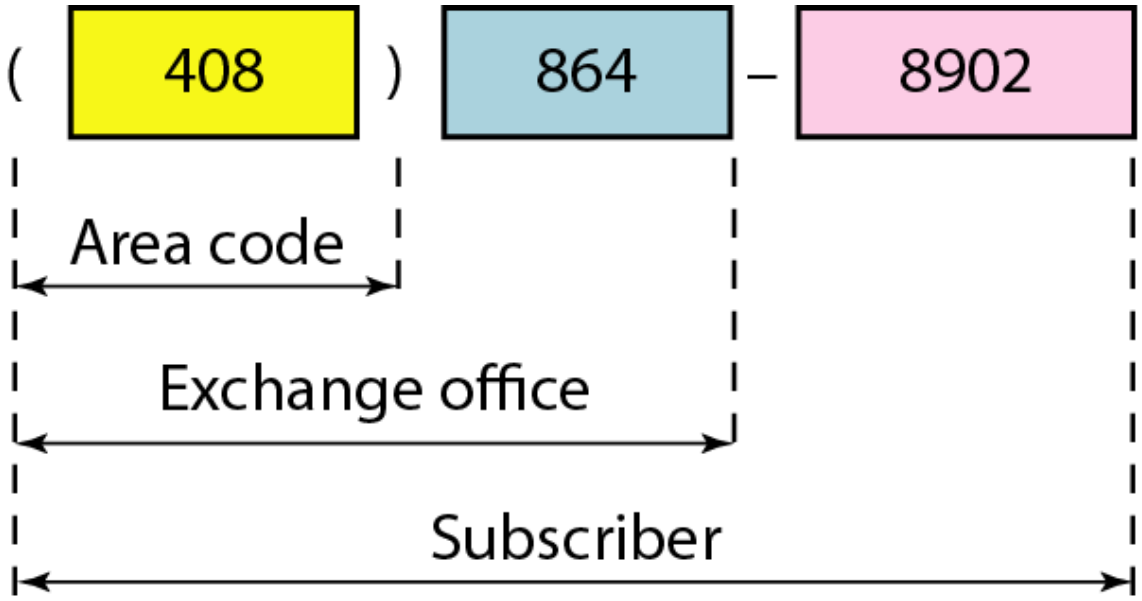
The first address in a block is
normally not assigned to any device;
it is used as the network address that represents the organization
to the rest of the world.

Two level hierarchy - Three level hierarchy- subnet mask - Address aggregation- problem solving.

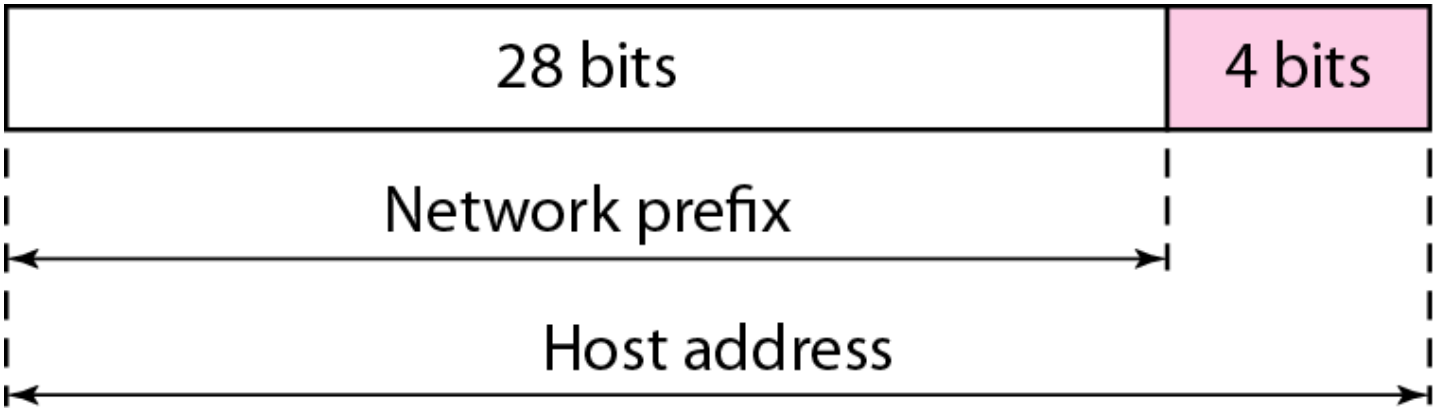
Hierarchy of IPv4 Addressing

- Each address in the block can be considered as a two-level hierarchical structure: the leftmost *n* bits (prefix) define the network; the rightmost 32 – *n* bits define the host.
- Why Hierarchy?

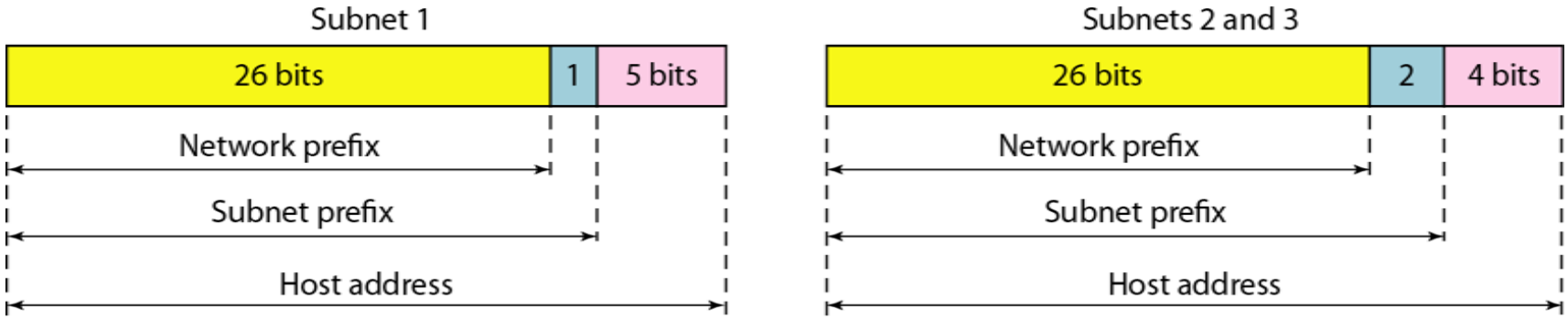
Figure 2 *Two levels of hierarchy in an IPv4 address*



Two Level of Hierarchy



Three Level of Hierarcny



Address Aggregation

- IP Address Aggregator is a utility developed to automate minimization process and convert bunch of IPv4 addresses into smallest continuous range(s) possible. IP aggregation is commonly performed by network engineers working with BGP & routers.
- This utility will help webmasters to configure server firewalls, apache, address masks and so on.

Session 5

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Special Addresses

Special Addresses

- An IP address (internet protocol address) is a numerical representation that uniquely identifies a specific interface on the network.
- Addresses in IPv4 are 32-bits long. This allows for a maximum of 4,294,967,296 (2^{32}) unique addresses. Addresses in IPv6 are 128-bits, which allows for 3.4 x 10^{38} (2^{128}) unique addresses.
- The total usable address pool of both versions is reduced by various reserved addresses and other considerations.
- IP addresses are binary numbers but are typically expressed in decimal form (IPv4) or hexadecimal form (IPv6) to make reading and using them easier for humans.

Special Addresses

- There are a few reserved IPv4 address spaces which cannot be used on the internet. These addresses serve special purpose and cannot be routed outside the Local Area Network.
- As in Classful IP Addressing, some blocks of addresses or some addresses in each block have been reserved for the special purpose & that's why they are termed as **special IP addresses.**
- The special addresses of classful addressing were inherited by the classless addressing when it was introduced in 1996.
- There can be an entire block of addresses reserved for special addressing or there can be some addresses in each block that are reserved for special addressing.

Special Addresses

1. Special Blocks of Addresses

- There are some blocks of addresses in IPv4 address space that are reserved for a special objective.
- The special blocks of addresses are listed below:

a) All Zeros Address

b) All Ones Address

c) Loopback Addresses

d) Private Addresses

e) Multicast Addresses

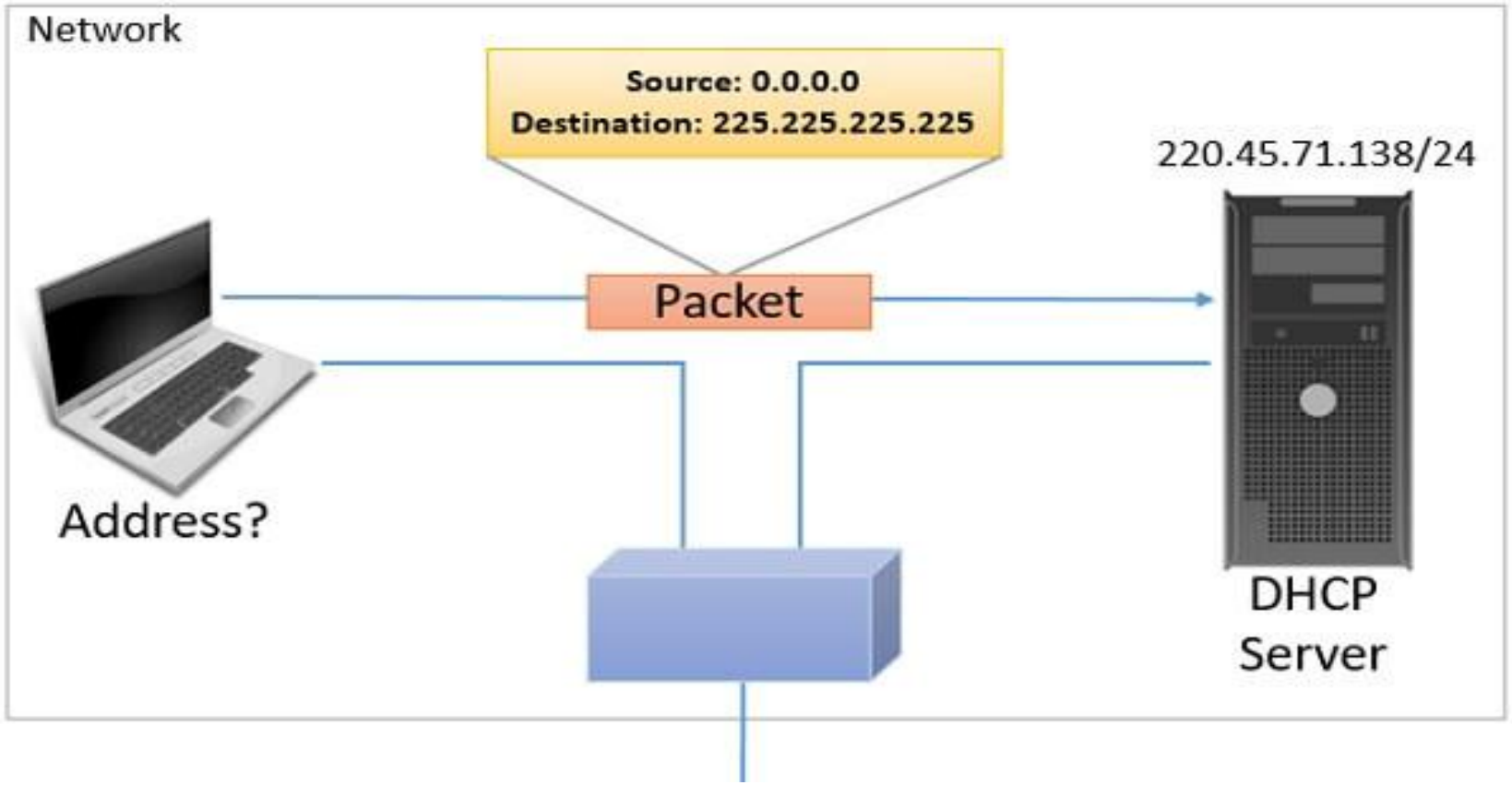
Special Addresses

a) All Zeros Address

- The all-zeros address block **0.0.0.0/32** is a special block in Ipv4 address space.
- The length of the **prefix** here is **32**. The number of addresses in this block is equal to $2^{32-32} = 2^0 = 1$. So, this block has only one address with all the 32 bits as zero. This address is the **first address** in the IPv4 address space.
- Any host having this IP address means the **host is not connected to the TC/IP network**. When the host wants to get connected to the internet, it sends a request packet to the **bootstrap server** which is also called a **DHCP server**.
- The packet sent by the host to DHCP server has **source address** as **0.0.0.0** and **225.225.225.225** as the **destination address.**
- The DHCP server then assigns the IP address to the host and host then get connected to the Internet.

Special Addresses

a) All Zeros Address



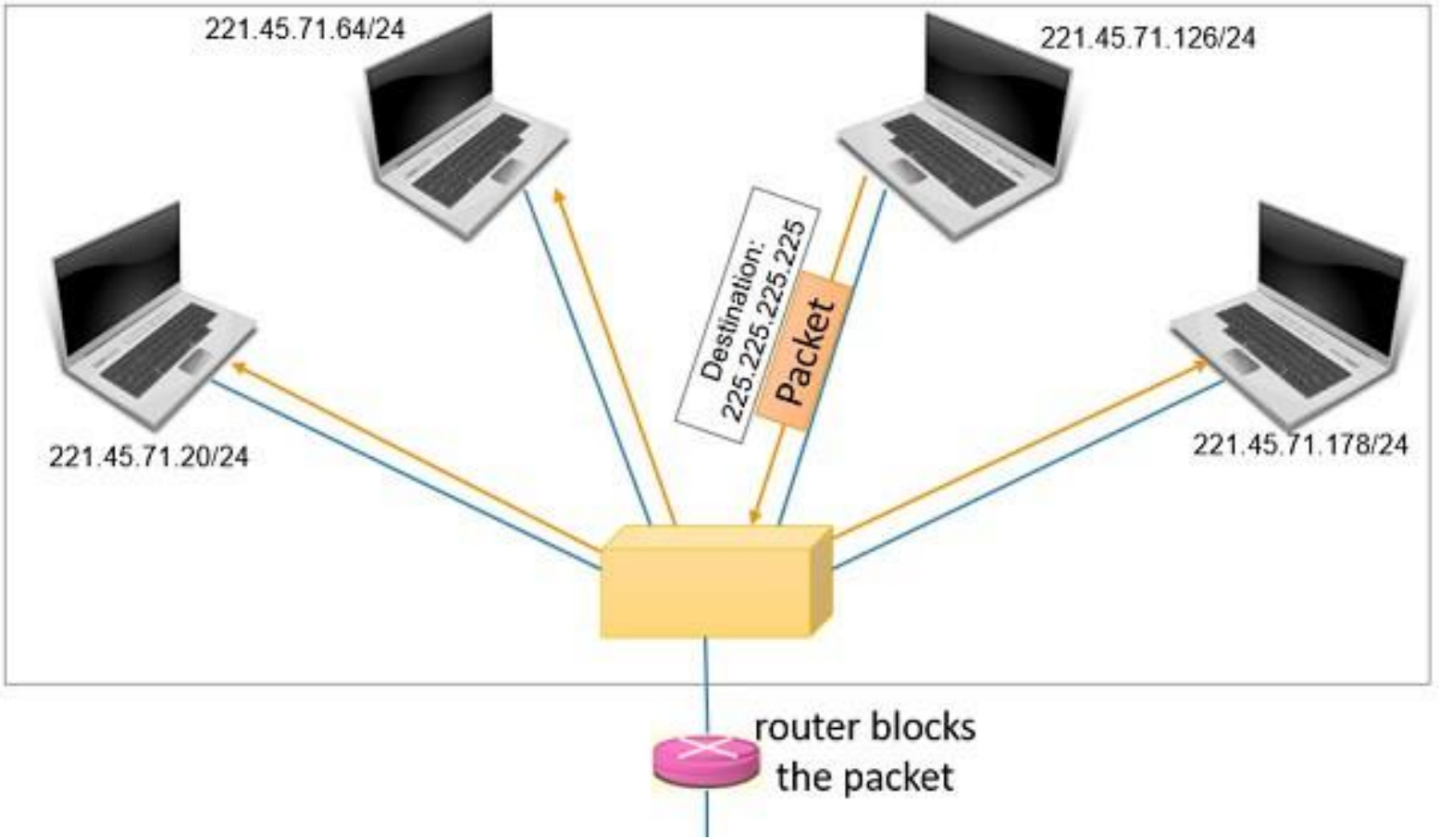
Special Addresses

b) All One Address

- The block **225.225.225.225/32** is also a special block in IPv4 address space.
- Here, all the **32 bits** of **IPv4 address** is '**1**'. The length of the prefix here is 32.
- The number of addresses in this special block can be calculated as $2^{32-32} = 2^0 = 1$.
- This is the **last address** in IPv4 address space. This address is also called **Limited Broadcast Address** we will see the reason why it is a **limited** broadcast address.
- If a host wants to send the message to **every** other host in the current network, which means the host wants to **broadcast** a message in the **current network**. Then the host uses this address as the **destination**

Special Addresses

b) All One Address



Special Addresses

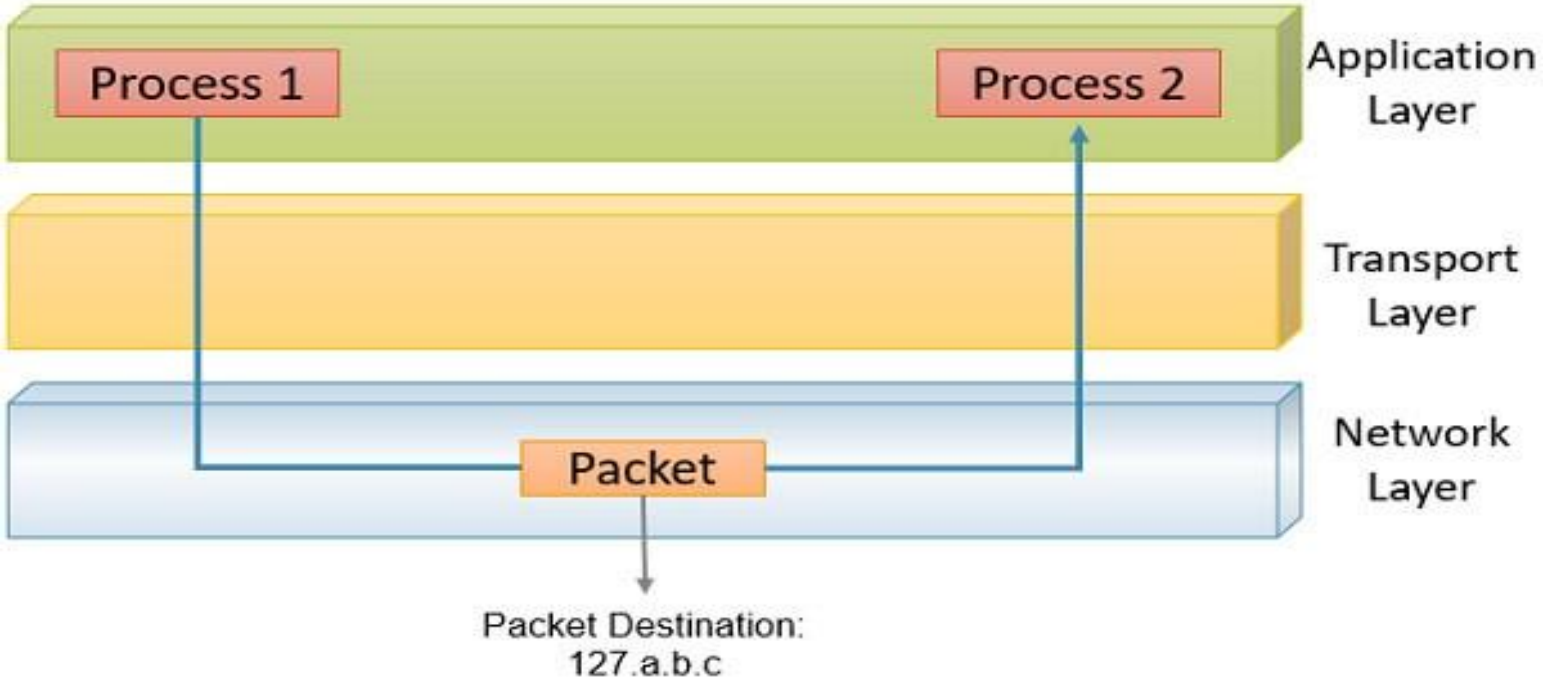
c) Loopback Addresses

- The special block **127.0.0.0/8** has addresses which are used as **loopback addresse**s. Now, the prefix length here is 8 so, the number of addresses can be calculated as $2^{32-8} = 2^{24}$ = **1,67,77,216**. This special block has 1,67,77,216 addresses. If we consider this address in classful addressing, then this block is the last block of class A.
- All the addresses starting with **127**. should be considered as loopback addresses. The **loopback address** can only be the **destination address** of a packet. The packet with loopback address **never leaves the machine** from which it is sent, it just **returns back** to the source.

Special Addresses

c) Loopback Addresses

- For example, it can be used to check whether the NIC is properly functioning or not. To check the network application on the system. Out of 1,67,77,216 loopback addresses only **127.0.0.1** is used rest 1,67,77,215 addresses are just total **v**



Special Addresses

d) Private Addresses

- The private IP addresses are never used globally. The packet with a private IP address is **not routed on the internet**.
- The private IP addresses are configured by the administrator of the network.
- Devices on the same network use private IP addresses to converse with each other.
- They do not require the internet for their communication. Like, the file servers, desktops and printers can communicate with each other without the requirement of internet.
- But, when they want to communicate with the device out of their network they translate a private IP address into the public IP address

Special Addresses

d) Private Addresses

- The range of private IP addresses is given below:

Block of Private IP addresses	Number of addresses in each block
10.0.0.0/8	16,777,216
172.16.0.0/12	1,047,584
192.168.0.0/16	65,536
169.254.0.0/16	65,536

Special Addresses

e) Multicast Addresses

- The block **224.0.0.0/4** has the multicast address. The length of the **prefix** is **4**.
- The number of addresses used for multicast communication is

  $2^{32-4} = 2^{28} =$ **26,84,35,456**.
- The multicast address is assigned to the group of the host instead of one single host.
- The packet sent to the multicast address is delivered to all the host of that group.

Special Addresses

2. Special IP Addresses in Each Block

- There are two special addresses which are in each block:

a) Network Address

b) Direct Broadcast Address

Special Addresses

a) Network Address

- In classful and classless addressing the first address of the block is the network address itself.
- The **first address** of the block has **all** the **suffix bits** as '**0**'.
- The network address is not allocated to any of the hosts in the network.
- If the block has been subnetted and the network has been divided into **subnetwork** then the first address of subnetwork will play the same role as the network address. The first address of the subnetwork is also termed as **subnetwork address** and this subnetwork address will not be assigned to any host in the subnetwork.
- In case the assigned block is **too small** then it is not possible to consider some of the addresses in the block as special address.

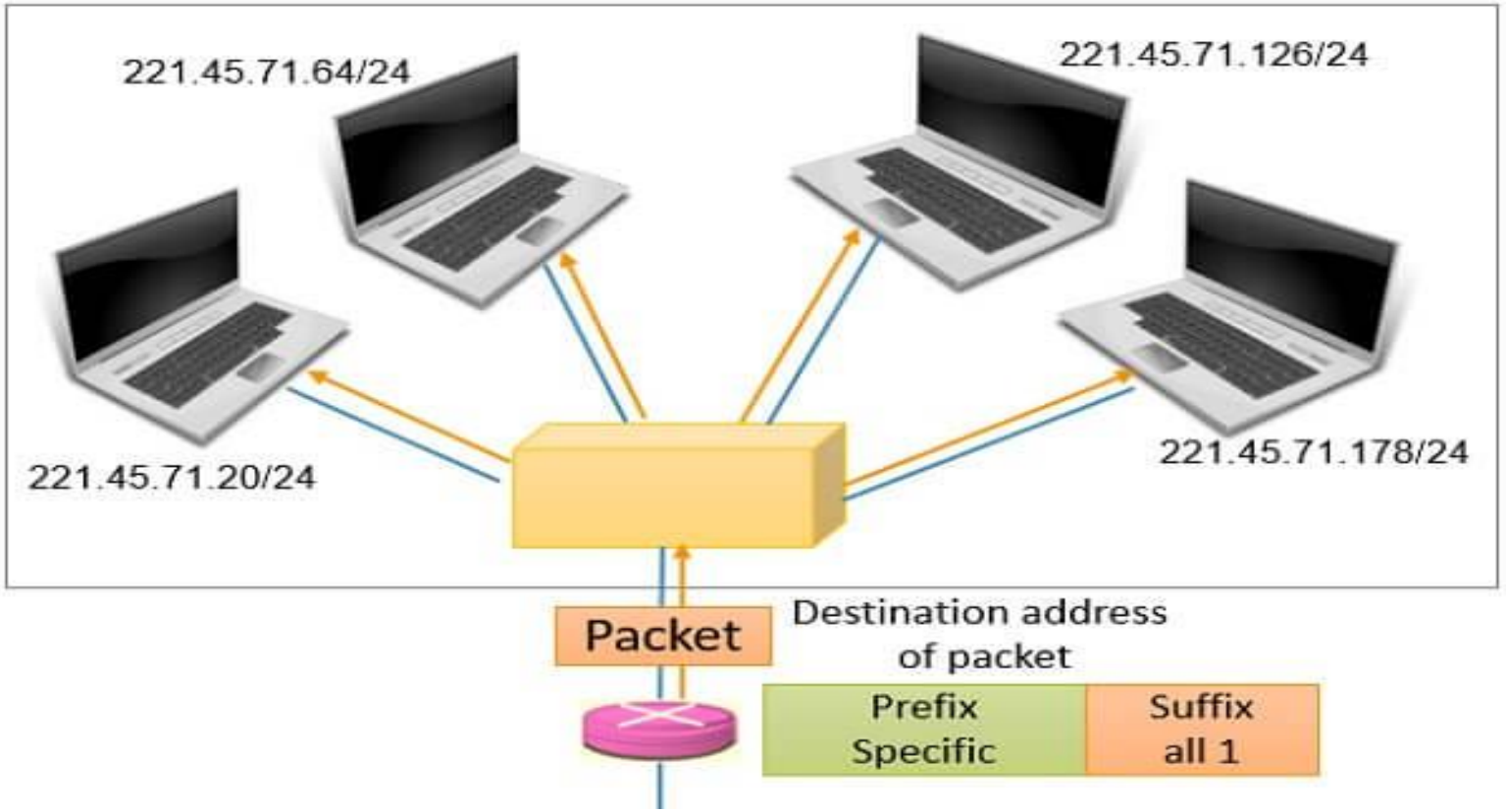
Special Addresses

b) Direct Broadcast Address

- As first address in the block is reserved as the network address.
- The **last address of the block** is reserved as a **direct broadcast address**.
- The direct-broadcast address has **all** its **suffix** bits as '**1**'.
- Whenever the router obtains the IPv4 packet with a destination address who's all suffix bits are 1 it broadcast that packet to all the host in the specific network.
- Direct broadcast address will always be used as the **destination address** in IPv4 packet.

Special Addresses

b) Direct Broadcast Address



This is about the special addresses and special blocks of addresses.

Session 6

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Classless Addressing
- Problem Solving

Classless Addressing

- **To overcome address depletion** and give **more organizations access to the Internet**, classless addressing was designed and implemented.

Classless Addressing

Address Blocks

- In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a **BLOCK (RANGE) OF ADDRESSES**.
- The size of the block (the number of addresses) varies based on the nature and size of the entity.

For example:

A household only two addresses

A large organization given thousands of addresses.

An ISP, as the Internet service provider given thousands or hundreds of thousands based on the number of customers it may serve.

Classless Addressing - Restriction

To simplify the handling of addresses, the Internet authorities impose **three restrictions** on classless address blocks:

1. Addresses in a block must be **contiguous**, one after another.
2. Number of addresses in a block must be a **power of 2 (I, 2, 4, 8, ...).**
3. First address must be evenly **divisible by the number of addresses**.

Slash Notation

Slash notation is also called CIDR (Classless inter-domain routing) notation.

A.B.C.D/*n*

Example An organization is given a block with the beginning address and the prefix length **205.16.37.24/29** (in slash notation).

What is the range of the block?

The beginning address is **205.16.37.24**. To find the last address we keep the first 29 bits and change the last 3 bits to 1s.

Beginning: **11001111 00010000 00100101 00011**000

Ending : **11001111 00010000 00100101 00011**111

We can argue that the length of the suffix is 32 − 29 or 3. So there are 2^3 = 8 addresses in this block. If the first address is 205.16.37.24, the last address is 205.16.37.31 (24 + 7 = 31).

68

Slash Notation

A block in classes A, B, and C can easily be represented in slash notation as **A.B.C.D/*n***

where *n* is either **8 (class A), 16 (class B), or 24 (class C)**.

What is the network address if one of the addresses is 167.199.170.82/27

The prefix length is 27, which means that we must keep the first 27 bits as is and change the remaining bits (5) to 0s.

The 5 bits affect only the last byte. The last byte is 01010010. Changing the last 5 bits to 0s, we get 01000000 or 64.

The network address is 167.199.170.64/27.

Problem Solving

An ISP is granted a block of addresses starting with 190.100.0.0/16. The ISP needs to distribute these addresses to three groups of customers as follows:

1. The first group has 64 customers; each needs 256 addresses.
2. The second group has 128 customers; each needs 128 addresses.
3. The third group has 128 customers; each needs 64 addresses.

Design the sub blocks and give the slash notation for each sub block.

Find out how many addresses are still available after these allocations?

Solution

Group 1

For this group, each customer needs 256 addresses. This means the suffix length is 8 ($2^8 = 256$).

The prefix length is then 32 - 8 = 24.

01: 190.100.0.0/24 □ 190.100.0.255/24

02: 190.100.1.0/24 □ 190.100.1.255/24

……

64: 190.100.63.0/24□ 190.100.63.255/24

Total = 64 × 256 = 16,384

Group 2

For this group, each customer needs 128 addresses. This means the suffix length is 7 ($2^7 = 128$).

The prefix length is then 32 − 7 = 25. The addresses are:

001: 190.100.64.0/25 □ 190.100.64.127/25

002: 190.100.64.128/25 □ 190.100.64.255/25

003:190.100.127.128/25 □ 190.100.127.255/25

Total = 128 × 128 = 16,384

Solution

Group 3

For this group, each customer needs 64 addresses. This means the suffix length is 6 (26 = 64).

The prefix length is then 32 - 6 = 26.

001:190.100.128.0/26 □
190.100.128.63/26

002:190.100.128.64/26 □
190.100.128.127/26

……

128:190.100.159.192/26 □
190.100.159.255/26

Total = 128 × 64 = 8,192

Number of granted addresses: 65,536

Number of allocated addresses: 40,960

Number of available addresses: 24,576

Important

- number of host addresses in a block

$$N = 2^{32-n}$$

N = no. of host addresses

n = length of prefix

- First address of a block

First Address = (any address) AND (subnet mask)

- Last address of a block

Last Address = (any address) OR [NOT (subnet mask)]

Problem Solving

Perform CIDR aggregation on the following IP Addresses-

200.96.86.0/24
200.96.87.0/24
200.96.88.0/24
200.96.89.0/24

Solution

Rule 01 - All the IP Addresses must be contiguous unallocated addresses.

Clearly, all IP addresses are contiguous.

Rule 01 - Correct

Rule 02 - Size of the block must be the power of 2

Each IP address prefix length is = 24

Suffix length is = 32 -24 = 8

Total number of IP Addresses = 28 + 28 + 28 + 28 = 4 x 2^8 = 2^2 x 2^8 = 2^10.

Rule 02 - Correct

Rule 03 - The first address of every block must be divisible by the length of the block.

First IP address - 200.96.86.0 - 11001000.01100000.01010110**.00000000**

Last 9 bits (9 least significant bits) are Zero.

That means this address not divisible by 2^10

Rule 03 - Incorrect

All 3 rules are not satisfied. Because of that cant **Perform CIDR aggregation**

Session 9

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Private Address, NAT, Supernetting
- Hub, Repeaters, Switch

Private address, Network addresses translation -Super netting.

PUBLIC & PRIVATE ADDRESSES IN IPV4

- If direct (routed) or indirect (proxy or translator) connectivity to the Internet is desired, there are two types of addresses employed on the Internet
  - **Public addresses**
  - **Private addresses**

Public addresses

- Public addresses are assigned by NETWORK INTERFACE CARD (NIC) - A network interface card (NIC) is a **circuit board or card that is installed in a computer** so that it can be connected to a network.
- Consist of class-based network IDs or blocks of CIDR-based addresses (called CIDR blocks) that are guaranteed to be globally unique to the Internet.
- When the public addresses are assigned, **routes are programmed into the routers of the Internet** so that traffic to the assigned public addresses can reach their locations.

Public Addresses

- Public ip are the ip that can be accessed by every one (i,e) every user has the access to this ip's.

  E.g: Yahoo.com, Google.com etc are the pubic ip's.

Private Addresses

- Private IP addresses are used for numbering the computers in a private network including **home, school/Colleges/Universities and business LANs in airports and hotels** which makes it possible for the computers in the network to communicate with each other.
- Private ip's are the ip that cannot be accessed by every one(i,e) they are privately owned by an organization / private concern. Only the user of that organisation has the access to this ip's.

Eg : SRM University

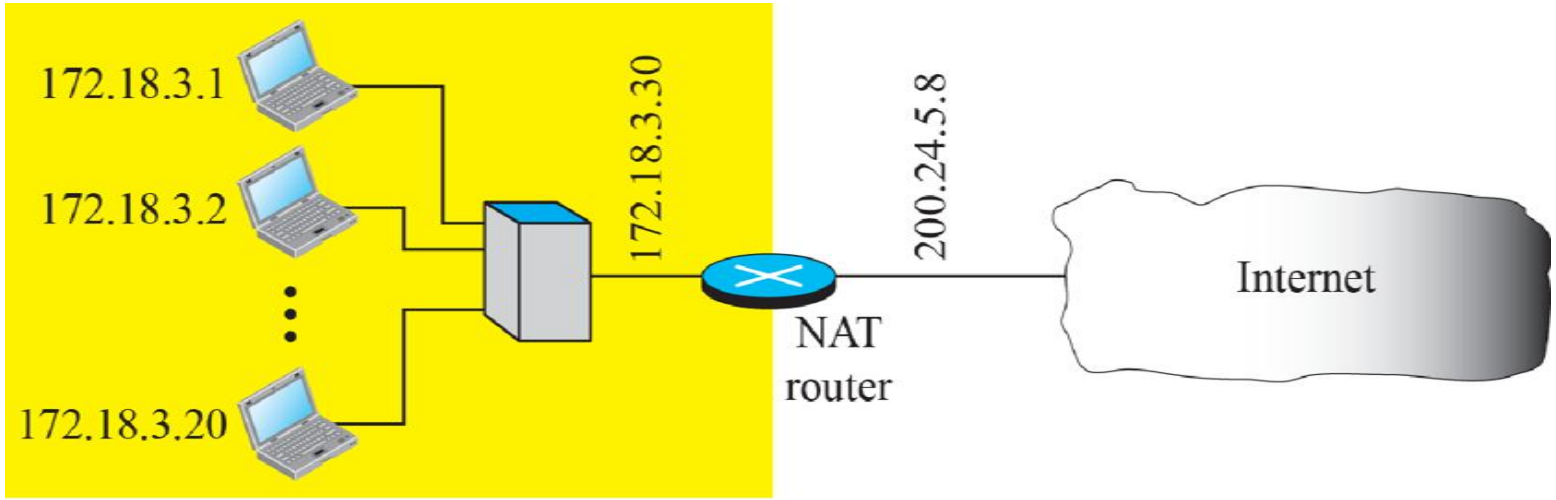
Range of private ip

- Four blocks are assigned as private addresses: 10.0.0.0/**8**, 172.16.0.0/**12**, 192.168.0.0/**16**.
- Range of private IP address are

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

NAT – Network Address Translation

- A technology that can provide the mapping between the private and universal addresses, and at the same time support virtual private networks.
- Allows a site to use a set of private addresses for internal communication and a set of global Internet addresses (atleast one) for communication with the rest of the world.



Site using private addresses

NAT – Network Address Translation

- It is the way that the router *translates* the IP addresses of packets that cross the internet/local network boundary.
  - When computer “A” sends a packet out “from” that of computer “A” – 192.168.1.2. When the router passes that packet on to the internet, it replaces the local IP address with the internet IP address assigned by the ISP.
  - It also keeps track, so that if a response comes back from somewhere on the internet, the router knows to do the translation in reverse – replace the internet IP address with the local IP address for machine “A” and then send that response packet on to machine “A”.
- NAT is not restricted to private-to-public address translation, though that is the most common application.
- NAT can also perform public-to-public address translation, as well as private-to-private address translation.

Example

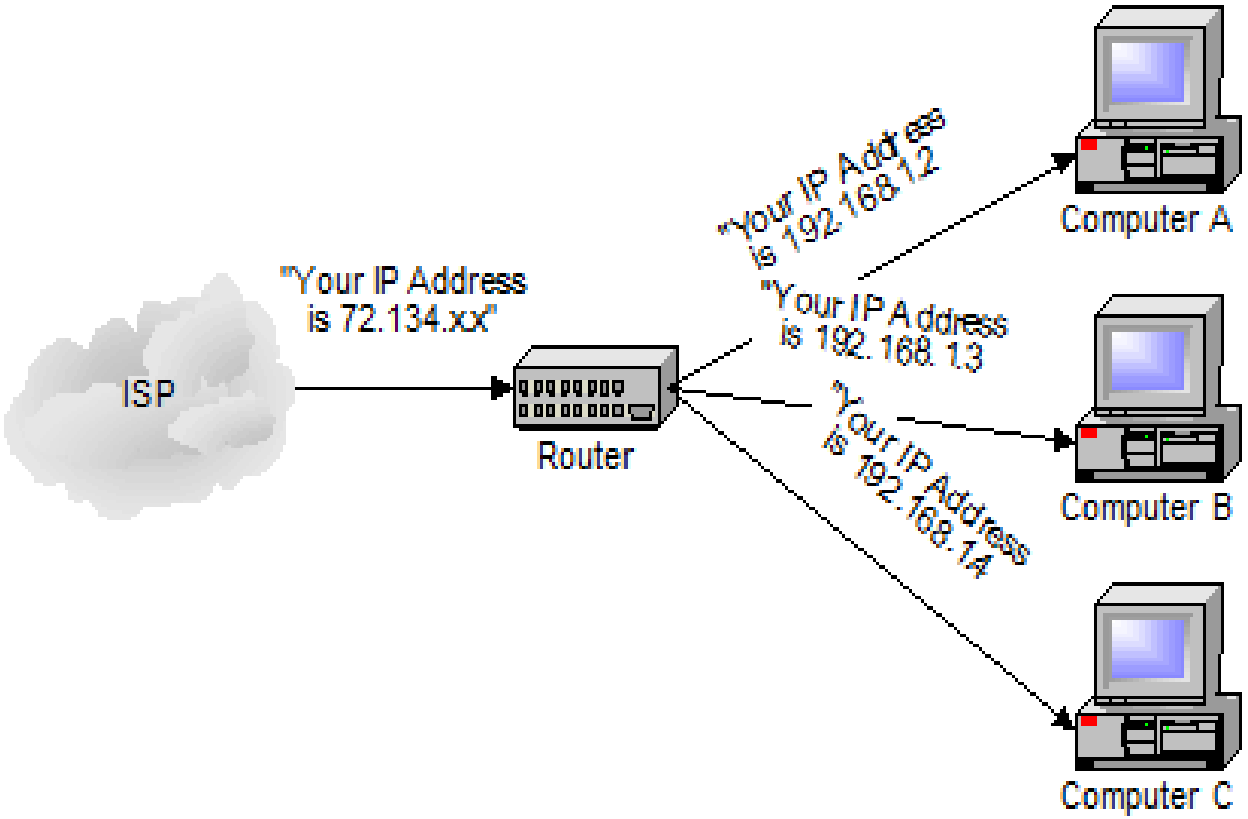
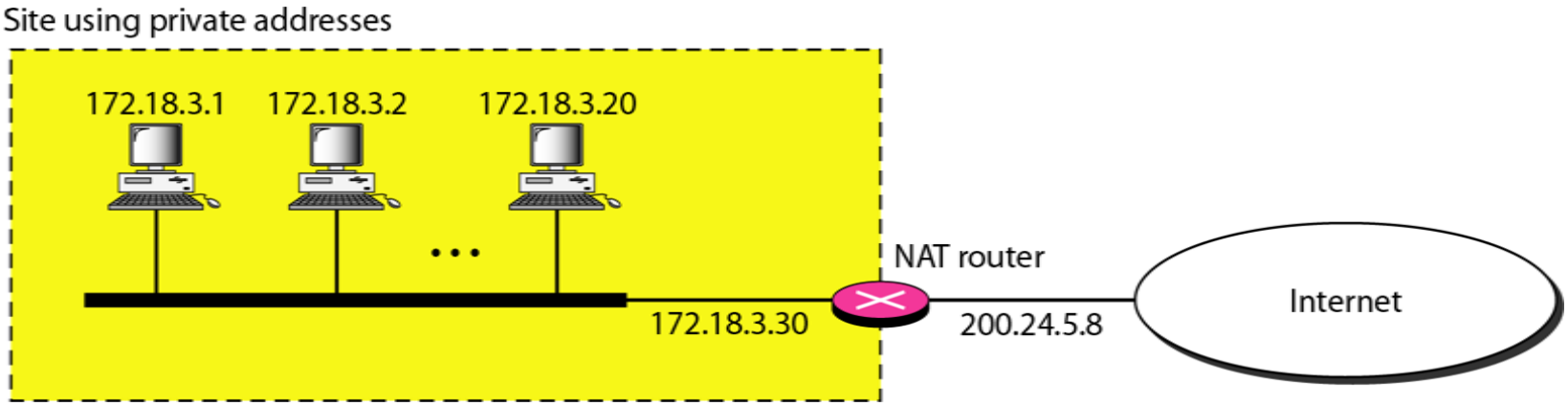
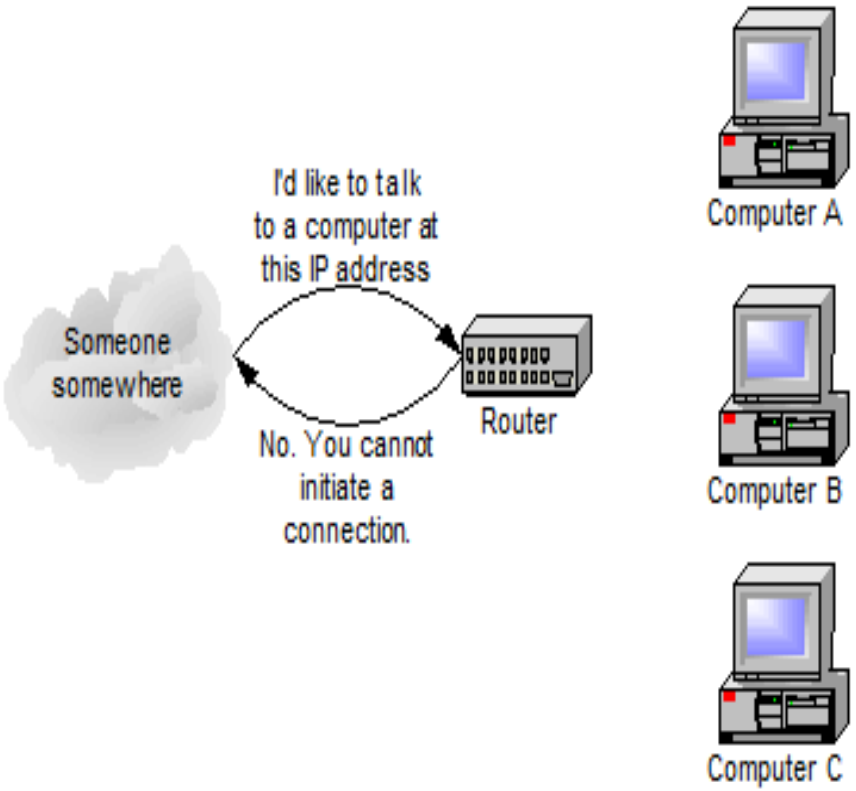

"Your IP Address is 72.134.xx"
ISP
Router
"Your IP Address is 192.168.1.2
"Your IP Address is 192.168.1.3
"Your IP Address is 192.168.1.4
Computer A
Computer B
Computer C

Figure 19.10 *A NAT implementation*



Network Address Translation (NAT)

- Benefits
  - Use of a single IP address among many devices in a network
  - Use of a dynamic IP address for home user for sharing
- Drawbacks
  - Machines on the internet cann initiate communications to loc machines – they can only respor to communications initiated l those local machines. The n effect is that the router then al acts as a firewall.



Subnetting vs supernetting

Subnetting:

- Divide a large address block into smaller sub-groups.
  - If an organization was granted a large block in class A or B, it could divide the addresses into **several contiguous groups and assign each group to smaller networks (called subnets).**
- Use of flexible net mask.

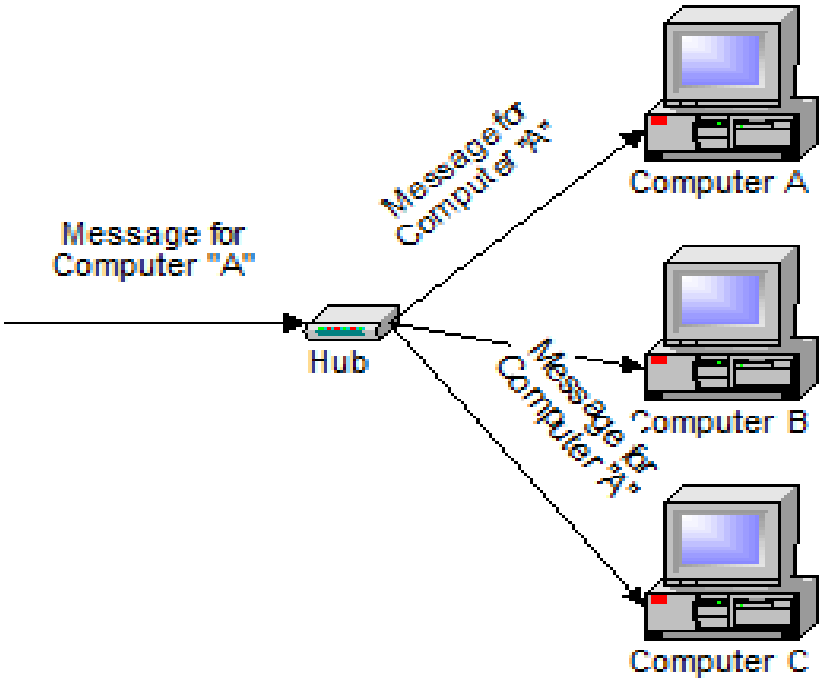
Supernetting

- In supernetting, an organization can combine several class C blocks to create a larger range of addresses.
- In other words, several networks are combined to create a supernetwork or a supemet.
- **For example:**
  - An organization that needs 1000 addresses can be granted four contiguous class C blocks.

Intermediate devices - Hub, Repeaters, Switch, Bridge- Gateways -Structure of a ROUTER

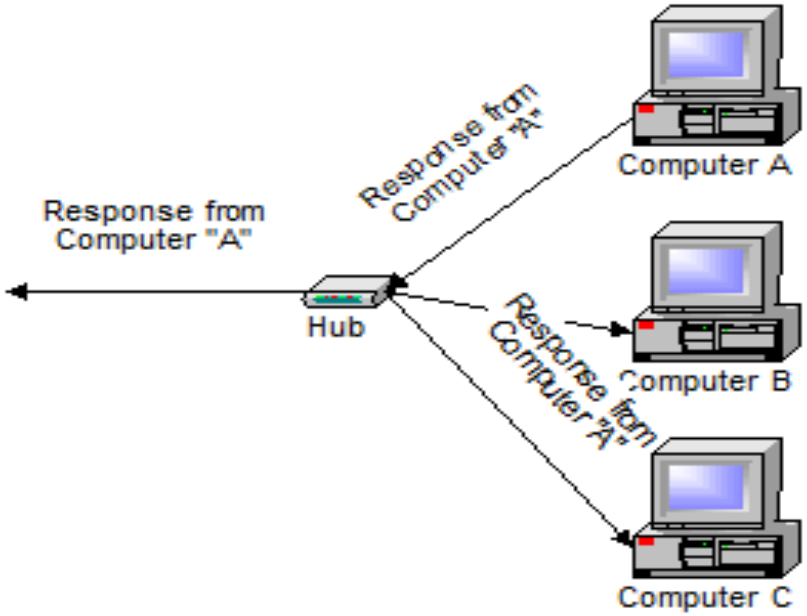
Intermediate devices - Hubs

- A **hub** is typically the least expensive, least intelligent, and least complicated. Its job is very simple – anything that comes in one port is sent out to the others. That is it broadcasts everything.
- If a message comes in for computer “A”, that message is sent out all the other ports, regardless of which one computer “A” is on:



Hubs

- And when computer “A” responds, its response also goes out to every other port on the hub:



- Every computer connected to the hub “sees” everything that every other computer on the hub sees. The computers themselves decide if they are the targeted recipient of the message and when a message should be paid attention to or not.

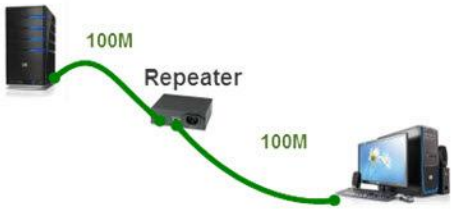
Types of Hub

- **Active Hub:-** These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.
- **Passive Hub :-** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

Drawbacks

- Hubs cannot filter data, so data packets are sent to all connected devices.
- They do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Repeaters

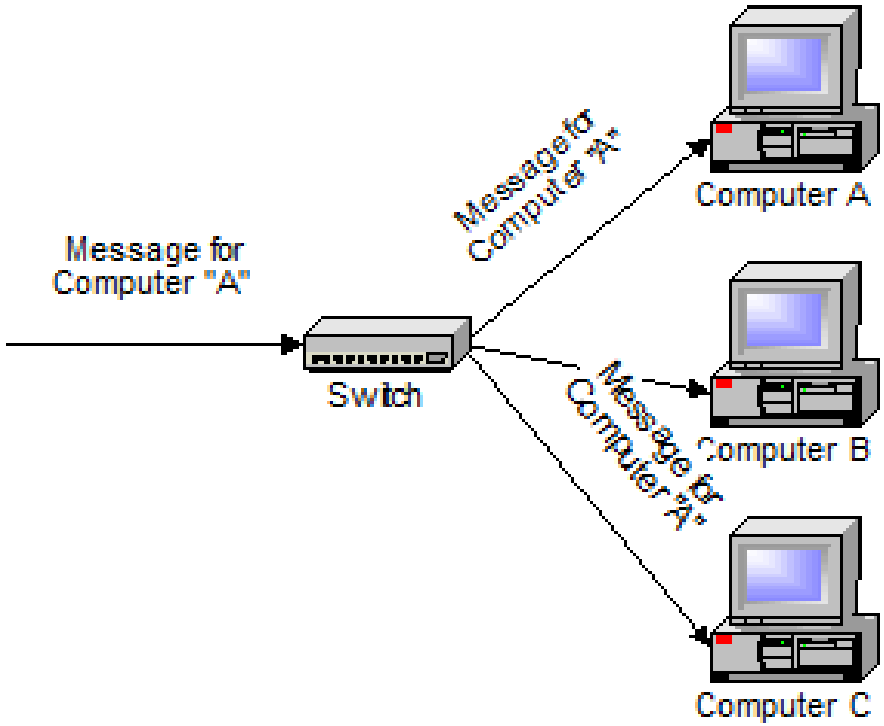


- A repeater operates at the physical layer.
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- They do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
- It is a 2 port device.

Because the functionality of repeaters has been built in to other devices, such as hubs and switches, repeaters are rarely used.

Switches

- A **switch** does essentially what a hub does, but more efficiently.
- By paying attention to the traffic that comes across it, it can "learn" where particular addresses are.
- Initially, a switch knows nothing and simply sends on incoming messages to all ports:



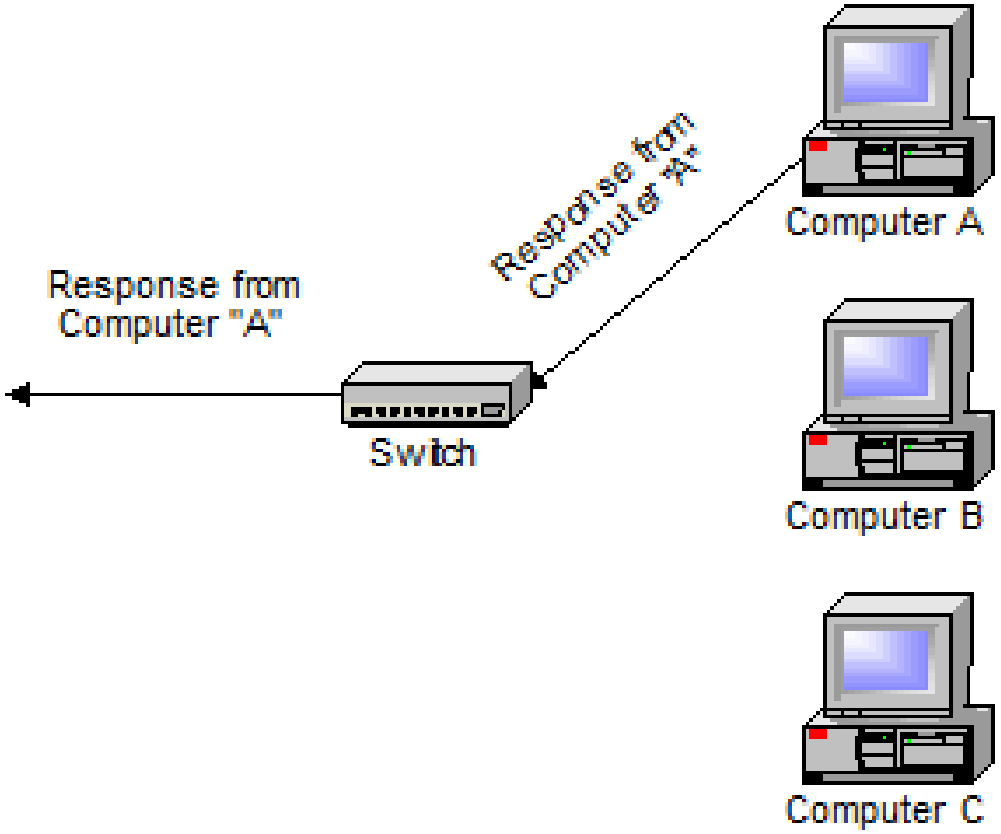
A 32-port Ethernet switch.

NETGEAR 5 port Network Switch

http://www.computerhope.com

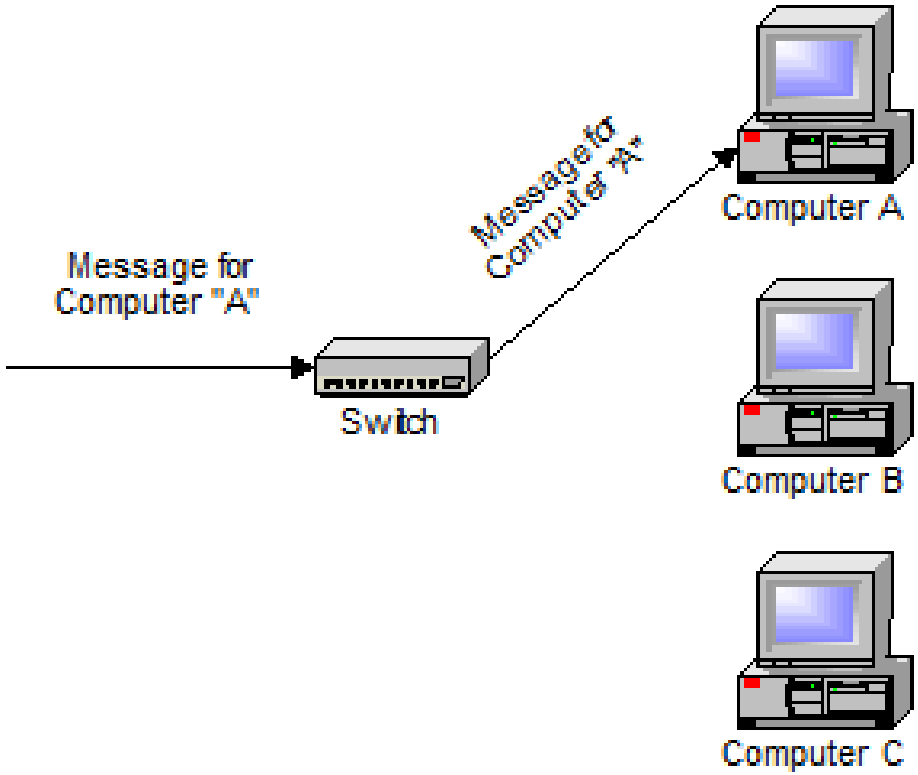
Switches

- Even accepting that first message, however, the switch has learned something – it knows on which connection the sender of the message is located.
- Thus, when machine “A” responds to the message, the switches only need to send that message out to the one connection:



Switches

- In addition to sending the response through to the originator, the switch has now learned something else – it now knows on which connection machine “A” is located.
- That means that subsequent messages destined for machine “A” need only be sent to that one port:



Switches

- Switches learn the location of the devices that they are connected to almost instantaneously.
- A switch is a data link layer device.
- The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.
- The net result is that most network traffic only goes where it needs to rather than to every port.
- On busy networks, this can make the network *significantly* faster.

Session 10

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

- Bridge
- Structure of Router

Bridges
Structure of router

2.10.1 What is a Bridge in a Computer Network?

- **Definition1:**

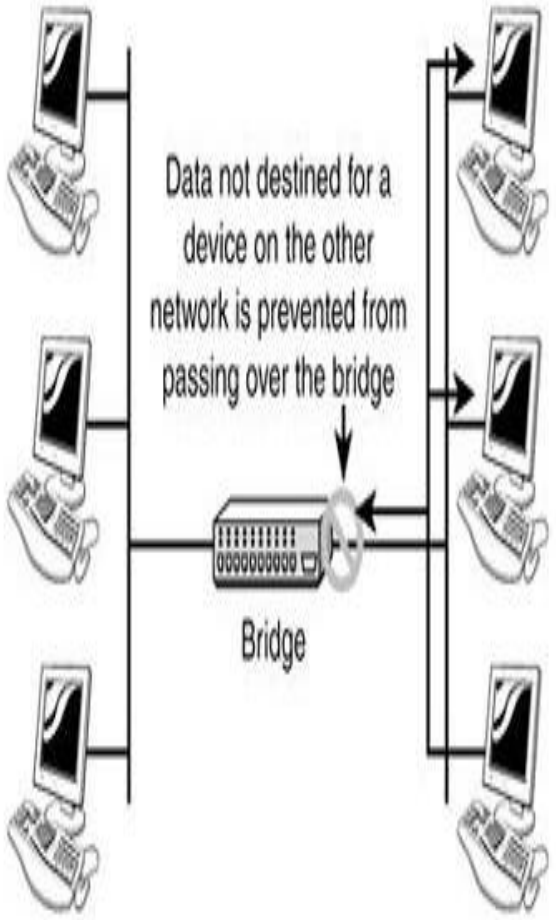
A bridge is one of the network devices in computer networks to connect two or more communication networks or network segments and creates a single network. It provides interconnection with other computer networks, which use the same protocol. The multiple local area networks (LANs) can be connected to form a larger local area network.

- **Definition2:**

A bridge in a computer network is one kind of network device, used to separate a network into sections. Every section in the network represents a collision domain that has separate bandwidth. So that network performance can be improved using a bridge. In the OSI model, a bridge works at layer-2 namely the data link layer. The main function of this is to examine the incoming traffic and examine whether to filter it or forward it.

2.10.2 Working Principle

- In a computer network, a bridge separates a LAN into different segments like segment1 & segment2, etc and the MAC address of all the PCs can be stored into the table.
- For instance, PC1 transmits the data to PC2, where the data will transmit to the bridge first.
- So the bridge reads the MAC address & decides whether to transmit the data to segment1 or segment2.
- Therefore, the PC2 is accessible in segment1, which means the bridge transmits the data in segment1 only & eliminates all the connected PCs in segment2.
- In this way, the bridge reduces traffic in a computer network.



2.10.3 Functions of Bridges in Computer Network

- The bridge allows to spit the local area network into many small segments.
- It performs the all tasks in data link layer in OSI model.
- Bridge helps to hold the MAC address of all computers in the network.
- It helps to decrease the traffic over the network.
- With using of MAC address, bridge gets to filter the all contents of source and destination points.
- It is used for making the interconnection two LAN networks along with single and same protocol.
- Bridge can work as single large LAN with connecting the multiple virtual LANs.
- Bridge has ability to switch any types of data packets like as Apple talk packets or IP packets over the network layer because in which payload field of the data frame is not considered. Only MAC address or destination address of the frame is acceptable to block or forward the data to each node in the computer network.

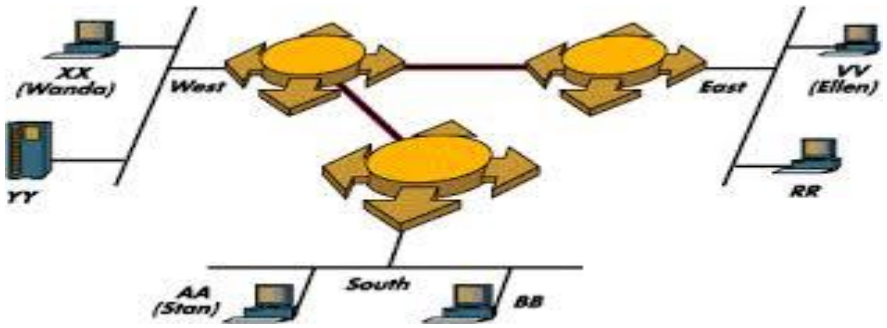
2.10.4 Types of Bridges

Bridges in the computer network are classified into five types which include the following.

1. Transparent Bridge.
2. Translational Bridge.
3. Source-route Bridge.
4. MAC-Layer Bridge.
5. Remote Type Bridge

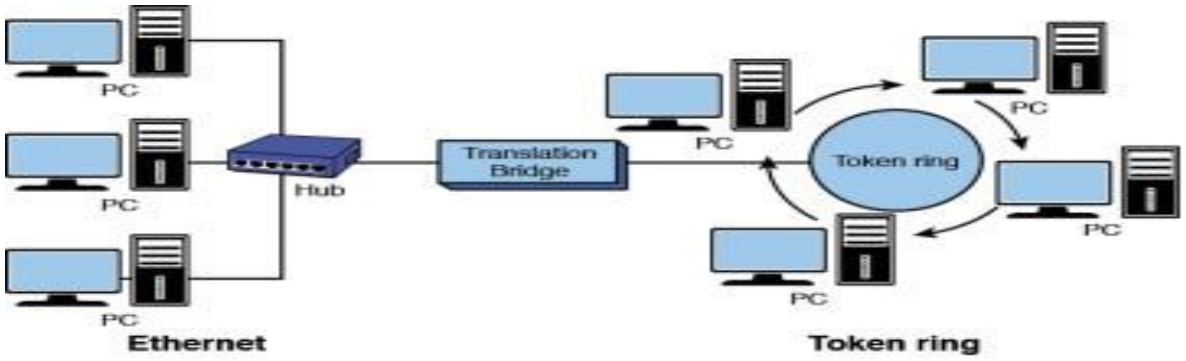
2.10.4 .1 Transparent Bridge

- It is also known as the “Learning Bridges“.
- Transparent bridge has not visibility to other installed stations or terminals over the computer network.
- It does not need to reconfigure the station because it is either added or deleted from the entire network.
- Main aim of the transparent bridge is getting to block or forwarding the data packets depend on the MAC address.
- It is getting more popularity while using in the networking.
- Transparent bridge is a plug and play bridge.
- This bridge creates its table of terminal addresses on its own.
- It allows to make its table for source location and able to self updating.



2.10.4.2 Translational Bridge

- A translational bridge plays a key role in changing a networking system from one type to another.
- These bridges are used to connect two different networks like token ring & Ethernet.
- This bridge can add or remove the data based on the traveling direction, and forward the frames of the data link layer in between LANs which uses various types of network protocols.
- The different network connections are Ethernet to FDDI/token ring otherwise Ethernet on UTP (unshielded twisted pair) to coax & in between FOC and copper wiring.



Translation bridge connecting different N/ws

2.10.4.3 Source-route Bridge

- Source-route bridge is introduced by IBM for using the Token ring networks.
- It allows to embed the all frame routes into one frame, and then this bridge takes the precise decisions that how the frame is forwarding with using of the network.
- In this technique, two same network segments can be linked to data link layer.
- Special frames are discovered by the host, it is known as the "Discovery Frame", and it spreads them over the entire network.
- Source-route Bridge helps to prevent the looping problems.

Figure 3-1 *Source-Route Bridged Network*

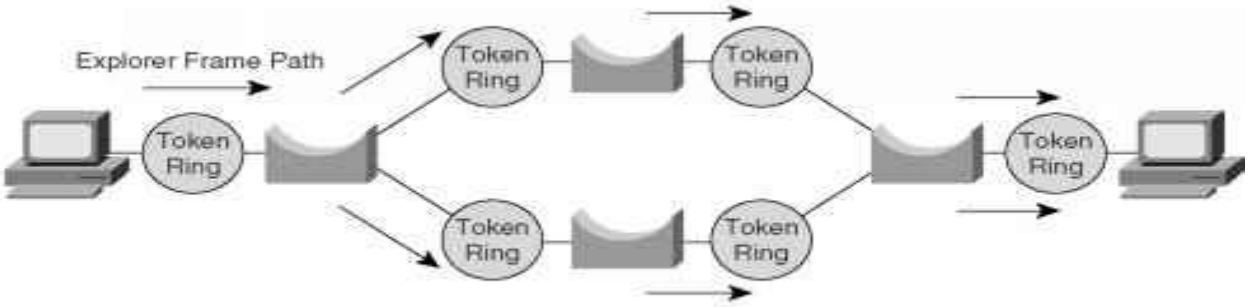
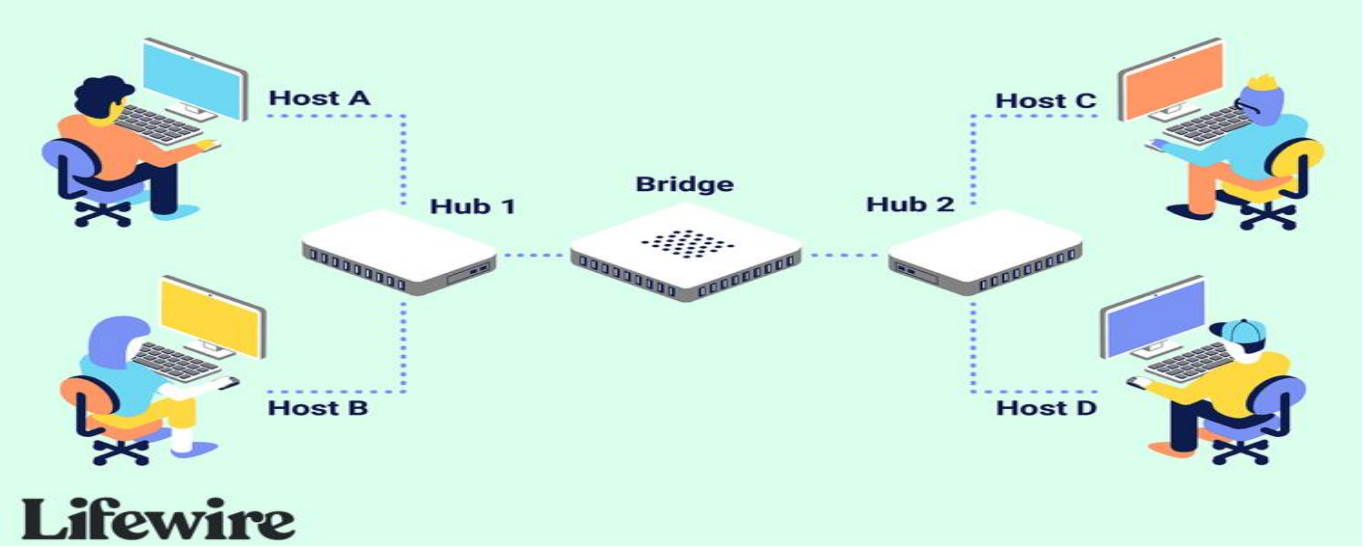


Figure 3-2 *SRB Ring/Bridge Routing Information*

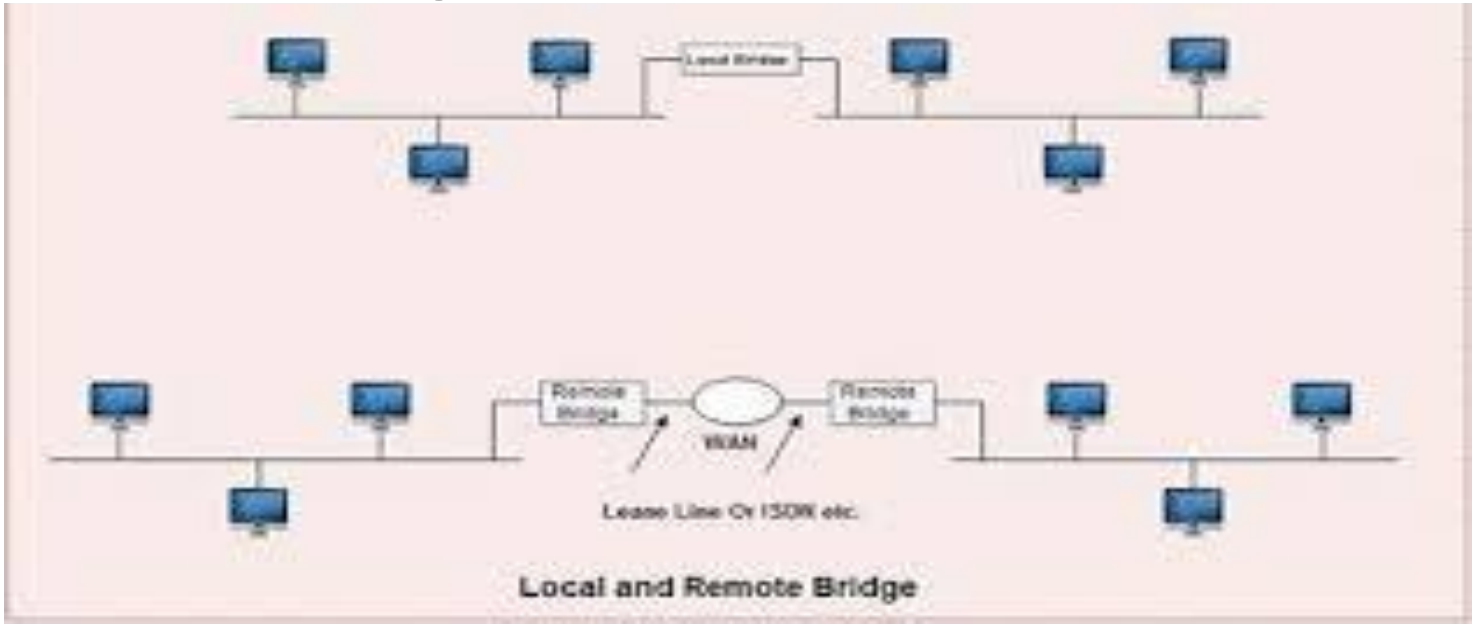
2.10.4.4 MAC-Layer Bridge

- MAC-layer Bridge is also known as the “Local Bridge“
- It offers the packet filtering and repeating services for network segments of the similar types.
- It does not require the packet filtering or buffering because it simply broadcast the incoming data packets to the accurate port or remove them.



2.10.4.5 Remote Type Bridge

- Remote Bridge allows to make connection two networks at different locations with using of WAN link like as MODEM or Leased Line.
- Its speed can be varied depend on the local and wide area links.
- This bridge has internal buffer to store the data received from LAN while it is waiting for transmission to the remote site.



Local and Remote Bridge

2.10.5.1 Advantages of Bridges

- Bridges are simple and significant.
- They prevent unnecessary traffic from crossing onto other network segments.
- Bridge can reduce the amount of network traffic on segments.
- It also make it possible to isolate a busy network from not-so-busy network.
- They can connect different network architectures like Ethernet & Token ring.
- Bridge have ability to look at the physical destination address of the frame and send the frame at the specific port.
- Bridge can filter the traffic, it increases throughput on a network.
- Connects different segments of network transmission

2.10.5.2 Disadvantages of Bridges

- It is unable to read specific IP addresses because they are more troubled with the MAC addresses.
- They cannot help while building the network between the different architectures of networks.
- It transfers all kinds of broadcast messages, so they are incapable to stop the scope of messages.
- It doesn’t handle more variable & complex data load which occurs from WAN.
- The speed of the network is slow when compared to the repeater due to the frame buffering and relays.

2.10.6 What is a Router?

- The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks.
- A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets.
- A router is used in LAN (Local Area Network) and WAN (Wide Area Network) environments.
- It shares information with other routers in networking.
- It uses the routing protocol to transfer the data across a network.
- It is more expensive than other networking devices like switches and hubs.

2.10.7 Features of Router

- A router works on the Network Layer of the OSI model, and it is able to communicate with its adjacent devices with the help of IP addresses and subnet.
- A router provides high-speed internet connectivity with the different types of ports like gigabit, fast-Ethernet, and STM link port.
- It allows the users to configure the port as per their requirements in the network.
- Routers main components are central processing unit (CPU), flash memory, RAM, Non-Volatile RAM, console, network, and interface card.
- Routers are capable of routing the traffic in a large networking system by considering the sub-network as an intact network.
- Routers filter out the unwanted interference, as well as carry out the data encapsulation and DEcapsulation process.
- Routers provide the redundancy as it always works in master and slave mode.
- It allows the users to connect several LAN and WAN.
- Furthermore, a router creates various paths to forward the data.

2.10.8 Types of Routers

There are various types of routers in networking are

- **Wireless Router:** generating a wireless signal range between 150 to 300 feet.
- **Brouter:** A brouter is a combination of the bridge and a router.
- **Core router:** the backbone of networks also provides various types of fast and powerful data communication interfaces.
- **Edge router:** lower-capacity device uses an External BGP (Border Gateway Protocol) to provides connectivity with remote networks over the internet.

Subscriber edge router belongs to an end-user organization and acts on a border device.

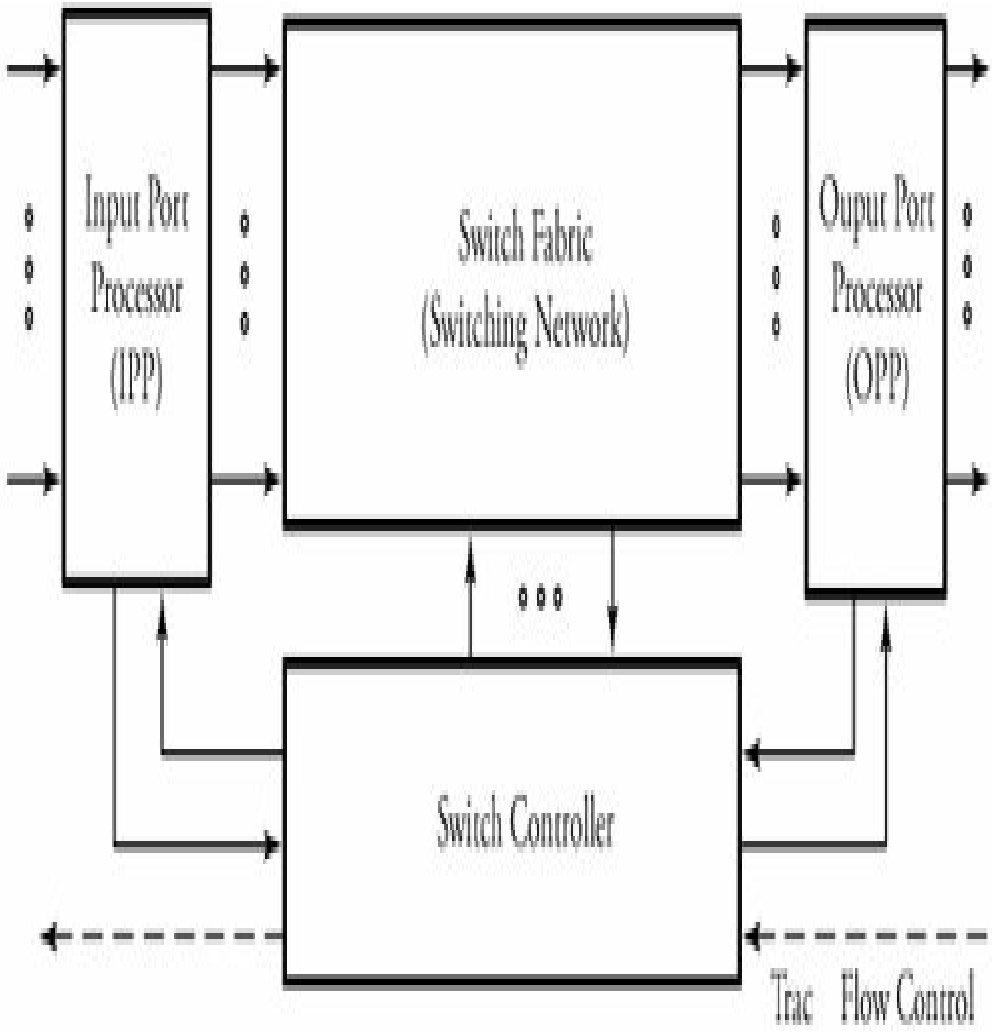
label edge router is boundary of Multiprotocol Label Switching (MPLS) networks and acts as a gateway between the LAN, WAN, or the internet.

- **Broadband routers:** To provide high-speed internet through phone and use Voice Over IP technology (VOIP) access to computers.

2.10.9 Router Structure

- Routers are the building blocks of wide area networks.
- Packets arrive at n input ports and are routed out from n output ports.
- The system consists of four main parts :

1. input port processors
2. output port processors
3. Switch fabric (switching network)
4. Switch controller .

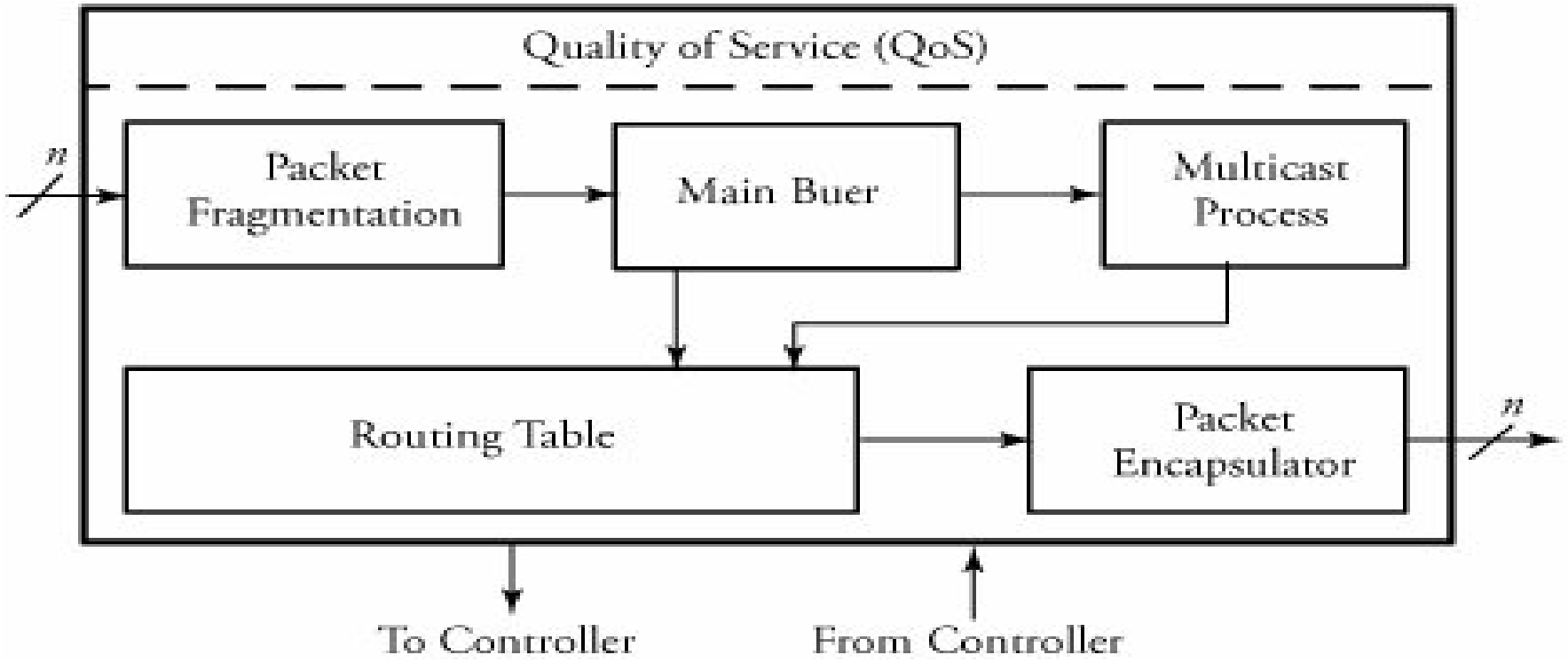


2.10.9.1 Input Port Processor (IPP)

- Input and output port processors, as interfaces to switch fabric, are commercially implemented together in router line cards contain some of the task of the physical and data link layers .
- The functionality of the data link layer is implemented as a separate chip in IPP that also provides a buffer to match the speed between the input and the switch fabric.
- Switch performance is limited by processing capability, storage elements, and bus bandwidth.
- The processing capability dictates the maximum rate of the switch.
- Due to the speed mismatch between the rate at which a packet arrives on the switch and the processing speed of the switch fabric, input packet rate dictates the amount of required buffering storage.
- The bus bandwidth determines the time taken for a packet to be transferred between the input and output ports.

Overview of a typical IPP in routers

- An input port processor (IPP) consists of several main modules are packet fragmentation , main buffer , multicast process , routing table , packet encapsulator , and a comprehensive QoS .



Packet Fragmentation

- Large packets cause different issues at the network and link layers.
- One application is large packets must be fragmented into smaller frames.
- Another example when large packets must be buffered at the input port interface of a router, as buffer slots are usually only 512 bytes long.
- One solution to this problem is to partition packets into smaller fragments and then reassemble them at the output port processor (OPP) after processing them in the switching system.
- simple packet fragmentation at the input buffer side of a switch.
- It is always desirable to find the optimum packet size that minimizes the delay.

Packet fragmentation: (a) without fragmentation; (b) with fragmentation

Routing Table

- It is a look-up table containing all available destination addresses and the corresponding switch output port.
- An external algorithm fills this routing lookup table.
- The purpose of the routing table is to look up an entry corresponding to the destination address of the incoming packet and to provide the output network port.
- As soon as a routing decision is made, all the information should be saved on the routing table.
- When a packet enters an IPP, the destination port of the switch should be chosen based on the destination address of the incoming packet.
- This destination port needs to be appended to the incoming packet as part of the switch header.
- To increase memory performance, queue sizes are fixed to reduce control logic.
- packets can arrive and leave the network in different order, a memory monitor is necessary to keep track of which locations in memory are free for use.

Routing Table

example of routing tables at routers between hosts A and B. Assume that host B's address is requested by a packet with destination address 182.15.0.0/22 arriving at router 1. The routing table of this router stores the best-possible path for each destination. Assume that for a given time, this destination is found in entry row 5. The routing table then indicates that port 2 of the router is the right output to go. The table makes the routing decision, based on the estimated cost of the link, which is also stated in the corresponding entry. When the packet arrives at router 2, this switch performs the same procedure.

Routing Table

Sequence Number	Destination IP Address	Router Port Number	Estimated Cost
4	143.28.3.0/21	1	4
5	182.15.0.0/22	2	56
6	155.76.2.0/22	2	56
7	131.46.0.0/24	1	4

Routing Table

Sequence Number	Destination IP Address	Router Port Number	Estimated Cost
41	135.18.5.0/21	2	3
42	182.15.0.0/22	1	0
43	197.76.2.0/23	2	3
44	171.55.0.0/21	2	3

Multicast Process

- It is necessary for copying packets when multiple copies of a packet are expected to be made on a switching node.
- Using a memory module for storage, copying is done efficiently.
- The copying function can easily be achieved by appending a counter field to memory locations to signify the needed number of copies of that location.
- The memory module is used to store packets and then duplicate multicast packets by holding memory until all instances of the multicast packet have exited IPP.
- Writing to memory takes two passes for a multicast packet and only one pass for a unicast packet.
- In order to keep track of how many copies a multicast packet needs, the packet counter in the memory module must be augmented after the multicast packet has been written to memory.
- Each entry in the memory module consists of a valid bit, a counter value, and memory data.

Packet Encapsulation

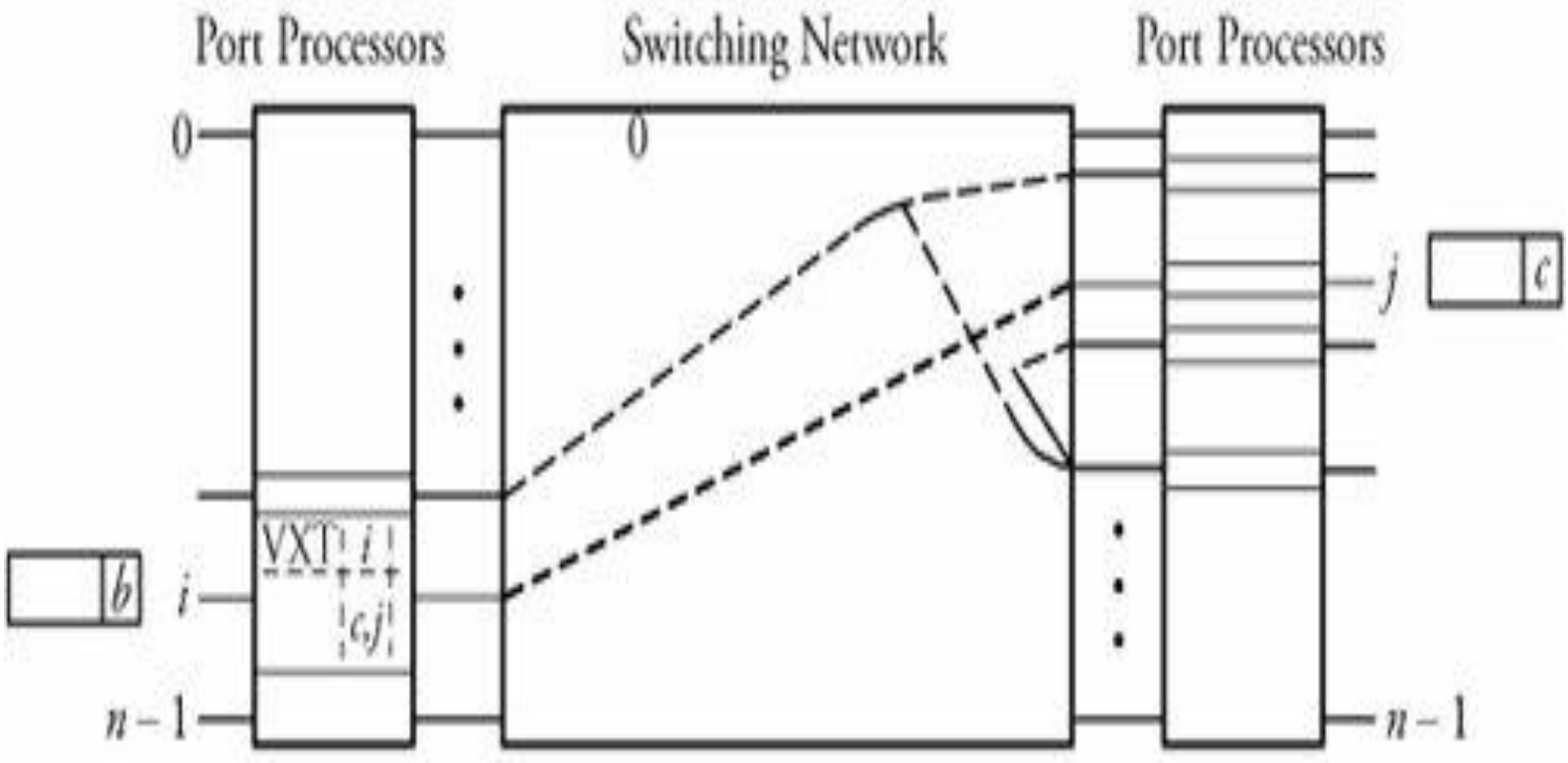
- It performs the routing table lookups and inserts the switch output port number into the network header.
- The serial-to-parallel multiplexing unit converts an incoming serial byte stream into a fully parallel data stream.
- This unit also processes the incoming IP header to determine whether the packet is unicast or multicast and extracts the type-of-service field.
- Once the full packet is received, it is stored into memory.
- The packet encapsulation unit formats the incoming packet with a header before forwarding the packet to the crossbar.

Congestion Controller

- This module shields the switching node from any disorders in the traffic flow.
- Congestion can be controlled in several ways.
- Sending a reverse-warning packet to the upstream node to avoid exceeding traffic is one common technology installed in the structure of advanced switching systems.
- Realistically, spacing between incoming packets is irregular.

2.10.9.2 Switch Fabric

- In this module packets are routed from input ports to the desired output ports.
- A packet can also be multicast to more than one output.
- Finally, in the output port processors, packets are buffered and resequenced in order to avoid packet misordering.
- In addition, a number of other important processes and functions taken place in each of the mentioned blocks.
- The following example shows, this model can work for ATM technology: Cells (packets) arrive at n input ports and are routed out from n output ports.
- When a cell carrying VCI b arrives from a given link i, the cell's VCI is used to index a virtual-circuit translation table (VXT) in the corresponding input port processor to identify the output link address j and a new VCI c .
- In the switching network, cells are routed to the desired outputs.



Interaction between an IPP and its switch fabric in a virtual-circuit switching router

2.10.9.3 Switch Controller

- The controller part of a switching system makes decisions leading to the transmission of packets to the requested output(s).
- The details of the controller are illustrated in Figure.
- The controller receives packets from an IPP, but only the headers of packets are processed in the controller.

Header Decoder Unit

- first converts the control information of an arriving packet into an initial requested output vector.
- This bit vector carries the information pertaining to the replication of a packet so that any bit of 1 represents a request for one of the corresponding switch outputs.

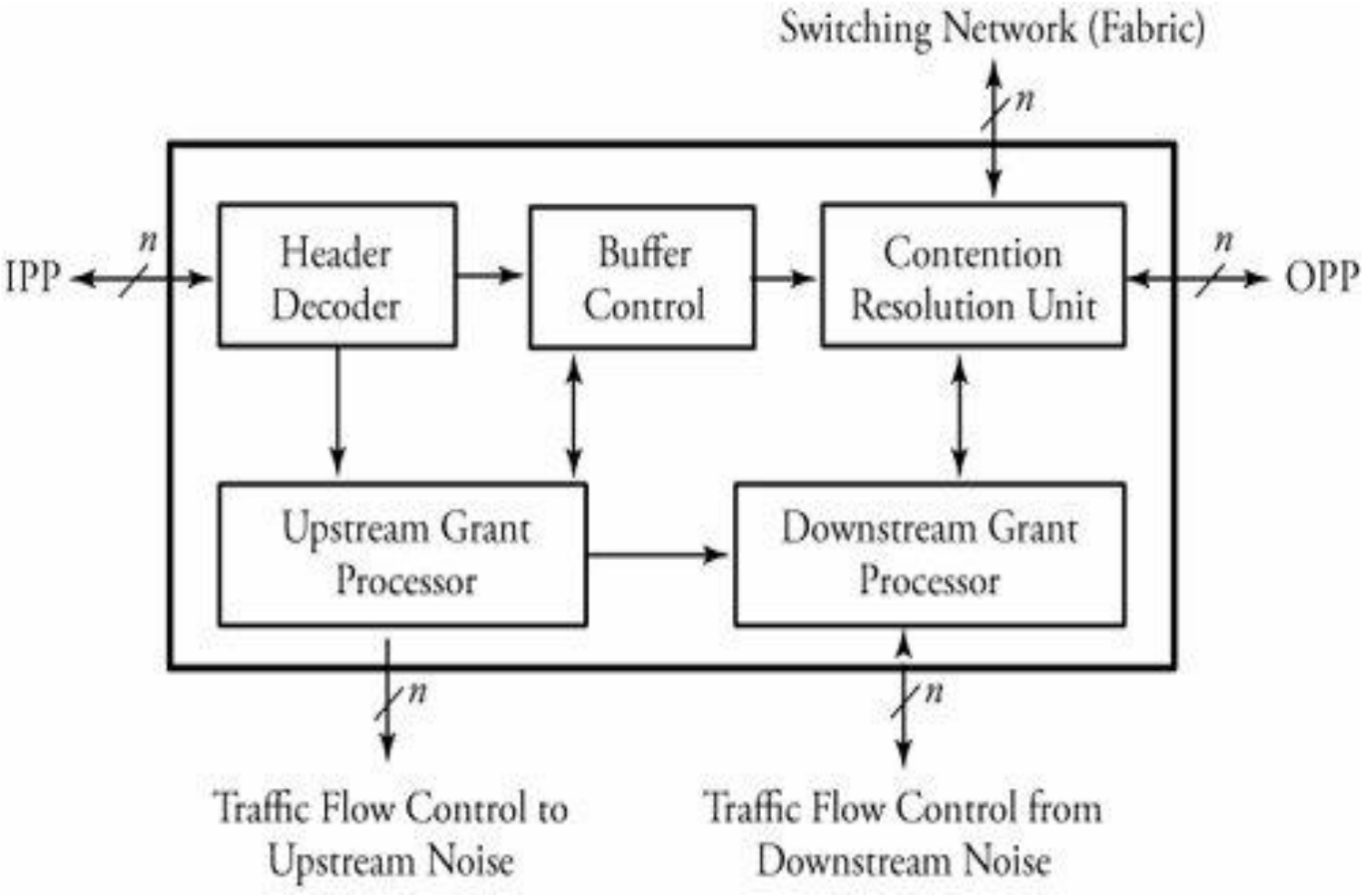
Buffer Control Unit

- generates a priority value for each packet to enable it for arbitration.
- This information, along with the request vector, enters an array of arbitration elements in the contention resolution unit.

Contention Resolution Unit.

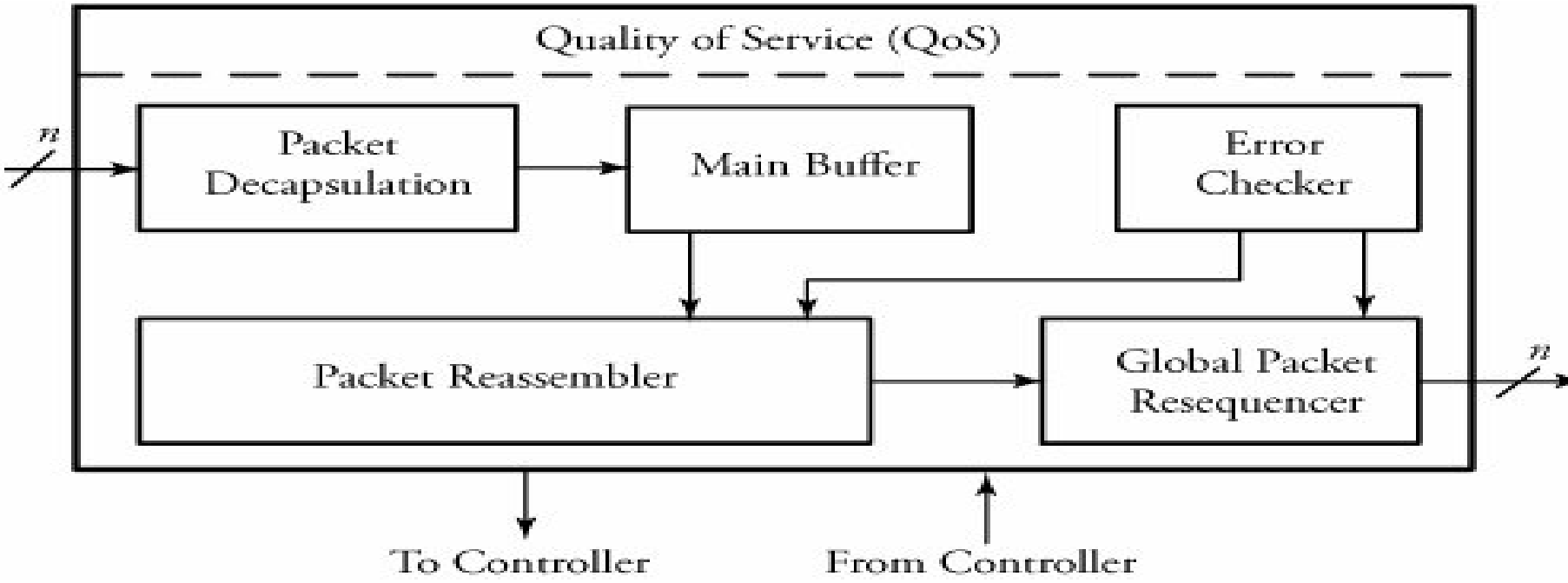
- Each packet in one column of an arbitration array contends with other packets on a shared bus to access the switch output associated with that column.
- After a packet wins the contention, its identity (buffer index number) is transmitted out to an OPP.
- buffer-control bit transferred to the switching fabric (network), signaling them to release the packet.
- buffer-control mechanism ensures that a losing packet in the competition remains in the buffer.
- buffer-control unit then raises the priority of the losing packet by 1 so that it can contribute in the next round of contention with a higher chance of winning.
- This process is repeated until eventually, the packet wins.
- winning packets are transmitted to the switch fabric if traffic flow control signals from downstream neighboring nodes are active.
- The upstream grant processor in turn generates a corresponding set of traffic flow control signals, which are sent to the upstream neighboring nodes.

Overview of a switching system controller



2.10.9.4 Output Port Processors (OPP)

- It includes parallel-to-serial multiplexing, main buffer, local packet resequencer, global packet resequencer, error checker, and packet reassembler, as shown in below fig.
- Similar to IPP, OPP also contributes to congestion control. Parallel-to-serial multiplexing converts the parallel-packet format into serial packet format.



Main Buffer

- The buffer unit serves as the OPP central shift register.
- The purpose of this buffer is to control the rate of the outgoing packets, which impacts the quality of service.
- After collecting signals serially from the switch fabric, the buffer forwards packets to resequencers.
- The queue runs on a clock driven by the link interface between the switch and an external link.
- This buffer must have features that support real-time and non-real -time data

Reassembler and Resequencer

- The output port processor receives a stream of packet fragments and has to identify and sort out all the related ones.
- The OPP reassembles them into a single packet, based on the information obtained from the fragment field of headers.
- For this process, the OPP must be able to handle the arrival of individual fragments at any time and in any order.
- Fragments may arrive out of order for many reasons.

- Misordered packets can occur because individual fragments, composed of a fairly large number of interconnections with different delay times, are independently routed through the switch fabric.
- A packet reassembler buffer is used to combine fragments of IP packets.
- This unit resequences receiving packet fragments before transmitting them to external circuits, updates the total-length field of the IP header, and decapsulates all the local headers.
- The resequencer's internal buffer stores misordered fragments until a complete sequence is obtained.
- The in-sequence fragments are reassembled and transmitted to the external circuit.
- A global packet resequencer uses this same procedure to enforce another reordering, this time on sequences, not fragments, of packets that belong to a single user .

Error Checker and CRC

- When a user sends a packet or a frame, a cyclic redundancy check (CRC) field is appended to the packet.
- The CRC is generated from an algorithm and is based on the data being carried in the packet.
- The CRC algorithms divide the message by another fixed-binary number in a polynomial form, producing a checksum as the remainder.
- The message receiver can perform the same division and compare the remainder with the received checksum.
- The error checker applies a series of error-checking processes on packets to ensure that no errors are on the packets and creates a stream of bits of a given length, called frames.
- A frame produces a checksum bit , called frame check sequence, which is attached to the data when transmitted.

Difference between Bridge and Router

Bridge	Router
A bridge is a networking device that is used to connect two local area networks (LANs) by using media access control addresses and transmit the data between them.	A router is also a networking device that sends the data from one network to another network with the help of their IP addresses.
A bridge is able to connect only two different LAN segments.	A router is capable of connecting the LAN and WAN.
A bridge transfers the data in the form of frames.	A router transfers the data in the form of packets.
It sends data based on the MAC address of a device.	It sends data based on the IP address of a device.
The bridge has only one port to connect the device.	The router has several ports to connect the devices.
The bridge does not use any table to forward the data.	The router uses a routing table to send the data.

	Key	Router	Bridge
1	Objective	Router main objective is to connect various networks.	Bridge main objective is to connect various LANs.
2	Layer	Router works in Network Layer.	Bridge works in Data Link Layer.
3	Address	Router scans device's IP Address.	Bridge scan device's MAC Address.
4	Data Format	Router sends data in form of packets.	Bridge also sends data in form of packets.
5	Routing Table	Router uses routing table.	Bridge do not use routing table.
6	Domain	Router works on more than single broadcast domains.	Bridge works on a single broadcast domain.
7	Ports	Router has more than two ports.	Bridge has only two ports.