Noida Institute of Engineering and Technology, Greater Noida

Network Layer

Unit: 3

Computer Networks
(ACSE0602)

B Tech 6th Sem

Sanjay Kumar Nayak
(Assistant Professor)
CSE
Department

Noida Institute of Engineering and Technology, Greater Noida

- Sanjay Nayak received his B.Tech degree in Computer Science & Engineering from institute of Institute of Engineering & Technology (IET), Lucknow . M.Tech degree from UPTU .

Curriculum

NOIDA INSTITUTE OF ENGG. & TECHNOLOGY, GREATER NOIDA, GAUTAM BUDDH NAGAR
(AN AUTONOMOUS INSTITUTE)

Bachelor of Technology
Computer Science and Engineering
EVALUATION SCHEME
SEMESTER-VI

Sl. No.	Subject Codes	Subject Name	Periods			Evaluation Scheme				End Semester		Total	Credit
			L	T	P	CT	TA	TOTAL	PS	TE	PE		
1	ACSE0601	Advanced Java Programming	3	0	0	30	20	50		100		150	3
2	ACSE0602	Computer Networks	3	1	0	30	20	50		100		150	4
3	ACSE0603	Software Engineering	3	0	0	30	20	50		100		150	3
4		Departmental Elective -III	3	0	0	30	20	50		100		150	3
5		Departmental Elective -IV	3	0	0	30	20	50		100		150	3
6		Open Elective-I	3	0	0	30	20	50		100		150	3
7	ACSE0651	Advanced Java Programming Lab	0	0	2				25		25	50	1
8	ACSE0652	Computer Networks Lab	0	0	2				25		25	50	1
9	ACSE0653	Software Engineering Lab	0	0	2				25		25	50	1
10	ACSE0659	Mini Project	0	0	2				50			50	1
11	ANC0602 / ANC0601	Essence of Indian Traditional Knowledge / Constitution of India, Law and Engineering	2	0	0	30	20	50		50		100	
12		MOOCs (For B.Tech. Hons. Degree)											
		GRAND TOTAL										**1100**	**23**

List of MOOCs (Coursera) Based Recommended Courses for Third Year (Semester-VI) B. Tech Students

Syllabus

B. TECH THIRD YEAR			
Course Code	**ACSE0602**	**L T P**	**Credits**
Course Title	**COMPUTER NETWORKS**	**3 1 0**	**4**

Course objective:
Objective of this course is to develop an understanding of computer networking basics, different components of computer networks, various protocols, modern technologies and their applications.

Pre-requisites: Basic knowledge of Computer system and their interconnection, operating system, Digital logic and design and hands on experience of programming languages.

Course Contents / Syllabus

UNIT-I	**Introduction**	**8 Hours**

Goals and applications of networks, Categories of networks, Organization of the Internet, ISP, The OSI reference model, TCP/IP protocol suite, Network devices and components, Mode of communications
Physical Layer: Network topology design, Types of connections, LAN, MAN and MAN Transmission media, Signal transmission and encoding, Network performance and transmission impairments, Switching techniques and multiplexing, IEEE standards.

UNIT-II	**Data Link layer**	**8 Hours**

Framing, Error Detection and Correction, Flow control (Elementary Data Link Protocols, Sliding Window protocols). Medium Access Control and Local Area Networks: Channel allocation, Multiple access protocols, LAN standards, Link layer switches & bridges.

UNIT-III	**Network Layer**	**8 Hours**

Point-to-point networks, Logical addressing, Basic internetworking (IP, CIDR, ARP, RARP, DHCP, ICMP), IPv4, Routing, forwarding and delivery, Static and dynamic routing, Routing algorithms and protocols, Congestion control algorithms, IPv6.

UNIT-IV	**Transport Layer**	**8 Hours**

Process-to-process delivery, Transport layer protocols (UDP and TCP), Connection management, Flow control and retransmission, Window management, TCP Congestion control, Quality of service.

UNIT-V	**Application Layer**	**8 Hours**

Domain Name System, World Wide Web and Hyper Text Transfer Protocol, Electronic mail, File Transfer Protocol, Remote login, Network management, Data compression, VPN, Cryptography – basic concepts, Firewalls.

Course outcome: After completion of this course students will be able to

CO 1	Build an understanding of the fundamental concepts and Layered Architecture of computer networking.	K2, K6
CO 2	Understand the basic concepts of link layer properties to detect error and develop the solution for error control and flow control.	K2, K6
CO 3	Design, calculate, and apply subnet masks and addresses to fulfil networking requirements and calculate distance among routers in subnet.	K3, K4, K6
CO 4	Understand the duties of transport layer, Session layer with connection management of TCP protocol.	K2, K4
CO 5	Discuss the different protocols used at application layer.	K2

Books

Text books:

1. Behrouz Forouzan, “Data Communication and Networking” Fourth Edition-2006, Tata McGraw Hill
2. Andrew Tanenbaum “Computer Networks”, Fifth Edition-2011, Prentice Hall.
3. William Stallings, “Data and Computer Communication”, Eighth Edition-2008, Pearson.

Reference Books:

1. Kurose and Ross, “Computer Networking- A Top-Down Approach”, Eighth Edition-2021, Pearson.
2. Peterson and Davie, “Computer Networks: A Systems Approach”, Fourth Edition-1996, Morgan Kaufmann

Course Objective

The objective of this course is to understand introduction of computer networks with suitable transmission media and different networking devices. Network protocols which are essential for the computer network are need to explain such as data link layer protocols and routing protocols.

A detail explanation of IP addressing , TCP/IP protocols and application layer protocols are covered in this course.

Course Outcome

Course outcome: After completion of this course students will be able to		
CO 1	Build an understanding of the fundamental concepts and Layered Architecture of computer networking.	K2, K6
CO 2	Understand the basic concepts of link layer properties to detect error and develop the solution for error control and flow control.	K2, K6
CO 3	Design, calculate, and apply subnet masks and addresses to fulfil networking requirements and calculate distance among routers in subnet.	K3, K4, K6
CO 4	Understand the duties of transport layer, Session layer with connection management of TCP protocol.	K2, K4
CO 5	Discuss the different protocols used at application layer.	K2

PO's

1.Engineering knowledge
2. Problem analysis
3. Design/development of solutions
4. Conduct investigations of complex problems
5. Modern tool usage
6. The engineer and society
7. Environment and sustainability
8. Ethics
9. Individual and team work
10. Communication
11. Project management and finance
12. Life-long learning

CO-PO Mapping

Computer Networks(ACSE- 603)									Year of Study: 2023-24			
CO	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
ACSE0602.1	3	2	2		2				2		2	3
ACSE0602.2	3	3	2									3
ACSE0602.3	3	3	3	3	2				2		2	3
ACSE0602.4	3	2	2		2							3
ACSE0602.5	3	3	2		2	3		2				3
Average	**3**	**2**	**2**		**2**	**2**		**2**	2		**2**	**3**

PSO's

On successful completion of graduation degree, The computer Science & Engineering graduates will be able to:

PSO1: identify, analyze real world problems and design their ethical solutions using artificial intelligence, robotics, virtual/augmented reality, data analytics, block chain technology, and cloud computing.

PSO2: design and develop the hardware sensor devices and related interfacing software systems for solving complex engineering problems.

PSO 3: understand inter-disciplinary computing techniques and to apply them in the design of advanced computing.

PSO 4: conduct investigation of complex problem with the help of technical, managerial, leadership qualities, and modern engineering tools provided by industry sponsored laboratories.

PSO's

CO	PSO1	PSO2	PSO3	PSO4
ACSE0602.1	2	2	2	2
ACSE0602.2	2	2	2	2
ACSE0602.3	2	2	2	3
ACSE0602.4	2	2	2	2
ACSE0602.5	2	2	2	2
Avg	2	2	2	2

Program Educational Objectives

PEO 1: To have an excellent scientific and engineering breadth so as to comprehend, analyze, design and provide sustainable solutions for real-life problems using state-of-the-art technologies.

PEO 2: To have a successful career in industries, to pursue higher studies or to support entrepreneurial endeavors and to face the global challenges.

PEO 3: To have an effective communication skills, professional attitude, ethical values and a desire to learn specific knowledge in emerging trends, technologies for research, innovation and product development and contribution to society.

PEO 4: To have life-long learning for up-skilling and re-skilling for successful professional career as engineer, scientist, entrepreneur and bureaucrat for betterment of society.

Result Analysis

COMPUTER NETWORKS (ACSE0602)	
Department wise Result of VI sem.	100
Subject wise result	99
Faculty wise result	99

End semester Question paper templates

Printed Pages—3 **ECS601**

(Following Paper ID and Roll No. to be filled in your Answer Book)

PAPER ID : 110601 **Roll No.** | | | | | | | | | | |

B.Tech.

(SEM. VI) THEORY EXAMINATION 2013-14

COMPUTER NETWORK

Time : 3 Hours *Total Marks : 100*

Note :– (1) Attempt **all** questions.

(2) All questions carry equal marks.

1. Attempt any **four** parts of the following : **(5×4=20)**
   (a) Discuss the TCP/IP protocol suite on the basis of protocol layering principle.
   (b) Define topology and explain the advantage and disadvantage of Bus, Star and Ring topologies.
   (c) Explain briefly the bus backbone and star backbone.
   (d) Explain the user access in ISDN.
   (e) Compare twisted pair, co-axial and fiber optic cable.
   (f) Explain the various types of Switching Methods with suitable examples.
2. Attempt any **four** parts of the following : **(5×4=20)**
   (a) State drawbacks of stop and wait protocols.
   (b) What is piggybacking ?
   (c) Which are the requirements of CRC ?

   (d) How can you compare pure ALOHA and Slotted ALOHA ?
   (e) Explain about CSMA/CD and CSMA/CA and its uses.
   (f) Differentiate between 802.3, 802.4 and 802.5 IEEE Standards.
3. Attempt any **two** parts of the following : **(10×2=20)**
   (a) What is meant by fragmentation ? Is fragmentation needed in concentrated virtual circuit internets, or in any datagram system.
   (b) Give an IP address, how will you extract its net-id and host-id and compare IPv4 and IPv6 with frame format.
   (c) (i) What is meant by unicast and multicast routing with suitable diagrams ?
   (ii) Write a short note on Leaky bucket algorithm.
4. Attempt any **two** parts of the following : **(10×2=20)**
   (a) Explain about the TCP header and working of TCP protocol and differentiate between TCP and UDP with frame format.
   (b) Define cryptography with the help of block diagram of Symmetric and Asymmetric key cryptography.
   (c) Write short notes on :
   (i) Digital audio
   (ii) Audio compression
   (iii) Streaming audio.

5. Attempt any **two** parts of the following : **(10×2=20)**
   (a) Explain the two mail access protocols in brief :
   (i) POP3
   (ii) IMAP
   (iii) SMTP
   (b) Write a short note on :
   (i) FTP
   (ii) DNS
   (iii) MIME
   (iv) TFTP
   (c) Explain about e-mail architecture and services.

Prerequisite and Recap

- **Networking components**
- **Concept of physical addressing**
- **Concept of OSI and TCP/IP model**

In previous unit

Data link layer duties

Multi access protocol

Error control

Content

Unit 3

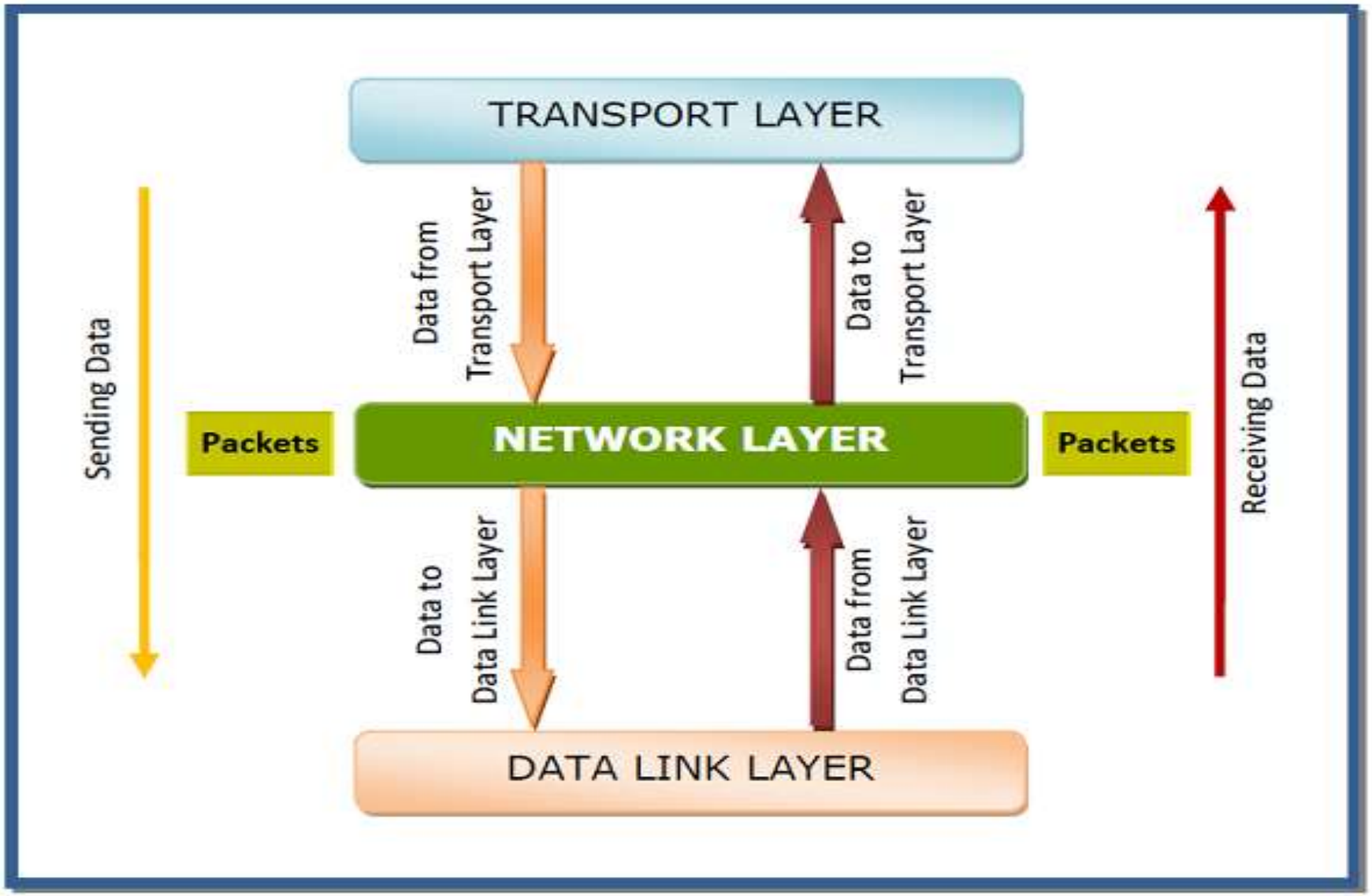
- Point-to-point networks
- Logical addressing (IPv4)
- Basic internetworking (IP, CIDR ARP, RARP, DHCP, ICMP)
- Routing, forwarding and delivery
- Static and dynamic routing
- Routing algorithms and protocols
- Congestion control algorithms
- IPv6.

Network Layer Functions

Objective: Study about basic concept of Network layer and its function

- Getting packets from the source all the way to the destination
- May require many hops through intermediate routers.
- It must know about the topology of the communication subnet (the set of all routers) and choose appropriate paths through it.
- It must take care to choose routers to avoid overloading some of the lines and routers while leaving others idle.
- When source and destination are in different networks, it has to deal with the differences.

Network Layer Functions



Network Layer Functions

The network layer performs several functions to facilitate data transmission in a network. Some of the functions performed are as follows:

1. Routing:

It is the process to determine the most effective route for data transmission in the network. When a data packet arrives at the router's input link, it determines the ideal route for data transmission in the network. It determines the path that will be used to transfer the packet further in the network.

2. Logical Addressing:

There are two types of addressing performed in the network: logical addressing and physical addressing. The data link layer performs the physical addressing, while the network layer does the logical addressing in the OSI model. Logical addressing is also used to distinguish between the source and destination system. The network layer adds a header to the packet, which includes the logical addresses of both the sender and the receiver.

Network Layer Functions

The network layer performs several functions to facilitate data transmission in a network. Some of the functions performed are as follows:

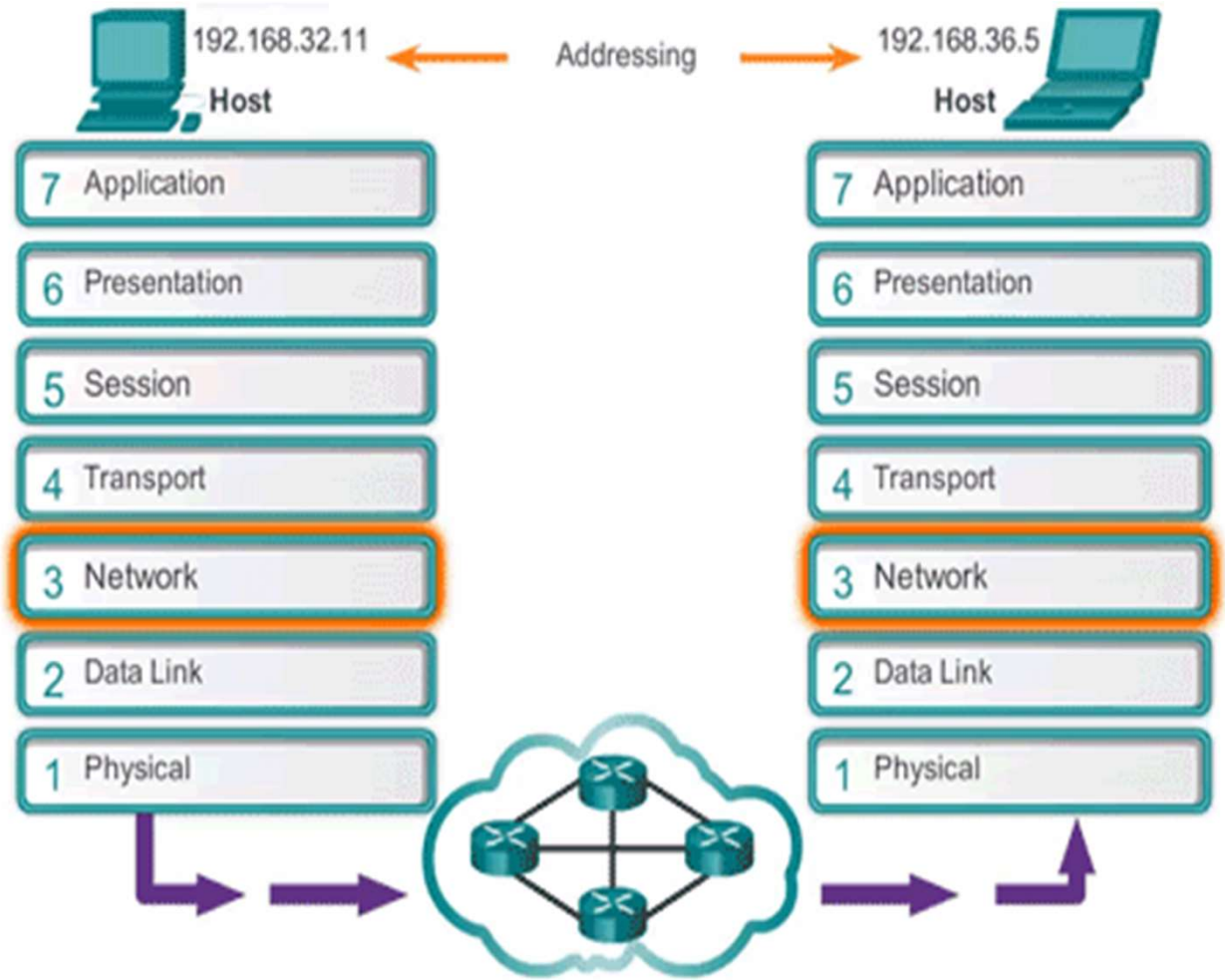
3. Internetworking:

This is the most important function performed by the network layer of the OSI model. It establishes the logical connection between nodes in the same or different networks.

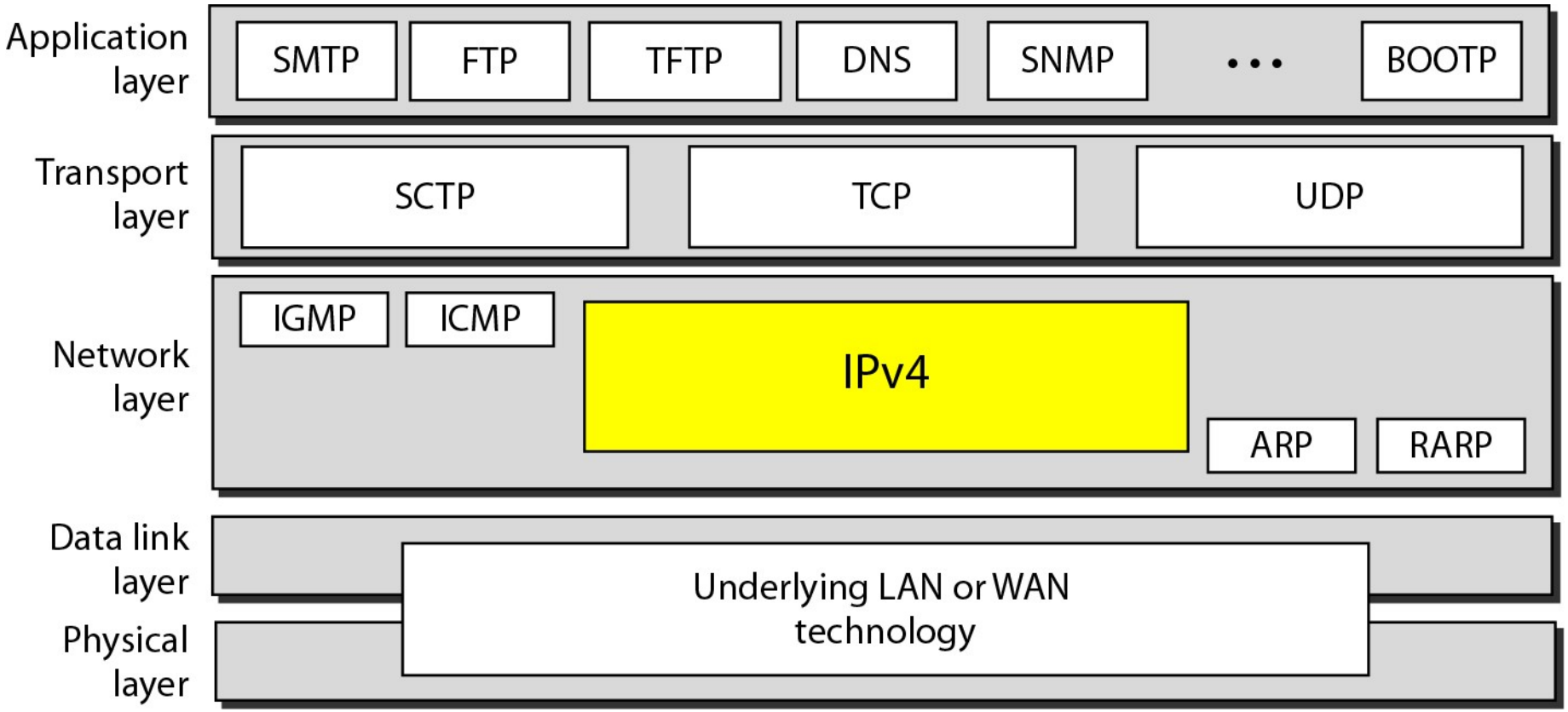
4. Fragmentation:

It is the conversion of data packets into the smallest individual data units capable of being transmitted in the network.

Network Layer



Network Layer Protocols



Network Layer Protocols

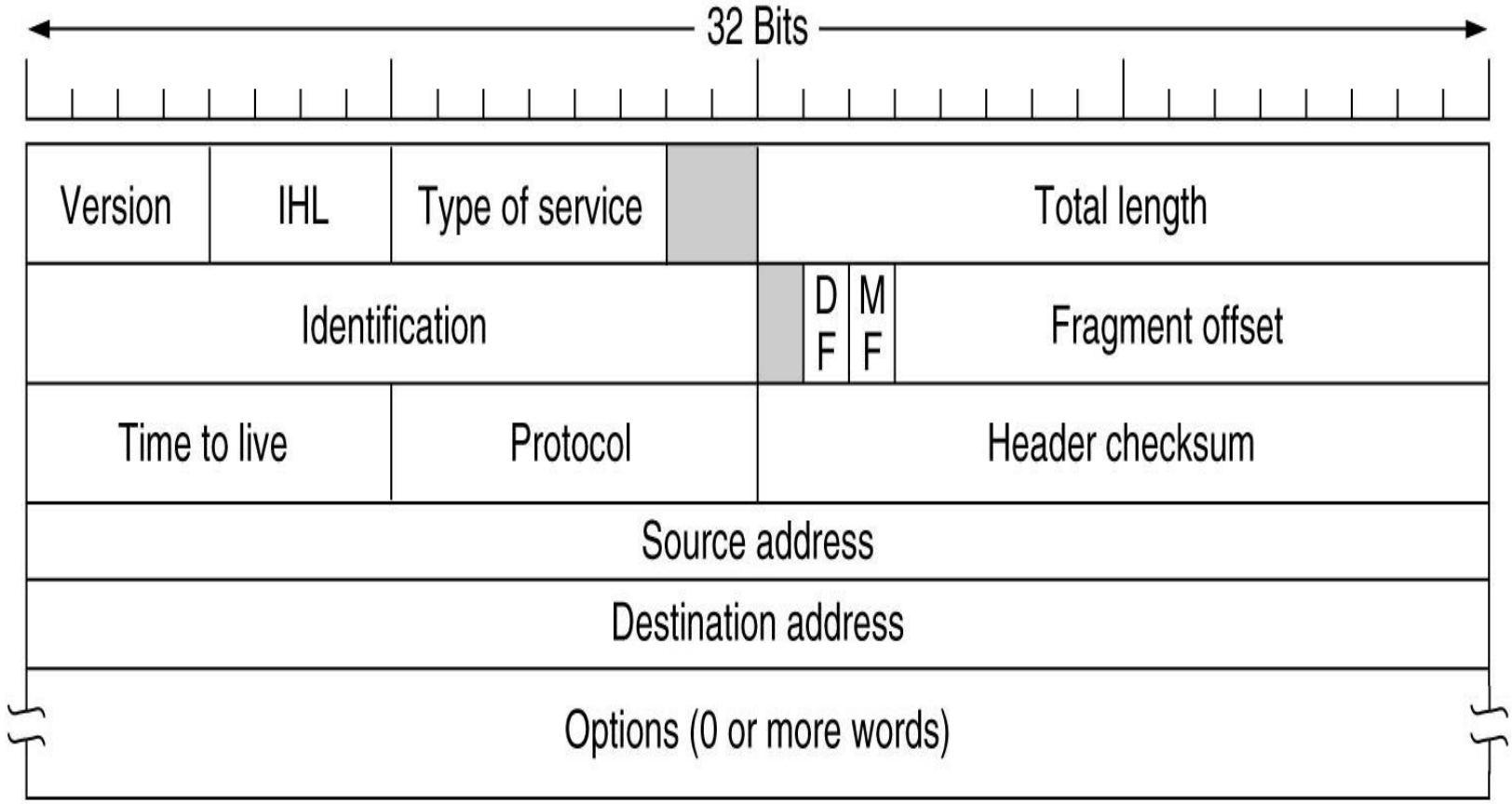
There are several network layer protocols in existence; however, only the following two are commonly implemented:

- **Internet Protocol version 4 (IPv4)**
- **Internet Protocol version 6 (IPv6)**

Other legacy network layer protocols that are not widely used include:

- Novell Internetwork Packet Exchange (IPX)
- AppleTalkConnectionless Network Service (CLNS/DECNet)

IPv4 Protocol



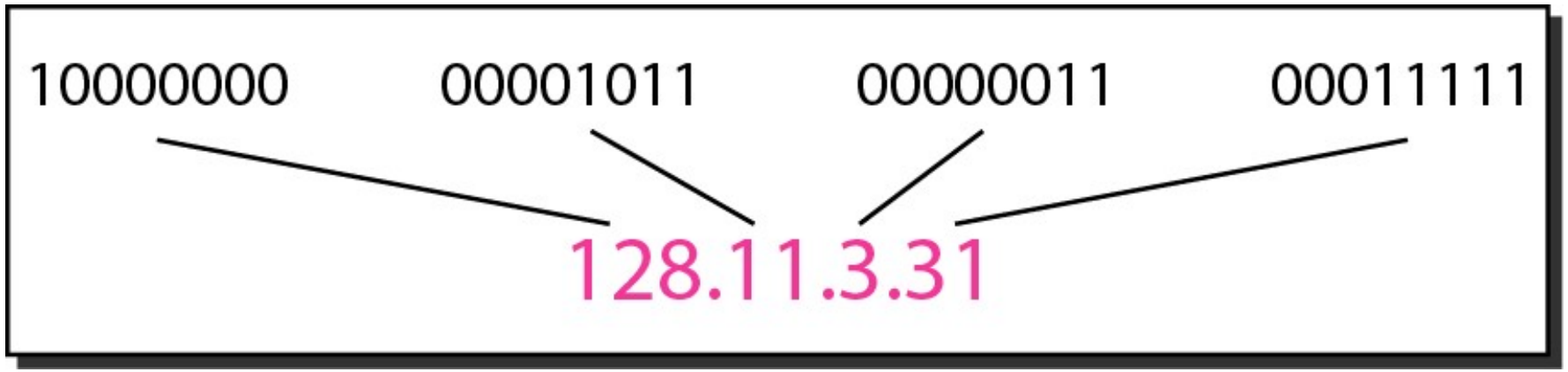
IPv4 Protocol

Objective: Study about basic concept of IP addressing and its type

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.

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

Dotted-decimal notation and binary notation for an IPv4 address



IPv4 Example

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

IPv4 example

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

IPv4 example

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

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

Solution

a. There must be no leading zero (045).

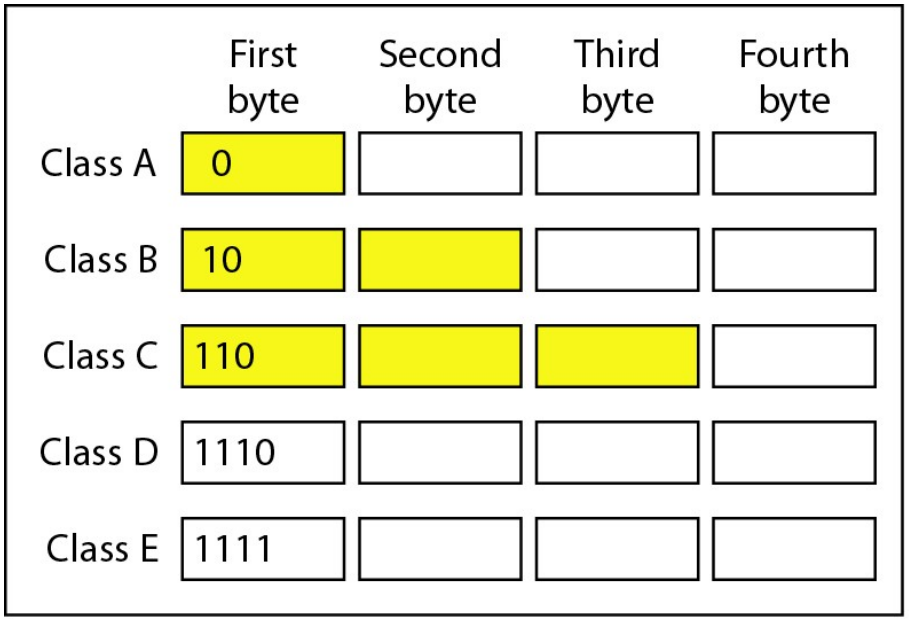
b. There can be no more than four numbers.

c. Each number needs to be less than or equal to 255.

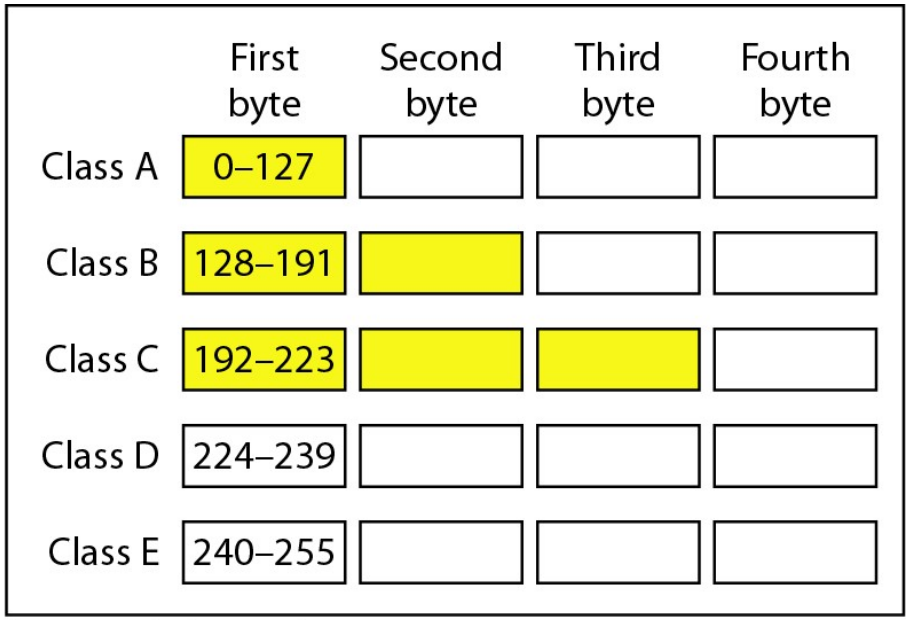
d. A mixture of binary notation and dotted-decimal notation is not allowed.

IPv4 address classification

Finding the classes in binary and dotted-decimal notation



a. Binary notation



b. Dotted-decimal notation

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

IPv4 address classification

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.

IPv4 address classification

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

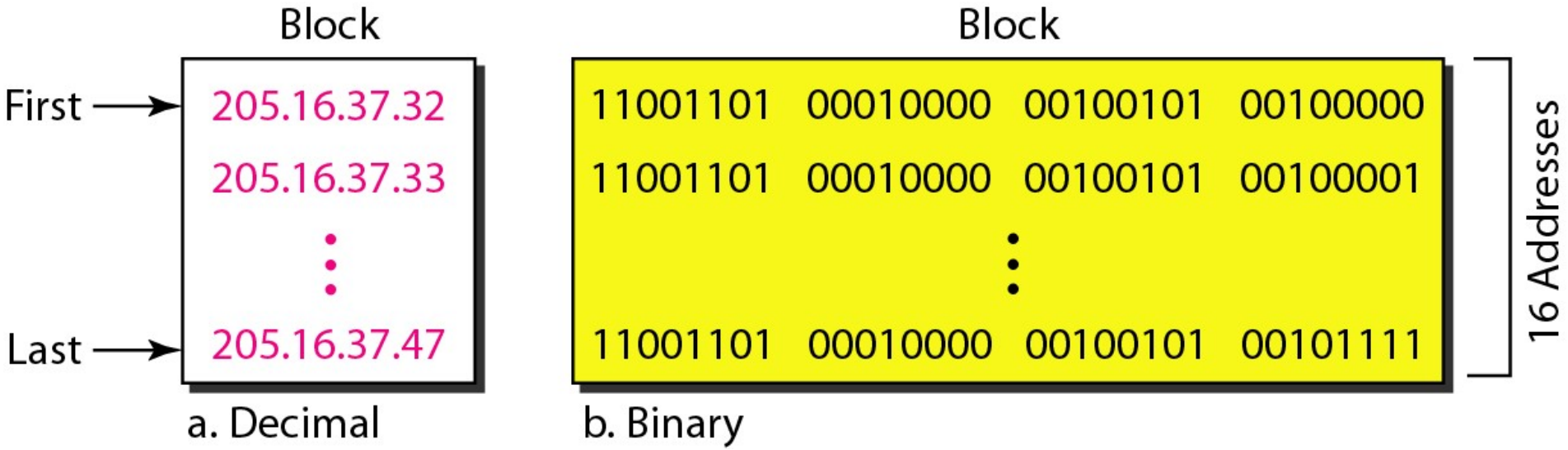
In classful addressing, a large part of the available addresses were wasted.

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

IPv4 address classification

A block of 16 addresses granted to a small organization



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

IPv4 address : classless addressing

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.

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

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

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

Daily Quiz

What is the primary function of the Network Layer in the OSI model?

A) Error detection

B) Data link

C) Routing

D) Physical transmission

Which protocol operates at the Network Layer for addressing and routing in the Internet?

A) TCP

B) IP

C) UDP

D) ICMP

Which of the following devices operates at the Network Layer?

A) Hub

B) Switch

C) Router

D) Repeater

What is the size of the IPv4 address?

A) 32 bits

B) 64 bits

C) 128 bits

D) 16 bits

IPv4 address : classless addressing

CLASSLESS ADDRESSING

IPv4 address : classless addressing

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

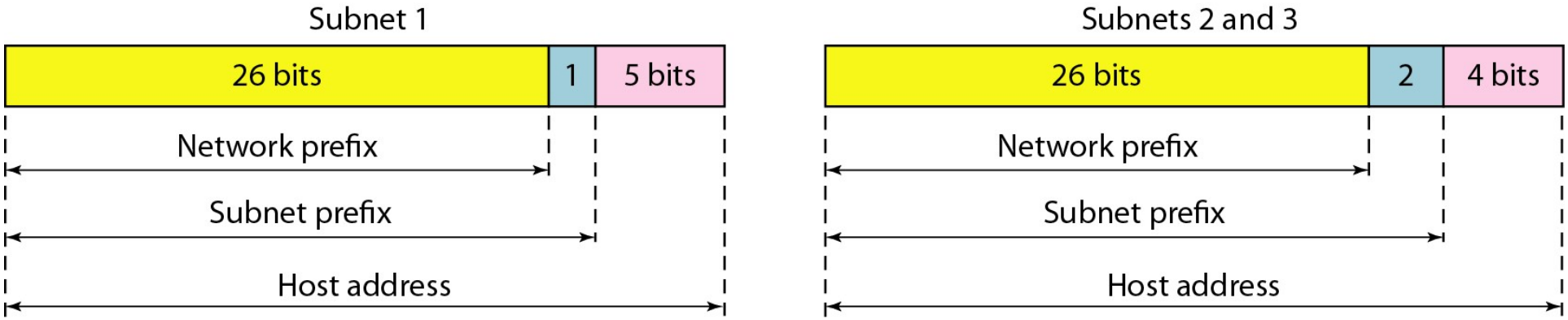
11001101 00010000 00100101 0010000

or

205.16.37.32.

IPv4 address : classless addressing

Three-level hierarchy in an IPv4 address



IPv4 address : classless addressing

An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:

a. The first group has 64 customers; each needs 256 addresses.

b. The second group has 128 customers; each needs 128 addresses.

c. The third group has 128 customers; each needs 64 addresses.

Design the sub blocks and find out how many addresses are still available after these allocations.

IPv4 address : classless addressing

Group 1

For this group, each customer needs 256 addresses. This means that 8 (log2 256) bits are needed to define each host. The prefix length is then 32 − 8 = 24. The addresses are

1st Customer:	*190.100.0.0/24*	*190.100.0.255/24*
2nd Customer:	*190.100.1.0/24*	*190.100.1.255/24*
. . .		
64th Customer:	*190.100.63.0/24*	*190.100.63.255/24*

Total = 64 × 256 = 16,384

IPv4 address : classless addressing

Group 2

For this group, each customer needs 128 addresses. This means that 7 (log2 128) bits are needed to define each host. The prefix length is then 32 − 7 = 25. The addresses are

1st Customer:	*190.100.64.0/25*	*190.100.64.127/25*
2nd Customer:	*190.100.64.128/25*	*190.100.64.255/25*
. . .		
128th Customer:	*190.100.127.128/25*	*190.100.127.255/25*

Total = 128 × 128 = 16,384

IPv4 address : classless addressing

Group 3

For this group, each customer needs 64 addresses. This means that 6 ($\log_2 64$) bits are needed to each host. The prefix length is then 32 − 6 = 26. The addresses are

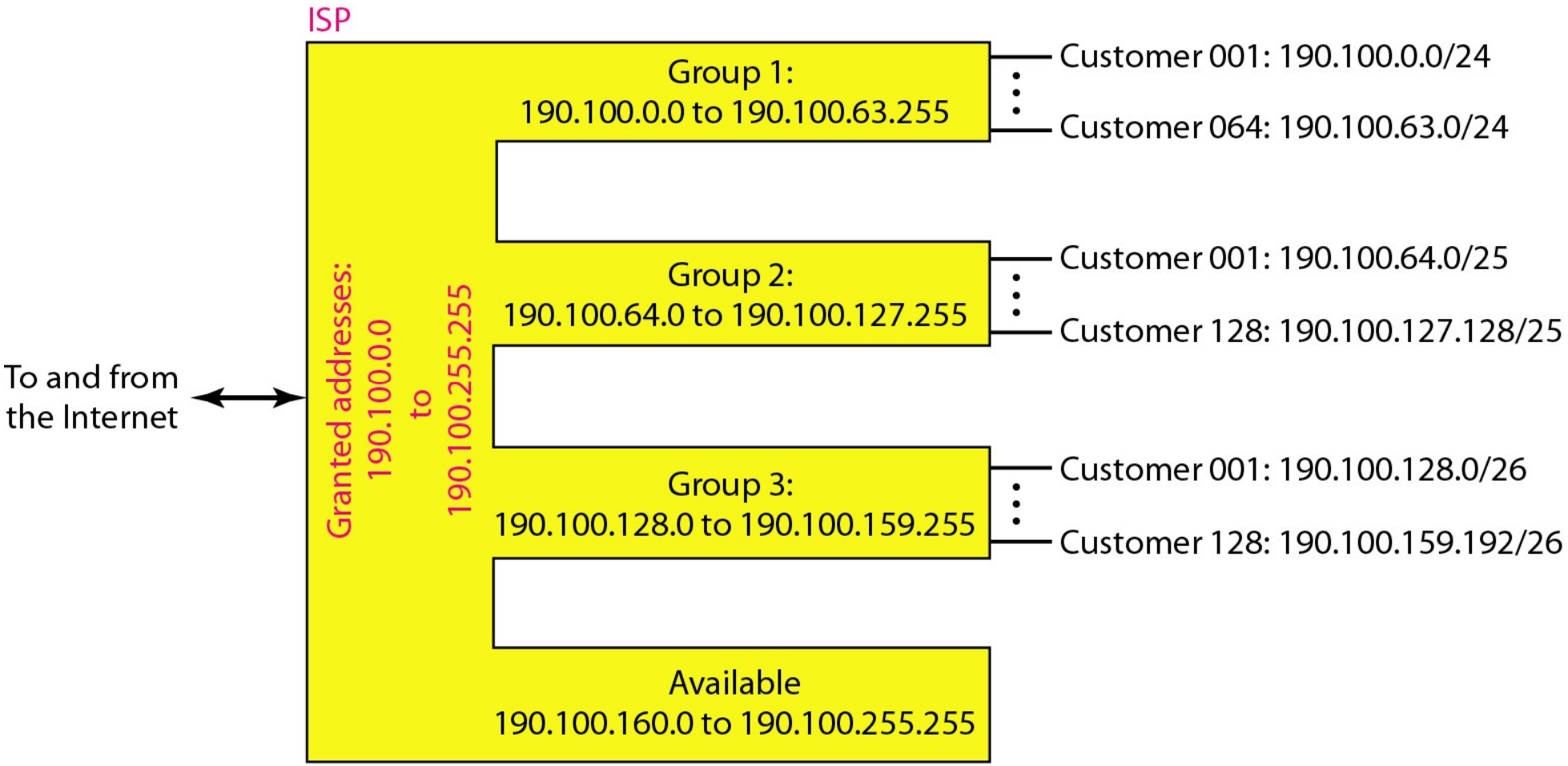
1st Customer:	*190.100.128.0/26*	*190.100.128.63/26*
2nd Customer:	*190.100.128.64/26*	*190.100.128.127/26*
. . .		
128th Customer:	*190.100.159.192/26*	*190.100.159.255/26*

Total = 128 × 64 = 8192

Number of granted addresses to the ISP: 65,536
Number of allocated addresses by the ISP: 40,960
Number of available addresses: 24,576

IPv4 address : classless addressing

An example of address allocation and distribution by an ISP

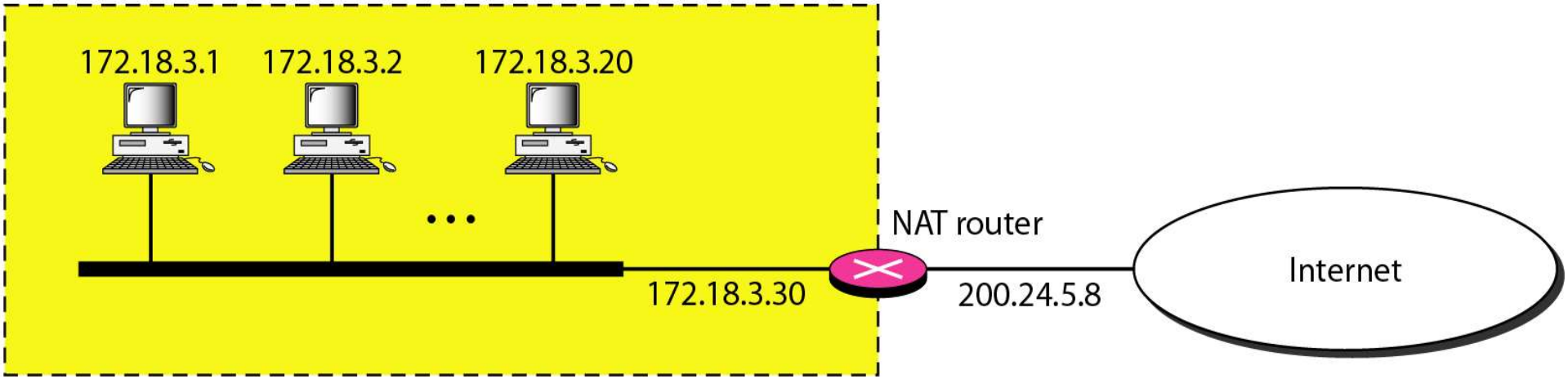


IPv4 address : classless addressing

Addresses for private networks

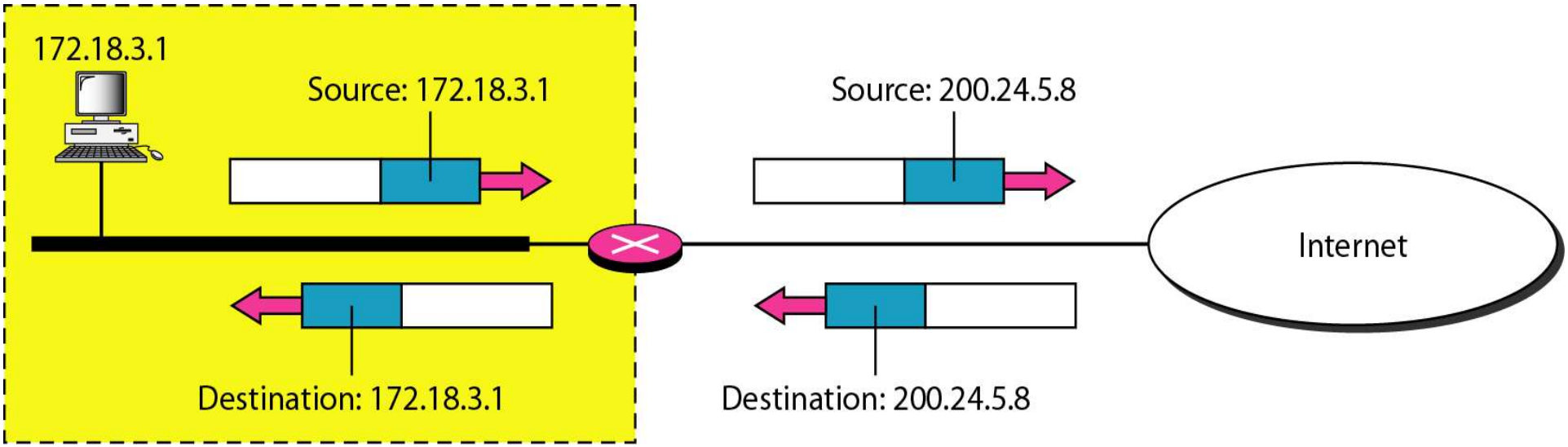
Range			Total
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

Site using private addresses



IPv4 address

Addresses in a NAT

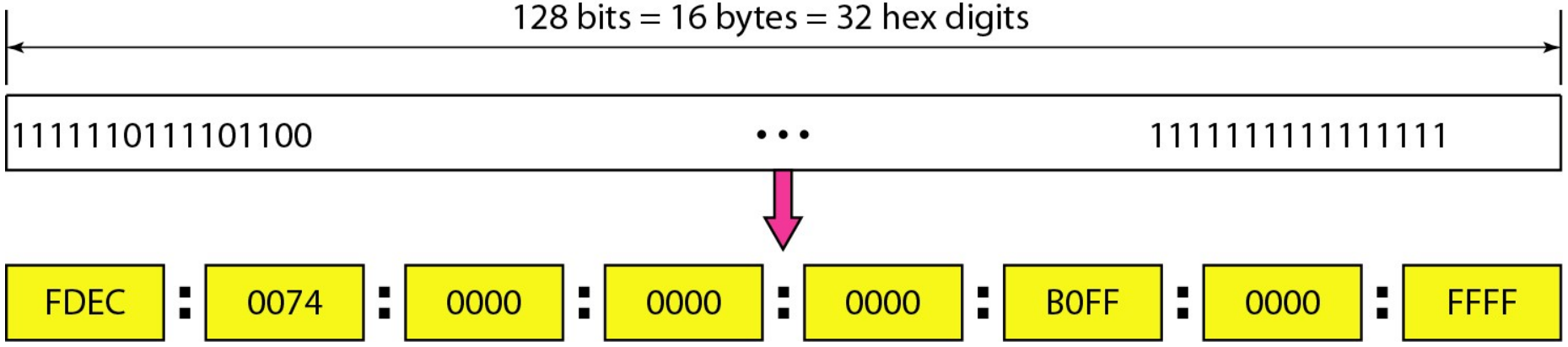


IPv6 address

Objective: Study about basic concept of IPv6 and its function

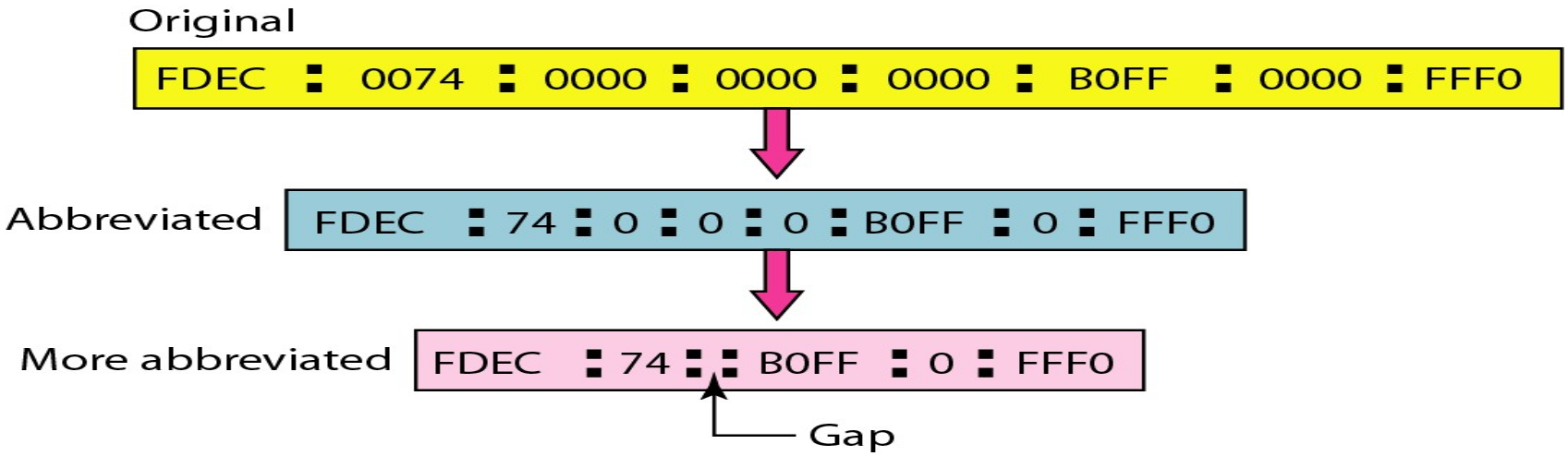
Despite all short-term solutions, address depletion is still a long-term problem for the Internet. This and other problems in the IP protocol itself have been the motivation for IPv6

An IPv6 address is 128 bits long.



IPv6 address

IPv6 address in binary and hexadecimal colon notation



IPv6 address

Expand the address 0:15::1:12:1213 to its original.

Solution

We first need to align the left side of the double colon to the left of the original pattern and the right side of the double colon to the right of the original pattern to find how many 0s we need to replace the double colon.

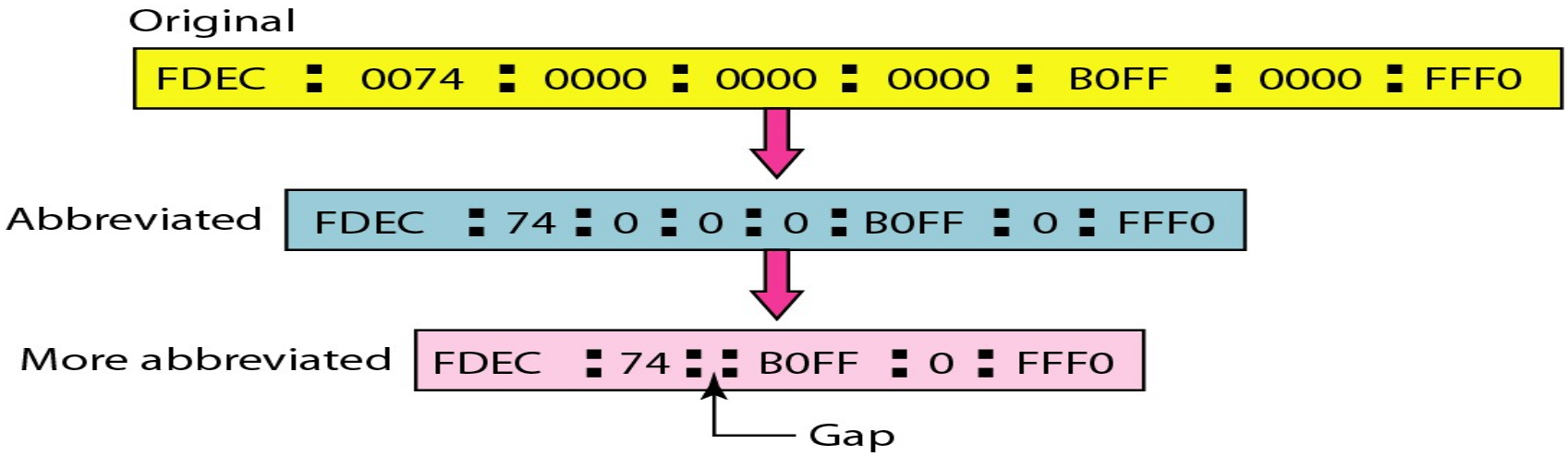
```
xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
 0:  15:                    :    1:  12:1213
```

This means that the original address is.

```
0000:0015:0000:0000:0000:0001:0012:1213
```

IPv6 address

IPv6 address in binary and hexadecimal colon notation

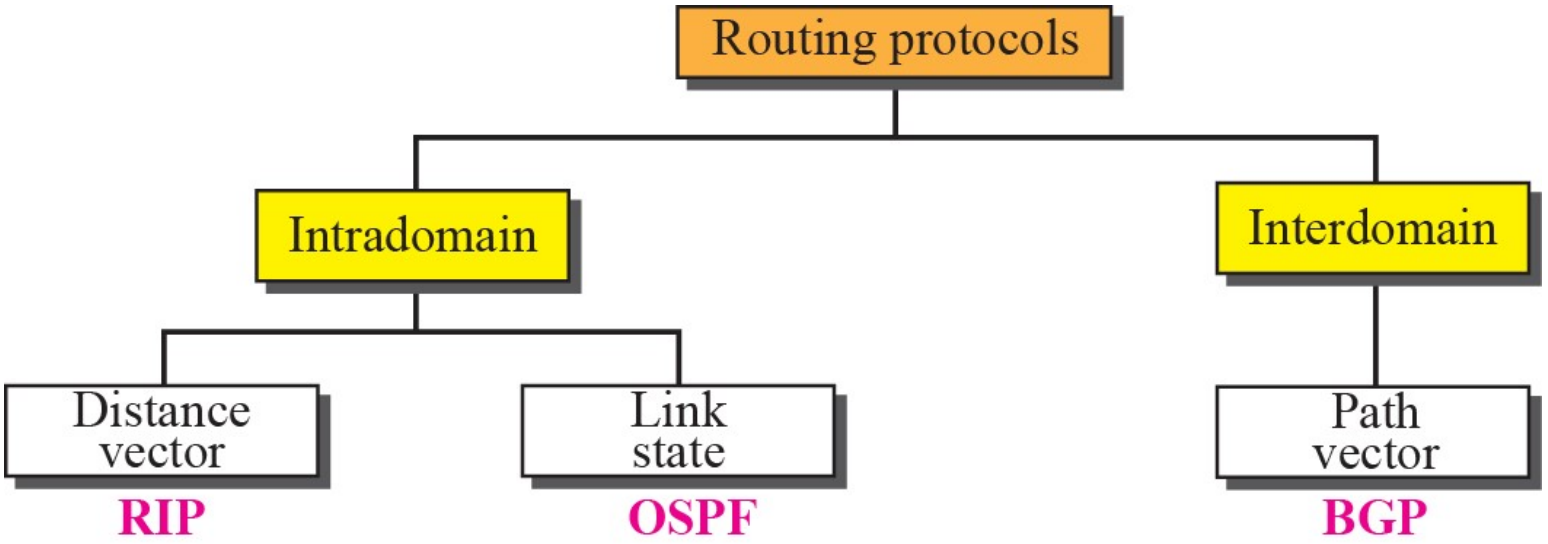


Routing

Objective: Study about basic concept of Routing and its type

An internet is a combination of networks connected by routers. When a datagram goes from a source to a destination, it will probably pass through many routers until it reaches the router attached to the destination network.

Routing


Routing protocols
Intradomain
Interdomain
Distance vector
Link state
Path vector
RIP
OSPF
BGP

Routing

DISTANCE VECTOR ROUTING: Updating of Routing table

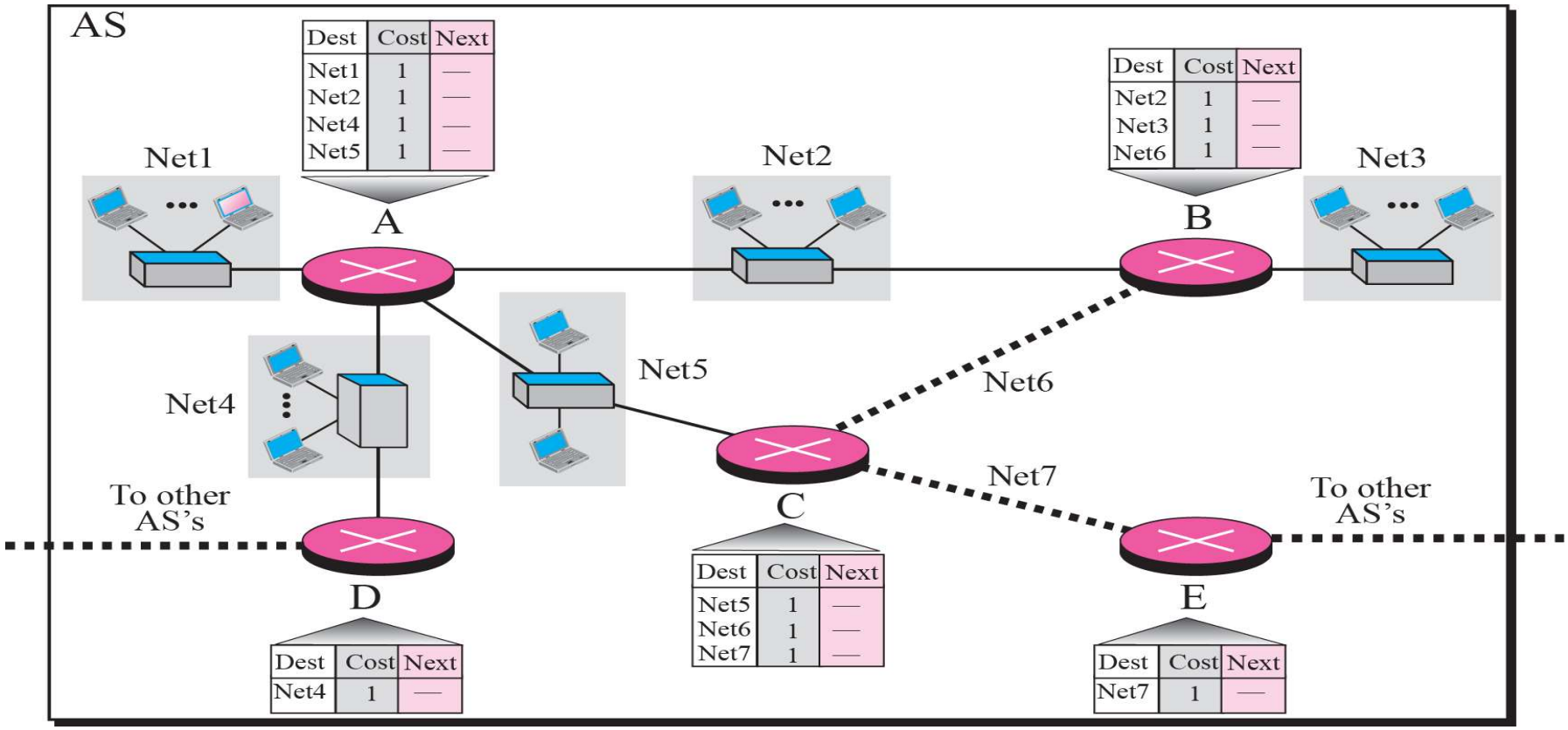
- If the next-node entry is different
  - The receiving node chooses the row with the smaller cost
  - If there is a tie, the old one is kept
- If the next-node entry is the same
  - i.e. the sender of the new row is the provider of the old entry
  - The receiving node chooses the new row, even though the new value is infinity.

Routing

- Periodic Update
  - A node sends its routing table, normally 30 seconds, in a periodic update
- Triggered Update
  - A node sends its routing table to its neighbors any time when there is a change in its routing table
    1. After updating its routing table, or
    2. Detects some failure in the neighboring links

Routing

Figure shows the initial routing table for an AS. Note that the figure does not mean that all routing tables have been created at the same time; each router creates its own routing table when it is booted.



Routing

Now assume router A sends four records to its neighbors, routers B, D, and C. shows the changes in B's routing table when it receives these records.

Dest	Cost	Next
Net1	1	—
Net2	1	—
Net4	1	—
Net5	1	—

A

Dest	Cost	Next
Net2	1	—
Net3	1	—
Net6	1	—

B

Routing Table B

Dest	Cost	Next
Net1	2	A
Net2	1	—
Net3	1	—
Net6	1	—

After receiving record 1

Routing Table B

Dest	Cost	Next
Net1	2	A
Net2	1	—
Net3	1	—
Net6	1	—

After receiving record 2

Routing Table B

Dest	Cost	Next
Net1	2	A
Net2	1	—
Net3	1	—
Net4	2	A
Net6	1	—

After receiving record 3

Routing Table B

Dest	Cost	Next
Net1	2	A
Net2	1	—
Net3	1	—
Net4	2	A
Net5	2	A
Net6	1	—

After receiving record 4

Routing

A

Dest	Cost	Next
Net1	1	—
Net2	1	—
Net3	2	B
Net4	1	—
Net5	1	—
Net6	2	C
Net7	2	C

B

Dest	Cost	Next
Net1	2	A
Net2	1	—
Net3	1	—
Net4	2	A
Net5	2	A
Net6	1	—
Net7	2	C

C

Dest	Cost	Next
Net1	2	A
Net2	2	A
Net3	2	B
Net4	2	A
Net5	1	—
Net6	1	—
Net7	1	—

D

Dest	Cost	Next
Net1	2	A
Net2	2	A
Net3	3	A
Net4	1	—
Net5	1	A
Net6	3	A
Net7	3	A

E

Dest	Cost	Next
Net1	3	C
Net2	3	C
Net3	3	C
Net4	3	C
Net5	2	C
Net6	2	C
Net7	1	—

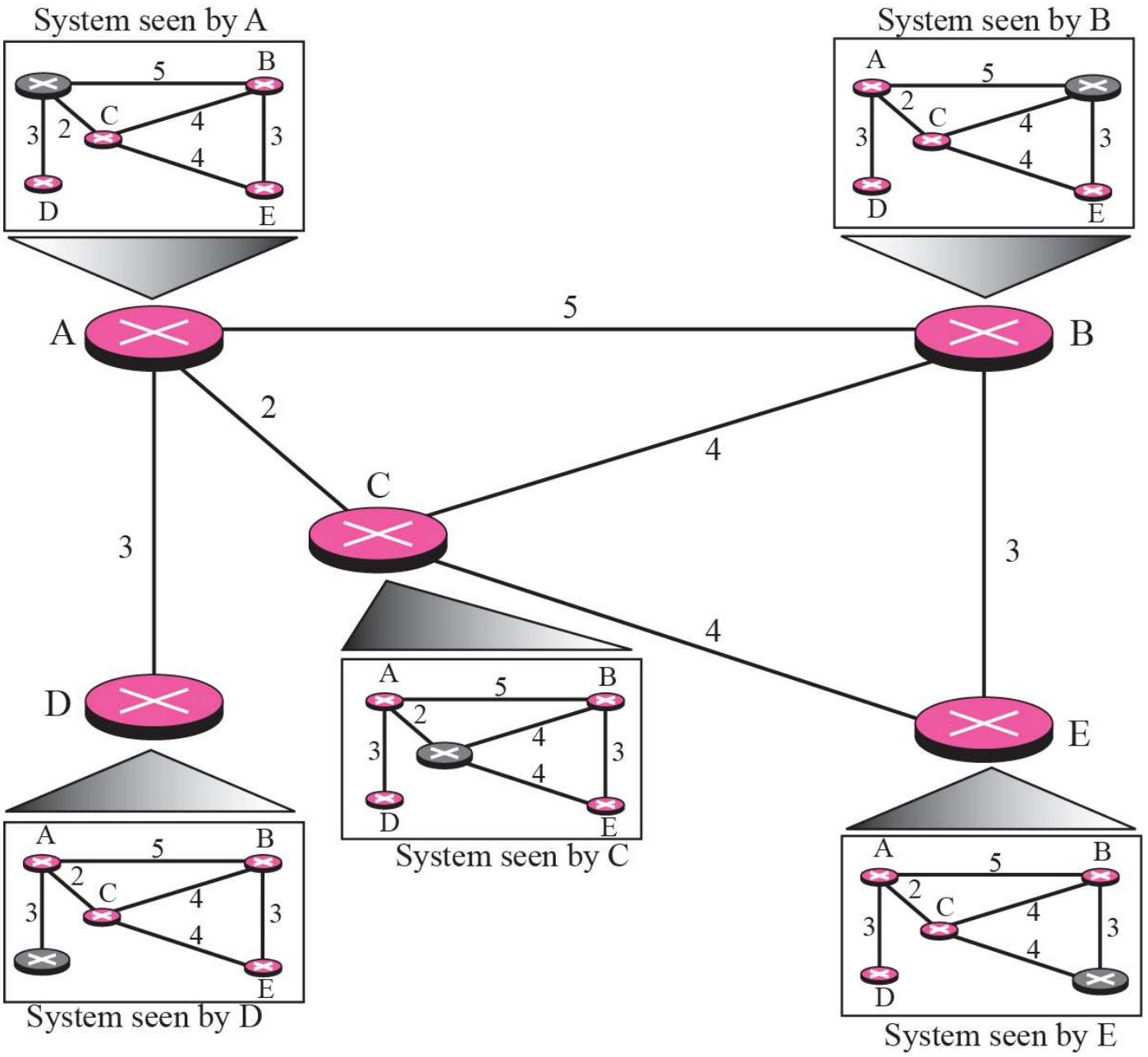
Routing

The Routing Information Protocol (RIP) is an intra-domain (interior) routing protocol used inside an autonomous system. It is a very simple protocol based on distance vector routing. RIP implements distance vector routing directly with some considerations.

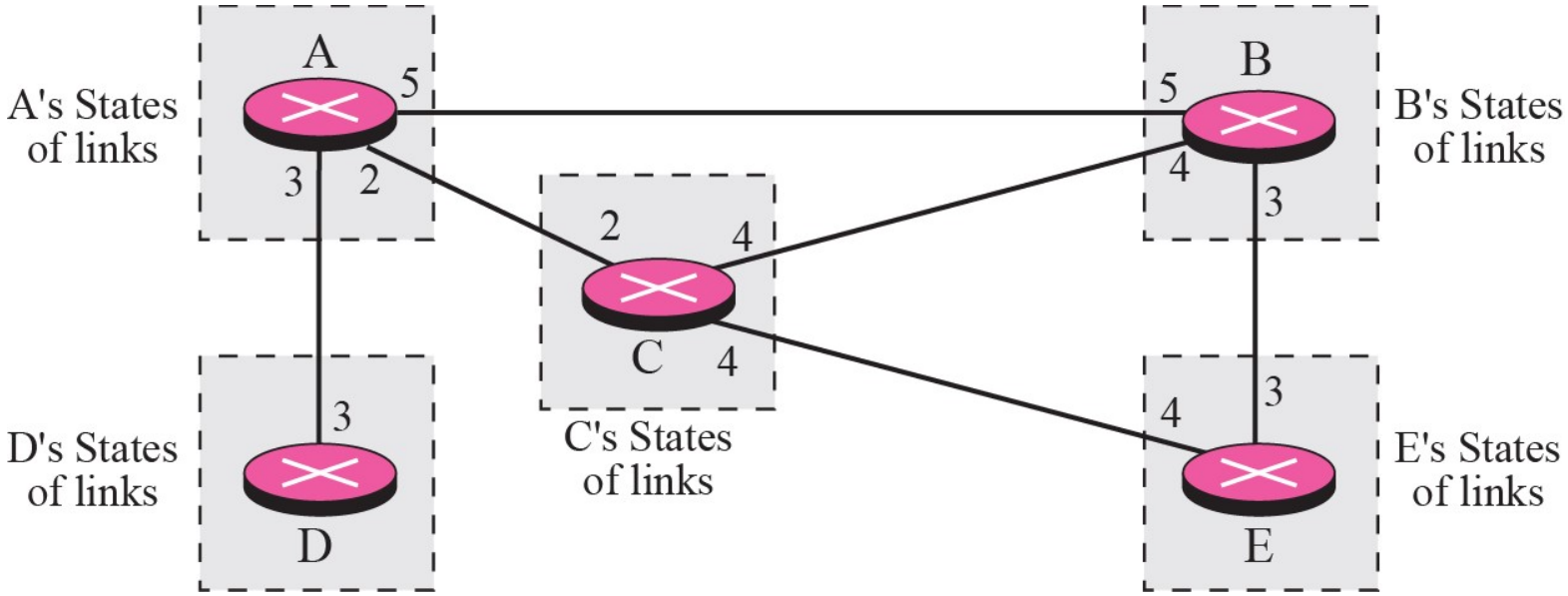
Routing: Link state Routing

Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain—the list of nodes and links, how they are connected including the type, cost (metric), and the condition of the links (up or down)—the node can use the Dijkstra algorithm to build a routing table.

Routing


System seen by A
System seen by B
System seen by C
System seen by D
System seen by E
A
B
C
D
E
5
2
4
3
4
3

Routing


A's States of links
A
5
3
2
B
5
4
3
B's States of links
2
4
C
4
C's States of links
D's States of links
3
D
4
3
E
E's States of links

Routing

Building Routing Tables

- Creation of the states of the links by each node, called the link state packets (LSP)
- Dissemination of LSPs to every other routers, called flooding (efficiently)
- Formation of a shortest path tree for each node
- Calculation of a routing table based on the shortest path tree

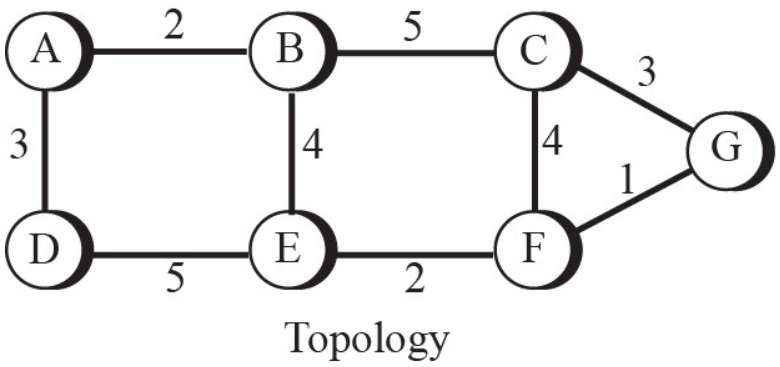
Routing

Creation of LSP

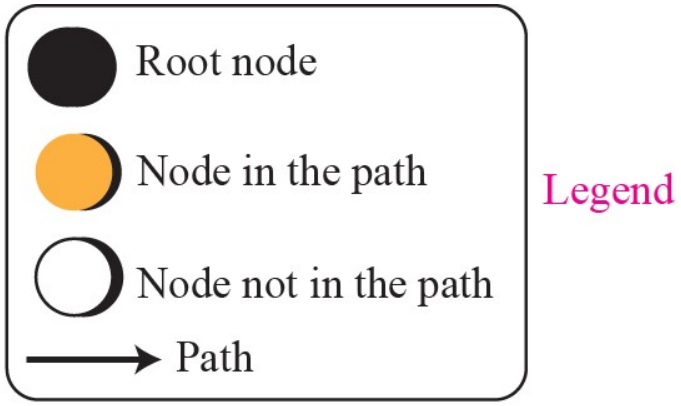
- LSP data: the node ID, the list of links, a sequence number, and age.
- LSP Generation
  - When there is a change in the topology of the domain
  - On a periodic basis
    - There is no actual need for this type of LSP, normally 60 minutes or 2 hours

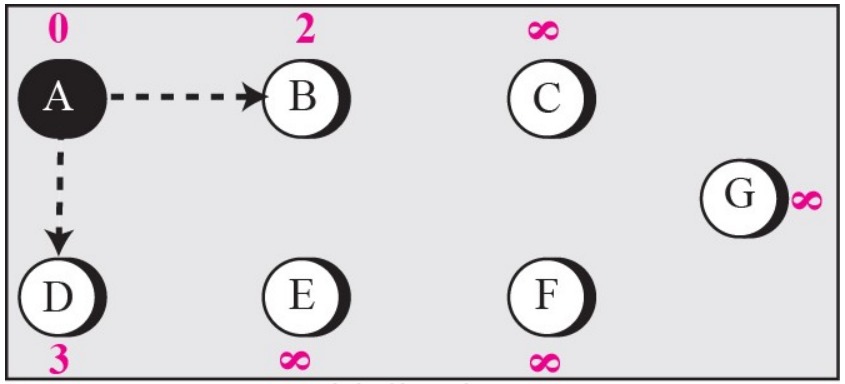
Routing

Forming shortest path three for router A in a graph



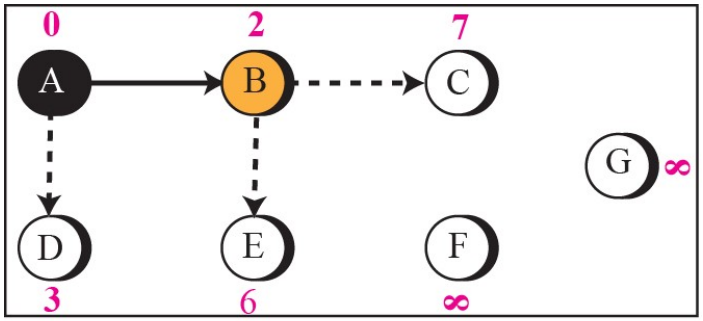
Topology



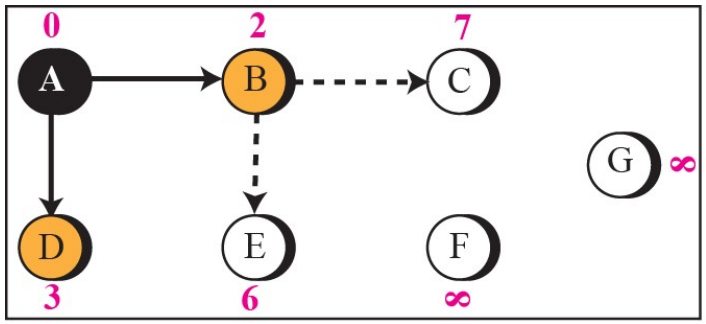


Initialization

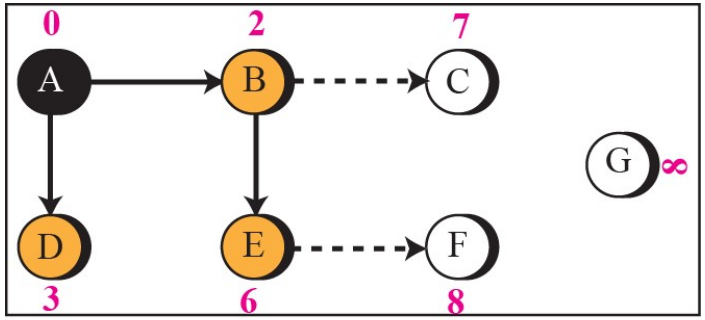
Routing



Iteration 1

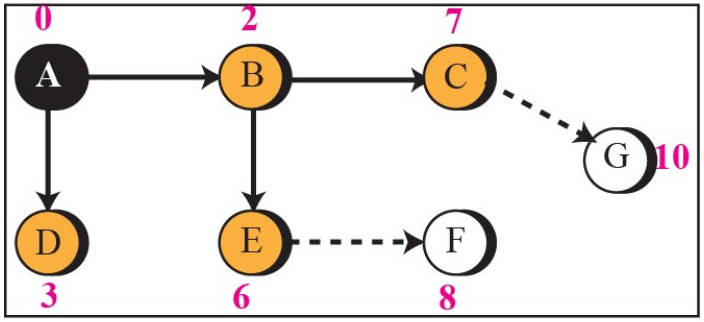


Iteration 2

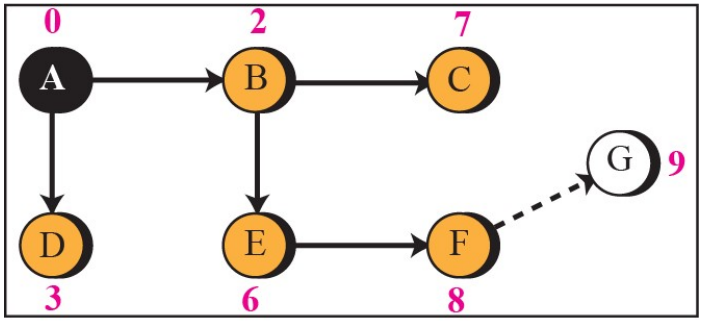


Iteration 3

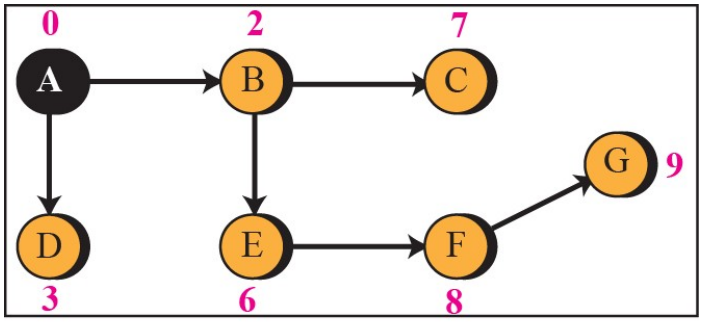
Routing



Iteration 4



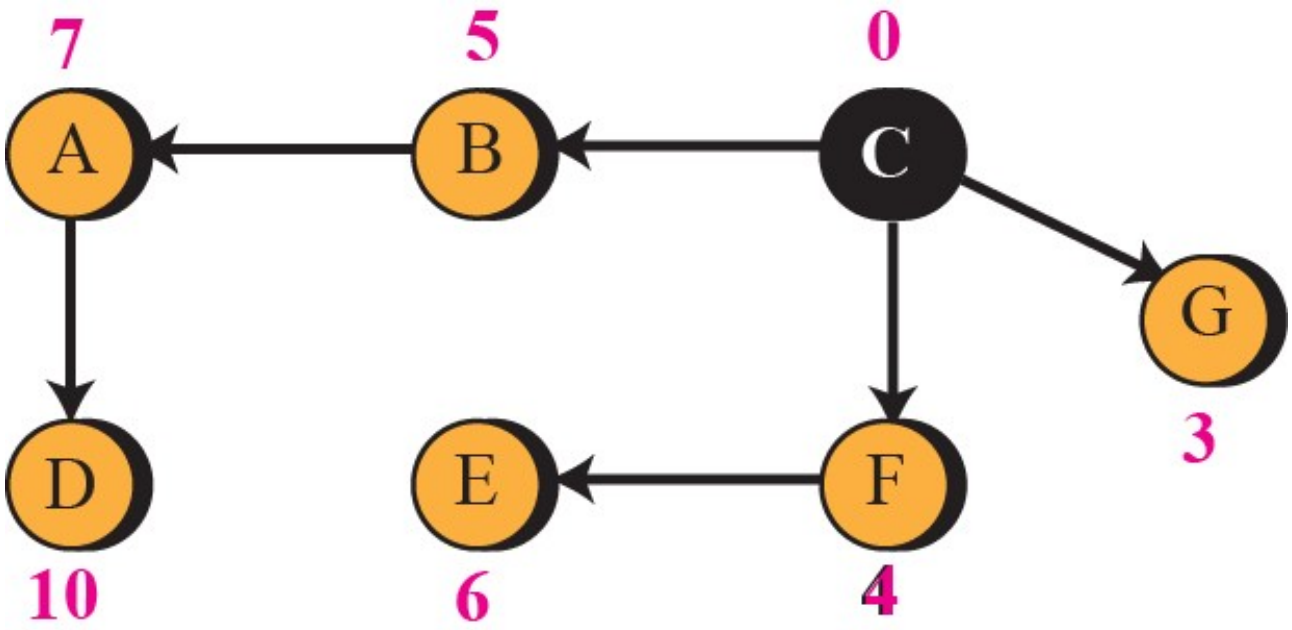
Iteration 5



Iteration 6

Routing

To show that the shortest path tree for each node is different, we found the shortest path tree as seen by node C.



Routing

Routing Table for Node A

Destination	*Cost*	*Next Router*
A	0	—
B	2	—
C	7	B
D	3	—
E	6	B
F	8	B
G	9	B

Daily Quiz

Which field in the IPv4 header is used for error checking and correction?

A) Source IP Address

B) Destination IP Address

C) Checksum

D) TTL (Time to Live)

Which routing algorithm considers the entire network topology to make routing decisions?

A) Distance Vector

B) Link State

C) RIP

D) OSPF

What is the purpose of the TTL (Time to Live) field in the IPv4 header?

A) Sets the maximum transmission speed

B) Limits the time a packet can live in the network

C) Specifies the time for a packet to reach its destination

D) Controls the packet priority

In IPv6, what is the size of the address space compared to IPv4?

A) Smaller

B) Same

C) Larger

D) Equal

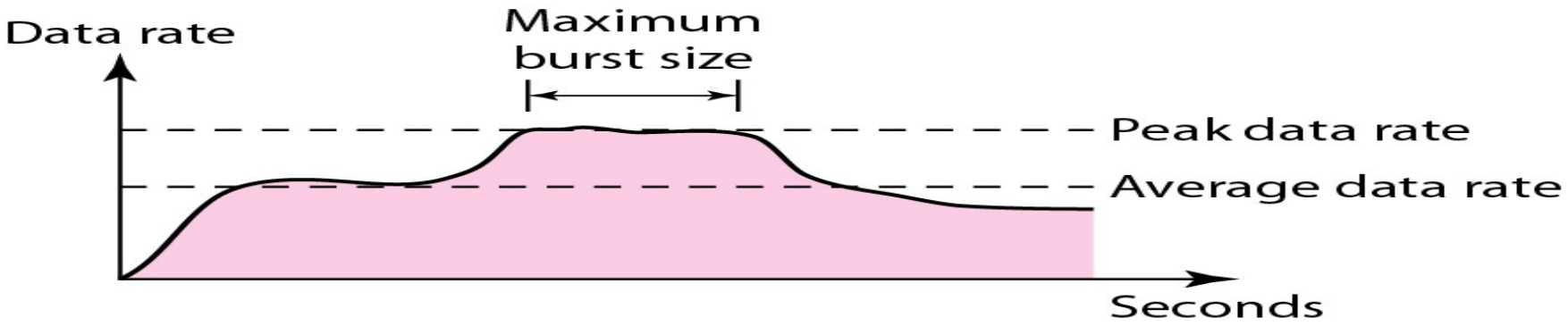
Congestion Control

Objective: Study about basic concept of congestion control and its type

Data traffic

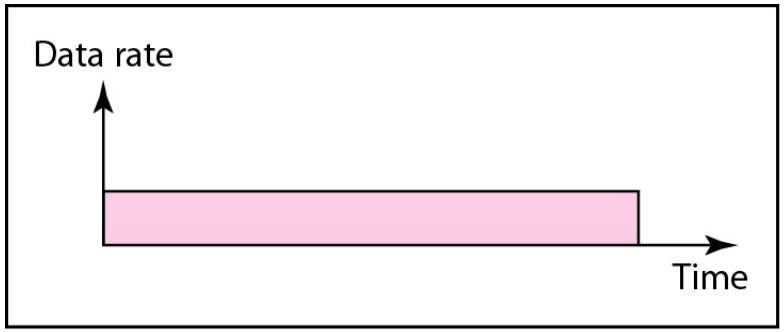
The main focus of congestion control and quality of service is data traffic. In congestion control we try to avoid traffic congestion. In quality of service, we try to create an appropriate environment for the traffic. So, before talking about congestion control and quality of service, we discuss the data traffic itself.

Traffic descriptors

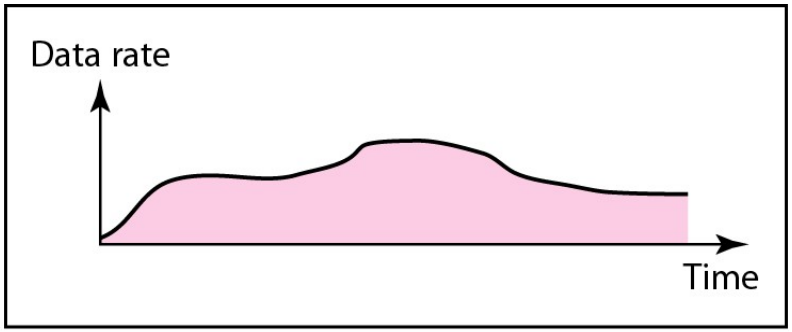


Congestion Control

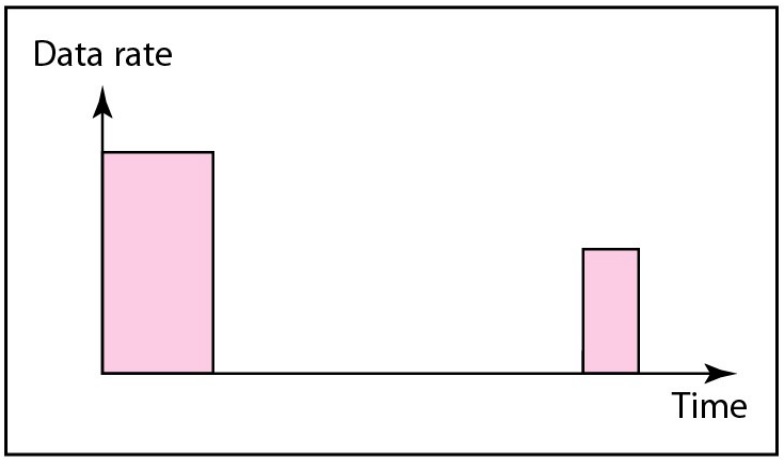
Three traffic profiles



a. Constant bit rate



b. Variable bit rate

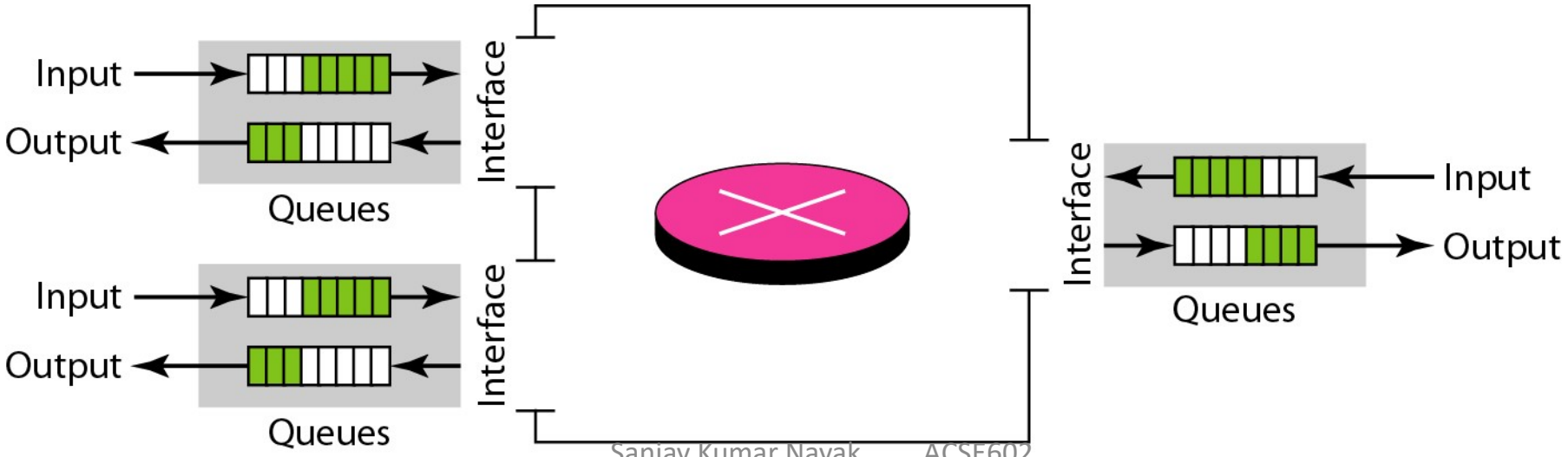


c. Bursty

Congestion Control

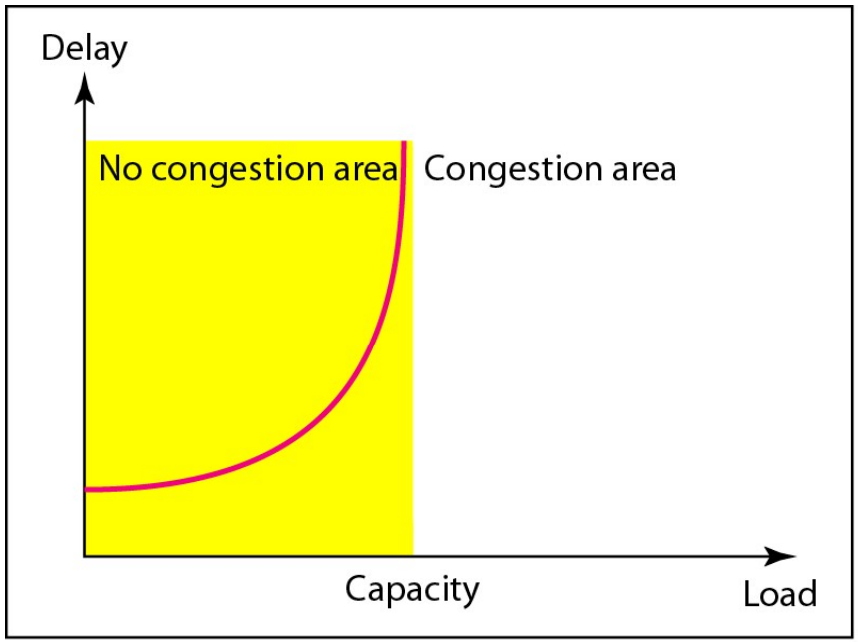
Congestion in a network may occur if the load on the network—the number of packets sent to the network—is greater than the capacity of the network—the number of packets a network can handle. Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

Queues in a router

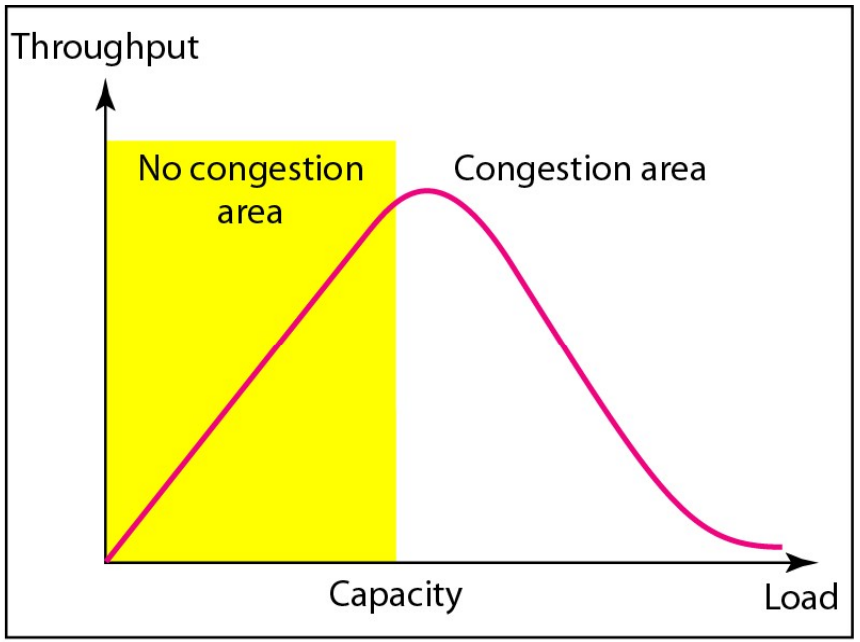


Congestion Control

Packet delay and throughput as functions of load



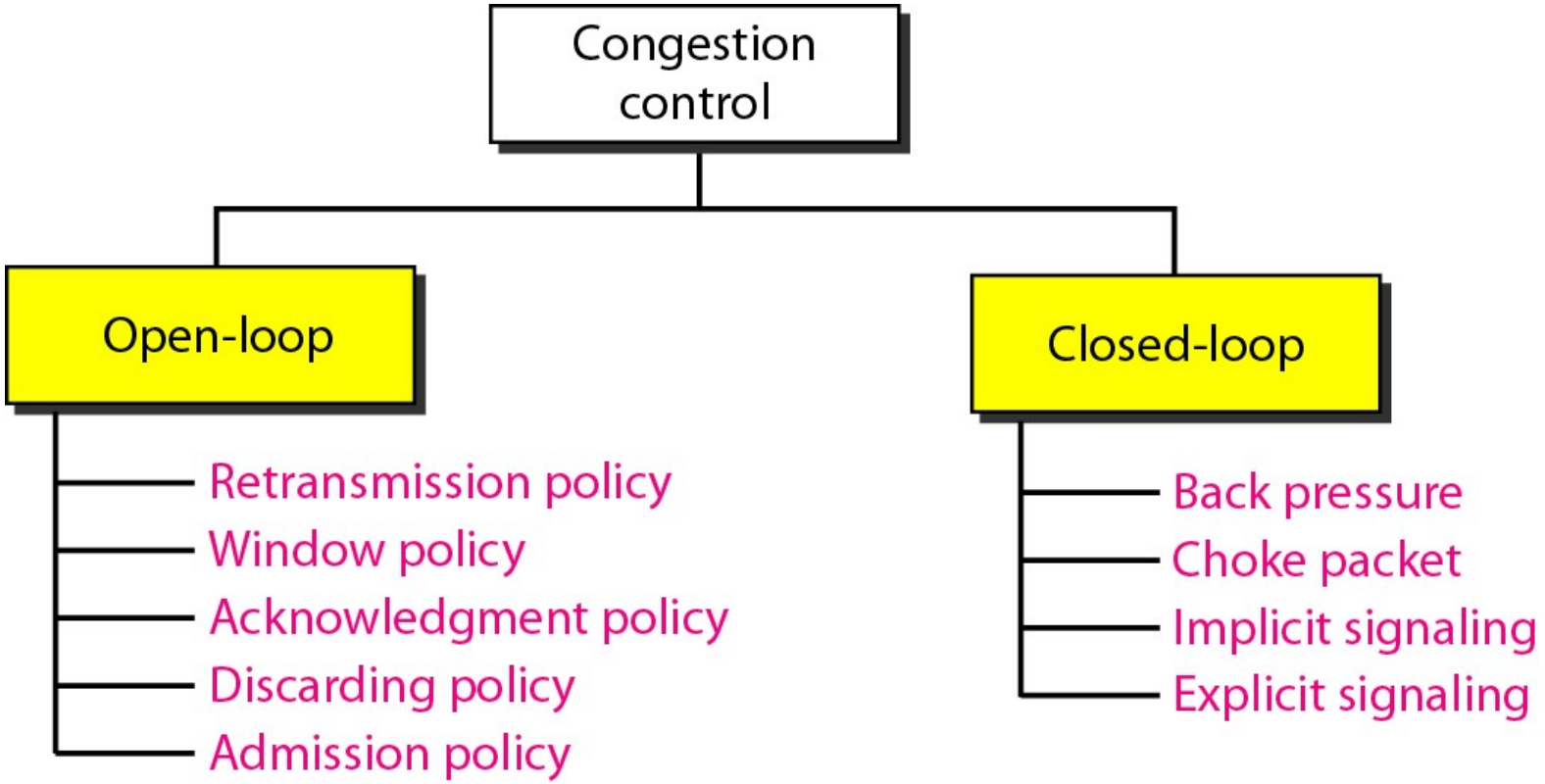
a. Delay as a function of load



b. Throughput as a function of load

Congestion Control

Congestion control categories



Congestion Control

OPEN LOOP CONGESTION CONTROL (PREVENTION TECHNIQUES)

In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination.

1.Retransmission Policy :Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion. The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion.

Congestion Control

2.Window Policy: The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control.

3.Acknowledgment Policy: The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires. A receiver may decide to acknowledge only N packets at a time. the acknowledgments are also part of the load in a network. Sending fewer acknowledgments means imposing less load on the network.

Congestion Control

4.Discarding Policy: A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission. For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented or alleviated.

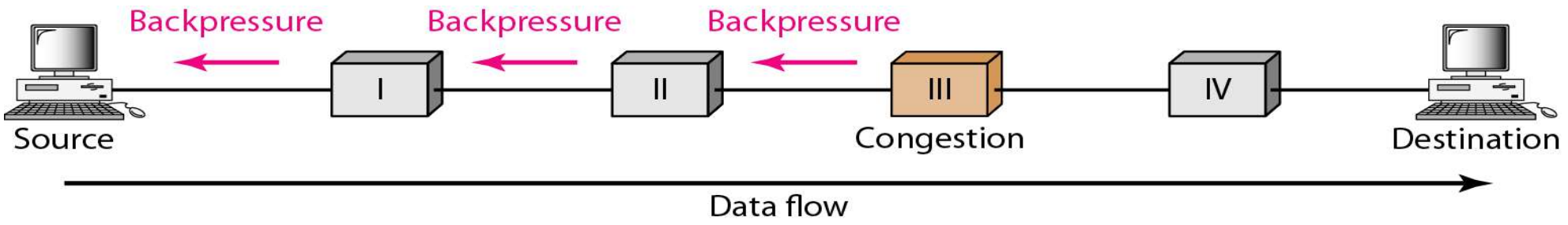
5.Admission Policy: An admission policy, which is a quality-of-service mechanism , can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtual-circuit connection if there is congestion in the network or if there is a possibility of future congestion

Congestion Control

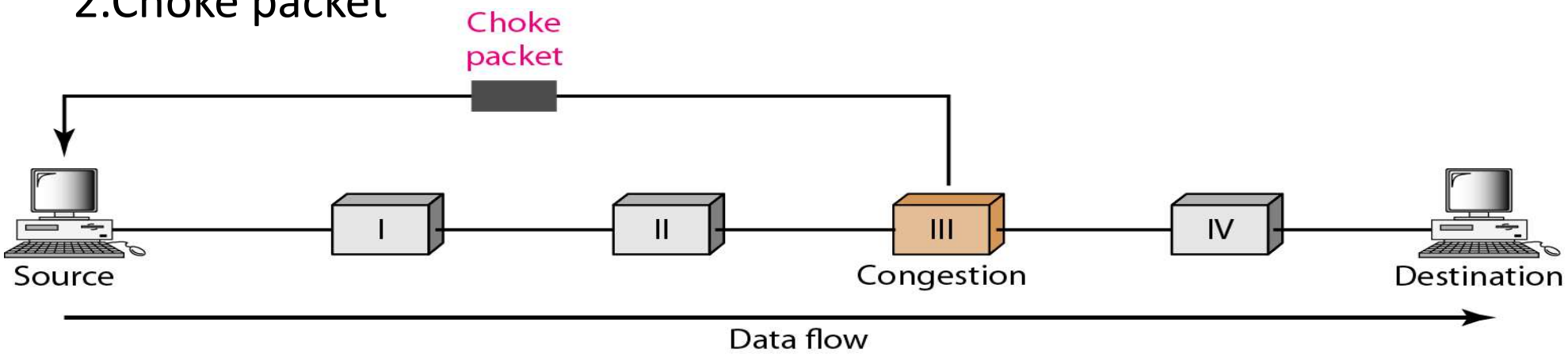
CLOSED LOOP CONGESTION CONTROL (REMOVAL TECHNIQUES)

Closed-loop congestion control mechanisms try to alleviate congestion after it happen

1. Backpressure method for alleviating congestion



2.Choke packet



Congestion Control

3. **Implicit Signaling:**

- **T**here is no communication between the congested node or nodes and the source.
- The source guesses that there is congestion somewhere in the network from other symptoms.
- For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down

Congestion Control

4. Explicit Signaling:

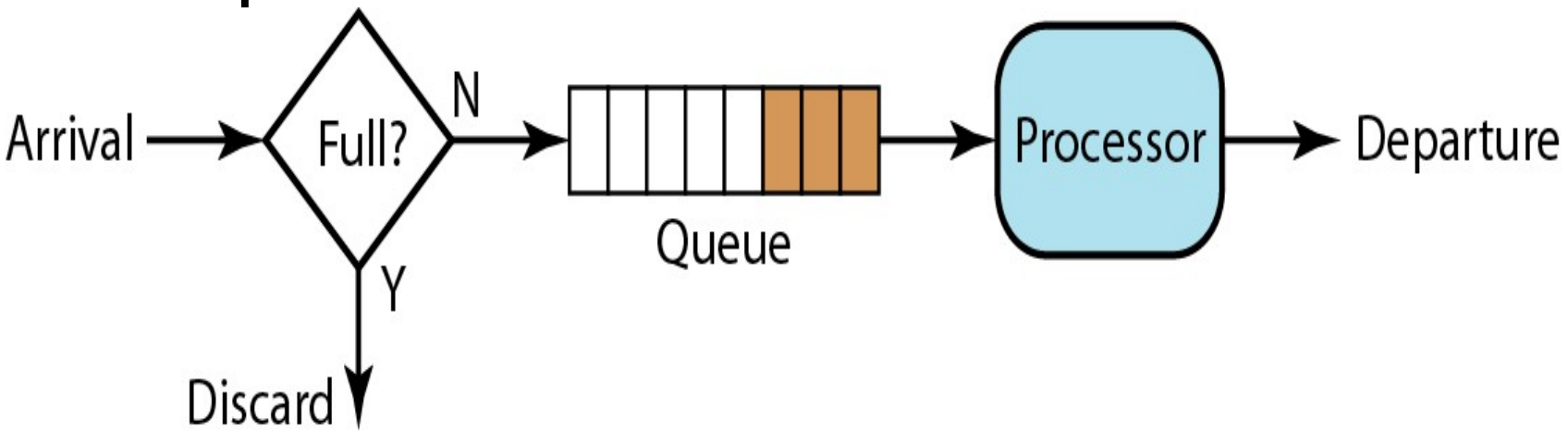
- The node that experiences congestion can explicitly send a signal to the source or destination.
- The explicit-signaling method, however, is different from the choke-packet method.
- In the choke-packet method, a separate packet is used for this purpose; in the explicit-signaling method, the signal is included in the packets that carry data.
- Explicit signaling can occur in either the forward or the backward direction. This type of congestion control can be seen in an ATM network

Congestion Control

TECHNIQUES TO IMPROVE QoS: There are some techniques that can be used to improve the quality of service. four common methods: scheduling, traffic shaping.

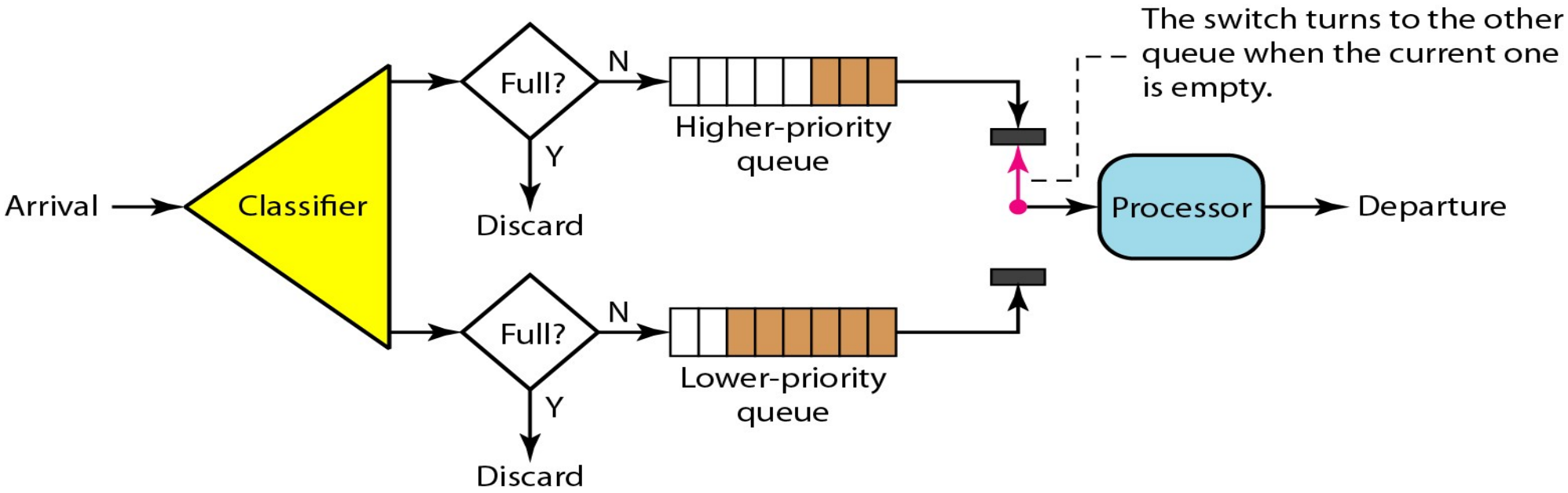
Scheduling: A good scheduling technique treats the different flows in a fair and appropriate manner. Several scheduling techniques are designed to improve the quality of service.

1.FIFO queue



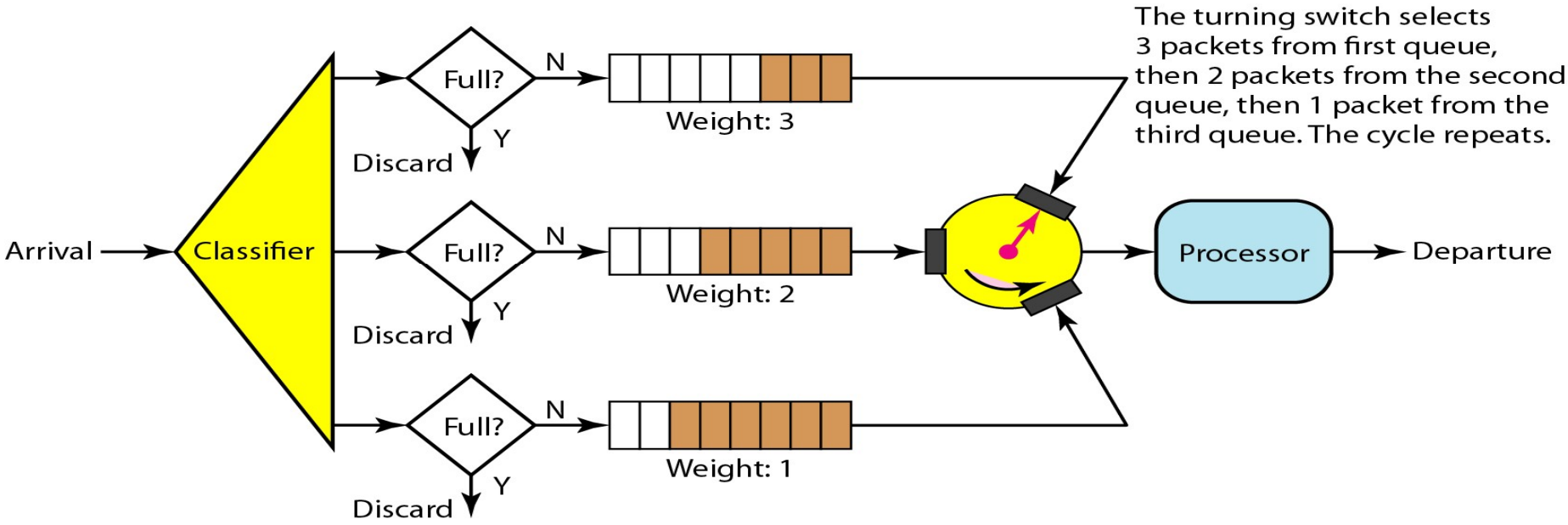
Congestion Control

2.Priority queuing:



Congestion Control

3.Weighted fair queuing

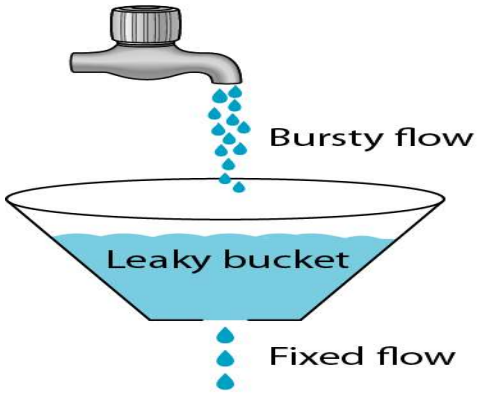


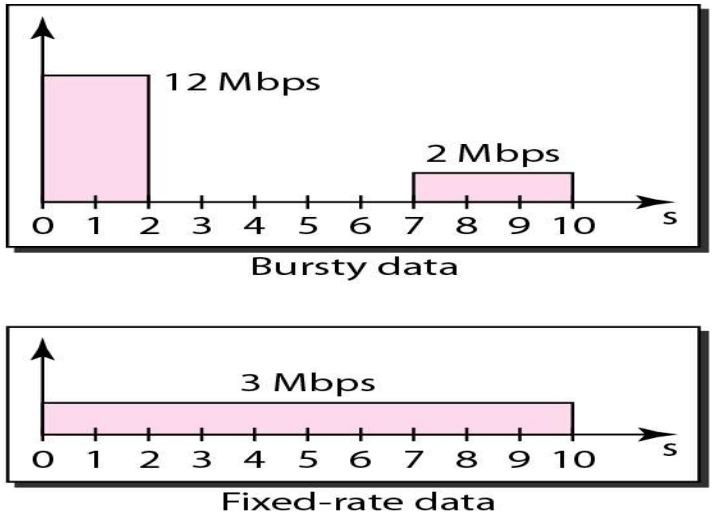
Congestion Control

Traffic Shaping :Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network.

Two techniques can shape traffic: leaky bucket and token bucket.

1. Leaky bucket

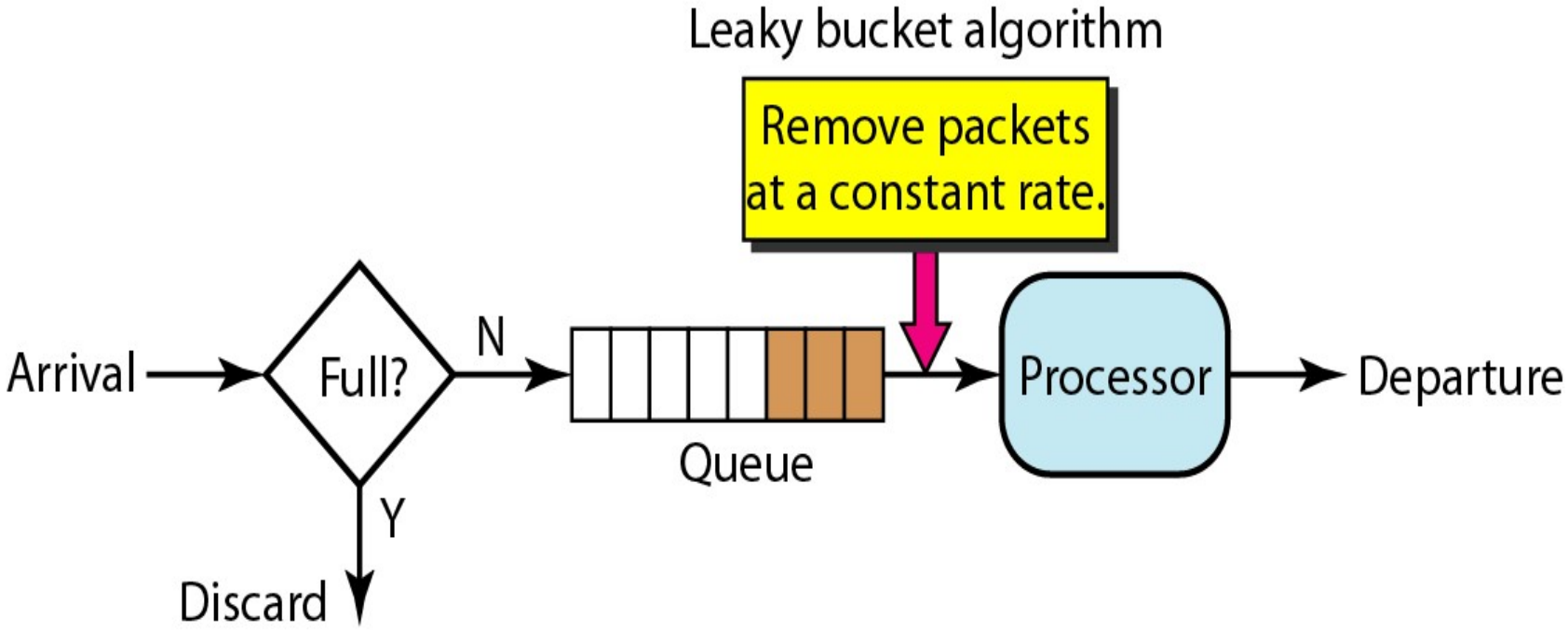




A leaky bucket algorithm shapes busty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.

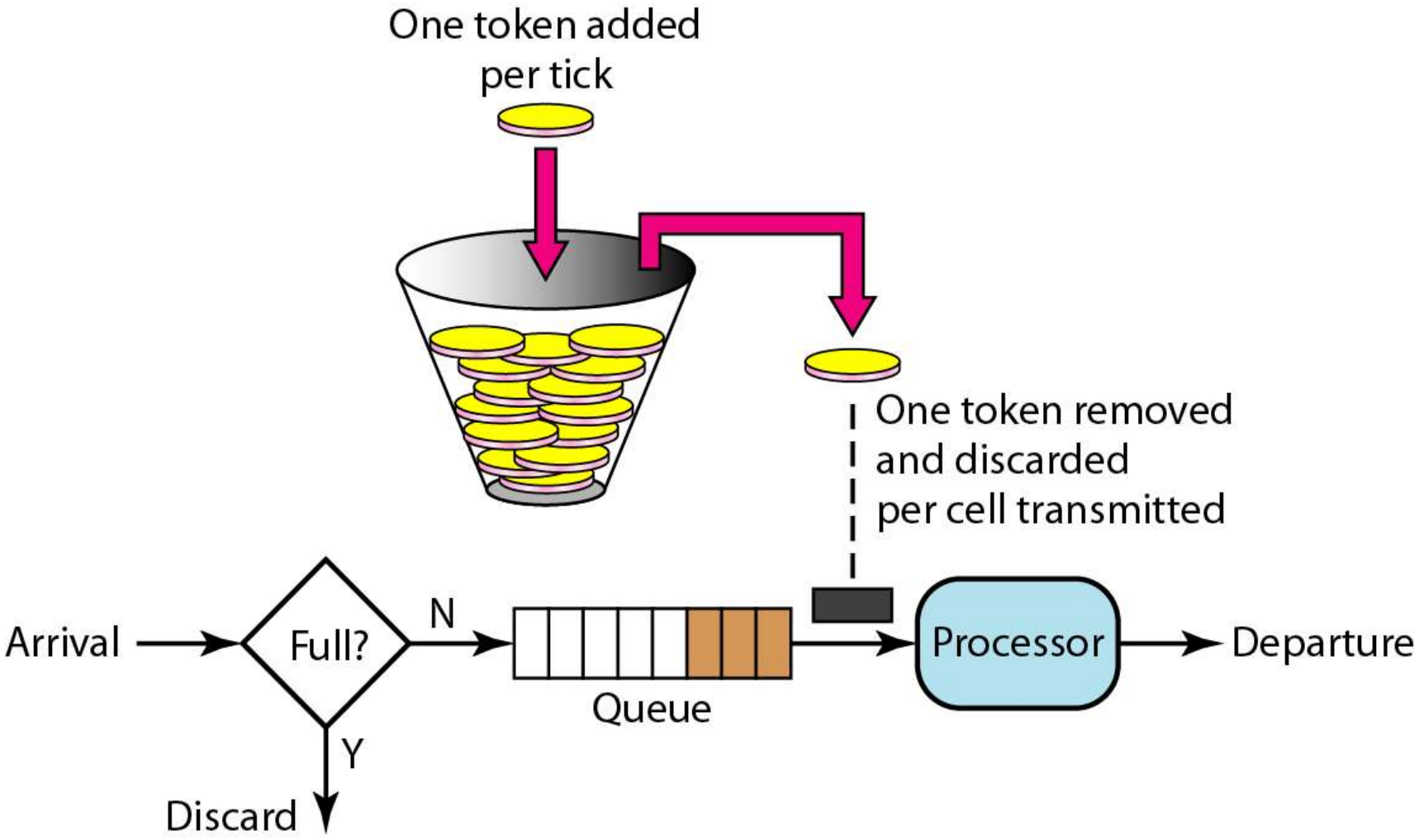
Congestion Control

Leaky bucket implementation



Congestion Control

2.Token bucket



ADDRESS MAPPING

A physical address is a local address. It is called a physical address because it is usually (but not always) implemented in hardware. An example of a physical address is the 48-bit MAC address in the Ethernet protocol, which is imprinted on the NIC installed in the host or router. The physical address and the logical address are two different identifiers

Mapping Logical to Physical Address: ARP

ARP stands for "Address Resolution Protocol".

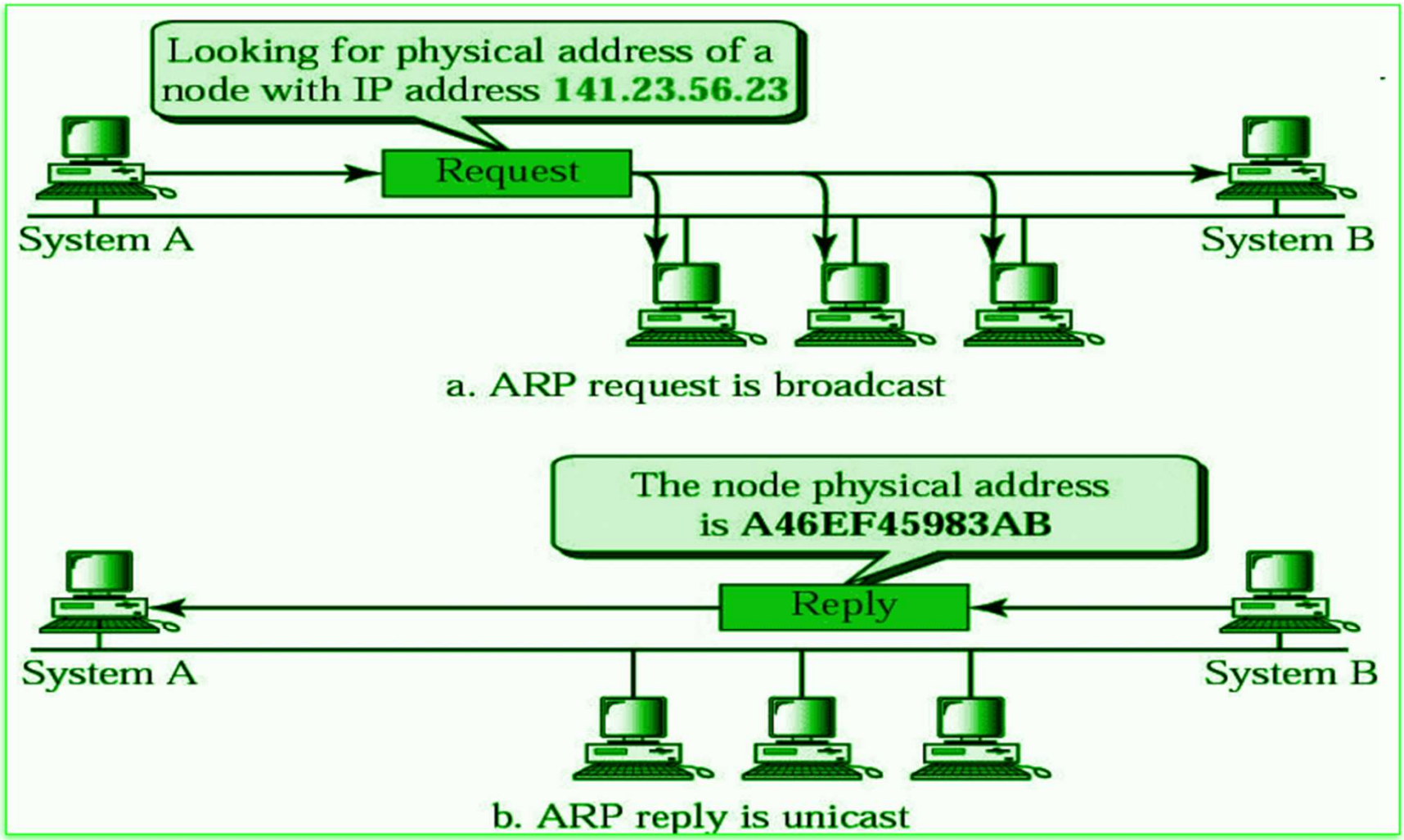
- It is a network protocol used to determine the MAC address (hardware address) from any IP address.

- This protocol is used when a device wants to communicate with another device over a local area network or ethernet.

ARP WORKING

How ARP Protocol Works?

Working flow diagram of ARP Protocol



ADDRESS MAPPING

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

There are occasions in which a host knows its physical address but needs to know its logical address. This may happen in two cases:

1. A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.
2. An organization does not have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease

RARP

- **Reverse Address Resolution Protocol (RARP)** finds the logical address for a machine that knows only its physical address.
- The machine can get its physical address (by reading its NIC, for example), which is unique locally.
- With RARP, the device would broadcast its MAC address and request an IP address, and a RARP server on the network would respond with the corresponding IP address.
- RARP was widely used in the past, it has largely been replaced by newer protocols such as DHCP (Dynamic Host Configuration Protocol), which provides more flexibility and functionality in assigning IP addresses dynamically.
- RARP is still used in some specialized applications, such as booting embedded systems and configuring network devices with pre-assigned IP addresses.

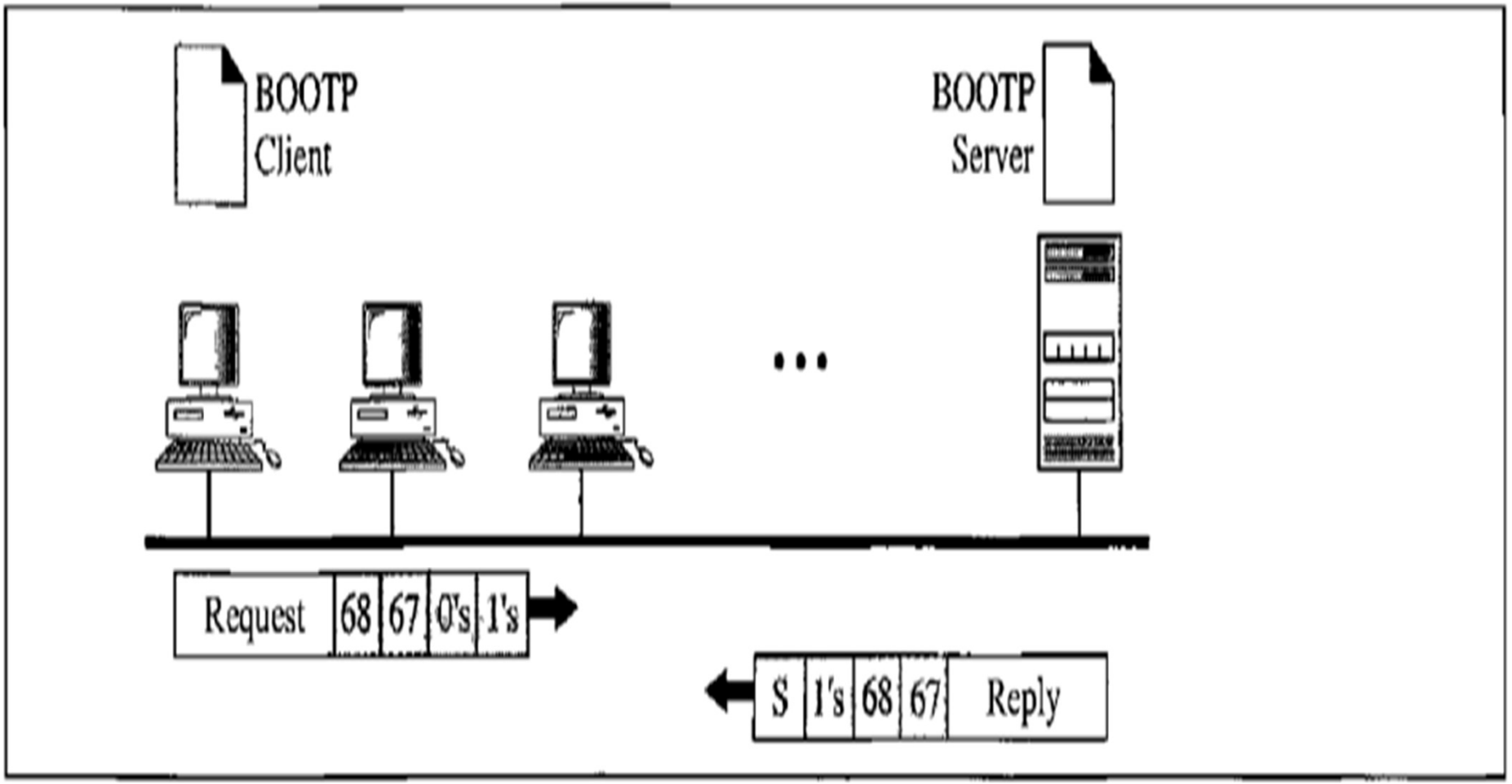
BOOTP

Bootstrap Protocol (BOOTP) is a networking protocol which is used by networking administration to give IP addresses to each member of that network for participating with other networking devices by the main server.

The Bootstrap Protocol (BOOTP) is a client/server protocol designed to provide physical address to logical address mapping. BOOTP is an application layer protocol. The administrator may put the client and the server on the same network or on different networks.

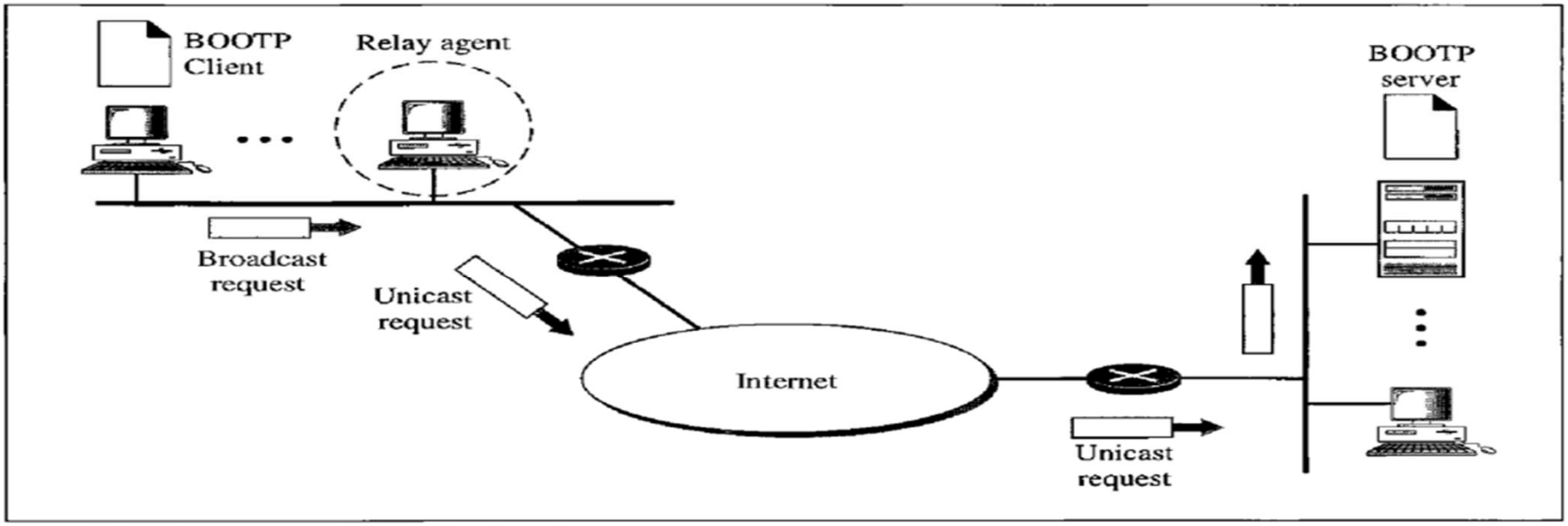
How a client can send an IP datagram when it knows neither its own IP address (the source address) nor the server's IP address (the destination address). The client simply uses all 0s as the source address and all 1s as the destination address

BOOTP



a. Client and server on the same network

BOOTP



b. Client and server on different networks

BOOTP is not a dynamic configuration protocol. When a client requests its IP address, the BOOTP server consults a table that matches the physical address of the client with its IP address.

if a host moves from one physical network to another? What if a host wants a temporary IP address? BOOTP cannot handle these situations because the binding between the physical and IP addresses is static and fixed in a table until changed by the administrator.

BOOTP is a static configuration protocol.

DHCP

The Dynamic Host Configuration Protocol (DHCP) has been devised to provide static and dynamic address allocation that can be manual or automatic

- **Static Address Allocation** In this capacity DHCP acts as BOOTP does. It is backward compatible with BOOTP, which means a host running the BOOTP client can request a static address from a DHCP server. A DHCP server has a database that statically binds physical addresses to IP addresses.

- **Dynamic Address Allocation** DHCP has a second database with a pool of available IP addresses. This second database makes DHCP dynamic. When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time.

Faculty Video Links, Youtube & NPTEL Video Links and Online Courses Details

- You tube/other Video Links

- https://www.youtube.com/watch?v=aqtd8iZlSAA
- https://www.youtube.com/watch?v=JhBnOamc_8s

Daily Quiz

1. Routing tables of a router keeps track of
   A. MAC Address Assignments
   B. Port Assignments to network devices
   C. Distribute IP address to network devices
   D. Routes to use for forwarding data to its destination
2. What is the use of Ping command?
   A. To test a device on the network is reachable
   B. To test a hard disk fault
   C. To test a bug in an Application
   D. To test a Pinter Quality
3. Router and 3 layer switch work on which layer of OSI model.
   A. Physical layer
   B. Data Link layer
   C. **Network layer**
   D. None

Daily Quiz

4. Which is correct for IPv4 and IPv6
   A. 32 & 128 B. 32 & 48 C. 48 & 128 D. 64 & 132
5. Find out wrong IP address
   A. 192.168.2.50 **B.168.02.34.1** C. 127.0.0.0 D. 111.2.56.39
6. Class C IP address default mask address
   A. 255.0.0.0 B. **255.255.255.0** C. 255.255.0.0 D. None
7. Hub work on which layer of OSI model
   A. **Physical layer** B. Data Link layer C. Network layer D. None
8. Main function of network layer of OSI model
   A. Routing B. Logical addressing C. **Both A&B** D. None
9. Which IP address version have five classes
   A. **IPv4** B. IPv6 C. Both A & B D. None
10. Supernetting found in which type of IP addresses
    A. Classfull B**. Classless** C. Both A &B D. None

Weekly Assignment

1. A computer on 6 mbps network is regulated by a token bucket

The token bucket is filled at a rate of 1 mbps. It is initially Filled to capacity with 8 mega bits. How long can the Computer transmit at the full 6 mbps.

Solution: S=C/(M-P)=8/(6-1)=1.6 sec (CO3)

Ans

Capacity C=8 Mb

S Burst length in sec

M=6Mbps

P=1 Mbps

MCQ s

1. Which of the following is true of the IP address 192.0.0.10? (CO4)

   A) The netid is 192.
   B) The hostid is 0.10.
   C) The network address is 192.0.0.0.
   D) none of the above

2. A subnet mask in class A has 14 1s. How many subnets does it define?

   A) 32
   B) 8
   C) 64
   D) none of the above

3. **Which IPv6 address type is used for loopback testing?**

   A) Unicast
   B) Multicast
   C) Anycast
   D) Loopback

MCQ s

4. Given the IP address 201.14.78.65 and the subnet mask 255.255.255.224, what is the subnet address?

A) 201.14.78.32
B) 201.14.78.65
C) 201.14.78.64
D) none of the above

5. Routers function in the _____ layers.

A) physical and data link
B) physical, data link, and network
C) data link and network
D) none of the above

Old Question Papers

- http://www.ululu.in/computer-networks-solved-sample-papers-btech-6th-semester/

Expected Questions for University Exam

1. Compare routers and gateways. (CO4)
2. Write the IP address range of each class. (CO4)
3. Explain the need of subnet. (CO4)
4. Write acronym for ARP, RARP, ICMP(CO4)
5. For the given IP address 192.168.2.9 find the class, network address and host address. (CO4)
6. Write down default mask for each class IP address. (CO4)
7. Write down subnet mask for given 192.12.3.9/26 IP address. (CO4)
8. List the functions of network layer. (CO4)

Summary

In this unit 3 we have studied about Network layer of OSI model, its functions and how it handles the packet received from transport layer. Routing methods are also explained and comparison IPv4 and IPv6 completed.
To manage the traffic congestion control is covered.

Recap of Unit

- Point-to-point networks
- Logical addressing (IPv4)
- Basic internetworking (IP, CIDR ARP, RARP, DHCP, ICMP)
- Routing, forwarding and delivery
- Static and dynamic routing
- Routing algorithms and protocols
- Congestion control algorithms
- IPv6.

References

Books:

1. Forouzen, "Data Communication and Networking",TMH

2. A.S. Tanenbaum, Computer Networks, Pearson Education

3. W. Stallings, Data and Computer Communication, MacmillanPress

Thank You