VIGNAN'S INSTITUTE OF MANAGEMENT AND TECHNOLOGY FOR WOMEN

[Sponsored by Lavu Educational Society]

(Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad.)

Kondapur (V), Ghatkesar (M), Medchal - Malkajgiri (D) - 501 301 Phone: +91 96529 10002/3

Accredited by NBA NATIONAL BOARD OF ACCREDITATION CSE & ECE

SAMPLE COURSE FILE

S. No	Description	Page No
1.	Department: Computer science and engineering Regulations:R-18 Year/Semster :III BTECH I sem Course: Computer Networks	2-191

Department of Computer Science and Engineering

INDEX

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal (Dt.) Malkajgiri Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Department of Computer Science and Engineering

	e.	Mid-2 question papers and results	
	f.	CO_PO mapping and attainment	
	g.	LECTURE NOTES	

1.

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

Department of Computer Science and Engineering

1. VISION , MISSION OF THE INSTITUTE & DEPARTMENT

Vision of the Institute

To empower female students with professional education using creative & innovative technical practices of global competence and research aptitude to become competitive engineers with ethical values and entrepreneurial skills.

Mission of the Institute

- To impart value based professional education through creative and innovative teaching-learning process to face the global challenges of the new era technology.
- To inculcate research aptitude and to bring out creativity in students by imparting engineering knowledge imbibing interpersonal skills to promote innovation, research and entrepreneurship.

Vision of the Department

To achieve value oriented and quality education with excellent standards on par with evolving technologies and produce technocrats of global standards with capabilities of facing futuristic challenges.

Mission of the Department

M1: To enrich advanced knowledge among students for reinforcing the domain knowledge and develop capabilities and skills to solve complex engineering problems.

M2: To impart value based professional education for a challenging career in Computer Science and Engineering.

M3: To transform the graduates for contributing to the socio-economic development and welfare of the society through value based education.

Vignan's Institute of Management & Technology for Women
Kondapur (V), Ghatkeser (M), Medchal, Malkajgiri (Dt.), Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Department of Computer Science and Engineering

2. PROGRAM EDUCATIONAL OBJECTIVES(PEO)

PEO1: To acquire logical and analytical skills in core areas of Computer Science & Information Technology.

PEO2: To adapt new technologies for the changing needs of IT industry through self-study, graduate work and professional development.

PEO3: To demonstrate professional and ethical attitude, soft skills, team spirit, leadership skills and execute assignments to the perfection.

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

3. PROGRAM OUTCOMES (POs)

1. **Engineering Knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. **Problem Analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. **Design/Development of Solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. **Conduct Investigations of Complex Problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. **Modern Tool Usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

6. **The Engineer and Society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. **Environment and Sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. **Individual and Team Work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend

and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. **Project Management and Finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

12. **Life-Long Learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

Department of Computer Science and Engineering

4.PROGRAM SPECIFIC OUTCOMES (PSO's):

PSO1: Software Development: Ability to grasp the software development life cycle of software systems and possess competent skills and knowledge of software design process.

PSO2: Industrial Skills Ability: Ability to interpret fundamental concepts and methodology of computer systems so that students can understand the functionality of hardware and software aspects of computer systems.

PSO3: Ethical and Social Responsibility: Communicate effectively in both verbal and written form, will have knowledge of professional and ethical responsibilities and will show the understanding of impact of engineering solutions on the society and also will be aware of contemporary issues.

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal, Malkajgiri (Dt.) Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

5.SYLLABUS-COPY:

III Year B.Tech. CSE I-Sem

L	T	P	C
3	0	0	3

Prerequisites

1. A course on "Programming for problem solving"
2. A course on "Data Structures"

Course Objectives

1. The objective of the course is to equip the students with a general overview of the concepts and fundamentals of computer networks.
2. Familiarize the students with the standard models for the layered approach to communication between machines in a network and the protocols of the various layers.

Course Outcomes

1. Gain the knowledge of the basic computer network technology.
2. Gain the knowledge of the functions of each layer in the OSI and TCP/IP reference model.
3. Obtain the skills of subnetting and routing mechanisms.
4. Familiarity with the essential protocols of computer networks, and how they can be applied in network design and implementation.

UNIT - I

Network hardware, Network software, OSI, TCP/IP Reference models, Example Networks: ARPANET, Internet.

Physical Layer: Guided Transmission media: twisted pairs, coaxial cable, fiber optics, Wireless transmission.

UNIT - II

Data link layer: Design issues, framing, Error detection and correction.

Elementary data link protocols: simplex protocol, A simplex stop and wait protocol for an error-free channel, A simplex stop and wait protocol for noisy channel.

Sliding Window protocols: A one-bit sliding window protocol, A protocol using Go-Back-N, A protocol using Selective Repeat, Example data link protocols.

Medium Access sub layer: The channel allocation problem, Multiple access protocols: ALOHA, Carrier sense multiple access protocols, collision free protocols. Wireless LANs, Data link layer switching.

UNIT – III

Network Layer: Design issues, Routing algorithms: shortest path routing, Flooding, Hierarchical routing, Broadcast, Multicast, distance vector routing, Congestion

Department of Computer Science and Engineering

Control Algorithms, Quality of Service, Internetworking, the Network layer in the internet.

UNIT – IV

Transport Layer: Transport Services, Elements of Transport protocols, Connection management, TCP and UDP protocols.

UNIT - V

Application Layer –Domain name system, SNMP, Electronic Mail; the World WEB, HTTP, Streaming audio and video.

TEXT BOOK:

1. Computer Networks -- Andrew S Tanenbaum, David. j. Wetherall, 5th Edition. Pearson Education/PHI

REFERENCE BOOKS:

1. An Engineering Approach to Computer Networks-S. Keshav, 2nd Edition, Pearson Education
2. Data Communications and Networking – Behrouz A. Forouzan. Third Edition TMH.

WEBSITES LINKS:

1. https://en.wikipedia.org/?title=Computer_network
2. http://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm
3. http://www.slackbook.org/html/basic-network-commands.html
4. http://www.computerhope.com/issues/ch000444.htm
5. http://www.howtogeek.com/168896/10-useful-windows-commands-you-should-know/

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal, Malkajgiri (Dt.) Pin-501301 (T.S.)

6.COURSE OBJECTIVES:

The main objectives of the course are:

- To introduce the Fundamentals of data computer networks
- To demonstrate the TCP/IP and OSI models with merits and demerits
- To demonstrate the Functions of various protocols of Data link layer.
- To demonstrate Functioning of various Routing protocols.
- To introduce the Functions of various Transport layer protocols TCP/UDP
- To understand the significance of application layer protocols
- To introduce the fundamental internet working prototocols.

7. COURSE OUTCOMES:

Course: COMPUTER NETWORKS
Course Code: CS503PC

Upon completion of the course the students get an idea of:

Course Code	**Course Outcomes**	**Blooms Taxonomy Levels**
CS503PC.1	Interpret the basics of Computer Networks and various protocols	BL 2
CS503PC.2	Generalize functionalities and services of each layer of OSI model.	BL 2
CS503PC.3	Explains the concept of data framing and error control mechanisms	BL 2
CS503PC.4	Compares Different routing and Transport protocols	BL 5
CS503PC.5	illustrate with world wide web concept	BL 3

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal (Dt.) Malkajgiri (Dt.) Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

8,INSTRUCTIONAL LEARNING OUTCOME:

UNIT I: NETWORK AND PHYSICAL LAYER

At the conclusion of this unit student should be able to:

1. Know the basics of Internet.
2. Describe the OSI and TCP IP reference models.
3. Compare both the models.
4. Describe Guided and Unguided transmission.

UNIT II: DATA LINK LAYER

At the conclusion of this unit student should be able to:

1. Know the basics of node to node communication.
2. Know the error detection and correction techniques(CRC)
3. Know the Go-Back-N,SR error detection protocol.
4. Gain the Knowledge of Channel allocation and collision protocols.
5. Gain the knowledge of WLAN and switching techniques

UNIT III: NETWORK LAYER

At the conclusion of this unit student should be able to:

1. Discuss elements of transport layer.
2. Explain routing algorithms of broadcast and multicast
3. Discuss Congestion control algorithms.
4. Discuss about QoS factors.
5. Know about internetworking consept.

UNIT IV: TRANSPORT LAYER

At the conclusion of this unit student should be able to:

1. Know anout element of transport layer
2. About Internet Transport Protocols UDP.

Vignan's Institute of Management Technology for Women ★ Kondapur (V), Ghatkesar (M), Medchal, Malkajgiri (D), Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

3. Explain TCP Service Model.
4. Know about congestion management

UNIT V: APPLICATION LAYER

At the conclusion of this unit student should be able to:

1. Application Layer services.
2. About client-server application.
3. Discuss HTTP, FTP, electronic mail, TELNET, DN

Department of Computer Science and Engineering

9.COURSE MAPPING WITH PEO'S AND PO & PSO:

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CS503PC.1	3	1								2		1	2	1	1
CS503PC.2	3	3								2		2	1	1	1
CS503PC.3	3	2	3							2		2	1	1	2
CS503PC.4	3	3	3	3						2		2	2	2	1
CS503PC.5	2	3	2	2						3		3	2	2	1
PO/PSO Average	2.8	2.4	1.6	1						2.2		2	1.6	1.4	1.2

14.UNIVERSITY QUESTION PAPERS OF PREVIOUS YEARS:

Code No: 135AE

R16

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year I Semester Examinations, November/December - 2018
DATA COMMUNICATION AND COMPUTER NETWORKS
(Common to CSE, IT)

Time: 3 hours

Max. Marks: 75

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART - A

(25 Marks)

1.a) List various components in a network. [2]
b) List and define different network topologies. [3]
c) Define bit stuffing and character stuffing. [2]
d) Briefly discuss about ALOHA. [3]
e) Why the class C is most commonly used Network class? [2]
f) Discuss how address mapping is performed. [3]
g) Mention Congestion Prevention Policies and how does it work. [2]
h) Flow control and Error control both are properties of Transport Layer and Data Link Layer. What you think is it duplicity of properties in both layer or is it ok? Comment. [3]
i) Define SNMP protocol. [2]
j) Discuss the properties of file transfer protocol. [3]

PART - B

(50 Marks)

2. With a neat diagram explain the OSI reference model in detail? Explain the functions performed in each layer. [10]

OR

3. What is multiplexing? Explain in detail about various types of multiplexing. [10]

4. Describe various error detection and correction technique. The generator polynomial is x^3+x+1. A sender want to send data 1001. Generate CRC code. Also describe error checking process if 3rd bit is inverted from the left. [10]

OR

5. What is high level data link control (HDLC)? Explain HDLC frame format in detail. [10]

6. What is classful addressing? Discuss class A, class B, class C, class D, class E address with its range in decimal dotted notation and example. [10]

OR

7. Give an example to explain any one of the multicasting routing algorithm. [10]

Vignan's Institute of Management & Technology for Women, Kondapur (V), Ghatkesar (M), Medchal, Malkajgiri (Dt.), Pin-501 301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For ...
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Department of Computer Science and Engineering

8. Discuss the transport layer service primitives. What do you understand by 3 way hand shake Technique? Also discuss the TCP connection management. [10]

OR

9. Compare and contrast between integrated services and Differential Services. [10]

10. Explain name – address and address – name resolution process. [10]

OR

11. Describe the various parts of e-mail address and show the process of sending and receiving e-mails. [10]

---ooOoo---

Department of Computer Science and Engineering

Code No: 115DT **R13**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year I Semester Examinations, November/December - 2017
COMPUTER NETWORKS
(Common to CSE, IT)

Time: 3 hours **Max. Marks: 75**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART - A

(25 Marks)

1.a) Write the advantages of optical fiber over twisted-pair and coaxial cables. [2]
b) What are the advantages of having layered architecture? [3]
c) Briefly explain the difference between switch and router. [2]
d) Sketch the Manchester encoding for the bit stream: 0001110101. [3]
e) Give the advantages of hierarchical routing. [2]
f) Differences between CO and CL. [3]
g) Explain DHCP. [2]
h) What are the functions of ICMP? [3]
i) What is the architecture of WWW? [2]
j) Explain the differences between POP3 and IMAP. [3]

PART - B

(50 Marks)

2.a) Compare and contrast the OSI and TCP/IP reference models.
b) What are the different types of error detection methods? Explain the CRC error detection technique using generator polynomial x^4+x^3+1 and data 11100011. [5+5]

OR

3.a) Discuss about the various transmission media available at the physical layer.
b) Explain about GBN Sliding Window Protocol. [5+5]

4.a) Explain the differences between the switching methods.
b) Elucidate the CSMA schemes. [5+5]

OR

5.a) Illustrate the frame structure of IEEE 802.3.
b) Give a detail note on the ALOHA protocols. [5+5]

6.a) Elucidate Distance Vector Routing Algorithm with example.
b) Describe the problem and solutions associated with distance vector routing. [5+5]

OR

7.a) Explain the general principles of congestion control.
b) Describe congestion control in datagram subnets. [5+5]

Department of Computer Science and Engineering

8.a) Elucidate the special IP addresses used in internet.
b) Discuss the significance and the operation of NAT. [5+5]

OR

9.a) Illustrate the connection establishment and release in transport layer.
b) How crash recovery is managed at the transport layer? [5+5]

10.a) Explain Real-time transport protocol.
b) When user clicks a hyperlink, what are the steps that occur between the user's click and the page being displayed? [5+5]

OR

11. Write short notes on the following: [10]
(a) MIME (b) Audio compression (c) DNS (d) Voice over IP.

---oo0oo---

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Department of Computer Science and Engineering

Code No: 125DT **R15**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
B. Tech III Year I Semester Examinations, May - 2018
COMPUTER NETWORKS
(Common to CSE, IT)

Time: 3 hours **Max. Marks: 75**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART - A

(25 Marks)

1.a) What is Internet. Differentiate it from intranet. [2]
b) Discuss the design issues of data link layer. [3]
c) When do we use hubs? [2]
d) What are main functionalities of routers? What is purpose of using multiprotocol routers? [3]
e) What is optimality principle? [2]
f) Discuss congestion control algorithms on brief. [3]
g) What is CIDR addressing [2]
h) Discuss the principles of internetworking. [3]
i) What is silly window syndrome? [2]
j) Draw TCP and UDP headers. [3]

PART - B

(50 Marks)

2. Compare and contrast OSI and TCP/IP reference models. Critique on each model. [10]

OR

3.a) Explain sliding window protocol.
b) Describe go back N protocol. [5+5]

4. Define collision. Explain collision free protocols. Mention advantage of each protocol. [10]

OR

5. Explain the following:
a) Bridges
b) Gateways
c) Repeaters. [10]

6.a) The major problem with distance vector routing algorithm is 'count to infinity'. How exchange complete path form router to destination instead of delay, helps in solving count to infinity problem.
b) Explain the design issues of network layer. [5+5]

OR

7. Discuss the hierarchical routing with examples. [10]

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Vignan's Institute of Management & Technology For Women
Kondapur, Ghatkesar (M), Malkajgiri (Dt.) Pin-501301

8. Given a network address of 192.168.100.0 and a subnet mask of 255.255.255.192.
   a) How many subnets are created?
   b) How many hosts are there per subnet? [5+5]

OR

9.a) Discuss ICMP Messages.
   b) Explain Tunneling in Internet layer. [5+5]

10. Illustrate the TCP connections, TCP releases with state transition diagram. [10]

OR

11. Describe DNS with diagrams and real-time examples. [10]

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Department of Computer Science and Engineering

15.UNIT-WISE QUESTION BANK MAPPING WITH BLOOMS TAXONOMY LEVELS AND COS

UNIT-WISE QUESTION BANK:

	Unit-1(Computer network Introduction)	**Blooms level**	**CO**
1	Give the different architecture of computer network	1	1
2	List different network hardware components	1	1
3	Compare bridge and routers	1	1
4	Define a) Bridge b)repeaters c)HUB d)routers	1	1
5	Explain categories /types of computer Networks.	1	1
6	Give the character /features of computer network	1	1
7	Give toplolgy oc computer networks	1	1
8	Give various data transmission mode	1	1
9	Give uses /application of computer network	1	1
10	what is network software? List various functions of software.	1	1
11	What is layered architecture? Give elements of layered architecture	1	1
12	Give important functions each layer in OSI reference model.	1	1
13	Difference between connection oriented and connectionless oriented services.	1	1
14	Compare OSi and TCP/IP reference models	1	1
15	Differentiate guided and un guided transmission media	1	1
	Long questions		
1	Explain different network hardware components in detail	2	1
2	Explain about a) Bridge b) Router c) Repeater d) HUB	2	1
3	Explain importance of software in network.	2	1
4	Explain OSI Reference model	2	1
5	Compare OSI and TCP/IP reference models	2	1
6	Explain various transmission modes	2	1
7	Explain applications of computer network.	2	1
8	Explain various topologies of computer network	2	1
9	Compare Twisted pair and coaxial cable transmission media	2	1
10	Compare guided and unguided transmission media	2	1
	unit-2 (Data link layer)		
1	What are the services /responsibilities of Data link layer or link layer	1	2
2	Give the design aspect of data link layer.	1	2
3	What are the DLL sub layers.	1	2
4	What are services provided by DLL layer to Network layer	1	2
5	What is framing ? list various framing methods.	1	2
6	Explain briefly is physical layer violation technique.	1	2
9	What is error detection and error correction	1	2
10	List various error detection techniques	1	2

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

Department of Computer Science and Engineering

11	Give algorithm of CRC error detection method.	1	2
12	Give different approaches to flow control	1	2
13	List various flow control protocols	1	2
14	List taxonomy of MAC protocols	1	2
15	Give the features of IEEE 802.11	1	2
	Long answers		
1.	Explain services provided by data link layer	2	2
2	What is framing ? explain different types of framing tecniques	2	2
3	Elicitate variuos services provided by DLL to network layer	2	2
4	What are the different types of error detection methods? Explain the CRC error detection technique using generator polynomial x4+x3+1 and data 11100011.	2	2
5	Explain Hamming code method of error detection and correction with example.	2	2
6	Explain CSMA and its versions	2	2
7	Compare CSMA/CD and CSMA/CA	2	2
8	List variuos collision free protocols .Explain a) Binary count down b) Adaptive tree walk protocols	2	2
9	Explain PCF and DCF in 802.11	2	2
10	Explain in detail 802.11standard.	2	2
	Unit-3-Network layer		
1	Explain shortest path routing algorithm with example	2	3
2	Compare adaptive and non-adaptive routing approach	2	3
3	Compare IPv4 and IPv6 formats.	2	3
4	Write note on tunnelling	2	3
5	Explain about IPv4 formats and addressing.	2	3
6	Explain distance vector routing methods.	2	3
	UNIT-4 Transport Layer		
1.	Give various services provided by transport layer.	2	4
2	Explain elements of transport layer	2	4
3	Explain characteristics factors of QoS	2	4
4	Explain crash recovery mechanism in transport layer	2	4
5	Compare TCP and UDP protocols	2	4
6	Describe in brief about TCP segment Header	2	4
7	Explain congestion control methods	2	4
8	Explain upward multiplexing and downward multiplexing	2	4
9	Explain in brief about TCP connection establishment and Release.	2	4
10	Describe in brief about TCP segment Header	5	4
11	Explain congestion control methods	2	4
12	Explain AIMD congestion control method	2	4
	UNIT-5: Application layer		
1	Explain working principle of domain name system.	2	5
2	Explain services provided by application layer	5	5
3	Explain Domain name system.	2	5

Department of Computer Science and Engineering

4	Describe video streaming Using a Media Server and RTSP	5	5
5	Explain working principle of domain name system.	2	5
6	Explain working of Email in detail	2	5

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

16. UNIT WISE QUIZ QUESTIONS (MCQS AND FILL IN THE BLANKS) WITH ANSWERS

UNIT-WISE QUIZ QUESTION

	UNIT-1	Answer
1	The physical path over which a message travels.	B
	A. Protocol B. Medium C. Signal D. All the above	
2	The information to be communicated in a data communications system is the	C
	A. Medium B. Protocol C. Message D. Transmission	
3	Frequency of failure and network recovery time after a failure are measures of the of a network.	B
	A. Performance B. Reliability C. Security D. Feasibility	
4	An unauthorized user is a network ________ issue.	C
	A.Performance B.Reliability C.Security D.All the above	
5	Which topology requires a central controller or hub?	B
	A. Mesh B. Star C. Bus D. Ring	
6	Which topology requires a multipoint connection?	B
	A. Mesh B. Bus C. Ring D. Star	
7	Communication between a computer and a keyboard involves ____________ transmission.	A
	A. simplex B.half-duplex C.full-duplex D.automatic	
8	Which organization has authority over interstate and international commerce in the communications field?	C
	A. ITU-T B.IEEE C.FCC D.ISOC	
9	are special-interest groups that quickly test, evaluate, and standardize new technologies	A
	A.Forums B.Regulatory agencies C.Standards organizations D.All of the above	
10	is the protocol suite for the current Internet.	A
	A.TCP/IP B.NCP C.UNIX D.ACM	
	FiLL in the Blanks	
1	In a ______ connection, two and only two devices are connected by a dedicated link.	Point-to-point
2	. ________ refers to the physical or logical arrangement of a network	Topology
3	In the original ARPANET, _______ were directly connected together.	IMPs
4	. ______ refers to the structure or format of the data, meaning the order in which they are presented.	syntax
5	A _______ is a data communication system within a building, plant, or campus, or between nearby buildings.	LAN
6	A ______ is a data communication system spanning states, countries, or the whole world.	WAN
7	. ____________ is a collection of many separate networks	Internet
8	____________ No of layers in ISO-OSI reference model	

Department of Computer Science and Engineering

9	_______ was the first network	ARPANET
10	Wireless technology refers to IEEE ________	802.11
	Answer Key:	
	UNIT-2(DLL)	
1	Data link control deals ______ communication	A
	A. node-to-node B. host-to-host C.process-to-process D.none of the above	
2	. In ______ There is no need of defining framing, boundaries of frames.	A
	A. fixed-size B. variable-size C. standard D.none of the above	
3	In____framing, we need a delimiter (flag) to define the boundary of two frames. n	B
	A. fixed-size B. variable-size C. standard D. none of the above	
4	In a ____________ protocol the data section of frame is sequence of	B
	A. byte-oriented B. bit-oriented C. either (a) or (b) D. None	
5	In____protocols, we use _____	A
	A.character-oriented; byte stuffing B. character-oriented; bit stuffing C. bit-oriented; character stuffing D.none of the above	
6	Bit stuffing means adding an extra 0 to the data section of the frame when ther is a sequence of bits with the same pattern as the	C
	A. header B. trailer C. flag D. none of the above	
7	control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment	A
	A. Flow B. Error C. Transmission D. none of the above	
8	The Simplest Protocol and the Stop-and-Wait Protocol are for channels	B
	A.noisy B. noiseless C. either (a) or (b) D. neither (a) nor (b)	
9	The Stop-And-W it ARQ, Go-Back-N ARQ, and the Selective Repeat ARQ are for channels	A
	A. noisy B. noiseless C. either (a) or (b) D. neither (a) nor (b)	
10	HDLC is an acronym for	B
	A. High-duplex line communication B. High-level data link control C. Half-duplex digit l link combination D. Host double-level circuit	
	Fill in the blanks	
1	In a Go-Back-N ARQ, if the window size is 63, _________ range sequence no.	0 to 63
2	Go-Back-N AR, if frames 4, 5, and 6 are received successfully, the receiver may send an ACK ________ to the sender.	7
3	ARQ stands for -------------	Automatic Repeat Request
4	For Stop-and-Wait ARQ, for 10 data packets sent,------acknowledgments are required	Exactly 10
5	In Selective Repeat ARQ, if 5 is the number of bits for the sequence number, then the maximum size of the send window must be -------	16
6	In Stop-and-Wait ARQ we use sequence numbers to number the frames. The sequence numbers are based on ------- arithmetic	Modulo-2
7	In _________, the station configuration is unbalanced we have one primary station and multiple secondary stations	NRM
8	In PPP, ________ is a three-way hand-shaking authentication protocol in which	CHAP

	the password is kept secrete it is never sent online	
9	HDLC stands for -----------------	High level data link control
10	In the -------- protocol we avoid unnecessary transmission by sending only frames that are corrupted	SR-ARQ
	UNIT-3(Network-layer)	
1	The IPv4 consists of	
	A. 4 B.8 C.32 D.64	C
2	Identify the class of the following IPv4 address :4.5.6.7	
	A.A B.B C.C D. none	A
3	What is the first address of a block of classless addresses if one of the addresses is 12.2.2.127/28?	C
	A.12.2.2.0 B.12.2.2.96 C.12.2.2.112 D. None	
4	In the forwarding full IP address of destination is given in the routing table	C
	A. next-hop B. network-specific C. host-specific D. default	
5	The use of hierarchy in routing table, what happens to its size	
	A.reduce B.increase C.both a and b D.none	A
6	What deals with the issue of creating and maintain routing table	
	A.Forwarding B.Routing C.DirectingD.None	B
7	Which routing table is updated periodically using one of the dynamic routing protocols	B
	A.static B.dynamic C.hierarchical D.None	
8	For the purpose of routing the internet is divided into	
	A.WAN B Autonomous network C Autonomous system D.None	C
9	Routing between autonomous systems is referred to as	
	A.inter domain routing B.intra domain routing C.both a and b D.none	A
10	In which routing least cost route between any two nodes is the route with minimum distance	B
	A.path vector B.distance vector C.link state D None	
	Fill in the Blanks	
1	The idea of address aggregation was designed to alleviate the increase in routing table entries when using-----------	Classless addressing
2	The principle of--------- states that routing table is sorted from longest mask to shortest mask	Longest mask matching
3	IPv4 header size--------------	20 to 60 byte long
4	-------- is necessary part of IPv6 datagram	Base header
5	nIPv6,the--------- field in the base header restrict the lifetime of the datagram	Hop limit
6	The -------- protocol is the transmission mechanism used by the TCP/IP	IP
7	In IPv6, options are inserted between the -------and -------data	Base header, upper layer data
8	IPv6 allows------security provision than IPv4	more
9	The sender is a router that has receive datagram destined for a host On another network .The logical address that is mapped to physical address is ---	IP address found in routing table
10	ICMP message is divided into two broad category------------	Query error

Department of Computer Science and Engineering

		reporting message
	UNIT-4	
1	One of responsibility of transport layer is	B
	A.Host-to-host B.process-to-processC.node-to-node D.None	
2.	UDP and TCP are which layer protocol	C
	A.data link B.network C.transport D.none	
3	Although there are several ways to achieve Process-to-process communication ,by which of the following way	A
	A.client-server B.client-client C.server-server D.none	
4	A port address in UDP is	B
	A.8 B.16 C.32 D.Any	
5	UDP packets are called	A
	A.user datagrams B.segments C.frames D.None	
6	What way we can avoid traffic congestion	A
	A.congestion control B.quality of service C.either (a) or (b) D.both (a) and (b)	
7	By which factor we can create appropriate environment for traffic	B
	A.congestion control B.quality of service C.either (a) or (b) D.both (a) and (b)	
8	What defines maximum data rate of the traffic	A
	A.peak data rate B Max.burst sie C.Effective band width D.None	
9	In which congestion control, policies applied to prevent congestion before it happens	A
	A.open-loop B.closed-loop C.either (a) or (b) D. Both (a) and (b)	
10	In which algorithm of TCP the size of the congestion window increases additively until congestion is detected	B
	A.slow-start B congestion avoidance C. congestion detection D.None	
	Fill in the blanks	
1	UDP is called ----------- transport protocol	Connectionless
2	UDP is acronym for ------------	unreliable
3	TCP groups a number of bytes together into a packet called -------	User datagram protocol
4	TCP is ---------- transport protocol	Segment
5	The communication in TCP is -----------	Connection oriented
6	The value of window size is determined by --------	Full duplex
7	A-------- traffic model has a data rate that does not change	Reciever
8	Congestion in network or inter network occurs because Routers and switches have---------	Constant bit rate
9	A---------- packet sent by a node to the source to inform it of congestion	queues
10	---------- is a flow characteristics that application can tolerate at different degree	Choke packet
	UNIT-5(application layer)	
1	FTP uses services of	

	A.UDP B.IP C.TCP D. None	
2	During an FTP session data connection opened	C
	A.exactly once B.exactly twice C many times D.None	
3	In DNS the names are defined in what structure	B
	A.a linear list B.an inverted-tree C.a graph D. none	
4	The root of DNS tree is---------	C
	A string of characters B.a string of 63 characters C.an empty string D.None	
5	In the Internet the domain name space (Tree) is divided into how many sections	A
	A.three B.two C.four D.none	
6	Which is not a application layer protocol?	D
	A. HTTP B SMTP C. FTP D. TCP	
7	Application layer offers which service.	A
	A.End to end B Process to process C. Both End to end and Process to process D. None of the mentioned	
8	E-mail is	C
	A. Loss-tolerant application B. Bandwidth-sensitive application C. Elastic application D. None of the mentioned	
9	Which of the following is used to contain an Internet standard?	A
	A.RFC B.IETF C. DNS D. PPP	
10	E) Which of the following protocols uses out-of-band signaling?	C
	A.HTTP B. SMTP C FTP D. All of the above	
	Fill-in the blanks	
1	The __________ translates internet domain and host names to IP address.	DNS
2	------------------ protocol delivers/stores mail to receiver server?	SMTP
3	When displaying a web page, the application layer uses the __________	HTTP
4	he packet of information at the application layer is called __________	message
5	Application layer offers ________ service.	End-to-end
6	Which DNS client maps an address to a name or a name to an address especially when required by a host?	Resolver
7	File transfer, access and management are handled by the------- layer	Application
8	Directory services handled by ---------- layer	Application
9	Email is service handled by ------------ layer	Application
10	During FTP session conections opens ---------- times	many

Vignan's Institute of Management & Technology For Women
Kondapur (M), Ghatkesar (M), Medchal (Dt) Malkajgiri (Dt) Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

17. REFERENCES, WEBSITES AND E-LINKS:

REFERENCES:

1 Data communication and Networks - Bhusan Trivedi, Oxford university press, 2016

2. Computer Networks -- Andrew S Tanenbaum, 4th Edition, Pearson Education

3. Understanding Communications and Networks, 3rd Edition, W. A. Shay, Cengage Learning.

WEBSITES

1. https://en.wikipedia.org/?title=Computer_network
2. http://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm
3. http://www.slackbook.org/html/basic-network-commands.html
4. http://www.computerhope.com/issues/ch000444.htm
5. http://www.howtogeek.com/168896/10-useful-windows-commands-you-should-know/

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal, Malkajgiri (Dt.), Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

CO-PO

ATTAINMENT

Vignan's Institute of Management & Technology For Women
Kondapur (V),
Ghatkesar (M),
Medchal
Malkajgiri (Dt.)
Pin-501301
(T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

VIGNAN'S INSTITUTE OF MANAGEMENT AND TECHNOLOGY FOR WOMEN

Sponsored by Lavu Educational Society, Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad.
Kondapur (V), Ghatkesar (M), Medchal - Malkajgiri (D) - 501 301 Phone: +91 96529 10002/3

Accredited by NBA
CSE & ECE

Department of Computer Science and Engineering

B.Tech Evaluation sheet

III Year I Semester I - Mid Examination November 2021
Computer Networks(CS503PC)

S. No	Q. No/Roll No	Descriptive [20]																Descriptive [10]	Objective [10]				Assignment [5]				Grand Total [25]	Total			Scaled to 10		
		1			2			3			4			CO1 [10]	CO2 [10]	CO3 [10]	Total [20]		CO1 [4]	CO2 [4]	CO3 [2]	Total [10]	CO1 [2]	CO2 [2]	CO3 [1]	Total [5]		CO1	CO2	CO3	CO1	CO2	CO3
		A	B	Total	A	B	Total	A	B	Total	A	B	Total															[16]	[16]	[13]	[10]	[10]	[10]
1	16UP1A05A9		6	6										6			6	3	4	3	2	9	2	2	1	5	17	12	5	3	7.5	8.33	10
2	18UP1A0542				6		6							6			6	3	4	3	2	9	2	2	1	5	17	12	5	3	7.5	8.33	10
3	19UP1A0501	3	3	6				6		6				6	6		12	6	4	3	2	9	2	2	1	5	20	12	11	3	7.5	6.88	10
4	19UP1A0502	4	4	8							8		8	8		8	16	8	3	3	2	8	2	2	1	5	21	13	5	11	8.13	8.33	8.46
5	19UP1A0503		4	4				4		4				4	4		8	4	4	3	2	9	2	2	1	5	18	10	9	3	6.25	5.63	10
6	19UP1A0504		5	5				5		5				5	5		10	5	4	4	2	10	2	2	1	5	20	11	11	3	6.88	6.88	10
7	19UP1A0505		5	5				4	4	8				5	8		13	7	4	2	2	8	2	2	1	5	20	11	12	3	6.88	7.5	10
8	19UP1A0506	4	4	8				4	4	8				8	8		16	8	4	4	2	10	2	2	1	5	23	14	14	3	8.75	8.75	10
9	19UP1A0507				9		9				9		9	9		9	18	9	4	4	2	10	2	2	1	5	24	15	6	12	9.38	10	9.23
10	19UP1A0508	5		5				5		5				5	5		10	5	4	4	2	10	2	2	1	5	20	11	11	3	6.88	6.88	10
11	19UP1A0509				6		6				6		6	6		6	12	6	4	4	2	10	2	2	1	5	21	12	6	9	7.5	10	6.92
12	19UP1A0510	5	4	9				5	4	9				9	9		18	9	4	4	2	10	2	2	1	5	24	15	15	3	9.38	9.38	10
13	19UP1A0511	5	4	9				5	4	9				9	9		18	9	4	3	2	9	2	2	1	5	23	15	14	3	9.38	8.75	10
14	19UP1A0512	5	4	9				4	5	9				9	9		18	9	4	3	2	9	2	2	1	5	23	15	14	3	9.38	8.75	10
15	19UP1A0513				5		5				5		5	5		5	10	5	4	3	2	9	2	2	1	5	19	11	5	8	6.88	8.33	6.15
16	19UP1A0514				7		7				7		7	7		7	14	7	4	3	2	9	2	2	1	5	21	13	5	10	8.13	8.33	7.69
17	19UP1A0515				6		6				6		6	6		6	12	6	4	3	2	9	2	2	1	5	20	12	5	9	7.5	8.33	6.92
18	19UP1A0516		5	5				5		5				5	5		10	5	3	3	2	8	2	2	1	5	18	10	10	3	6.25	6.25	10
19	19UP1A0517		3	3							3		3	3		3	6	3	3	3	2	8	2	2	1	5	16	8	5	6	5	8.33	4.62
20	19UP1A0518	5	4	9							9		9	9		9	18	9	3	4	2	9	2	2	1	5	23	14	6	12	8.75	10	9.23
21	19UP1A0519	4	4	8				4	4	8				8	8		16	8	3	4	2	9	2	2	1	5	22	13	14	3	8.13	8.75	10
22	19UP1A0520				6		6				6		6	6		6	12	6	4	4	2	10	2	2	1	5	21	12	6	9	7.5	10	6.92
23	19UP1A0521				10		10	10		10				10	10		20	10	4	4	2	10	2	2	1	5	25	16	16	3	10	10	10
24	19UP1A0522	4	4	8				5	3	8				8	8		16	8	4	4	2	10	2	2	1	5	23	14	14	3	8.75	8.75	10
25	19UP1A0523	3	2	5				5		5				5	5		10	5	4	3	2	9	2	2	1	5	19	11	10	3	6.88	6.25	10
26	19UP1A0524				5		5	5		5				5	5		10	5	4	4	2	10	2	2	1	5	20	11	11	3	6.88	6.88	10
27	19UP1A0525	4	4	8							8		8	8		8	16	8	4	4	2	10	2	2	1	5	23	14	6	11	8.75	10	8.46
28	19UP1A0526	4	5	9				9		9				9	9		18	9	4	4	2	10	2	2	1	5	24	15	15	3	9.38	9.38	10
29	19UP1A0527	3	2	5				5		5				5	5		10	5	4	4	2	10	2	2	1	5	20	11	11	3	6.88	6.88	10
30	19UP1A0528	4	5	9				9		9				9	9		18	9	4	4	2	10	2	2	1	5	24	15	15	3	9.38	9.38	10
31	19UP1A0529				9		9				9		9	9		9	18	9	4	4	2	10	2	2	1	5	24	15	6	12	9.38	10	9.23
32	19UP1A0530	4	4	8				3	5	8				8	8		16	8	4	3	2	9	2	2	1	5	22	14	13	3	8.75	8.13	10
33	19UP1A0531	4	3	7							7		7	7		7	14	7	4	3	2	9	2	2	1	5	21	13	5	10	8.13	8.33	7.69
34	19UP1A0532	3	2	5				5		5				5	5		10	5	4	3	2	9	2	2	1	5	19	11	10	3	6.88	6.25	10
35	19UP1A0533				10		10				10		10	10		10	20	10	4	3	2	9	2	2	1	5	24	16	5	13	10	8.33	10

Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)
Technology For Women

Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

36	19UP1A0534				10		10				10		10	10		10	20	10	4	4	2	10	2	2	1	5	25	16	6	13	10	10	10
37	19UP1A0535				4		4	4		4				4	4		8	4	4	4	2	10	2	2	1	5	19	10	10	3	6.25	6.25	10
38	19UP1A0536	4	4	8				4	4	8				8	8		16	8	4	4	2	10	2	2	1	5	23	14	14	3	8.75	8.75	10
39	19UP1A0537				4		4				4		4	4		4	8	4	1	3	2	6	2	2	1	5	15	7	5	7	4.38	8.33	5.38
40	19UP1A0538				2		2				2		2	2		2	4	2	0	0	2	2	2	2	1	5	9	4	2	5	2.5	3.33	3.85
41	19UP1A0539	4	4	8							8		8	8		8	16	8	0	1	2	3	2	2	1	5	16	10	3	11	6.25	5	8.46
42	19UP1A0540				7		7				7		7	7		7	14	7	4	4	2	10	2	2	1	5	22	13	6	10	8.13	10	7.69
43	19UP1A0541				7		7				7		7	7		7	14	7	4	4	2	10	2	2	1	5	22	13	6	10	8.13	10	7.69
44	19UP1A0542	3	4	7				5	2	7				7	7		14	7	2	4	2	8	2	2	1	5	20	11	13	3	6.88	8.13	10
45	19UP1A0543	3	4	7				7		7				7	7		14	7	4	4	2	10	2	2	1	5	22	13	13	3	8.13	8.13	10
46	19UP1A0544	3	3	6							6		6	6		6	12	6	3	4	2	9	2	2	1	5	20	11	6	9	6.88	10	6.92
47	19UP1A0545				9		9				9		9	9		9	18	9	4	4	2	10	2	2	1	5	24	15	6	12	9.38	10	9.23
48	19UP1A0546				10		10				10		10	10		10	20	10	4	2	2	8	2	2	1	5	23	16	4	13	10	6.67	10
49	19UP1A0547	3	3	6				6		6				6	6		12	6	4	4	2	10	2	2	1	5	21	12	12	3	7.5	7.5	10
50	19UP1A0548	2	4	6				6		6				6	6		12	6	4	4	2	10	2	2	1	5	21	12	12	3	7.5	7.5	10
51	19UP1A0549	3	4	7							7		7	7		7	14	7	4	4	2	10	2	2	1	5	22	13	6	10	8.13	10	7.69
52	19UP1A0550				9		9				9		9	9		9	18	9	2	4	2	8	2	2	1	5	22	13	6	12	8.13	10	9.23
53	19UP1A0551				5		5	4	1	5				5	5		10	5	4	1	2	7	2	2	1	5	17	11	8	3	6.88	5	10
54	19UP1A0552				8		8	4	4	8				8	8		16	8	3	4	2	9	2	2	1	5	22	13	14	3	8.13	8.75	10
55	19UP1A0553				5		5	3	2	5				5	5		10	5	3	4	2	9	2	2	1	5	19	10	11	3	6.25	6.88	10
56	19UP1A0554	3	3	6				2	4	6				6	6		12	6	3	4	2	9	2	2	1	5	20	11	12	3	6.88	7.5	10
57	19UP1A0555	3	2	5				3	2	5				5	5		10	5	2	4	2	8	2	2	1	5	18	9	11	3	5.63	6.88	10
58	19UP1A0556				9		9				4	5	9	9		9	18	9	4	1	2	7	2	2	1	5	21	15	3	12	9.38	5	9.23
59	19UP1A0557	2	2	4				2	2	4				4	4		8	4	4	2	2	8	2	2	1	5	17	10	8	3	6.25	5	10
60	19UP1A0558				7		7				3	4	7	7		7	14	7	4	4	2	10	2	2	1	5	22	13	6	10	8.13	10	7.69
61	19UP1A0559				8		8	4	4	8				8	8		16	8	3	3	2	8	2	2	1	5	21	13	13	3	8.13	8.13	10
62	19UP1A0560				8		8				4	4	8	8		8	16	8	4	4	2	10	2	2	1	5	23	14	6	11	8.75	10	8.46
63	19UP1A0561	3	2	5				4	1	5				5	5		10	5	3	0	2	5	2	2	1	5	15	10	7	3	6.25	4.38	10
64	19UP1A0562				6		6				3	3	6	6		6	12	6	4	4	1	9	2	2	1	5	20	12	6	8	7.5	10	6.15
65	19UP1A0563	4	4	8				8		8				8	8		16	8	4	4	1	9	2	2	1	5	22	14	14	2	8.75	8.75	6.67
66	19UP1A0564	4	3	7				7		7				7	7		14	7	4	4	1	9	2	2	1	5	21	13	13	2	8.13	8.13	6.67

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

Vignan's Institute [illegible] Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

67	19UP1A0565	5		5							5		5	5		5	10	5	0	0	2	2	2	2	1	5	12	7	2	8	4.38	3.33	6.15
68	19UP1A0566				5		5				5		5	5		5	10	5	4	4	2	10	2	2	1	5	20	11	6	8	6.88	10	6.15
69	19UP1A0567				9		9				4	5	9	9		9	18	9	4	4	2	10	2	2	1	5	24	15	6	12	9.38	10	9.23
70	19UP1A0568	3	2	5							5		5	5		5	10	5	4	3	0	7	2	2	1	5	17	11	5	6	6.88	8.33	4.62
71	19UP1A0569				7		7				4	3	7	7		7	14	7	4	4	0	8	2	2	1	5	20	13	6	8	8.13	10	6.15
72	19UP1A0570				7		7	4	3	7				7	7		14	7	4	0	1	5	2	2	1	5	17	13	9	2	8.13	5.63	6.67
73	19UP1A0571				9		9				5	4	9	9		9	18	9	4	4	0	8	2	2	1	5	22	15	6	10	9.38	10	7.69
74	19UP1A0572	3	2	5				3	2	5				5	5		10	5	4	0	2	6	2	2	1	5	16	11	7	3	6.88	4.38	10
75	19UP1A0573				5		5				3	2	5	5		5	10	5	4	3	2	9	2	2	1	5	19	11	5	8	6.88	8.33	6.15
76	19UP1A0574	4	4	8				5	3	8				8	8		16	8	4	4	2	10	2	2	1	5	23	14	14	3	8.75	8.75	10
77	19UP1A0575				5		5				2	3	5	5		5	10	5	1	2	2	5	2	2	1	5	15	8	4	8	5	6.67	6.15
78	19UP1A0576	4	2	6				4	2	6				6	6		12	6	4	4	1	9	2	2	1	5	20	12	12	2	7.5	7.5	6.67
79	19UP1A0577				5		5				5		5	5		5	10	5	4	4	1	9	2	2	1	5	19	11	6	7	6.88	10	5.38
80	19UP1A0578				5		5				5		5	5		5	10	5	4	4	2	10	2	2	1	5	20	11	6	8	6.88	10	6.15
81	19UP1A0579	3	4	7							4	3	7	7		7	14	7	4	4	1	9	2	2	1	5	21	13	6	9	8.13	10	6.92
82	19UP1A0580				8		8				4	4	8	8		8	16	8	1	2	2	5	2	2	1	5	18	11	4	11	6.88	6.67	8.46
83	19UP1A0581				7		7				3	4	7	7		7	14	7	3	4	2	9	2	2	1	5	21	12	6	10	7.5	10	7.69
84	19UP1A0582				6		6							6			6	3	3	3	2	8	2	2	1	5	16	11	5	3	6.88	8.33	10
85	19UP1A0583																		0	0	0	0	2	0	1	3	3	2	0	1	3.33	0	3.33
86	19UP1A0584				5		5	5		5				5	5		10	5	4	4	0	8	2	2	1	5	18	11	11	1	6.88	6.88	3.33
87	19UP1A0585				10		10				5	5	10	10		10	20	10	4	4	2	10	2	2	1	5	25	16	6	13	10	10	10
88	19UP1A0586				5		5	3	2	5				5	5		10	5	4	4	1	9	2	2	1	5	19	11	11	2	6.88	6.88	6.67
89	19UP1A0587				4		4	4		4				4	4		8	4	1	2	2	5	2	2	1	5	14	7	8	3	4.38	5	10
90	19UP1A0588				5		5	2	3	5				5	5		10	5	2	2	2	6	2	2	1	5	16	9	9	3	5.63	5.63	10
91	19UP1A0589	4	5	9							5	4	9	9		9	18	9	4	4	1	9	2	2	1	5	23	15	6	11	9.38	10	8.46
92	19UP1A0590				5		5				3	2	5	5		5	10	5	4	4	1	9	2	2	1	5	19	11	6	7	6.88	10	5.38
93	19UP1A0591				5		5	3	2	5				5	5		10	5	4	4	1	9	2	2	1	5	19	11	11	2	6.88	6.88	6.67
94	19UP1A0592	3	2	5				2	3	5				5	5		10	5	4	4	1	9	2	2	1	5	19	11	11	2	6.88	6.88	6.67
95	19UP1A0593				9		9				5	4	9	9		9	18	9	4	4	2	10	2	2	1	5	24	15	6	12	9.38	10	9.23
96	19UP1A0594				8		8				4	4	8	8		8	16	8	4	4	1	9	2	2	1	5	22	14	6	10	8.75	10	7.69
97	19UP1A0595				3		3	3		3				3	3		6	3	0	2	2	4	2	2	1	5	12	5	7	3	3.13	4.38	10
98	19UP1A0596				4		4	2	2	4				4	4		8	4	4	4	2	10	2	2	1	5	19	10	10	3	6.25	6.25	10
99	19UP1A0597	4	3	7							4	3	7	7		7	14	7	3	1	2	6	2	2	1	5	18	12	3	10	7.5	5	7.69
100	19UP1A0598	5	4	9				4	5	9				9	9		18	9	4	4	2	10	2	2	1	5	24	15	15	3	9.38	9.38	10
101	19UP1A0599	2	4	6				3	3	6				6	6		12	6	3	4	2	9	2	2	1	5	20	11	12	3	6.88	7.5	10
102	19UP1A05A0				8		8	4	4	8				8	8		16	8	4	4	2	10	2	2	1	5	23	14	14	3	8.75	8.75	10
103	19UP1A05A1				4		4				1	3	4	4		4	8	4	2	2	2	6	2	2	1	5	15	8	4	7	5	6.67	5.38
104	19UP1A05A2				5		5				4	1	5	5		5	10	5	4	4	2	10	2	2	1	5	20	11	6	8	6.88	10	6.15
															Average																7.52	7.97	8.46

Faculty

HOD

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

PRINCIPAL

Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Department of Computer Science and Engineering

B.Tech Evaluation sheet

IV Year I Semester II - Mid Examination <Month Year>

Computer Network(CS503PC)

Section - CSE -A & B

S. No	Q. No/Roll No	Descriptive [20]																Descriptive [10]	Objective [10]				Assignment [5]				Grand Total [25]	Total			Scaled to 10		
		1			2			3			4			CO3 [10]	CO4 [10]	CO5 [10]	Total [20]		CO3 [2]	CO4 [4]	CO5 [4]	Total [10]	CO3 [1]	CO4 [2]	CO5 [2]	Total [5]		CO3	CO4	CO5	CO3	CO4	CO5
		A	B	Total	A	B	Total	A	B	Total	A	B	Total															[13]	[16]	[16]	[10]	[10]	[10]
1	16UP1A05A9							3	1	4						4	4	2	1	4	4	9	1	2	2	5	16	2	6	10	6.67	10	6.25
2	18UP1A0542				6		6		4	4					6	4	10	5	2	4	4	10	1	2	2	5	20	3	12	10	10	7.5	6.25
3	19UP1A0501	4		4							4	4	8	4		8	12	6	2	4	4	10	1	2	2	5	21	7	6	14	5.38	10	8.75
4	19UP1A0502	4		4							5	5	10	4		10	14	7	2	4	4	10	1	2	2	5	22	7	6	16	5.38	10	10
5	19UP1A0503				10		10								10		10	5	2	4	4	10	1	2	2	5	20	3	16	6	10	10	10
6	19UP1A0504				10		10				1	3	4		10	4	14	7	2	4	4	10	1	2	2	5	22	3	16	10	10	10	6.25
7	19UP1A0505	3	5	8							5	5	10	8		10	18	9	2	4	4	10	1	2	2	5	24	11	6	16	8.46	10	10
8	19UP1A0506	3	5	8							5	3	8	8		8	16	8	2	4	4	10	1	2	2	5	23	11	6	14	8.46	10	8.75
9	19UP1A0507				9		9				5	4	9		9	9	18	9	2	4	4	10	1	2	2	5	24	3	15	15	10	9.38	9.38
10	19UP1A0508				10		10				5		5		10	5	15	8	2	4	4	10	1	2	2	5	23	3	16	11	10	10	6.88
11	19UP1A0509	4		4				4		4				4		4	8	4	2	4	4	10	1	2	2	5	19	7	6	10	5.38	10	6.25
12	19UP1A0510				7		7				5	5	10		7	10	17	9	2	4	4	10	1	2	2	5	24	3	13	16	10	8.13	10
13	19UP1A0511				9		9				4	3	7		9	7	16	8	2	4	4	10	1	2	2	5	23	3	15	13	10	9.38	8.13
14	19UP1A0512				10		10				3	3	6		10	6	16	8	2	4	4	10	1	2	2	5	23	3	16	12	10	10	7.5
15	19UP1A0513				10		10				5		5		10	5	15	8	2	4	4	10	1	2	2	5	23	3	16	11	10	10	6.88
16	19UP1A0514				10		10		4	4	3	3	6		10	6	16	8	2	4	4	10	1	2	2	5	23	3	16	12	10	10	7.5
17	19UP1A0515				8		8					4	4		8	4	12	6	2	4	4	10	1	2	2	5	21	3	14	10	10	8.75	6.25
18	19UP1A0516				8		8								8		8	4	2	4	4	10	1	2	2	5	19	3	14	6	10	8.75	10
19	19UP1A0517				8		8				3		3		8	3	11	6	2	4	4	10	1	2	2	5	21	3	14	9	10	8.75	5.63
20	19UP1A0518				9		9				3	5	8		9	8	17	9	2	4	4	10	1	2	2	5	24	3	15	14	10	9.38	8.75
21	19UP1A0519				10		10				4	1	5		10	5	15	8	2	4	4	10	1	2	2	5	23	3	16	11	10	10	6.88
22	19UP1A0520	4	4	8				3		3				8		3	11	6	2	4	4	10	1	2	2	5	21	11	6	9	8.46	10	5.63
23	19UP1A0521	1		1	10		10							1	10		10	5	1	4	4	9	1	2	2	5	19	3	16	6	2.31	10	10
24	19UP1A0522	4		4	7		7	5	3	8				4	7	8	15	8	2	4	4	10	1	2	2	5	23	7	13	14	5.38	8.13	8.75
25	19UP1A0523		2	2	6		6							2	6		6	3	2	4	4	10	1	2	2	5	18	5	12	6	3.85	7.5	10
26	19UP1A0524				8		8				4	1	5		8	5	13	7	2	4	4	10	1	2	2	5	22	3	14	11	10	8.75	6.88
27	19UP1A0525				9		9				4.	4	8		9	8	17	9	2	4	4	10	1	2	2	5	24	3	15	14	10	9.38	8.75
28	19UP1A0526	4	1	5							5	5	10	5		10	15	8	2	4	4	10	1	2	2	5	23	8	6	16	6.15	10	10
29	19UP1A0527	5	5	10				3	1	4				10		4	14	7	2	4	4	10	1	2	2	5	22	13	6	10	10	10	6.25
30	19UP1A0528	4	5	9							5	4	9	9		9	18	9	2	4	4	10	1	2	2	5	24	12	6	15	9.23	10	9.38
31	19UP1A0529	3	5	8							5	3	8	8		8	16	8	2	4	4	10	1	2	2	5	23	11	6	14	8.46	10	8.75
32	19UP1A0530	1		1							5	5	10	1		10	11	6	2	4	4	10	[illegible]	2	2	5	21	4	6	16	3.08	10	10
33	19UP1A0531	4	5	9	3		3							9	3		9	5	2	4	4	10	1	[illegible]	2	5	20	12	9	6	9.23	5.63	10
34	19UP1A0532				9		9	4	1	5					9	5	14	7	2	4	4	10	1	2	2	5	22	3	15	11	10	9.38	6.88
35	19UP1A0533				8		8	5	5	10					8	10	18	9	2	4	4	10	[illegible]	2	2	5	24	3	14	16	10	8.75	10

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

36	19UP1A0534	4	4	8				4	4	8				8		8	16	8	2	4	4	10	1	2	2	5	23	11	6	14	8.46	10	8.75
37	19UP1A0535				10		10				5		5		10	5	15	8	1	4	4	9	1	2	2	5	22	2	16	11	6.67	10	6.88
38	19UP1A0536	4	4	8				5	5	10				8		10	18	9	2	4	4	10	1	2	2	5	24	11	6	16	8.46	10	10
39	19UP1A0537				10		10				3	3	6		10	6	16	8	2	4	2	8	1	2	2	5	21	3	16	10	10	10	6.25
40	19UP1A0538	4	3	7				3		3				7		3	10	5	2	4	3	9	1	2	2	5	19	10	6	8	7.69	10	5
41	19UP1A0539	5	5	10							5	4	9	10		9	19	10	2	3	4	9	1	2	2	5	24	13	5	15	10	8.33	9.38
42	19UP1A0540							5	5	10	5		5			10	10	5	2	3	4	9	1	2	2	5	19	3	5	16	10	8.33	10
43	19UP1A0541				7		7	4	4	8					7	8	15	8	2	4	4	10	1	2	2	5	23	3	13	14	10	8.13	8.75
44	19UP1A0542	4	4	8							4	4	8	8		8	16	8	2	4	3	9	1	2	2	5	22	11	6	13	8.46	10	8.13
45	19UP1A0543	5	5	10							4	4	8	10		8	18	9	2	3	4	9	1	2	2	5	23	13	5	14	10	8.33	8.75
46	19UP1A0544	3		3							4	4	8	3		8	11	6	2	4	4	10	1	2	2	5	21	6	6	14	4.62	10	8.75
47	19UP1A0545				8		8				5	5	10		8	10	18	9	2	4	4	10	1	2	2	5	24	3	14	16	10	8.75	10
48	19UP1A0546	4	5	9				4	3	7				9		7	16	8	2	4	4	10	1	2	2	5	23	12	6	13	9.23	10	8.13
49	19UP1A0547				6		6				5	5	10		6	10	16	8	2	4	4	10	1	2	2	5	23	3	12	16	10	7.5	10
50	19UP1A0548				8		8				4	1	5		8	5	13	7	2	4	4	10	1	2	2	5	22	3	14	11	10	8.75	6.88
51	19UP1A0549				10		10					3	3		10	3	13	7	2	4	4	10	1	2	2	5	22	3	16	9	10	10	5.63
52	19UP1A0550				10		10				5		5		10	5	15	8	2	4	4	10	1	2	2	5	23	3	16	11	10	10	6.88
53	19UP1A0551				10		10				5		5		10	5	15	8	2	4	3	9	1	2	2	5	22	3	16	10	10	10	6.25
54	19UP1A0552				10		10				4	4	8		10	8	18	9	2	4	4	10	1	2	2	5	24	3	16	14	10	10	8.75
55	19UP1A0553	5	5	10				5		5				10		5	15	8	2	4	4	10	1	2	2	5	23	13	6	11	10	10	6.88
56	19UP1A0554				10		10				4	4	8		10	8	18	9	2	4	3	9	1	2	2	5	23	3	16	13	10	10	8.13
57	19UP1A0555				10		10	1	2	3					10	3	13	7	2	4	4	10	1	2	2	5	22	3	16	9	10	10	5.63
58	19UP1A0556				10		10	5	2	7					10	7	17	9	2	4	4	10	1	2	2	5	24	3	16	13	10	10	8.13
59	19UP1A0557	4	3	7							5	4	9	7		9	16	8	2	4	4	10	1	2	2	5	23	10	6	15	7.69	10	9.38
60	19UP1A0558				10		10				4	4	8		10	8	18	9	2	4	3	9	1	2	2	5	23	3	16	13	10	10	8.13
61	19UP1A0559				8		8				5	5	10		8	10	18	9	2	3	4	9	1	2	2	5	23	3	13	16	10	8.13	10
62	19UP1A0560				8		8				5	5	10		8	10	18	9	2	4	4	10	1	2	2	5	24	3	14	16	10	8.75	10
63	19UP1A0561	5	5	10					5	5				10		5	15	8	2	4	3	9	1	2	2	5	22	13	6	10	10	10	6.25
64	19UP1A0562				10		10				4	4	8		10	8	18	9	1	4	4	9	1	2	2	5	23	2	16	14	6.67	10	8.75
65	19UP1A0563				10		10				3	3	6		10	6	16	8	2	4	4	10	1	2	2	5	23	3	16	12	10	10	7.5
66	19UP1A0564	3	5	8				5	5	10				8		10	18	9	2	4	4	10	1	2	2	5	24	11	6	16	8.46	10	10

Vignan's Institute of Management & Technology for Women Kondapur (V) Ghatkesar (M) Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V), Ghatkesar(M), Medchal-Malkajgiri(Dt)-501301
Telangana State

67	19UP1A0565				10		10	5		5					10	5	15	8	2	3	4	9	1	2	2	5	22	3	15	11	10	9.38	6.88
68	19UP1A0566	5	3	8	8		8				5	5	10	8	8	10	18	9	2	4	4	10	1	2	2	5	24	11	14	16	8.46	8.75	10
69	19UP1A0567	5	5	10				5	3	8				10		8	18	9	2	4	4	10	1	2	2	5	24	13	6	14	10	10	8.75
70	19UP1A0568				10		10	5		5					10	5	15	8	2	4	4	10	1	2	2	5	23	3	16	11	10	10	6.88
71	19UP1A0569				10		10				3	3	6		10	6	16	8	2	4	4	10	1	2	2	5	23	3	16	12	10	10	7.5
72	19UP1A0570	5	5	10				4	4	8				10		8	18	9	1	4	4	9	1	2	2	5	23	12	6	14	9.23	10	8.75
73	19UP1A0571	5		5	8		8				5	5	10	5	8	10	18	9	2	4	4	10	1	2	2	5	24	8	14	16	6.15	8.75	10
74	19UP1A0572				10		10					5	5		10	5	15	8	2	4	4	10	1	2	2	5	23	3	16	11	10	10	6.88
75	19UP1A0573				7		7	5	5	10					7	10	17	9	2	4	4	10	1	2	2	5	24	3	13	16	10	8.13	10
76	19UP1A0574	3	5	8							5	3	8	8		8	16	8	2	4	4	10	1	2	2	5	23	11	6	14	8.46	10	8.75
77	19UP1A0575				7		7				5	5	10		7	10	17	9	2	4	4	10	1	2	2	5	24	3	13	16	10	8.13	10
78	19UP1A0576				10		10					5	5		10	5	15	8	2	4	4	10	1	2	2	5	23	3	16	11	10	10	6.88
79	19UP1A0577				10		10	5		5					10	5	15	8	2	4	4	10	1	2	2	5	23	3	16	11	10	10	6.88
80	19UP1A0578	5	5	10							4		4	10		4	14	7	2	4	4	10	1	2	2	5	22	13	6	10	10	10	6.25
81	19UP1A0579	5	4	9	9		9				5	4	9	9	9	9	18	9	2	4	4	10	1	2	2	5	24	12	15	15	9.23	9.38	9.38
82	19UP1A0580				8		8				4	3	7		8	7	15	8	2	4	4	10	1	2	2	5	23	3	14	13	10	8.75	8.13
83	19UP1A0581	5		5	9		9	4	5	9				5	9	9	18	9	2	4	4	10	1	2	2	5	24	8	15	15	6.15	9.38	9.38
84	19UP1A0582	5		5							5		5	5		5	10	5	2	4	4	10	1	2	2	5	20	8	6	11	6.15	10	6.88
85	19UP1A0583																		0	0	0	0					0	0	0	0	0	0	0
86	19UP1A0584				10		10								10		10	5	2	4	4	10	1	2	2	5	20	3	16	6	10	10	10
87	19UP1A0585	4	5	9							5	4	9	9		9	18	9	2	4	4	10	1	2	2	5	24	12	6	15	9.23	10	9.38
88	19UP1A0586				10		10	3	3	6					10	6	16	8	2	4	4	10	1	2	2	5	23	3	16	12	10	10	7.5
89	19UP1A0587				10		10					2	2		10	2	12	6	2	4	4	10	1	2	2	5	21	3	16	8	10	10	5
90	19UP1A0588	5	5	10							5	3	8	10		8	18	9	2	4	4	10	1	2	2	5	24	13	6	14	10	10	8.75
91	19UP1A0589				10		10				5	5	10		10	10	20	10	2	4	4	10	1	2	2	5	25	3	16	16	10	10	10
92	19UP1A0590	2		2	6		6				5	5	10	2	6	10	16	8	2	4	4	10	1	2	2	5	23	5	12	16	3.85	7.5	10
93	19UP1A0591				10		10								10		10	5	2	4	4	10	1	2	2	5	20	3	16	6	10	10	10
94	19UP1A0592				10		10				5	3	8		10	8	18	9	2	4	4	10	1	2	2	5	24	3	16	14	10	10	8.75
95	19UP1A0593				10		10	3	3	6					10	6	16	8	2	4	4	10	1	2	2	5	23	3	16	12	10	10	7.5
96	19UP1A0594				10		10				5	3	8		10	8	18	9	2	4	4	10	1	2	2	5	24	3	16	14	10	10	8.75
97	19UP1A0595	2	5	7				5		5				7		5	12	6	2	4	4	10	1	2	2	5	21	10	6	11	7.69	10	6.88
98	19UP1A0596				10		10				5	2	7		10	7	17	9	2	4	4	10	1	2	2	5	24	3	16	13	10	10	8.13
99	19UP1A0597		5	5					4	4				5		4	9	5	2	1	4	7	1	2	2	5	17	8	3	10	6.15	5	6.25
100	19UP1A0598				10		10				4	3	7		10	7	17	9	2	4	4	10	1	2	2	5	24	3	16	13	10	10	8.13
101	19UP1A0599		5	5				4		4				5		4	9	5	2	4	4	10	1	2	2	5	20	8	6	10	6.15	10	6.25
102	19UP1A05A0				10		10				4	4	8		10	8	18	9	2	4	4	10	1	2	2	5	24	3	16	14	10	10	8.75
103	19UP1A05A1				10		10					3	3		10	3	13	7	2	4	4	10	1	2	2	5	22	3	16	9	10	10	5.63
104	19UP1A05A2	5		5	10		10	4		4				5	10	4	14	7	2	4	4	10	1	2	2	5	22	8	16	10	6.15	10	6.25
															Average																8.80	9.38	8.07

Faculty

HOD

Head of the Department
Computer Science and Engineering
Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal-Malkajgiri (D)

Vignan's Institute of Management & Technology For Women
Kondapur (V) Ghatkesar (M) Medchal Malkajgiri (Dt)

PRINCIPAL

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V), Ghatkesar(M), Medchal-Malkajgiri(Dt)-501301
Telangana State

VIGNAN'S IN TI UTE OF MANAGE IE IT AND TECHNOLOGY FOR WOMEN

Sponsored by Lavu Educational Society, Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad.
Kondapur (V), Ghatkesar (M), Medchal - Malkajgiri (D) - 501 301 Phone: +91 96529 10002/3

Accredited By NBA CSE & ECE

Department of Computer Science and Engineering

Name of the Course:Computer Networks | Subject Code: CS503PC | Year of Study: 2021-22

SN	Roll no	Marks Obtained in Internal Assessments								External Exams Marks [75]	Total Marks [100]	Attainment Level	Achieved or not
		CO1	CO2	CO3	CO4	CO5	Total Marks For the Course	Total Internal Evaluation (50M)	Normalized to 25M				
1	16UP1A05A9	5.63	8.33	13.335	10	6.25	33	43.545	17	13	30	0	N
2	18UP1A0542	5.63	8.33	15	7.5	6.25	37	42.71	19	27	46	1	Y
3	19UP1A0501	5.63	6.88	12.69	10	8.75	41	43.95	21	32	53	2	Y
4	19UP1A0502	6.88	8.33	7.69	10	10	43	42.9	22	41	63	3	Y
5	19UP1A0503	4.38	5.63	15	10	10	38	45.01	19	34	53	2	Y
6	19UP1A0504	5	6.88	15	10	6.25	42	43.13	21	43	64	3	Y
7	19UP1A0505	5	7.5	14.23	10	10	44	46.73	22	42	64	3	Y
8	19UP1A0506	6.88	8.75	14.23	10	8.75	46	48.61	23	37	60	2	Y
9	19UP1A0507	7.5	10	10.77	9.38	9.38	48	47.03	24	50	74	3	Y
10	19UP1A0508	5	6.88	15	10	6.88	43	43.76	22	49	71	3	Y
11	19UP1A0509	5.63	10	7.305	10	6.25	40	39.185	20	30	50	1	Y
12	19UP1A0510	7.5	9.38	15	8.13	10	48	50.01	24	34	58	2	Y
13	19UP1A0511	7.5	8.75	15	9.38	8.13	46	48.76	23	37	60	2	Y
14	19UP1A0512	7.5	8.75	15	10	7.5	46	48.75	23	32	55	2	Y
15	19UP1A0513	5	8.33	9.23	10	6.88	42	39.44	21	30	51	2	Y
16	19UP1A0514	6.25	8.33	10	10	7.5	44	42.08	22	27	49	1	Y
17	19UP1A0515	5.63	8.33	9.615	8.75	6.25	41	38.575	21	27	48	1	Y
18	19UP1A0516	5	6.25	13.335	8.75	10	37	43.335	19	28	47	1	Y
19	19UP1A0517	3.75	8.33	8.075	8.75	5.63	37	34.535	19	29	48	1	Y
20	19UP1A0518	7.5	10	10.385	9.38	8.75	47	46.015	24	31	55	2	Y
21	19UP1A0519	6.88	8.75	13.335	10	6.88	45	45.845	23	30	53	2	Y
22	19UP1A0520	5.63	10	8.845	10	5.63	42	40.105	21	27	48	1	Y
23	19UP1A0521	8.13	10	11.155	10	10	44	49.285	22	32	54	2	Y
24	19UP1A0522	6.88	8.75	12.69	8.13	8.75	46	45.2	23	32	55	2	Y
25	19UP1A0523	5	6.25	11.925	7.5	10	37	40.675	19	9	28	0	N
26	19UP1A0524	5	6.88	15	8.75	6.88	42	42.51	21	26	47	1	Y
27	19UP1A0525	6.88	10	10.385	9.38	8.75	47	45.395	24	32	56	2	Y
28	19UP1A0526	7.5	9.38	13.075	10	10	47	49.955	24	36	60	2	Y
29	19UP1A0527	5	6.88	15	10	6.25	42	43.13	21	33	54	2	Y
30	19UP1A0528	7.5	9.38	14.615	10	9.38	48	50.875	24	40	64	3	Y
31	19UP1A0529	7.5	10	10	10	8.75	47	46.25	24	31	55	2	Y
32	19UP1A0530	6.88	8.13	11.54	10	10	43	46.55	22	29	51	2	Y
33	19UP1A0531	6.25	8.33	9.615	5.63	10	41	39.825	21	27	48	1	Y
34	19UP1A0532	5	6.25	15	9.38	6.88	41	42.51	21	37	58	2	Y
35	19UP1A0533	8.13	8.33	11.155	8.75	10	48	46.365	24	32	56	2	Y

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal, Malkajgiri (Dt.), Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

36	19UP1A0534	8.13	10	10.385	10	8.75	48	47.265	24	41	65	3	Y
37	19UP1A0535	4.38	6.25	13.335	10	6.88	41	40.845	21	26	47	1	Y
38	19UP1A0536	6.88	8.75	14.23	10	10	47	49.86	24	35	59	2	Y
39	19UP1A0537	4.38	8.33	7.69	10	6.25	36	36.65	18	36	54	2	Y
40	19UP1A0538	3.13	3.33	5.385	10	5	28	26.845	14	3	17	0	N
41	19UP1A0539	6.88	5	8.845	8.33	9.38	40	38.435	20	42	62	3	Y
42	19UP1A0540	6.25	10	10	8.33	10	41	44.58	21	28	49	1	Y
43	19UP1A0541	6.25	10	10	8.13	8.75	45	43.13	23	30	53	2	Y
44	19UP1A0542	6.25	8.13	10.895	10	8.13	42	43.405	21	28	49	1	Y
45	19UP1A0543	6.25	8.13	15	8.33	8.75	45	46.46	23	42	65	3	Y
46	19UP1A0544	5.63	10	6.54	10	8.75	41	40.92	21	29	50	1	Y
47	19UP1A0545	7.5	10	10.77	8.75	10	48	47.02	24	42	66	3	Y
48	19UP1A0546	8.13	6.67	10.77	10	8.13	46	43.7	23	46	69	3	Y
49	19UP1A0547	5.63	7.5	15	7.5	10	44	45.63	22	27	49	1	Y
50	19UP1A0548	5.63	7.5	15	8.75	6.88	43	43.76	22	30	52	2	Y
51	19UP1A0549	6.25	10	10	10	5.63	44	41.88	22	27	49	1	Y
52	19UP1A0550	7.5	10	10	10	6.88	45	44.38	23	36	59	2	Y
53	19UP1A0551	5	5	15	10	6.25	39	41.25	20	27	47	1	Y
54	19UP1A0552	6.88	8.75	13.335	10	8.75	46	47.715	23	31	54	2	Y
55	19UP1A0553	5	6.88	13.335	10	6.88	42	42.095	21	41	62	3	Y
56	19UP1A0554	5.63	7.5	13.335	10	8.13	43	44.595	22	32	54	2	Y
57	19UP1A0555	5	6.88	11.665	10	5.63	40	39.175	20	33	53	2	Y
58	19UP1A0556	7.5	5	10.77	10	8.13	45	41.4	23	38	61	3	Y
59	19UP1A0557	4.38	5	13.845	10	9.38	40	42.605	20	38	58	2	Y
60	19UP1A0558	6.25	10	10	10	8.13	45	44.38	23	35	58	2	Y
61	19UP1A0559	6.88	8.13	13.335	8.13	10	44	46.475	22	36	58	2	Y
62	19UP1A0560	6.88	10	10.385	8.75	10	47	46.015	24	34	58	2	Y
63	19UP1A0561	5	4.38	13.335	10	6.25	37	38.965	19	32	51	2	Y
64	19UP1A0562	5	10	7.95	10	8.75	43	41.7	22	37	59	2	Y
65	19UP1A0563	6.25	8.75	15	10	7.5	45	47.5	23	41	64	3	Y
66	19UP1A0564	5.63	8.13	14.23	10	10	45	47.99	23	34	57	2	Y

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

67	19UP1A0565	5	3.33	7.69	9.38	6.88	34	32.28	17	34	51	2	Y
68	19UP1A0566	5	10	8.46	8.75	10	44	42.21	22	36	58	2	Y
69	19UP1A0567	7.5	10	10.77	10	8.75	48	47.02	24	48	72	3	Y
70	19UP1A0568	3.75	8.33	9.23	10	6.88	40	38.19	20	41	61	3	Y
71	19UP1A0569	5	10	10	10	7.5	43	42.5	22	47	69	3	Y
72	19UP1A0570	5.63	5.63	14.615	10	8.75	40	44.625	20	44	64	3	Y
73	19UP1A0571	6.25	10	8.845	8.75	10	46	43.845	23	46	69	3	Y
74	19UP1A0572	5	4.38	15	10	6.88	39	41.26	20	34	54	2	Y
75	19UP1A0573	5	8.33	9.23	8.13	10	43	40.69	22	38	60	2	Y
76	19UP1A0574	6.88	8.75	14.23	10	8.75	46	48.61	23	30	53	2	Y
77	19UP1A0575	5	6.67	8.075	8.13	10	39	37.875	20	42	62	3	Y
78	19UP1A0576	5	7.5	15	10	6.88	43	44.38	22	44	66	3	Y
79	19UP1A0577	4.38	10	9.23	10	6.88	42	40.49	21	37	58	2	Y
80	19UP1A0578	5	10	9.23	10	6.25	42	40.48	21	26	47	1	Y
81	19UP1A0579	5.63	10	9.615	9.38	9.38	45	44.005	23	41	64	3	Y
82	19UP1A0580	6.88	6.67	9.23	8.75	8.13	41	39.66	21	45	66	3	Y
83	19UP1A0581	6.25	10	7.69	9.38	9.38	45	42.7	23	53	76	3	Y
84	19UP1A0582	5.63	8.33	11.41	10	6.88	36	42.25	18	37	55	2	Y
85	19UP1A0583	0	0	0	0	0	0	0	0	0	0	0	0
86	19UP1A0584	3.75	6.88	15	10	10	38	45.63	19	41	60	2	Y
87	19UP1A0585	8.13	10	10.77	10	9.38	49	48.28	25	47	72	3	Y
88	19UP1A0586	4.38	6.88	15	10	7.5	42	43.76	21	43	64	3	Y
89	19UP1A0587	4.38	5	10	10	5	35	34.38	18	16	34	0	N
90	19UP1A0588	5	5.63	11.665	10	8.75	40	41.045	20	35	55	2	Y
91	19UP1A0589	6.88	10	10.77	10	10	48	47.65	24	52	76	3	Y
92	19UP1A0590	4.38	10	6.155	7.5	10	42	38.035	21	42	63	3	Y
93	19UP1A0591	4.38	6.88	15	10	10	39	46.26	20	32	52	2	Y
94	19UP1A0592	4.38	6.88	15	10	8.75	43	45.01	22	44	66	3	Y
95	19UP1A0593	7.5	10	10.77	10	7.5	47	45.77	24	53	77	3	Y
96	19UP1A0594	6.25	10	10.385	10	8.75	46	45.385	23	46	69	3	Y
97	19UP1A0595	3.75	4.38	7.18	10	6.88	33	32.19	17	31	48	1	Y
98	19UP1A0596	4.38	6.25	15	10	8.13	43	43.76	22	39	61	3	Y
99	19UP1A0597	6.25	5	7.69	5	6.25	35	30.19	18	38	56	2	Y
100	19UP1A0598	7.5	9.38	15	10	8.13	48	50.01	24	50	74	3	Y
101	19UP1A0599	5.63	7.5	11.41	10	6.25	40	40.79	20	14	34	0	N
102	19UP1A05A0	6.88	8.75	15	10	8.75	47	49.38	24	42	66	3	Y
103	19UP1A05A1	4.38	6.67	8.075	10	5.63	37	34.755	19	44	63	3	Y
104	19UP1A05A2	5	10	7.305	10	6.25	42	38.555	21	48	69	3	Y
	Avg	5.82	7.97	11.47	9.38	8.07	42.10	42.72	21.30	35.03	56.33	2.06	98.0

PRINCIPAL
Vignan's Institute of Management & Technology For Wom.
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

CO No	CO wise Internal assessment results				Course wise External assessment				Overall Grade of attainment
	1	2	3	4	5	6	7	8	
	Class Avg [10]	Average targeted attainment [10]	% Attainment level	Attainment grade	Class Average [75]	Average Targeted attainment	Attainment level	Attainment grade	
1	5.88	5.25	60.19	3	56.87	30	98.06	3	3.00
2	8.05	5.30	89.32	3					
3	11.59	5.45	99.03	3					
4	9.47	5.50	99.03	3					
5	8.15	5.65	93.20	3					
Average	8.63	5.43	88.15	3.00					

CO - ATTAINMENT

CO	Internal % Attainment level	External % Attainment level	Direct Attainment	Indirect Attainment	Final Attainment %	Attainment Level
CO-I	60.19	98.06	88.59	90.28	88.93	2.67
CO-II	89.32	98.06	95.87	90.28	94.75	2.84
CO-III	99.03	98.06	98.30	90.28	96.70	2.90
CO-IV	99.03	98.06	98.30	90.28	96.70	2.90
CO-V	93.20	98.06	96.84	90.28	95.53	2.87
					Average	2.84

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

CO- PO and CO-PSO Mapping

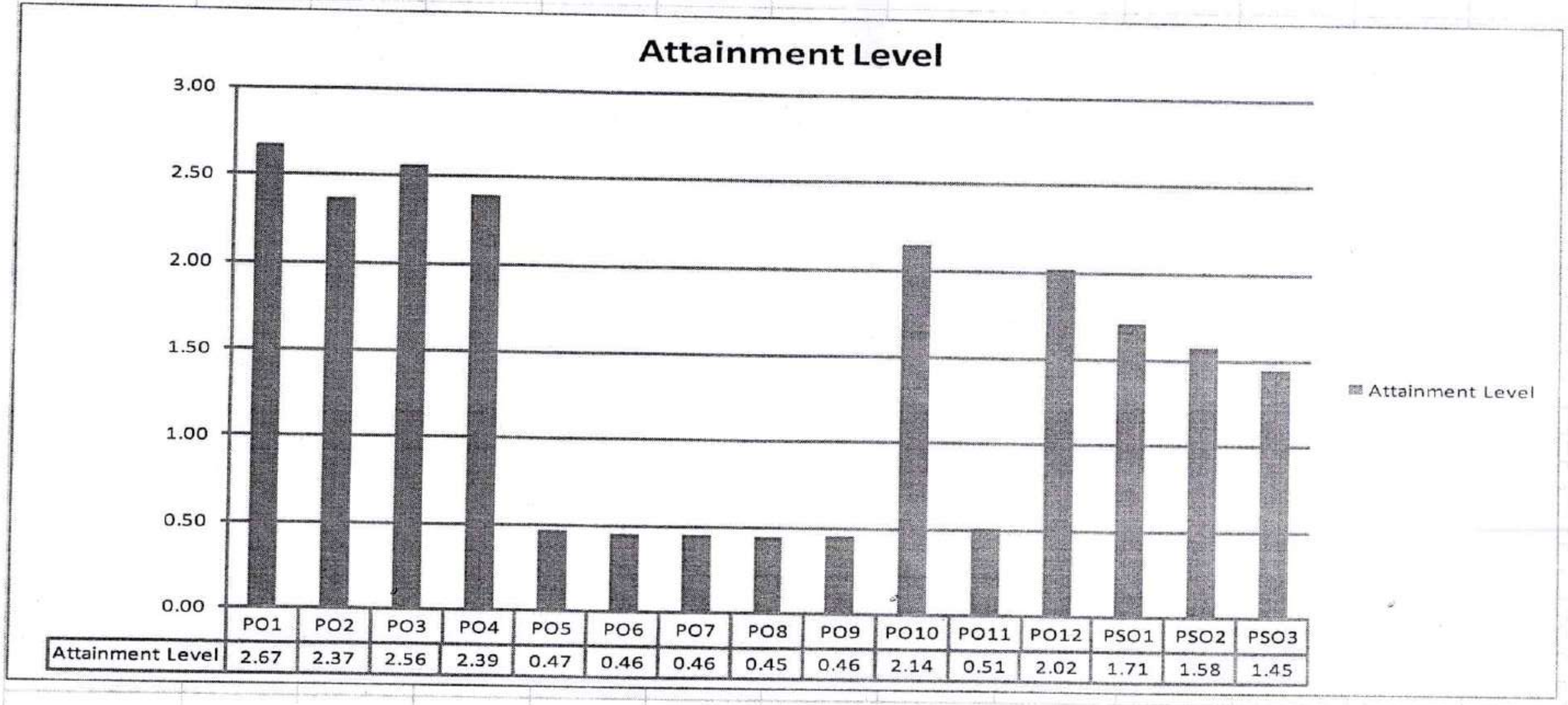
Course	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	ATTAINMENT LEVELS	ATTAINMENT (%)
CS702PC.1	3	1								2		1	2	1	1	2.67	88.93
CS702PC.2	3	3								2		2	1	1	1	2.84	94.75
CS702PC.3	3	2	3							2		2	1	1	2	2.90	96.70
CS702PC.4	3	3	3	3						2		2	2	2	1	2.90	96.70
CS702PC.5	2	3	2	2						3		3	2	2	1	2.87	95.53
Average	**2.8**	**2.4**	**2.67**	**2.5**	**0**	**0**	**0**	**0**	**0**	**2.2**	**0**	**2**	**1.6**	**1.4**	**1.2**	**2.84**	**94.52**

PO Attinment

PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
Weighted Sum	1322.3	1143.27	771.26	481.16	0	0	0	0	0	1040.75	0	951.82	753.77	664.84	569.31
Attainment (%)	88.15	76.22	85.7	80.19	0	0	0	0	0	69.38	0	63.45	50.25	44.32	37.95
Attainment Level (Direct) (80%)	2.64	2.29	2.57	2.41	0	0	0	0	0	2.08	0	1.9	1.51	1.33	1.14
Alumni Survey (7%)	2.93	2.61	2.42	2.39	2.20	2.19	2.21	2.21	2.24	2.31	2.38	2.39	2.47	2.55	2.66
Graduate Exit Survey (5%)	2.79	2.70	2.63	2.54	2.64	2.56	2.63	2.70	2.66	2.63	2.79	2.64	2.80	2.63	2.82
Employer's Survey (5%)	2.40	2.57	2.32	1.92	2.18	2.27	2.21	2.11	2.14	2.32	2.56	2.40	2.24	2.51	2.52
Parent's f/b Survey (3%)	3.00	3.00	2.77	2.47	2.47	2.17	2.04	1.92	2.18	2.22	2.46	2.54	2.57	2.76	2.9
Over All Attainment	2.67	2.37	2.56	2.39	0.47	0.46	0.46	0.45	0.46	2.14	0.51	2.02	1.71	1.58	1.45

Vignan's Institute of Management & Technology For Women
Kondapur (V) Ghatkesar (M) Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State



	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
Attainment Level	2.67	2.37	2.56	2.39	0.47	0.46	0.46	0.45	0.46	2.14	0.51	2.02	1.71	1.58	1.45

Faculty

HOD

Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Malkajgiri (Dt.) Pin-501301 (T.S.)

PRINCIPAL

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

VIGNAN'S INSTITUTE OF MANAGEMENT AND TECHNOLOGY FOR WOMEN

Sponsored by Lavu Educational Society, Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad.
Kondapur (V), Ghatkesar (M), Medchal - Malkajgiri (D) - 501 301 Phone: +91 96529 10002/3

LECTURE NOTES

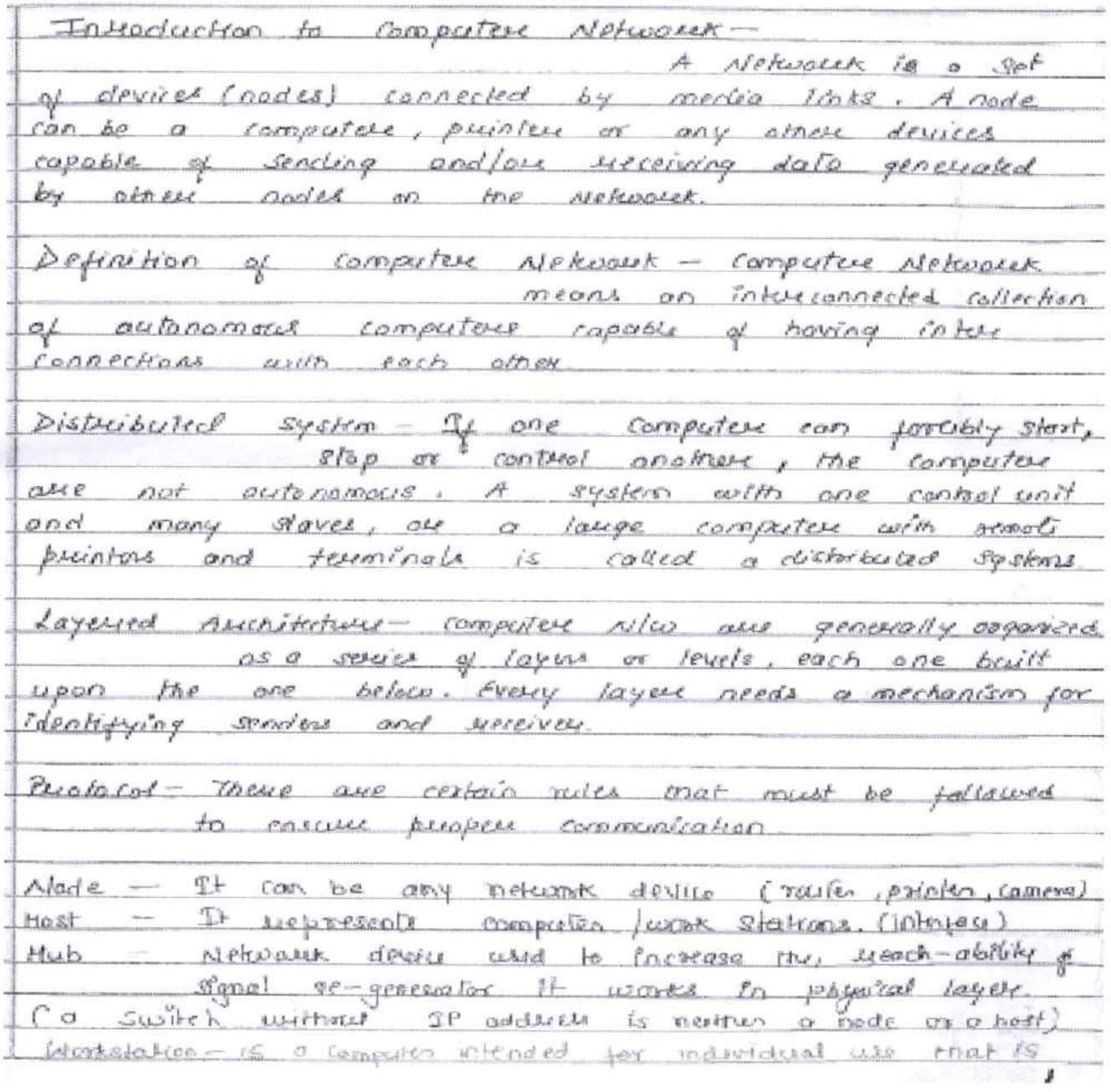
Vignan's Institute of Manage.ment & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

CN-UNIT – I

Network hardware, Network software, OSI, TCP/IP Reference models, ExampleNetworks: ARPANET, Internet. Physical Layer: Guided Transmission media: twisted pairs, coaxial cable, fiber optics

Introduction



Introduction to Computer Network –

A Network is a set of devices (nodes) connected by media links. A node can be a computer, printer or any other devices capable of sending and/or receiving data generated by other nodes on the network.

Definition of Computer Network – Computer Network means an interconnected collection of autonomous computers capable of having inter connections with each other

Distributed system – If one computer can forcibly start, stop or control another, the computer are not autonomous. A system with one control unit and many slaves, or a large computer with remote printers and terminals is called a distributed systems.

Layered Architecture – computer N/w are generally organized as a series of layers or levels, each one built upon the one below. Every layer needs a mechanism for identifying senders and receiver.

Protocol – There are certain rules that must be followed to ensure proper communication

Node – It can be any network device (router, printer, camera)
Host – It represents computer / work stations. (interface)
Hub – Network device used to increase the reach-ability of signal re-generator it works in physical layer.
(a switch without IP address is neither a node or a host)
Workstation – is a computer intended for individual use that is

Computer Network Types

Types of Networks.—

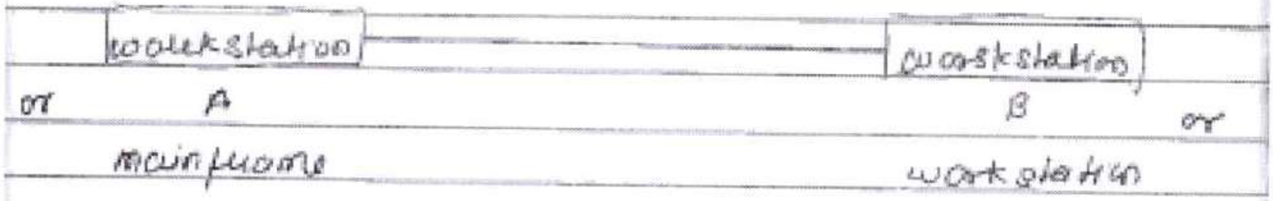
On the basis of transmission techno-logy networks are classified into three categories.

Point-to-point 2. Multipoint 3. Broadcast n/w

Basic Concepts—

- Line configuration
- Topology
- Transmission mode
- categories of networks
- Internetwork

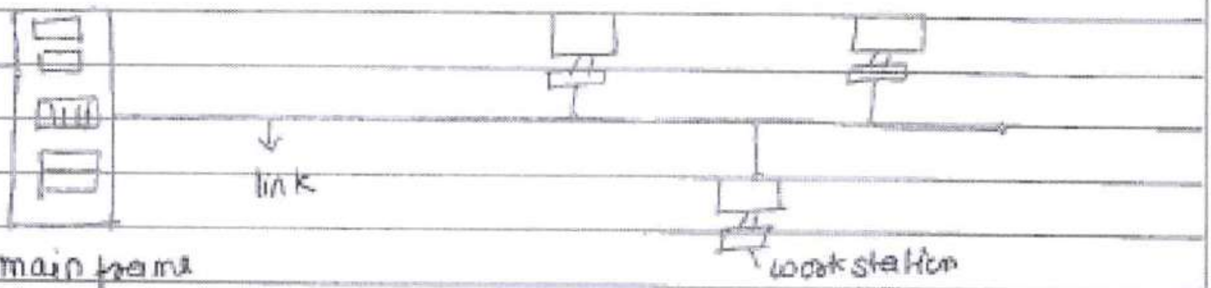
Line configuration — defines the attachment of communication devices to a link



point to-point line configuration

Point-to-point provides a dedication link between two devices. (use an actual length of wire or cable) or microwave or satellite links are also possible

satellite
A
Link
satellite
B



Multipoint (also called multidrop) line configuration is one in which more than two specific devices shares a single link (capacity of the channel is shared, either spatially or temporary)

Topology :- defines the physical or logical arrangement of links in a network.

Mesh	point-to-point	(n-1) dev I/O ports	n(n-1)/2 ~~devices~~ wire
Star		n I/O ports	n wire
Tree			
Ring		2n I/O ports	n wire
Bus — multipoint			

The lucky Ducky Corporation has a fully connected mesh network consisting of eight devices. Calculate the total number of cable links needed and the number of ports for each device. (mesh / star / ring)

Transmission Mode - refers to the direction of information flow between two devices.

- Simplex — unidirectional — key → 🖥 TV Radio
- Half Duplex — direction of data at a time — walki - talkie internet browser
- full Duplex — Direction of data all the time — cellphone two lane road

Categories of Network -

LAN / MAN / WAN

Internetworks - two or more n/ws are connected.

In satellite communication, up-link frequency and down-link frequency are different. why?
Interference can be avoided

In a broad sense, a railway track is an example of
Half duplex

The topology with highest reliability is - Mesh.

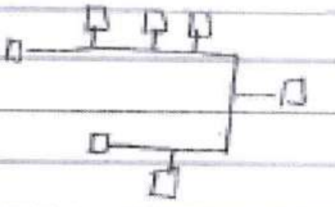
The method of communication in which transmission takes place in both directions; but only one direction at a time is called - Half duplex

Security and privacy are less of an issue for devices in a which topology? Bus

bus
A cable break in a which topology stops all x-mission

In a mesh topology, the relationship b/w one device and another is peer-to-peer

A network that contains multiple hubs is most likely configured in a Tree



Q Assume six devices are arranged in a mesh topology? How many cables are needed? How many ports are needed for each device?

Layered Architecture—

Established in 1947, the International standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards An ISO standard that covers all aspects of network communications is the open system Inter-connection model (OSI)

The purpose of the OSI model is to open communication between different systems without requiring changes to the logic of the underlying Hardware & Software. It is not a protocol, It is a model for understanding and designing a network architecture that is flexible, robust and interoperable

Mnemonic —

Please Do Not Touch Steve's Pet Alligator

Peer-to-peer process - Between machines, layer x on one machine communicates with layer x another machine. This communication is governed by an agreed-upon series of rules + conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes.

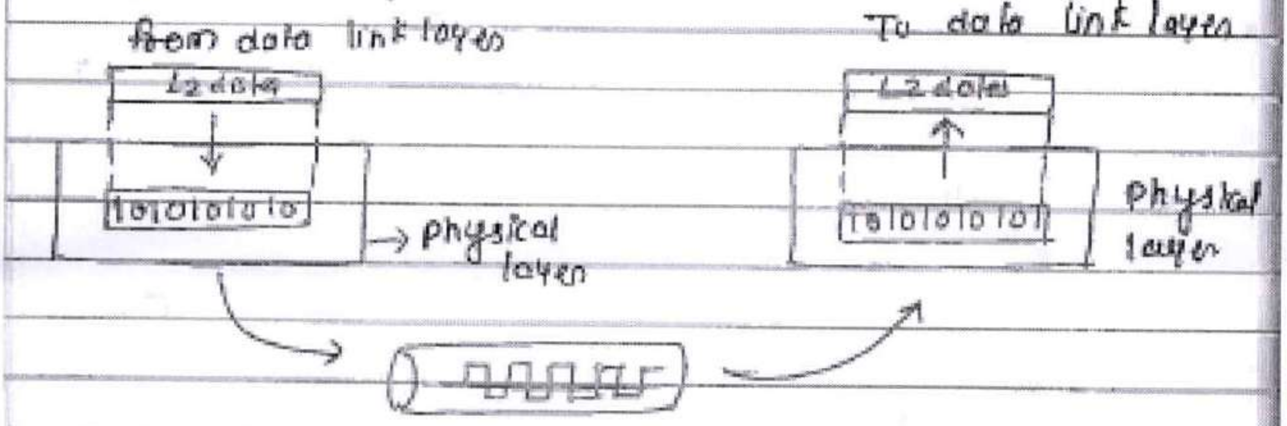
Interfaces between Layers!— Each interface defines what information ~~by an interfaces~~ bfw & services a layer must provide for the layer above it.

Organizations of layer - Layers 1, Layers 2 and Layers 3 are the network support layers. They deal with the physical aspects of moving data from one device to another.

layers 5, 6 and 7 can be thought of as the user support layers, they allow interoperability among unrelated Software systems.

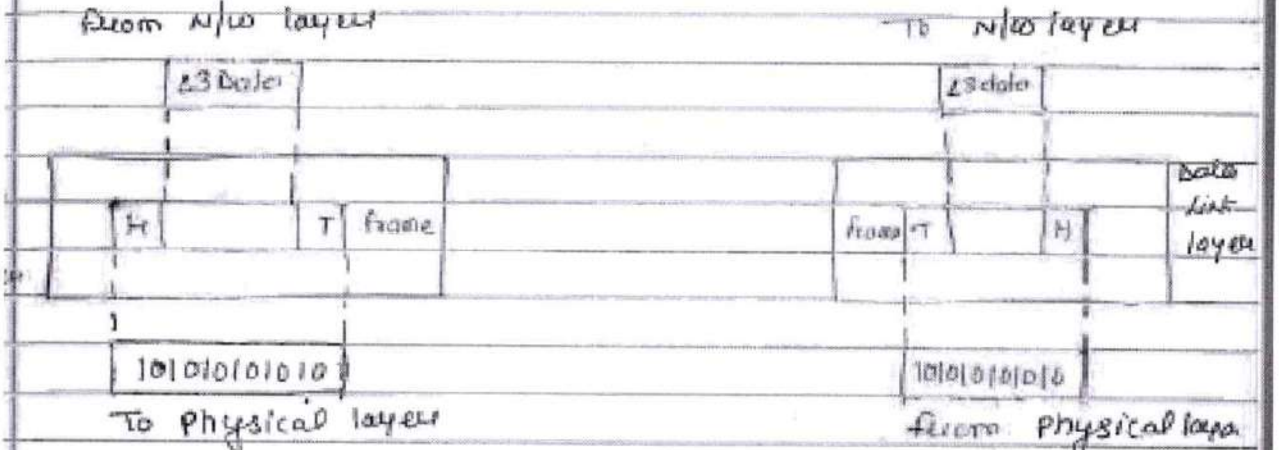
Functions of the layers —

Physical layer - coordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical & electrical specifications of the interface & transmission medium.



It defines the characteristics of the interface b/w the devices and the transmission medium.
It consist data, in a stream of bits without any interpretation.
Data rate - the number of bits sent each second.
Synchronization - The sender & receiver must be synchronized at the bit level.
Line Configuration.
Physical Topology
Transmission mode

delivery, It makes the physical layer appear error free to the upper layer



Responsibilities —

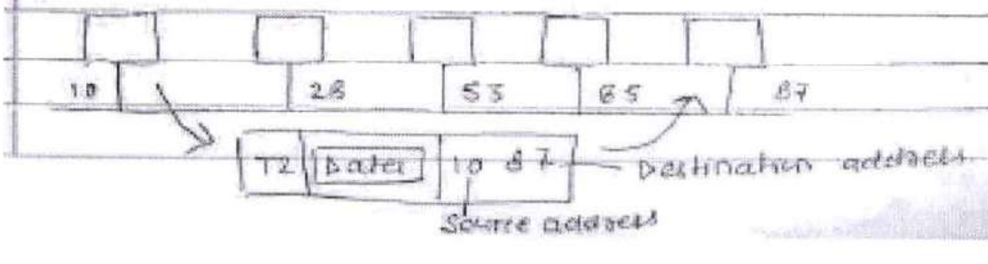
Framing - It (DLL) divides the stream of bits received from the n/w layer into manageable data units called frames

Physical addressing - If frames are to be distributed to different systems on the n/w, the DLL adds a header to the frame to define the physical address of the sender and/or receiver of the frame.

Flow control:- DLL imposes a flow control mechanism to prevent overwhelming the receiver.

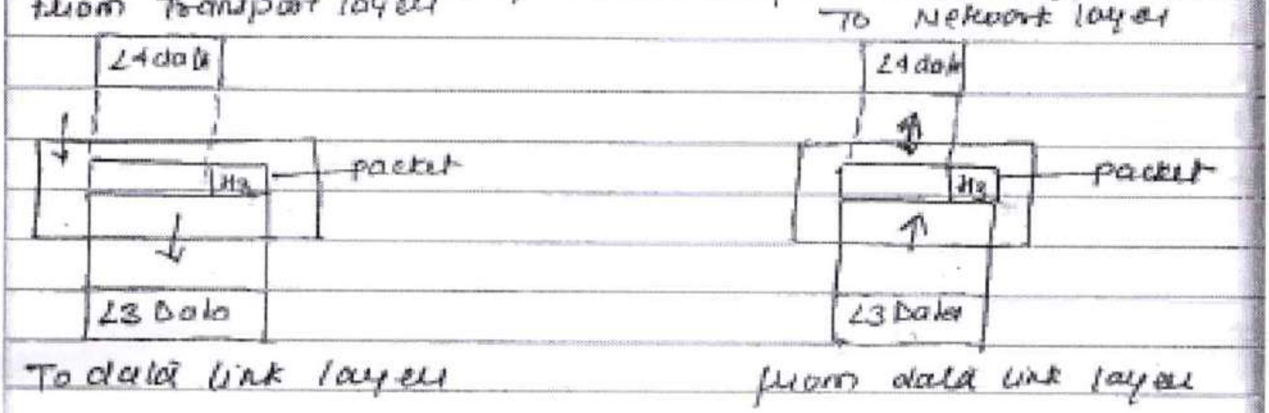
Error control:- It is normally achieved through a trailer added to the end of the frame.

Access control:- When two or more devices are connected to the same link, DLL protocols are necessary to determine which device has control over the link at any given time.



Network layer:- It is responsible for the source-to-destination delivery of a packet possibly across multiple n/w (links). whereas the data link layer oversees the delivery of the packet b/w two systems on the same n/w. (links), the n/w layer ensures that each ~~pak~~ packet get from its point of origin to its final destination.

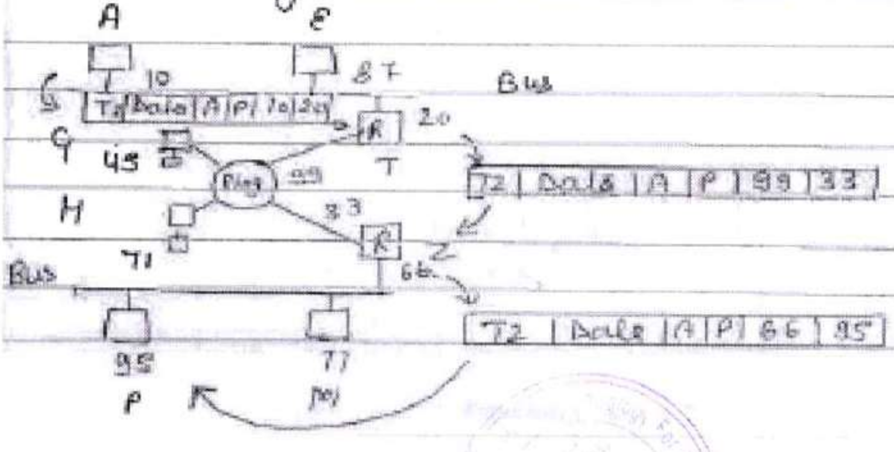
Note- If two systems are connected to the same link, there is usually no need for a n/w layer.



Responsibilities -

Logical addressing - If a packet passes the n/w boundary, we need another addressing system to help distinguish the source & destination systems.

Routing:- When independent n/w or links are connected together to create an internetwork or a large n/w



Transport Layer:- It is responsible for Source-to-destination delivery of the entire message. Whereas the network layer oversees end-to-end delivery of individual packet, it doesn't recognize b/w those packets.

A connection is a single logical path b/w the source and destination that is associated with all packets in a message
1. Connection Establishment
2. Data Transfer
3. Connection Release

Responsibility -

Service-point addressing - Computers often run several programs at the same time. For this reason, source-to-destination delivery means not only from one computer to the next but also a specific process (running progm) on one computer to a specific process (running progm) on the other. The transport layer header therefore must include a type of address called a service-point address or port address.

- o N/w layer gets each packet to the correct computer.
- o Transport layer gets the entire message to the correct process on that computer.

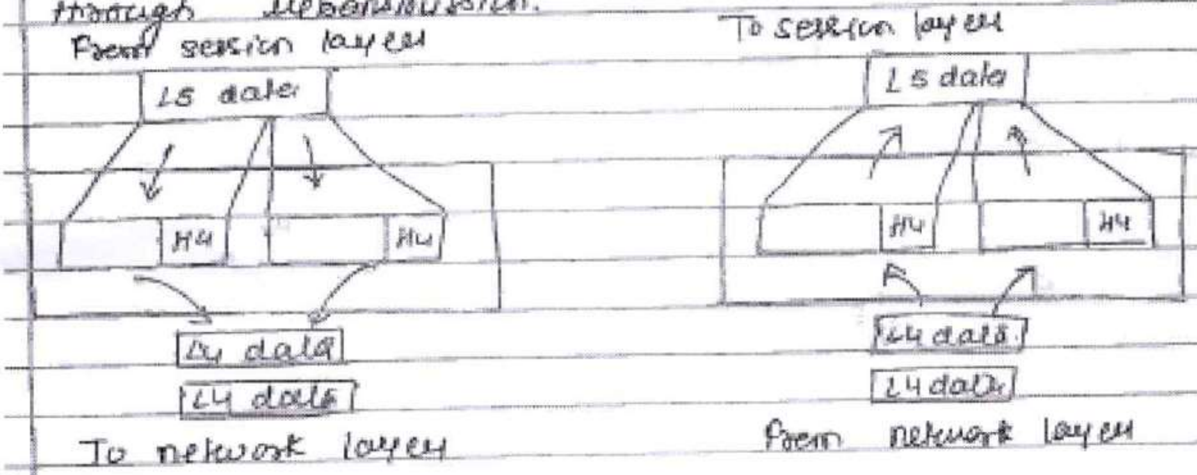
Segmentation and Reassembly - A message is divided into transmittable segment, each segment containing a sequence number. These sequence no. enables the transport layer to reassemble the message correctly upon arriving at the destination & to identify & replace packets that were lost in the transmission.

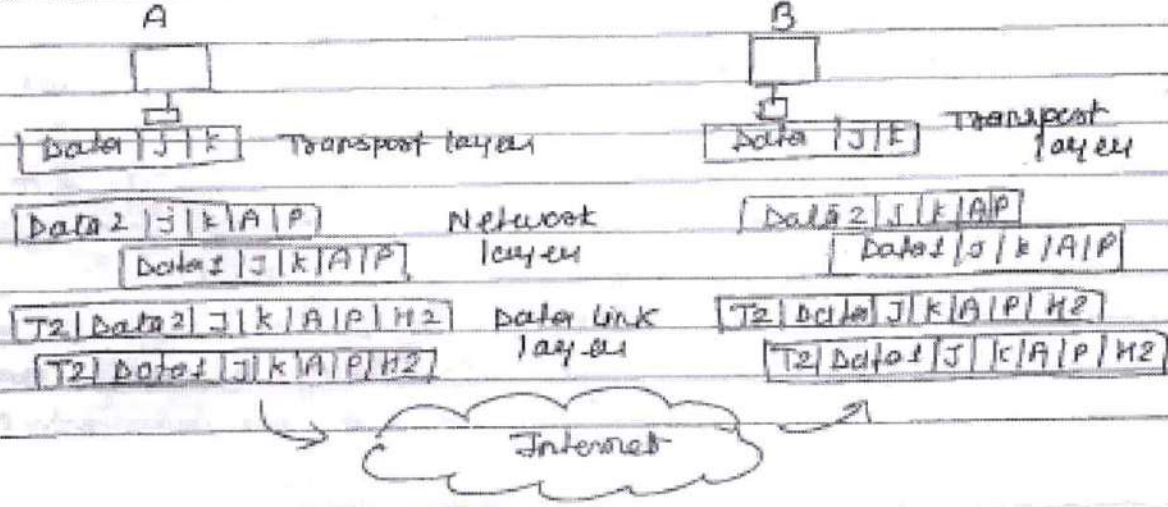
Connection control - Either connectionless or connection-oriented. Connection-less transport layer treat packet (each) as an independent packet.

Connection- oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets.

Flow control:- Like DLL, transport layer is responsible for flow control. It is performed end-to-end rather than across a single link

Error control:- Error control at the layer is performed end-to-end rather than across a single link. (Sending transport layer make sure that the entire message arrives at the receiving transport layer without error (damage, loss or duplication)). It is usually achieved through retransmission.



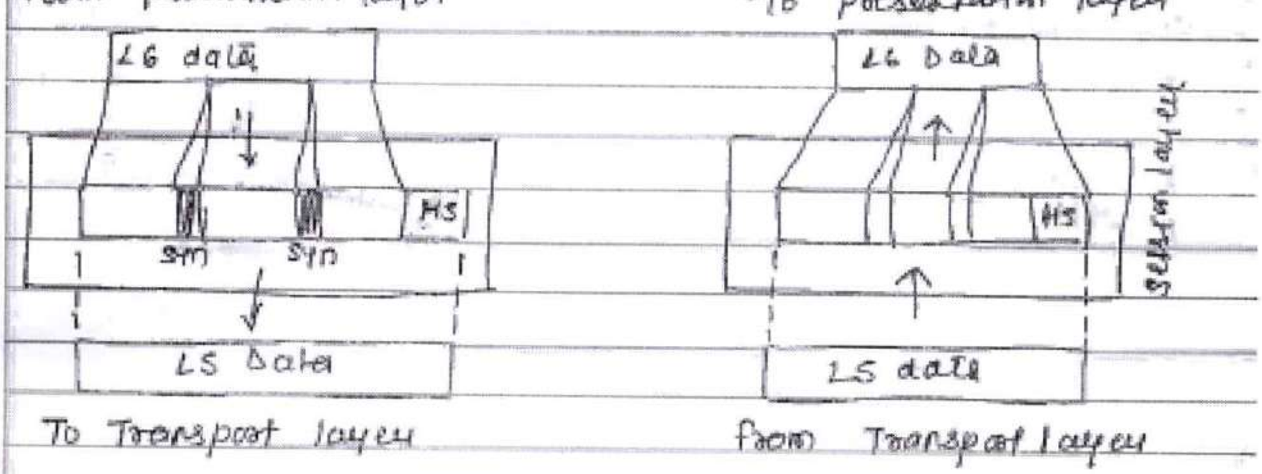


Session layer:— It is the n/w dialog controller. It establishes, maintains & Synchronizes the interaction b/w communicating systems

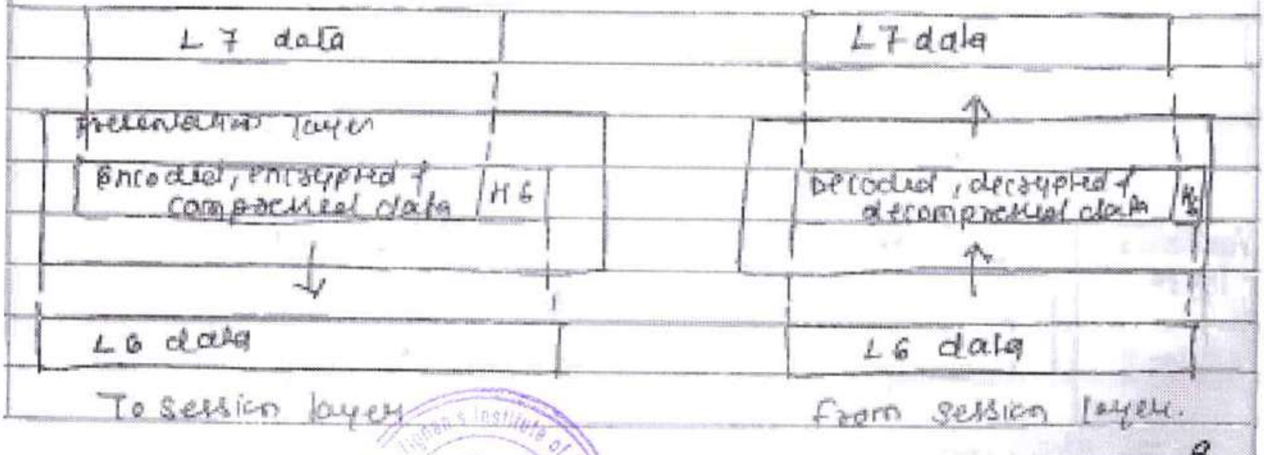
Responsibilities —

Dialog Control- Session layer allows two systems to enter into a dialog. It allow the communication b/w processes to take place either in Half-duplex or Full-duplex.

Synchronization- Session layer allows a process to add checkpoints into a stream of data.



Presentation layer:- It is concerned with the syntax & Semantics of the information exchanged b/w two systems.



Responsibilities —

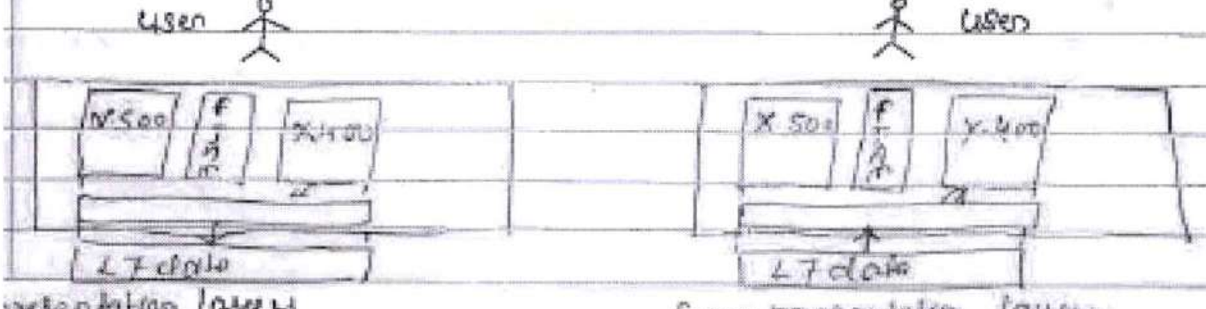
Translation- The processes (running program) in two systems are usually exchanging in the form of character strings, numbers and so on. This layer is responsible for interoperability b/w these different encoding methods

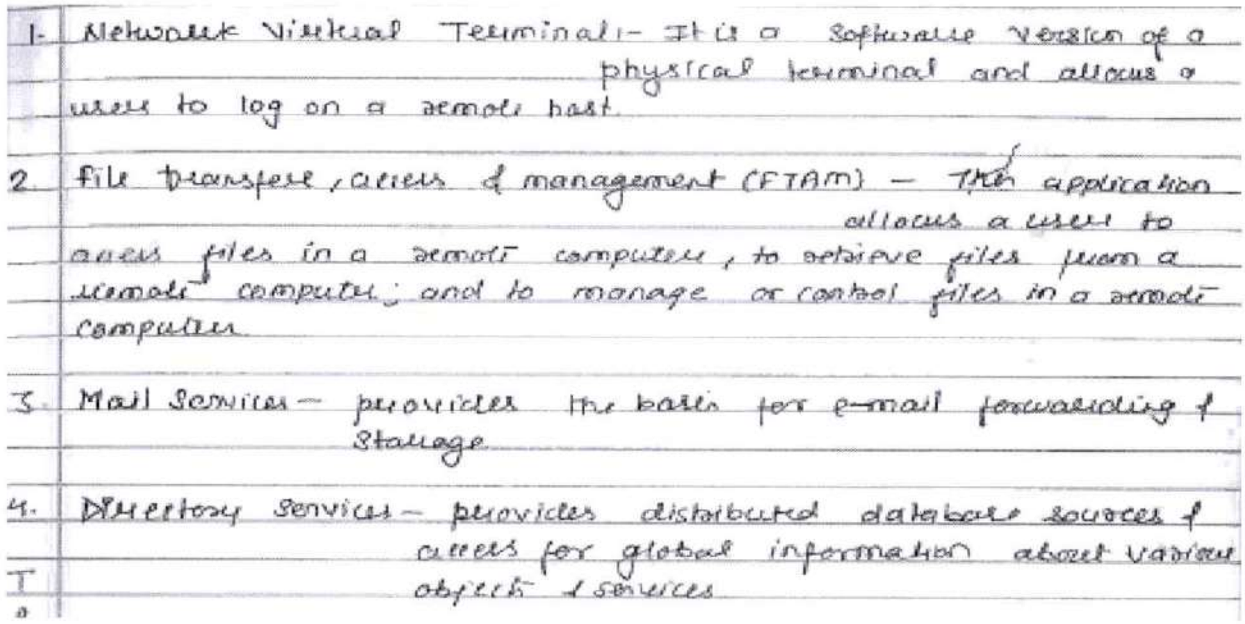
Encryption- To carry sensitive information, a system must be able to assure privacy.

Encryption means that the sender transforms the original information to another form and sends the resulting message out over the Network.
Decryption reverses the original process to transform the message back to its original form.

Compression- Data compression reduces the number of bits to be transmitted.

Application Layer- enables the user, whether human or software, to access the network.
It provides user interfaces and support for services such as electronic-mail, remote file access & transfer, shared database management and other types of distributed information services.





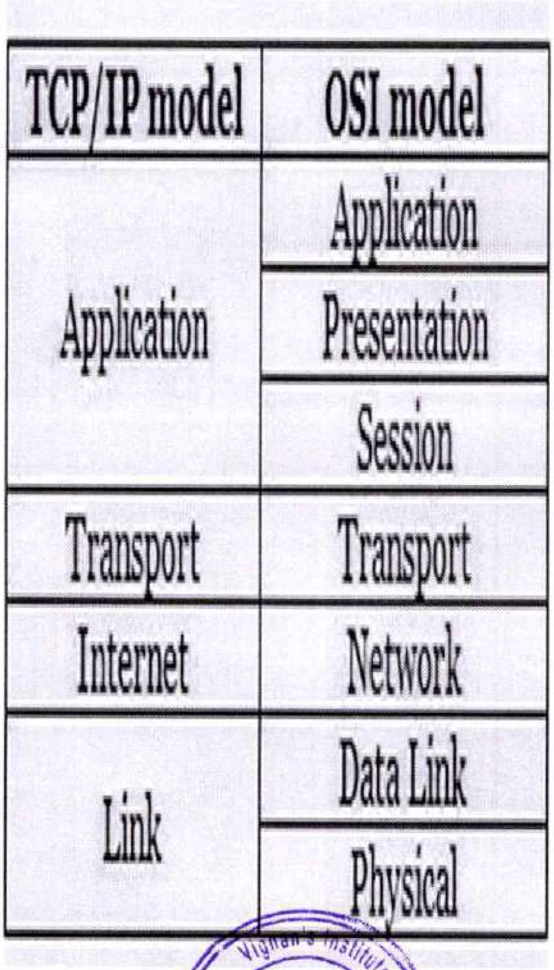
1. Network Virtual Terminal:- It is a software version of a physical terminal and allows a user to log on a remote host.

2. File transfer, access & management (FTAM) - This application allows a user to access files in a remote computer, to retrieve files from a remote computer; and to manage or control files in a remote computer

3. Mail Services - provides the basis for e-mail forwarding & storage

4. Directory Services - provides distributed database sources & access for global information about various objects & services

The TCP/IP Reference Model



TCP/IP model	OSI model
Application	Application
	Presentation
	Session
Transport	Transport
Internet	Network
Link	Data Link
	Physical

Difference between OSI and TCP/IP Reference Models

S.NO	OSI	TCP/IP
1	Has 7 layers	Has 4 Layers
2	OSI is a generic, protocol independent standard; Generally it is used as a guidance tool.	TCP/IP model is implemented like OSI, based on standard protocols around which the Internet has developed.
3	Defines Services, Protocols and Interfaces Very clearly and makes clear distinction between them. It is protocol independent.	In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
4	Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
5	Network layer of OSI model provides both connection oriented and connectionless service.	The Network layer in TCP/IP model provides connectionless service.
6	Transport Layer is Connection Oriented	Transport Layer is both Connection Oriented and Connection less.

Example Networks

The Internet: The internet is a globally connected network system facilitating worldwide communication and access to data resources through a vast collection of private, public, business, academic and government networks.

- The internet originated with the U.S. government, which began building a computer network in the 1960s known as ARPANET. In 1985, the U.S. National Science Foundation (NSF) commissioned the development of a university network backbone called NSFNET.
- The system was replaced by new networks operated by commercial internet service providers in 1995. The internet was brought to the public on a larger scale at around this time.
- Since then, the Internet has grown and evolved over time to facilitate services like: Email,Web-enabled audio/video conferencing services ,Online movies and gaming, Data transfer/file-sharing, often through File Transfer Protocol (FTP), Instant messaging, Internet forums ,Social networking, Online shopping, and Financial services ect.

Advanced Research Projects Agency Network (ARPANET)

- The Advanced Research Projects Agency Network (ARPANET) is a predecessor to the modern Internet. It was conceptualized in the 1950s, when computer scientists needed something better than the then available but unreliable switching nodes and network links.
- There were also only a limited number of large, powerful research computers, and researchers with access were separated geographically.

- The Advanced Research Projects Agency (ARPA) commissioned the development of an advanced and reliable way to connect these computers through a newly devised packet switching network, which was known as ARPANET.
- The ARPANET was a project funded by the U.S. government during the Cold War with USSR, in order to build a robust and reliable communications network. This was done by connecting various computers that could simultaneously communicate in a network that would not go down and continue running when a single node was taken out.
- The initial groundwork for a computer network was laid by BBN with other associates in 1963. And they were able to connect three computer terminals ARPA-sponsored computers:

  i. The System Development Corporation (SDC) Q-32 at Santa Monica
  ii. Project Genie at the University of California, Berkeley
  iii. Multics at the Massachusetts Institute of Technology

- When Taylor needed to talk to someone at another computer, he would transfer to a different terminal for each connection. This was frustrating and led to the concept of one terminal/computer connected to a number of other terminals. This idea paved the way for the ARPANET and, eventually, the modern Internet.
- Paul Baran of Rand Corporation concluded that the strongest kind of network would be a packet switched network that would use any available communication line, regardless of the status of other lines. The ARPANET originally connected four computers, as follows:

  i. A Honeywell DDP 516 computer at University of California, Los Angeles
  ii. An SDS-940 computer at the Stanford Research Institute
  iii. An IBM 360/75 at University of California, Santa Barbara
  iv. A DEC PDP-10 at the University of Utah

- Compatibility issues surfaces as more computers were connected to the network. These problems were solved in 1982 through the development of Transfer Control Protocol/Internet Protocol (TCP/IP).

Early ARPANET Architecture

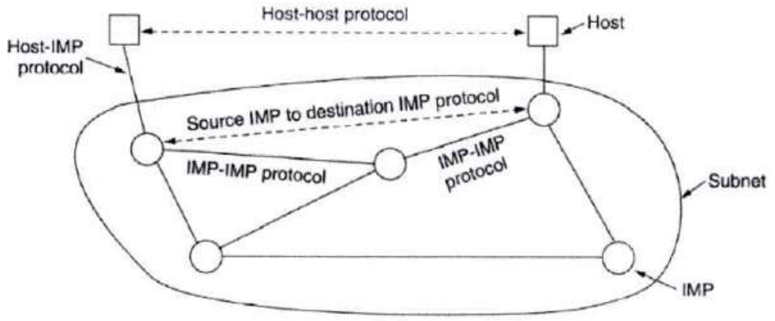


Figure 1-26. The original ARPANET design.

- BBN, a consulting firm build the subnet and wrote the subnet software. The software was split into two parts: subnet and host.
- The subnet software consisted of the IMP end of the host-IMP connection, the IMP-IMP protocol, and a source IMP to destination IMP protocol designed to improve reliability.
- Outside the subnet, software was also needed, namely, the host end of the host-IMP connection, the host-host protocol, and the application software.

Standards Organization

Standard is a common set of rules. Standards define what is needed for interoperability: no more, no less. Standards fall into two categories: De facto and de jure.

- **De facto** (Latin for ''from the fact'') standards are those that have just happened, without any formal plan. HTTP, the protocol on which the Web runs, started life as a de facto standard.
- **De jure** (Latin for ''by law'') standards, in contrast, are adopted through the rules of some formal standardization body.

- International standardization authorities are generally divided into two classes: those established by treaty among national governments, and those comprising voluntary, nontreaty organizations.
- In the area of computer network standards, there are several organizations of each type, notably ITU, ISO, IETF and IEEE and 3GPP(Third Generation Partnership Project) all of which we will discuss below.

IEEE and ITU:

- IEEE (Institute of Electrical and electronics Engineers): The IEEE is incorporated under the Not-for-Profit Corporation Law of the state of New York, United States. It was formed in 1963.
- ITU (International Telecommunication Union). Its job was to standardize international telecommunications, which in those days meant telegraphy.
- In 1947, ITU became an agency of the United Nations. ITU has about 200 governmental members, including almost every member of the United Nations.

ITU and its Sectors:

- ITU has three main sectors. We will focus primarily on ITU-T, the Telecommunications Standardization Sector, which is concerned with telephone and data communication systems.
- ITU-R, the Radio communications Sector, is concerned with coordinating the use by competing interest groups of radio frequencies worldwide.
- The other sector is ITU-D, the Development Sector. It promotes the development of information and communication technologies.

ISO:

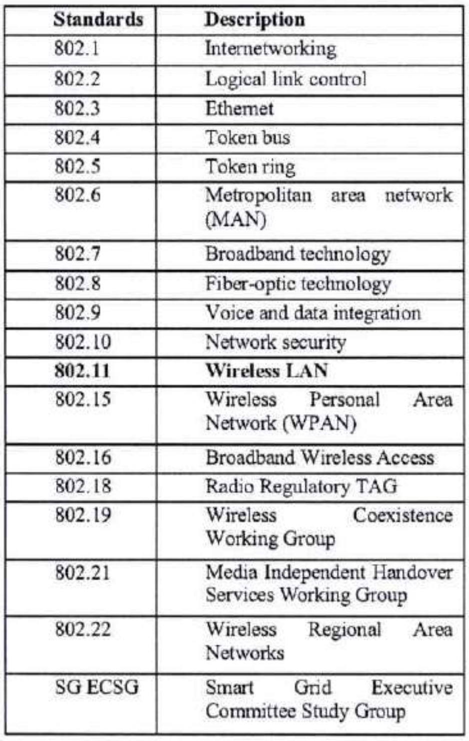
- International standards are produced and published by ISO (International Standards Organization), a voluntary nontreaty organization founded in 1946. Its members are the national standards organizations of the 157 member countries.
- On issues of telecommunication standards, ISO and ITU-T often cooperate (ISO is a member of ITU-T) to avoid the irony of two official and mutually incompatible international standards.
- ISO has over 200 Technical Committees (TCs), numbered in the order of their creation, each dealing with a specific subject. TC1 deals with the nuts and bolts (standardizing screw thread pitches). JTC1 deals with information technology, including networks, computers, and software.

Standards Establishment Procedure:

The procedure used by ISO for adopting standards has been designed to achieve as broad a consensus as possible.

- The process begins when one of the national standards organizations feels the need for an international standard in some area.
- A working group is then formed to come up with a CD (Committee Draft).

- The CD is then circulated to all the member bodies, which get 6 months to criticize it. If a substantial majority approves, a revised document, called a DIS (Draft International Standard) is produced and circulated for comments and voting.
- Based on the results of this round, the final text of the IS (International Standard) is prepared, approved, and published.
- In areas of great controversy, a CD or DIS may have to go through several versions before acquiring enough votes, and the whole process can take years.



Standards	Description
802.1	Internetworking
802.2	Logical link control
802.3	Ethernet
802.4	Token bus
802.5	Token ring
802.6	Metropolitan area network (MAN)
802.7	Broadband technology
802.8	Fiber-optic technology
802.9	Voice and data integration
802.10	Network security
802.11	**Wireless LAN**
802.15	Wireless Personal Area Network (WPAN)
802.16	Broadband Wireless Access
802.18	Radio Regulatory TAG
802.19	Wireless Coexistence Working Group
802.21	Media Independent Handover Services Working Group
802.22	Wireless Regional Area Networks
SG ECSG	Smart Grid Executive Committee Study Group

IEEE 802 Standard

IEEE 802 Standards:

Explains networking model and related standards, provides detailed implementation specifications for no of networking technologies.

NIST:

- NIST (National Institute of Standards and Technology) is part of the U.S. Department of Commerce. It used to be called the National Bureau of Standards.
- It issues standards that are mandatory for purchases made by the U.S. Government, except for those of the Department of Defense, which defines its own standards.

Metrics and UNITS used in Communication:

Exp.	Explicit	Prefix	Exp.	Explicit	Prefix
10^{-3}	0.001	milli	10^{3}	1,000	Kilo
10^{-6}	0.000001	micro	10^{6}	1,000,000	Mega
10^{-9}	0.000000001	nano	10^{9}	1,000,000,000	Giga
10^{-12}	0.000000000001	pico	10^{12}	1,000,000,000,000	Tera
10^{-15}	0.000000000000001	femto	10^{15}	1,000,000,000,000,000	Peta
10^{-18}	0.000000000000000001	atto	10^{18}	1,000,000,000,000,000,000	Exa
10^{-21}	0.000000000000000000001	zepto	10^{21}	1,000,000,000,000,000,000,000	Zetta
10^{-24}	0.000000000000000000000001	yocto	10^{24}	1,000,000,000,000,000,000,000,000	Yotta

Who's Who in the Internet Standards World

Internet Standards refer to all the documented requirements both in technology as well as methodology pertaining to the Internet. The standardization process has three steps.

- **Proposed Standard:** These are the standards that are ready for implementation. However, they can be revised according to circumstances of deployment.
- **Draft Standard:** When a Proposed Standard has been meticulously tested by at least two sites for at least 4 months, they are considered as Draft Standard. Draft Standard has been merged with Internet standard to form the future Internet standard.
- **Internet Standard:** These are technically matured standards that define the protocols and formats of messages. The fundamental standards are those which form the Internet Protocol (IP).

The organizations of Internet Standards are

1. Internet Engineering Task Force (IETF) : IETF formulates, publishes and regulates Internet Standards, particularly those related to TCP/IP. The organization is open standard, with no formal memberships. Development of IETF standards is open to all. Any interested person can participate for their development. IETF documents are free and easily available over the Internet. IETF specifications are on individual protocols that may be used in different systems.

2. Internet Society (ISOC): ISOC was founded in the US in 1992 as a non-profit organization to provide support on technical development of the Internet. It presently conducts a range of activities on Standards, Education, Access, and Policies.

3. Internet Architecture Board (IAB): IAB is a committee of IETF and an advisory body of ISOC. The board comprises researchers and professionals for developing technical aspects of the Internet. The responsibilities of IAB are

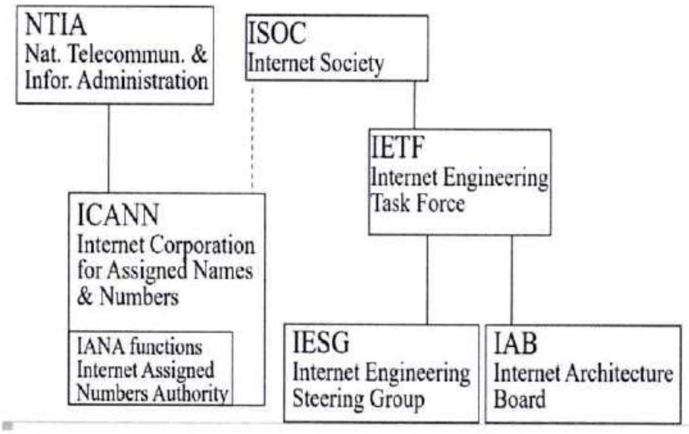
- Supervise architectural standards of different networks and IP.
- Review issues related to Internet Standards.
- Provide guidance to IETF and ISOC.

4. Internet Research Task Force (IRTF) : IRTF is composed of a number of research groups whose overall objective is focused on the long-term development of the Internet. It is a parallel organization to IETF. The participants are individual contributors who have long-term memberships. The research groups work on Internet protocols, applications, technology and overall architecture.

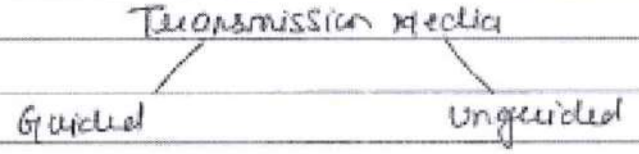
5. Internet Assigned Numbers Authority: The Internet Assigned Numbers Authority is a standards organization that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System, media types, and other Internet Protocol-related symbols and Internet numbers.

6. World Wide Web Consortium (W3C): It is the foremost international standards organization for the World Wide Web (www). It is a community of a large number of member organizations, who work together to develop web standards and improve web services. Some of the popular standards developed by W3C are HTML, HTTP, XML, CSS, etc.

Internet Organization


NTIA
Nat. Telecommun. & Infor. Administration
ISOC
Internet Society
IETF
Internet Engineering Task Force
ICANN
Internet Corporation for Assigned Names & Numbers
IANA functions
Internet Assigned Numbers Authority
IESG
Internet Engineering Steering Group
IAB
Internet Architecture Board

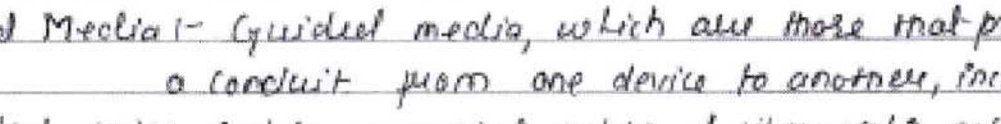
Transmission Media :- Signals travel from transmitter to receiver via a path. This path, called the medium, can be guided or unguided. A guided medium is contained within physical boundaries, while an unguided medium is boundless.



Guided Media :- Guided media, which are those that provide a conduit from one device to another, include twisted pair cable, coaxial cable & fiber-optic cable.

Twisted-pair Cable consists of two insulated copper wires twisted together. Twisting allows each wire to have approximately the same noise environment.

• Unshielded Twisted-pair (UTP) cable :- It is the most common type of telecommunication medium in use today. Its frequency range is suitable for transmitting both data & voice.
Frequency range from 100 Hz to 5 MHz.



Twisted pair cable

Electronics Industries Association (EIA) has developed standards to grade UTP cables by quality. Categories are determined by cable quality, with 1 as the lowest and 5 as the highest.

CN-UNIT-II

(Data link layer: Design issues, framing, Error detection and correction. Elementary data link protocols: simplex protocol, A simplex stop and wait protocol for an error-free channel, A simplex stop and wait protocol for noisy channel. Sliding Window protocols: A one-bit sliding window protocol, A protocol using Go-Back-N, A protocol using Selective Repeat, Example data link protocols. Medium Access sub layer: The channel allocation problem, Multiple access protocols: ALOHA, Carrier sense multiple access protocols, collision free protocols. Wireless LANs, Data link layer switching.)

Introduction:

- Data link layer is one of the most complicated layers and has complex functionalities and liabilities.
- This Layer hides the details of underlying hardware and represents itself to upper layer as the medium to communicate.
- Data link layer works between two hosts which are directly connected in some sense. This direct connection could be point to point or broadcast.
- Data link layer is responsible for converting data stream to signals bit by bit and to send that over the underlying hardware.
- Data Link Layer is second layer of OSI Layered Model.
- At the receiving end, Data link layer picks up data from hardware which are in the form of electrical signals, assembles them in a recognizable frame format, and hands over to upper layer.

Data Link Layer Design Issues

- The data link layer uses the services of the physical layer to send and receive bits over communication channels.
- It has a number of functions, including:

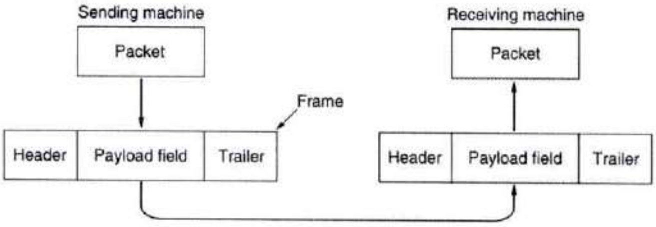
  1. Providing a well-defined service interface to the network layer.

  2. Dealing with transmission errors.

  3. Regulating the flow of data so that slow receivers are not swamped by fast senders.

- To accomplish these goals, the data link layer takes the packets it gets from the network layer and encapsulates them into frames for transmission.
- Each frame contains a frame header, a payload field for holding the packet, and a frame trailer.
- Frame management forms the heart of what the data link layer does.

Relationship between Packet and Frame



Data link layer and its sub-layers:

Data link layer has two sub-layers:

1. **Logical Link Control:** It deals with protocols, flow-control, and error control
2. **Media Access Control:** It deals with actual control of media

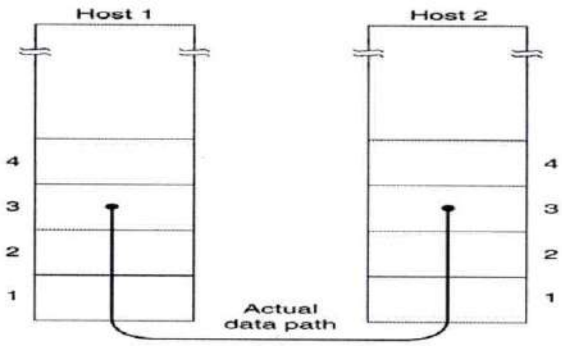
Functionality of Data-link Layer

- **Services provided to the Network Layer:** The function of the data link layer is to provide services to the network layer
- **Framing:**Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.
- **Addressing:** Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.
- **Synchronization:** When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.
- **Flow Control:** Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machine to exchange data on same speed.
- **Multi-Access:** When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.
- **Error Control:** Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

Services Provided to the Network Layer

❑ The principal service is transferring data from the network layer on the source machine to the network layer on the destination machine.

❑ On the source machine, a process, in the network layer that hands some bits to the data link layer for transmission to the destination. The job of the data link layer is to transmit the bits to the destination machine so they can be handed over to the network layer there.



(b)

The data link layer can be designed to offer various services

1. **Unacknowledged connectionless service:** Unacknowledged connectionless service consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them.

2. **Acknowledged connectionless service**: When this service is offered, there are still no logical connections used, but each frame sent is individually acknowledged. In this way, the sender knows whether a frame has arrived correctly or been lost.

3. **Acknowledged connection-oriented service**: With this service, the source and destination machines establish a connection before any data are transferred. Each frame sent over the connection is numbered, and the data link layer guarantees that each frame sent is indeed received. Furthermore, it guarantees that each frame is received exactly once and that all frames are received in the right order.

FRAMING

To provide service to the network layer, the data link layer must use the service provided to it by the physical layer. Data Link Layer accepts a raw bit stream from physical layer and arranges them into frames before attempt to deliver it to the destination

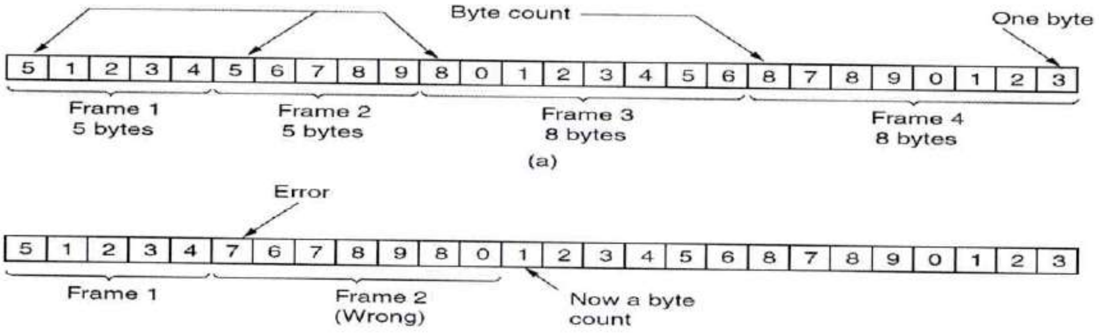
- The process of Breaking up the bit stream into discrete messages is called framing
- The usual approach is for the data link layer to break up the bit stream into discrete frames, compute a short token called a checksum for each frame, and include the checksum in the frame when it is transmitted.
- When a frame arrives at the destination, the checksum is recomputed. If the newly computed checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and takes steps to deal with it.

FRAMING METHODS

1. Byte count.
2. Flag bytes with byte stuffing.
3. Flag bits with bit stuffing.
4. Physical layer coding violations.

1. Byte count:

- The first framing method uses a field in the header to specify the number of bytes in the frame. When the data link layer at the destination sees the byte count, it knows how many bytes follow and hence where the end of the frame is.
- For four small example frames of sizes 5, 5, 8, and 8 bytes, respectively.

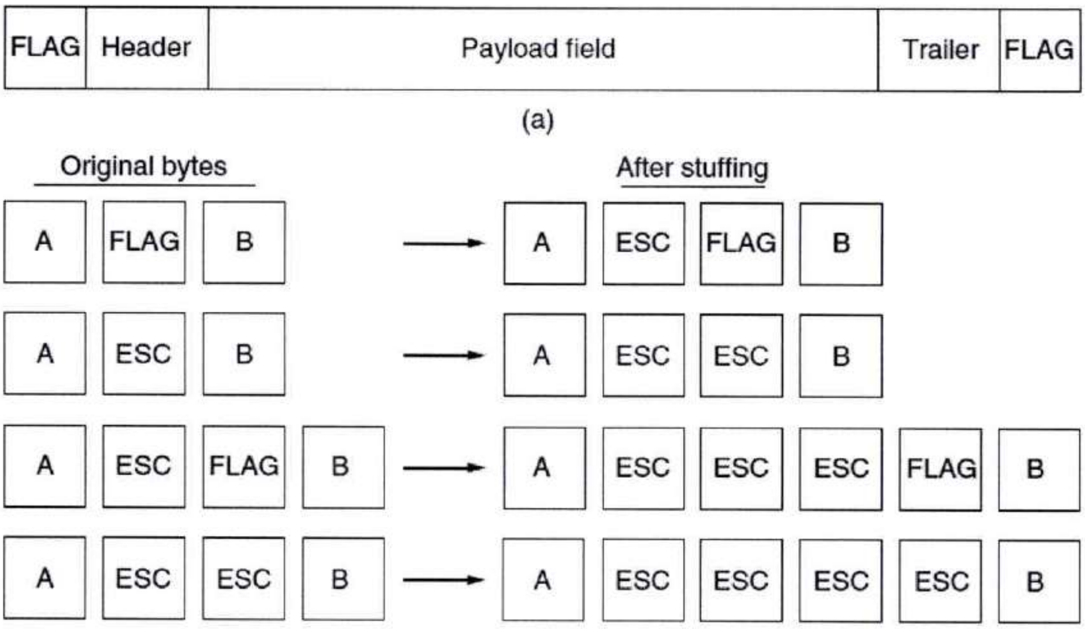


The trouble with Byte count:

- The trouble with this algorithm is that the count can be garbled by a transmission error. For example, if the byte count of 5 in the second frame becomes a 7 due to a single bit flip, the destination will get out of synchronization. It will then be unable to locate the correct start of the next frame.
- Even if the checksum is incorrect so the destination knows that the frame is bad, it still has no way of telling where the next frame starts.
- Sending a frame back to the source asking for a retransmission does not help either, since the destination does not know how many bytes to skip over to get to the start of the retransmission. For this reason, the byte count method is rarely used by itself.

2. Flag bytes with byte stuffing

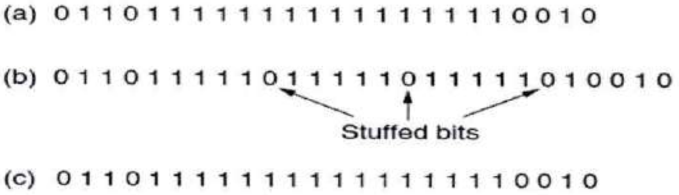
- Here a flag byte, is used as both the starting and ending delimiter. Two consecutive flag bytes indicate the end of one frame and the start of the next. Thus, if the receiver ever loses synchronization it can just search for two flag bytes to find the end of the current frame and the start of the next frame.
- A problem we have to solve is it may happen that the flag byte occurs in the data, especially when binary data such as photographs or songs are being transmitted. This situation would interfere with the framing.
- One way to solve this problem is to have the sender's data link layer insert a special escape byte (ESC) just before each ''accidental'' flag byte in the data. Thus, a framing flag byte can be distinguished from one in the data by the absence or presence of an escape byte before it.
- The data link layer on the receiving end removes the escape bytes before giving the data to the network layer. This technique is called byte stuffing.



3. Flag bits with bit stuffing

- In this method each frame begins and ends with a special bit pattern, 01111110. This pattern is a flag byte.
- Whenever the sender's data link layer encounters five consecutive 1s in the data, it Automatically stuffs a 0 bit into the outgoing bit stream.
- This bit stuffing is analogous to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data. It also ensures a minimum density of transitions that help the physical layer maintain synchronization. USB (Universal Serial Bus) uses bit stuffing for this reason.
- When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, It automatically de-stuffs (i.e., deletes) the 0 bit.
- If the user data contain the flag pattern, 01111110, this flag is transmitted as 011111010 but stored in the receiver's memory as 01111110.
- With bit stuffing, the boundary between two frames can be unambiguously recognized by the flag pattern. Thus, if the receiver loses track of where it is, all it has to do is scan the input for flag sequences, since they can only occur at frame boundaries and never within the data.

THE DATA LINK LAYER


(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0
(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0
Stuffed bits
(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

Bit stuffing. (a) The original data. (b) The data as they appear on the line. (c) The data as they are stored in the receiver's memory after destuffing.

Disadvantages of Byte/Bit Stuffing

- With both bit and byte stuffing, a side effect is that the length of a frame now depends on the contents of the data it carries.
- For instance, if there are no flag bytes in the data, 100 bytes might be carried in a frame of roughly 100 bytes. If, however, the data consists solely of flag bytes, each flag byte will be escaped and the frame will become roughly 200 bytes long.
- With bit stuffing, the increase would be roughly 12.5% as 1 bit is added to every byte.

4. Physical layer coding violations

- The final framing method is physical layer coding violations and is applicable to networks in which the encoding on the physical medium contains some redundancy.
- In such cases normally, a 1 bit is a high-low pair and a 0 bit is a low-high pair.
- The combinations of low-low and high-high which are not used for data may be used for marking frame boundaries.

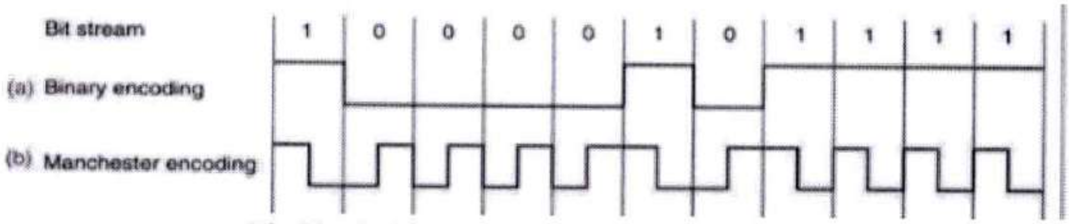


Fig:Physical layer coding violations

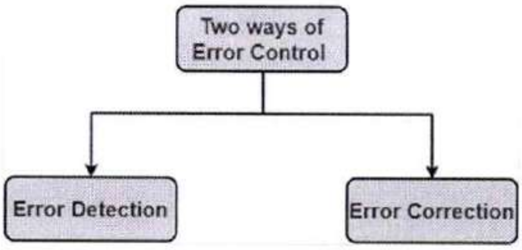
Error Control

Error control is basically process in data link layer of detecting or identifying and re-transmitting data frames that might be lost or corrupted during transmission. The usual way to ensure reliable delivery is to provide the sender with some feedback about what is happening at the other end of the line. Typically, the protocol calls for the receiver to send back special control frames bearing positive or negative acknowledgements about the incoming frames. If the sender receives a positive acknowledgement about a frame, it knows the frame has arrived safely. On the other hand, a negative acknowledgement means that something has gone wrong and the frame must be transmitted again.

The issues with transmission are either hardware error or acknowledgement packet may lost, in this case the sender may wait for acknowledgement or tries to retransmit the same packet. The solution for this is managing the timers and sequence numbers so as to ensure that each frame is ultimately passed to the network layer at the destination exactly once, no more and no less, is an important part of the duties of the data link layer.

Ways of doing Error Control:

There are basically two ways of doing Error control as given below.



1.Error Detection: Error detection, as name suggests, simply means detection or identification of errors. These errors may cause due to noise or any other impairments during transmission from transmitter to the receiver, in communication system. It is class of technique for detecting garbled i.e. unclear and distorted data or message.

2.Error Correction: Error correction, as name suggests, simply means correction or solving or fixing of errors. It simply means reconstruction and rehabilitation of original data that is error-free. But error correction method is very costly and is very hard.

Error Detection and Error Correction

- **Error**: A condition when the receiver's information does not match with the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.
- **Error Detecting Codes**: Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message. Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors

The process of identifying transmission errors is called Error Detection. Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use **error-detecting** codes.

Some popular techniques for error detection are:

1. Simple Parity check
2. Two-dimensional Parity check
3. Checksum
4. Cyclic redundancy check

These techniques are used for only error detection, for Error correction a concept called Hamming Codes will be used.

Simple Parity check

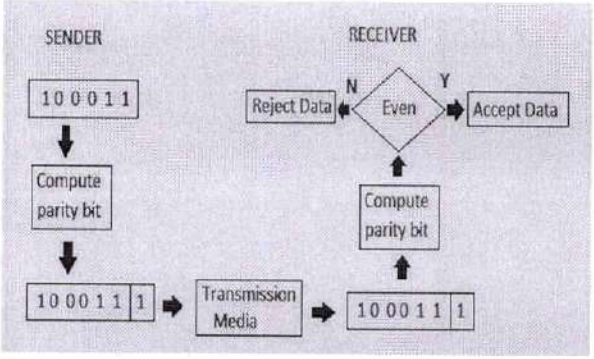
Blocks of data from the source are subjected to a check its parity

Where a parity of:

- 1 is added to the block if it contains odd number of 1's, and
- 0 is added if it contains even number of 1's

- This scheme makes the total number of 1's even, that is why it is called even parity checking.

How Even Parity Works



Simple Parity Check Advantages

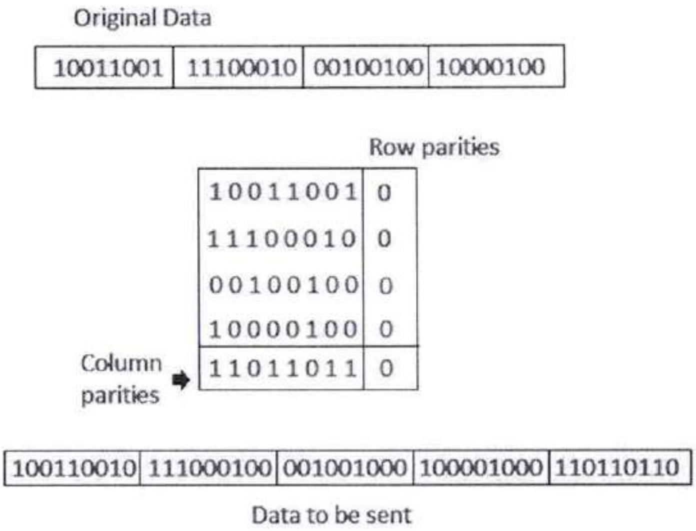
- Less Expensive i.e. provides better channel utilization or efficiency . Efficiency=(n/n+1)*100.
- Can detect one bit Errors
- **Transmission efficiency is defined** as the total number of information bits (i.e., bits in the message sent by the user) divided by the total bits in transmission (i.e., information bits plus overhead bits). For example, let's calculate the transmission efficiency of 7-bit ,We have 1 bit for parity. Therefore, there are 7 bits of information in each letter, but the total bits per letter is 10 (7 + 1). The efficiency of the simple parity check is, 7 bits of information divided by 8 total bits, or 87 percent.

Disadvantages:

- Can't able to detect multiple bit errors
- Can't detect location of the erroneous bit
- Can't do any corrections in fact only used for error detection.

Two-dimensional Parity check

- Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end these are compared with the parity bits calculated on the received data.
- It can detect up to **3** bit errors but not suitable to find **4** bit errors.



Original Data

10011001	11100010	00100100	10000100

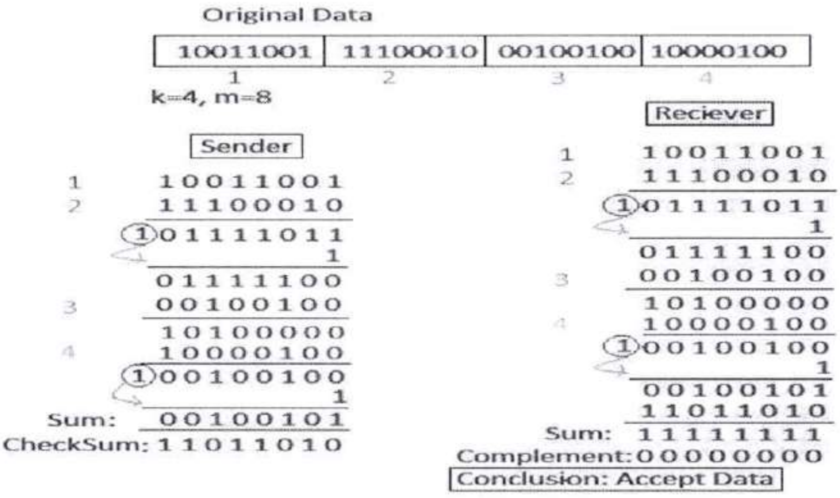
		Row parities
	10011001	0
	11100010	0
	00100100	0
	10000100	0
Column parities	11011011	0

100110010	111000100	001001000	100001000	110110110

Data to be sent

Checksum

- Checksum is the calculated summery of the data portion.
- In checksum error detection scheme, the data is divided into k segments each of m bits.
- In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.
- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.



Original Data

10011001	11100010	00100100	10000100
1	2	3	4

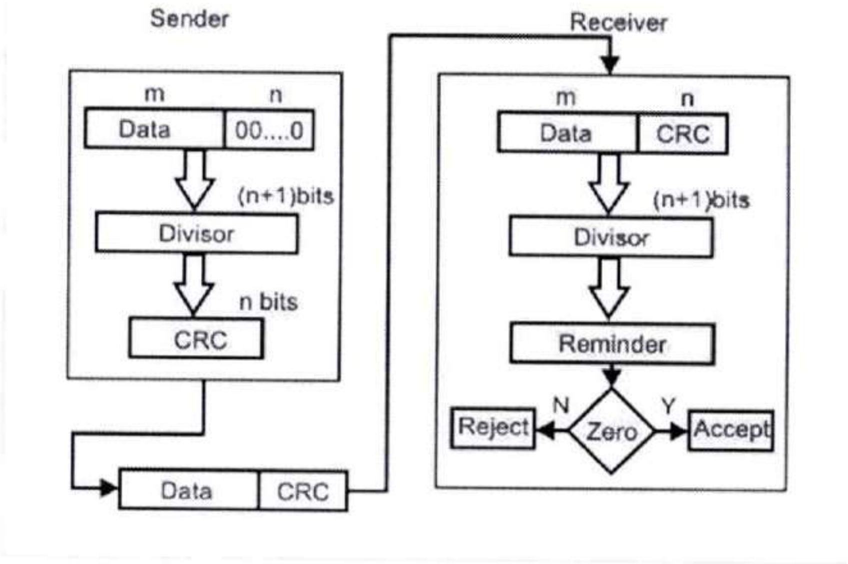
k=4, m=8

```
        Sender                              Reciever
                                       1     10011001
1         10011001                     2     11100010
2         11100010                          (1)01111011
         (1)01111011                                  1
                   1                          01111100
          01111100                     3      00100100
3         00100100                            10100000
          10100000                     4      10000100
4         10000100                          (1)00100100
         (1)00100100                                  1
                   1                          00100101
Sum:      00100101                            11011010
CheckSum: 11011010                     Sum:   11111111
                              Complement:00000000
                              Conclusion: Accept Data
```

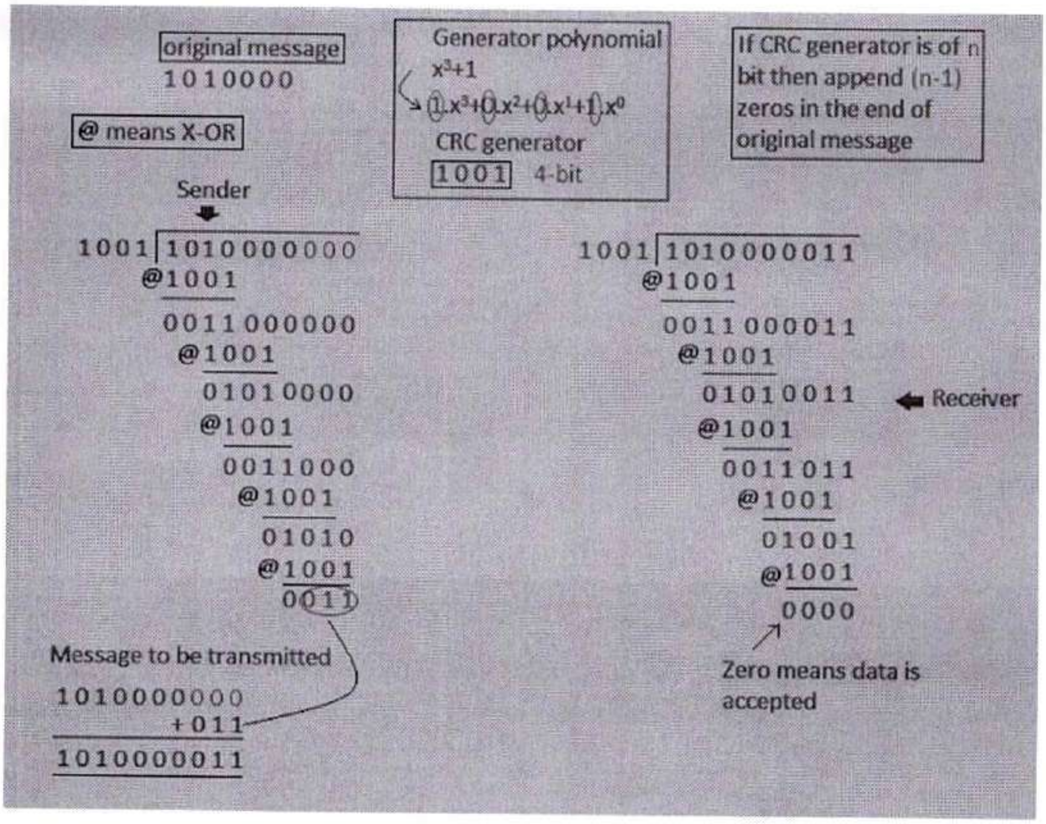
Cyclic redundancy check (CRC)

- Unlike checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.

- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



Example:



original message
1010000

@ means X-OR

Generator polynomial
x^3+1
$1.x^3+0.x^2+0.x^1+1.x^0$
CRC generator
1001 4-bit

If CRC generator is of n bit then append (n-1) zeros in the end of original message

Sender

```
1001|1010000000
     @1001
      0011000000
        @1001
         01010000
         @1001
          0011000
            @1001
             01010
             @1001
              0011
```

Message to be transmitted

```
1010000000
      +011
1010000011
```

Receiver

```
1001|1010000011
     @1001
      0011000011
        @1001
         01010011
         @1001
          0011011
            @1001
             01001
             @1001
              0000
```

Zero means data is accepted

Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)
Vignan's Institute of Management & Technology For Women

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

Error Correction

Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.Error Correction can be handled in two ways:

- **Backward error correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
- **Forward error correction:** In this case, the receiver uses the error-correcting code which automatically corrects the errors.

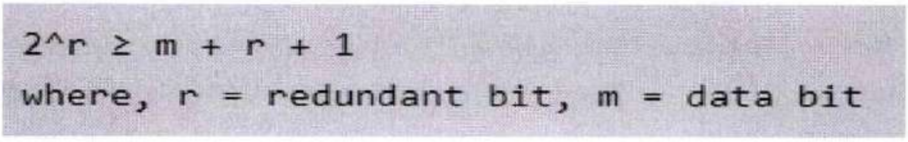
The four different error-correcting codes: 1. Hamming codes. 2. Binary convolutional codes. 3. Reed-Solomon codes. 4. Low-Density Parity Check codes.

Hamming Code

- Whenever a data packet is transmitted over a network, there are possibilities that the data bits may get lost or damaged during transmission.
- The hamming code technique, which is an error-detection and error-correction technique, was proposed by R.W. Hamming.
- Hamming code is a Forward error correction Technique.

Redundant bits

- Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer.
- The number of redundant bits can be calculated using the following formula:



```
2^r ≥ m + r + 1
where, r = redundant bit, m = data bit
```

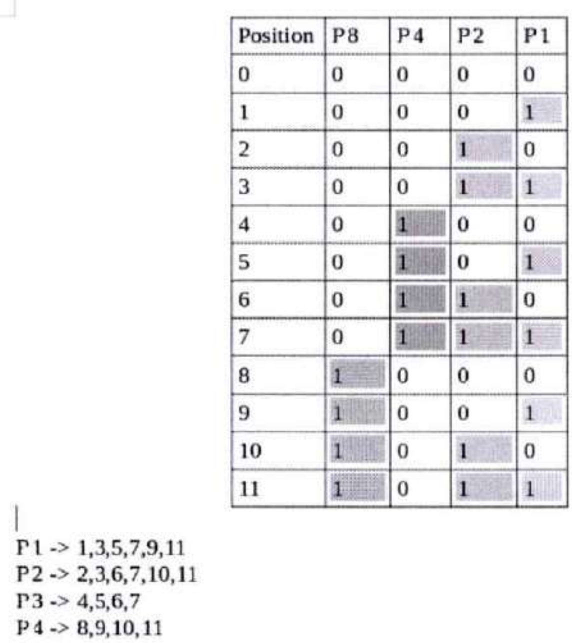
- Suppose the number of data bits is 7, then the number of redundant bits can be calculated using: = 2^4 ≥ 7 + 4 + 1;Thus, the number of redundant bits= 4

General Algorithm of Hamming code

- Write the bit positions starting from 1 in binary form
- All the bit positions that are a power of 2 are marked as parity bits (1, 2, 4, 8, etc).
- All the other bit positions are marked as data bits.
- Each data bit is included in a unique set of parity bits, as determined its bit position in binary form.
- Parity bit 1 covers all the bits positions whose binary representation includes a 1 in the least significant position (1, 3, 5, 7, 9, 11, etc).**(CHECK ONE-SKIP ONE)**

- Parity bit 2 covers all the bits positions whose binary representation includes a 1 in the second position from the least significant bit (2, 3, 6, 7, 10, 11, etc). **(CHECK TWO –SKIP TWO)**
- Parity bit 4 covers all the bits positions whose binary representation includes a 1 in the third position from the least significant bit (4–7, 12–15, 20–23, etc).**(CHECK FOUR-SKIP FOUR)**
- Parity bit 8 covers all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit bits (8–15, 24–31, 40–47, etc).**(CHEK EIGHT- SKIP EIGHT)**
- Since we check for even parity set a parity bit to 1 if the total number of ones in the positions it checks is odd.
- Set a parity bit to 0 if the total number of ones in the positions it checks is even.

Setting the value of Parity Bit



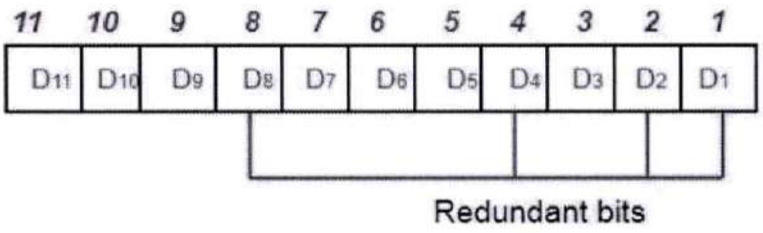
Position	P8	P4	P2	P1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0
11	1	0	1	1

P1 -> 1,3,5,7,9,11
P2 -> 2,3,6,7,10,11
P3 -> 4,5,6,7
P4 -> 8,9,10,11

Determining the position of redundant bits

These redundancy bits are placed at the positions which correspond to the power of 2. As in the above example:

- ❖ The number of data bits = 7
- ❖ The number of redundant bits = 4
- ❖ The total number of bits = 11
- ❖ The redundant bits are placed at positions corresponding to power of 2- 1, 2, 4, and 8

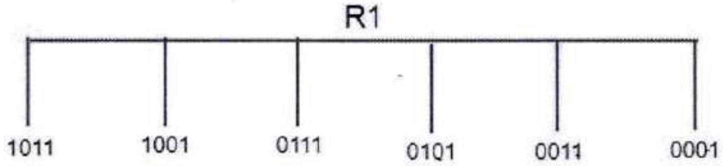


Suppose the data to be transmitted is 1011001, the bits will be placed as follows:

11	10	9	8	7	6	5	4	3	2	1
1	0	1	R8	1	0	0	R4	1	R2	R1

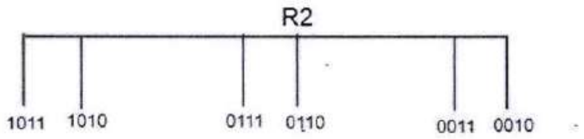
Determining the Parity bits

- ▶ R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position.R1: bits 1, 3, 5, 7, 9, 11



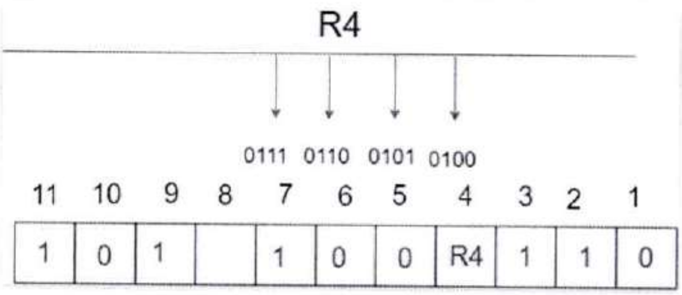
11	10	9	8	7	6	5	4	3	2	1
1	0	1		1	0	0		1		R1

- ▶ To find the redundant bit R1, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R1 is an even number the value of R1 (parity bit's value) = 0
- ▶ R2 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the second position from the least significant bit.R2: bits 2,3,6,7,10,11



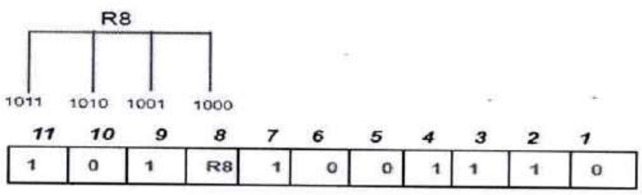
11	10	9	8	7	6	5	4	3	2	1
1	0	1		1	0	0		1	R2	0

- ▶ To find the redundant bit R2, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R2 is odd the value of R2(parity bit's value)=1
- ▶ R4 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the third position from the least significant bit.R4: bits 4, 5, 6, 7



11	10	9	8	7	6	5	4	3	2	1
1	0	1		1	0	0	R4	1	1	0

- ▶ To find the redundant bit R4, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R4 is odd the value of R4(parity bit's value) = 1
- ▶ R8 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit.R8: bit 8,9,10,11



11	10	9	8	7	6	5	4	3	2	1
1	0	1	R8	1	0	0	1	1	1	0

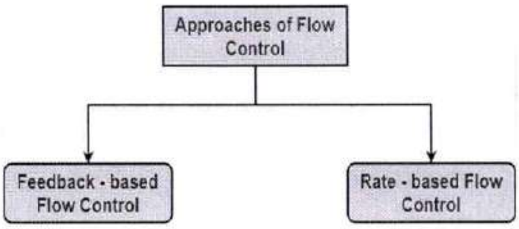
- ▶ To find the redundant bit R8, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R8 is an even number the value of R8(parity bit's value)=0.

11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	1	0	0	1	1	1	0

Flow Control

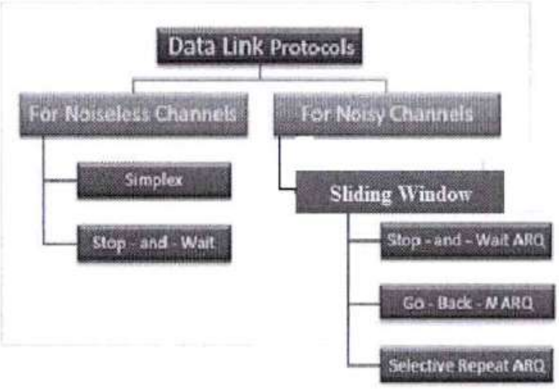
- **Flow control** is design issue at Data Link Layer. It is technique that generally observes proper flow of data from sender to receiver. It regulates speed of delivery and so that a fast sender does not drown a slow receiver.
- **Flow control** is basically technique that gives permission to two of stations that are working and processing at different speeds to just communicate with one another.
- **Flow control** in Data Link Layer simply restricts sender and coordinates number of frames can send just before it waits for an acknowledgment from receiver.

Approaches to Flow Control


Approaches of Flow Control
Feedback - based Flow Control
Rate - based Flow Control

- **Feedback – based Flow Control:**In this technique, sender simply transmits data to receiver, then receiver transmits data back to sender and also allows sender to transmit more amount of data. This simply means that sender transmits data or frames after it has received acknowledgments from user.
- **Rate – based Flow Control:**In this technique, usually when sender sends data at faster speed to receiver and receiver is not being able to receive data at the speed, then the built-in mechanism in protocol will just limit overall rate at which data is being transferred by sender without any feedback or acknowledgment from receiver.

Feedback-based flow control schemes offered by Data Link Layer are



Utopian Simplex Protocol

- The Simplex protocol is hypothetical protocol designed for unidirectional data transmission over an ideal channel, i.e. a channel through which transmission can never go wrong.
- It has distinct procedures for sender and receiver. The sender simply sends all its data available onto the channel as soon as they are available with its buffer.
- The receiver is assumed to process all incoming data instantly.
- It is hypothetical since it does not handle flow control or error control. It's also called as **utopian**(good place/ideal) protocol.

Stop-and-Wait Flow Control for Noiseless Channels.

This method is the easiest and simplest form of flow control. In this method, basically message or data is broken down into various multiple frames, and then receiver indicates its readiness to receive frame of data. It works under the following assumptions-

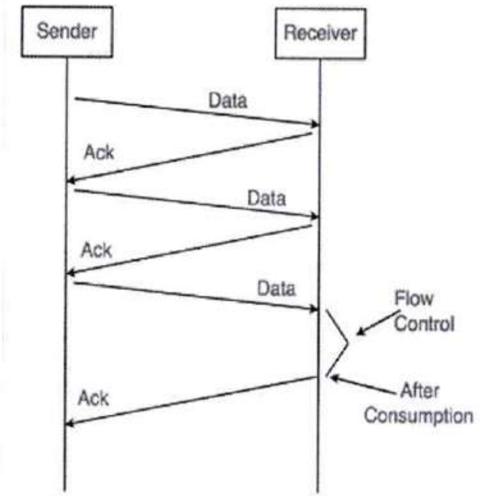
- Communication channel is perfect.

- No error occurs during transmission.

Working of Stop and wait Flow Control:

- Sender sends a data packet to the receiver.
- Sender stops and waits for the acknowledgement for the sent packet from the receiver.
- Receiver receives and processes the data packet.
- Receiver sends an acknowledgement to the sender.
- After receiving the acknowledgement, sender sends the next data packet to the receiver.

This process is continued until sender transmits EOT (End of Transmission) frame. In this method, only one of frames can be in transmission at a time. It leads to inefficiency i.e. less productivity if propagation delay is very much longer than the transmission delay.



The above figure shows the working of the stop and wait protocol. If there is a sender and receiver, then sender sends the packet and that packet is known as a data packet. The sender will not send the second packet without receiving the acknowledgment of the first packet. The receiver sends the acknowledgment for the data packet that it has received. Once the acknowledgment is received, the sender sends the next packet. This process continues until all the packet are not sent. The main advantage of this protocol is its simplicity but it has some disadvantages also. For example, if there are 1000 data packets to be sent, then all the 1000 packets cannot be sent at a time as in Stop and Wait protocol, one packet is sent at a time.

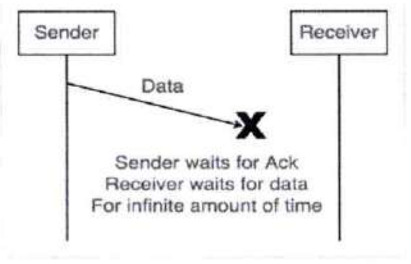
Advantages –

- This method is very easiest and simple and each of the frames is checked and acknowledged well.
- It can also be used for noisy channels.
- This method is also very accurate.

Disadvantages –

- This method is fairly slow.
- In this, only one packet or frame can be sent at a time.
- It is very inefficient and makes the transmission process very slow.
- In stop and wait protocol lost data packet, lost acknowledgement and delayed acknowledgement would causes performance issues.

1. Problems occur due to lost data



Suppose the sender sends the data and the data is lost. The receiver is waiting for the data for a long time. Since the data is not received by the receiver, so it does not send any acknowledgment. Since the sender does not receive any acknowledgment so it will not send the next packet. This problem occurs due to the lost data.

In this case, two problems occur:

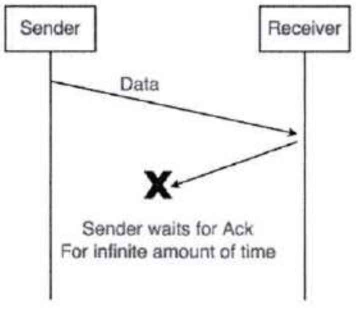
- Sender waits for an infinite amount of time for an acknowledgment.
- Receiver waits for an infinite amount of time for a

2. Problems occur due to lost acknowledgment

Suppose the sender sends the data and it has also been received by the receiver. On receiving the packet, the receiver sends the acknowledgment. In this case, the acknowledgment is lost in a network, so there is no chance for the sender to receive the acknowledgment. There is also no chance for the sender to send the next packet as in stop and wait protocol, the next packet cannot be sent until the acknowledgment of the previous packet is received.

In this case, one problem occurs:

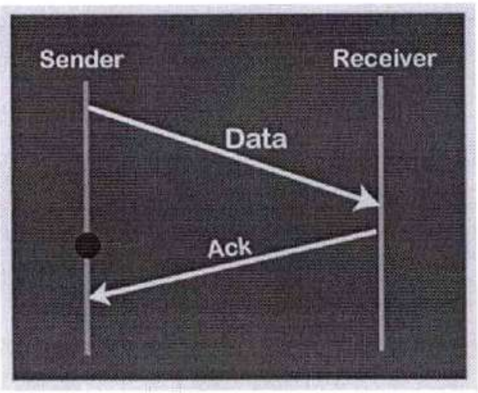
- Sender waits for an infinite amount of time for an acknowledgment.



3. Problem due to the delayed data or acknowledgment

Suppose the sender sends the data and it has also been received by the receiver. The receiver then sends the acknowledgment but the acknowledgment is received after the timeout period on the sender's side. As the acknowledgment is received late, so acknowledgment can be wrongly considered as the acknowledgment of some other or previously sent data packet.

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State



Stop – and – Wait ARQ for Noisy Channel

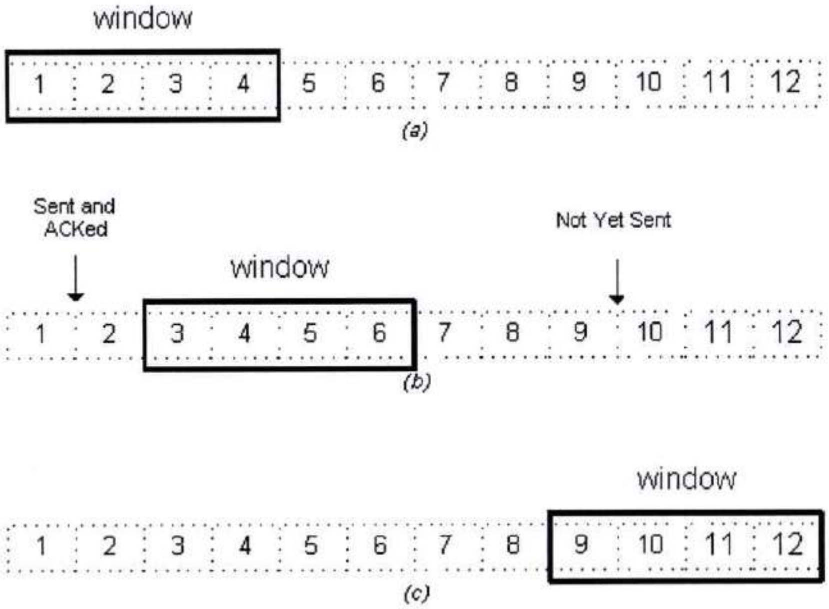
- Stop – and – wait Automatic Repeat Request (Stop – and – Wait ARQ) is a variation of the stop-and-wait protocol with added error control mechanisms, appropriate for noisy channels.
- The sender keeps a copy of the sent frame. It then waits for a finite time to receive a positive acknowledgement from receiver. If the timer expires or a negative acknowledgement is received, the frame is retransmitted.
- If a positive acknowledgement is received then the next frame is sent.

Sliding Window Protocols:

In spite of the use of timers, the stop and wait protocol still suffers from a few drawbacks. Firstly, if the receiver had the capacity to accept more than one frame, its resources are being underutilized. Secondly, if the receiver was busy and did not wish to receive any more packets, it may delay the acknowledgement. However, the timer on the sender's side may go off and cause an unnecessary retransmission. These drawbacks are overcome by the sliding window protocols.

- In sliding window protocols the sender's data link layer maintains a 'sending window' which consists of a set of sequence numbers corresponding to the frames it is permitted to send.
- Similarly, the receiver maintains a 'receiving window' corresponding to the set of frames it is permitted to accept.
- The window size is dependent on the retransmission policy and it may differ in values for the receiver's and the sender's window.
- The sequence numbers within the sender's window represent the frames sent but as yet not acknowledged.
- Whenever a new packet arrives from the network layer, the upper edge of the window is advanced by one. When an acknowledgement arrives from the receiver the lower edge is advanced by one.
- The receiver's window corresponds to the frames that the receiver's data link layer may accept. When a frame with sequence number equal to the lower edge of the window is received, it is passed to the network layer, an acknowledgement is generated and the window is rotated by one.

- If however, a frame falling outside the window is received, the receiver's data link layer has two options. It may either discard this frame and all subsequent frames until the desired frame is received or it may accept these frames and buffer them until the appropriate frame is received and then pass the frames to the network layer in sequence.



(a)

(b)

(c)

In this simple example, there is a 4-byte sliding window. Moving from left to right, the window "slides" as bytes in the stream are sent and acknowledged. Sliding window offers **piggybacking**, in two-way communication, whenever a frame is received, the receiver waits and does not send the control frame (acknowledgement or ACK) back to the sender immediately. This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as **piggybacking.** It is used to improve the efficiency of the bidirectional protocols. The major advantage of piggybacking is better use of available channel bandwidth, and the disadvantage of piggybacking is additional complexity and If the data link layer waits too long before transmitting the acknowledgement, then re-transmission of frame would take place.

Advantages –

- It performs much better than stop-and-wait flow control.
- This method increases efficiency.
- Multiples frames can be sent one after another.

Disadvantages –

- The main issue is complexity at the sender and receiver due to the transferring of multiple frames.
- The receiver might receive data frames or packets out the sequence.

Go Back 'n' and Selective Repeat ARQ

In the stop-and-wait protocol, the sender can send only one frame at a time and cannot send the next frame without receiving the acknowledgment of the previously sent frame, whereas, in the case of sliding window protocol, the multiple frames can be sent at a time. Most sliding window protocols also employ ARQ (Automatic Repeat reQuest) mechanism. In ARQ, the sender waits for a positive acknowledgement before proceeding to the next frame. If no acknowledgement is received within a certain time interval it retransmits the frame. The variations of sliding window protocol are Go-Back-N ARQ and Selective Repeat ARQ.

ARQ is of two types:

1. **Go Back 'n':**

In Go-Back-N ARQ, **N** is the sender's window size. Suppose we say that Go-Back-3, which means that the three frames can be sent at a time before expecting the acknowledgment from the receiver. It uses the principle of protocol pipelining in which the multiple frames can be sent before receiving the acknowledgment of the first frame. If we have five frames and the concept is Go-Back-3, which means that the three frames can be sent, i.e., frame no 1, frame no 2, frame no 3 can be sent before expecting the acknowledgment of frame no 1. In Go-Back-N ARQ, the frames are numbered sequentially as Go-Back-N ARQ sends the multiple frames at a time that requires the numbering approach to distinguish the frame from another frame, and these numbers are known as the sequential numbers. The number of frames that can be sent at a time totally depends on the size of the sender's window. So, we can say that 'N' is the number of frames that can be sent at a time before receiving the acknowledgment from the receiver. If the acknowledgment of a frame is not received within an agreed-upon time period, then all the frames available in the current window will be retransmitted. Suppose we have sent the frame no 5, but we didn't receive the acknowledgment of frame no 5, and the current window is holding three frames, then these three frames will be retransmitted.

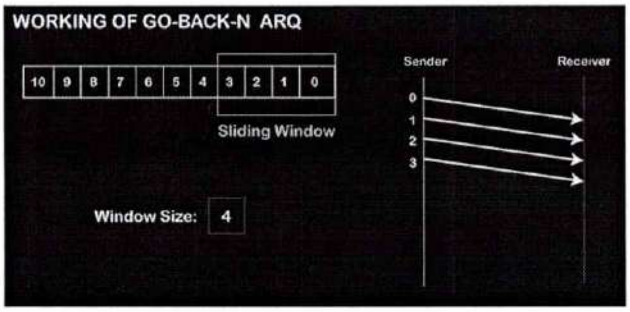
- The sequence number of the outbound frames depends upon the size of the sender's window. N is the sender's window size.
- If the size of the sender's window is 4 then the sequence number will be 0,1,2,3,0,1,2,3,0,1,2, and so on.

The number of bits in the sequence number is 2 to generate the binary sequence 00,01,10,11.

Working of Go-Back-N ARQ

Suppose there are a sender and a receiver, and let's assume that there are 11 frames to be sent. These frames are represented as 0,1,2,3,4,5,6,7,8,9,10, and these are the sequence numbers of the frames. Let's consider the window size as 4, which mean that the four frames can be sent at a time before expecting the acknowledgment of the first frame.

Firstly, the sender will send the first four frames to the receiver, i.e., 0,1,2,3, and now the sender is expected to receive the acknowledgment of the 0^{th} frame.



CN-UNIT - III

Network Layer: Design issues, Routing algorithms: shortest path routing, Flooding, Hierarchical routing, Broadcast, Multicast, distance vector routing, Congestion Control Algorithms, Quality of Service, Internetworking, the Network layer in the internet.

Introduction to Network Layer

- The Network Layer is the third layer of the OSI model.
- It handles the service requests from the transport layer and further forwards the service request to the data link layer.
- The network layer translates the logical addresses into physical addresses
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- The main role of the network layer is to move the packets from sending host to the receiving host.

Network layer design issues

1. **Store-and-Forward Packet Switching:** Store and forward is a data communication technique in which a message transmitted from a source node is stored at an intermediary device before being forwarded to the destination node.
2. **Services provided to the Transport Layer:** The network layer provides services to the transport layer at the network layer/transport layer interface.But before providing these services to the transfer layer following goals must be kept in mind.

- Offering services must not depend on router technology.
- The transport layer needs to be protected from the type, number and topology of the available router.
- The network addresses for the transport layer should use uniform numbering pattern also at LAN and WAN connections.
- Based on the connections there are 2 types of services provided :
- Connectionless – The routing and insertion of packets into subnet is done individually. No added setup is required.
- Connection-Oriented – Subnet must offer reliable service and all the packets must be transmitted over a single route.

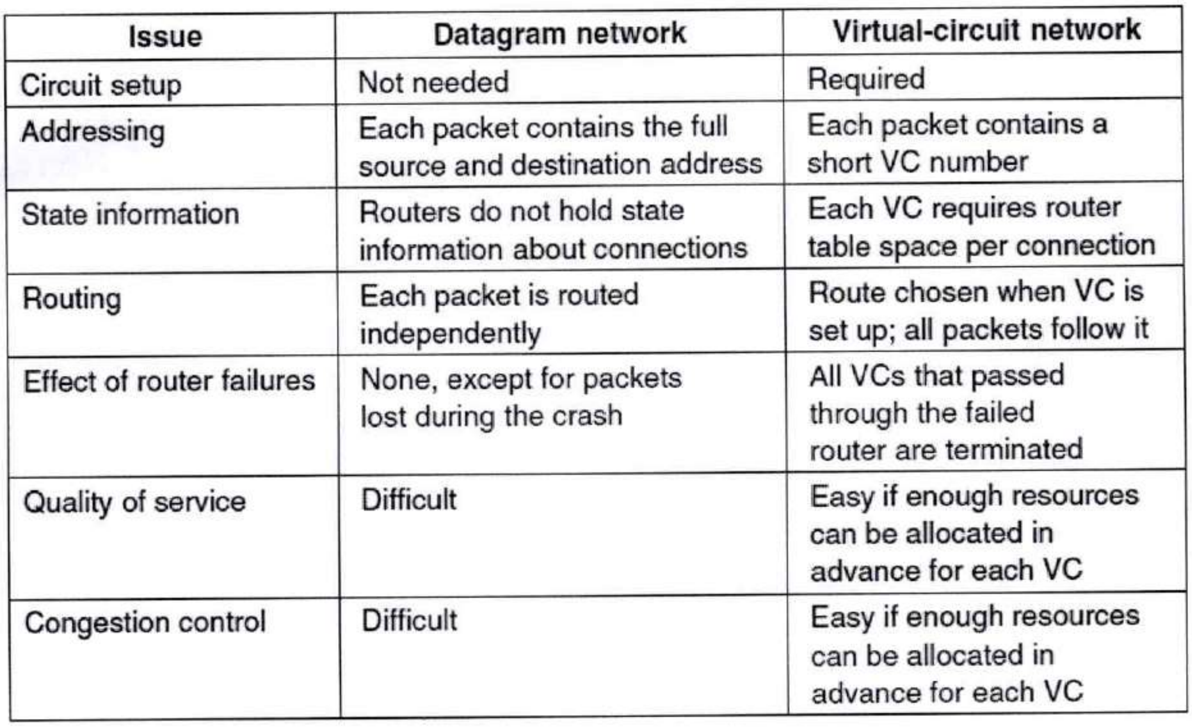
3. Implementation of Connectionless Service:

- If connectionless service is offered, packets are injected into the network individually and routed independently of each other.
- No advance setup is needed. In this context, the packets are frequently called **datagrams** and the network is called a **datagram network.**

4. **Implementation of Connection-Oriented Service:**

- If connection-oriented service is used, a path from the source router all the way to the destination router must be established before any data packets can be sent.
- This connection is called a **VC (virtual circuit),** and the network is called a **virtual-circuit network.**
- To use a connection-oriented service, first we establishes a connection, use it and then release it.
- In connection-oriented services, the data packets are delivered to the receiver in the same order in which they have been sent by the sender.
- With connection-oriented service, each packet carries an identifier telling which virtual circuit it belongs to.

Comparison of Virtual-Circuit and Datagram Networks



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

Classification of Routing Algorithms

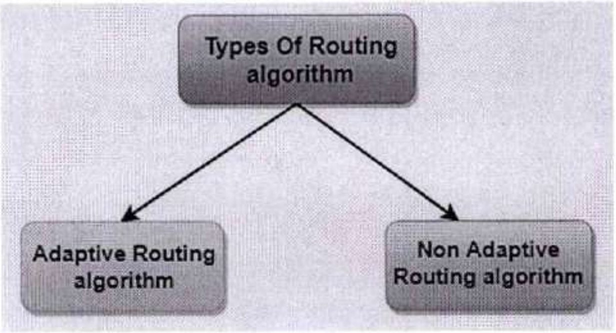
- **Routing** is process of establishing the routes that data packets must follow to reach the destination. In this process, a routing table is created which contains information regarding routes which data packets follow.

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

- Various routing algorithm are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach destination efficiently.

Classification of Routing Algorithms: The routing algorithms can be classified as follows:


Types Of Routing algorithm
Adaptive Routing algorithm
Non Adaptive Routing algorithm

1. Adaptive Algorithms: These are the algorithms which change their routing decisions whenever network topology or traffic load changes. The changes in routing decisions are reflected in the topology as well as traffic of the network. Also known as dynamic routing, these make use of dynamic information such as current topology, load, delay, etc. to select routes. Optimization parameters are distance, number of hops and estimated transit time.
Further these are classified as follows:

- **(a) Isolated –** In this method each, node makes its routing decisions using the information it has without seeking information from other nodes. The sending nodes doesn't have information about status of particular link. Disadvantage is that packet may be sent through a congested network which may result in delay.

- **(b) Centralized –** In this method, a centralized node has entire information about the network and makes all the routing decisions. Advantage of this is only one node is required to keep the information of entire network and disadvantage is that if central node goes down the entire network is done. Link state algorithm is referred to as a global algorithm since it is aware of the cost of each link in the network.

- **(c) Distributed –** In this method, the node receives information from its neighbours and then takes the decision about routing the packets. Disadvantage is that the packet may be delayed if there is change in between interval in which it receives information and sends packet. It is also known as decentralized algorithm as it computes the least-cost path between source and destination

2. Non-Adaptive Algorithms –

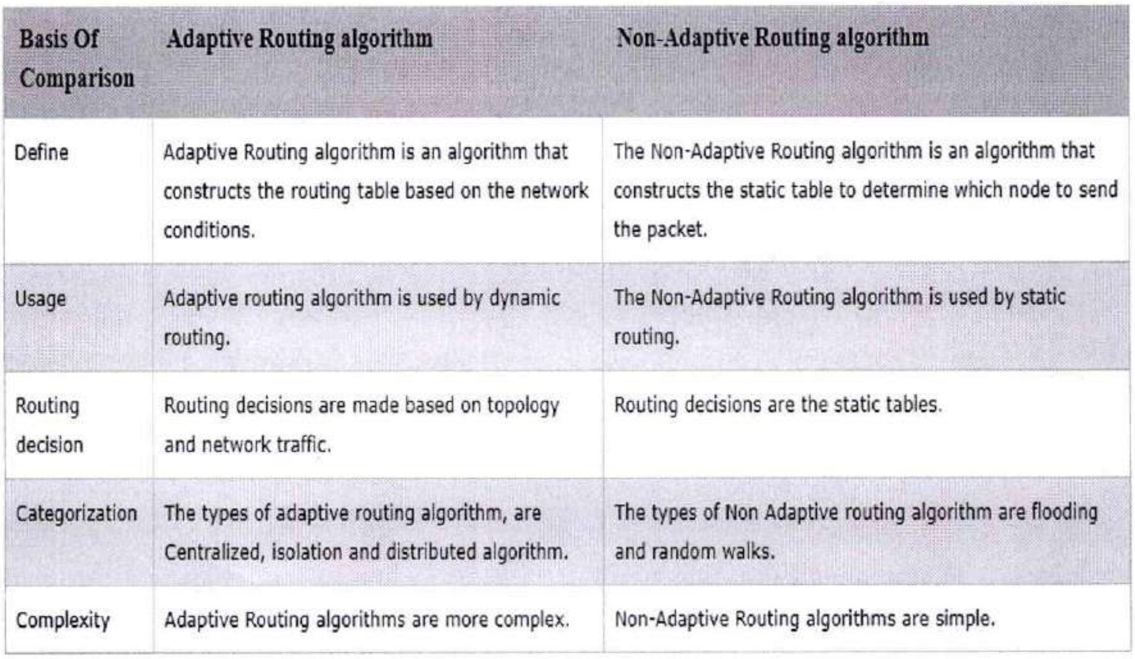
These are the algorithms which do not change their routing decisions once they have been selected. This is also known as static routing, as route to be taken is computed in advance and downloaded to routers when router is booted.

Further these are classified as follows:

- **(a) Flooding –** This adapts the technique in which every incoming packet is sent on every outgoing line except from which it arrived. One problem with this is that packets may go in loop and as a result of which a node may receive duplicate packets. These problems can be overcome with the help of sequence numbers, hop count and spanning tree.

- **(b) Random walk** – In this method, packets are sent host by host or node by node to one of its neighbours randomly. This is highly robust method which is usually implemented by sending packets onto the link which is least queued.

Differences b/w Adaptive and Non-Adaptive Routing Algorithm



Basis Of Comparison	Adaptive Routing algorithm	Non-Adaptive Routing algorithm
Define	Adaptive Routing algorithm is an algorithm that constructs the routing table based on the network conditions.	The Non-Adaptive Routing algorithm is an algorithm that constructs the static table to determine which node to send the packet.
Usage	Adaptive routing algorithm is used by dynamic routing.	The Non-Adaptive Routing algorithm is used by static routing.
Routing decision	Routing decisions are made based on topology and network traffic.	Routing decisions are the static tables.
Categorization	The types of adaptive routing algorithm, are Centralized, isolation and distributed algorithm.	The types of Non Adaptive routing algorithm are flooding and random walks.
Complexity	Adaptive Routing algorithms are more complex.	Non-Adaptive Routing algorithms are simple.

Shortest Path Algorithm:

Shortest path algorithm is a type of static routing algorithm. The shortest path problem is about finding a path between 2 vertices in a graph such that the total sum of the edges weights is minimum. This problem could be solved easily using **Dijkstra Algorithm** which finds the shortest paths between a source and all destinations in the network.

It depends on the following concept: Shortest path contains at most n−1 edges, because the shortest path couldn't have a cycle.

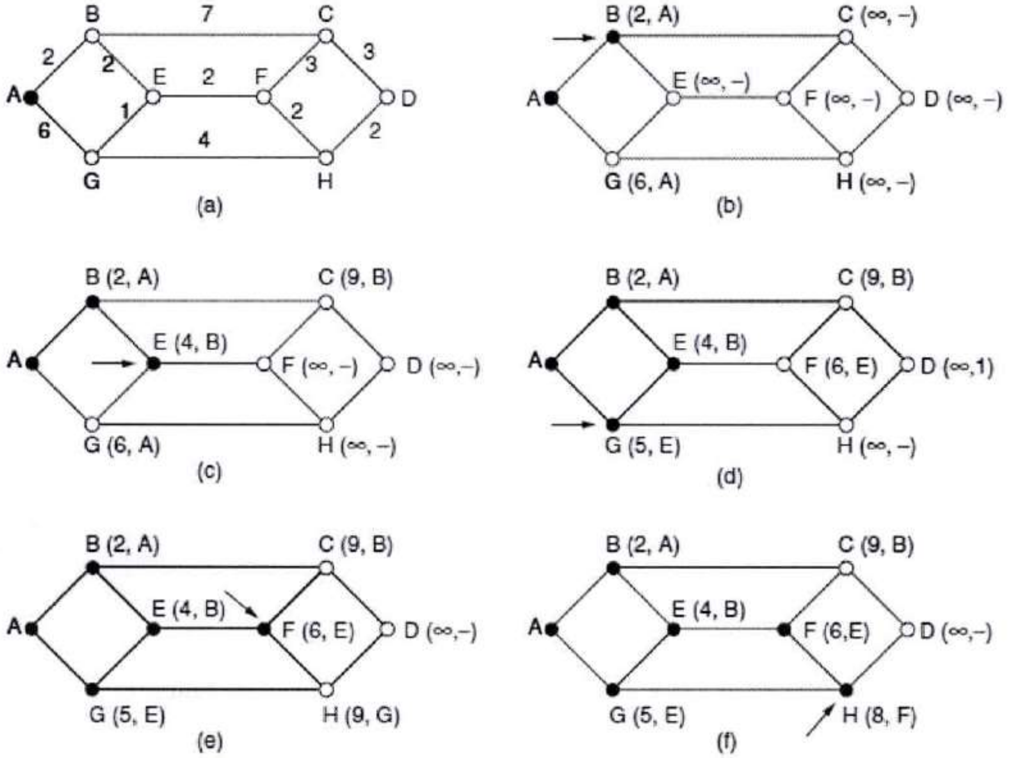
Algorithm Steps:

- The outer loop traverses from 0 : n−1.
- Loop over all edges, check if the next node distance < current node distance + edge weight, in this case update the next node distance to "current node distance + edge weight".

This algorithm depends on the relaxation principle where the shortest distance for all vertices is gradually replaced by more accurate values until eventually reaching the optimum solution. In the beginning all vertices have a distance of "Infinity", but only the distance of the source vertex = 0, then update all the connected vertices with the new distances (source vertex distance + edge weights), then apply the same concept for the new vertices with new distances and so on.

- Each node is labeled with its distance from the source node along the best known path.
- Initially, no paths are known, so all nodes are labeled with infinity. As the algorithm proceeds and paths are found, the labels may change, reflecting better paths.
- A label may be either tentative or permanent. Initially, all labels are tentative. When it is discovered that a label represents the shortest possible path from the source to that node, it is made permanent and never changed thereafter.

- Let us assume the weights represent, for example, distance. We want to find the shortest path from *A* to *D* from the following Graph.



The first six steps used in computing the shortest path from *A* to *D*.
The arrows indicate the working node.

- We start out by marking node *A* as permanent, indicated by a filled-in circle. Then we examine, in turn, each of the nodes adjacent to *A* (the working node), relabeling each one with the distance to *A*.
- Whenever a node is relabeled, we also label it with the node from which the probe was made so that we can reconstruct the final path later.
- If the network had more than one shortest path from *A* to *D* and we wanted to find all of them, we would need to remember all of the probe nodes that could reach a node with the same distance.
- Having examined each of the nodes adjacent to *A*, we examine all the tentatively labeled nodes in the whole graph and make the one with the smallest label permanent, as shown in Fig. 5-7(b). This one becomes the new working node.

- We now start at *B* and examine all nodes adjacent to it. If the sum of the label on *B* and the distance from *B* to the node being considered is less than the label on that node, we have a shorter path, so the node is relabeled.
- After all the nodes adjacent to the working node have been inspected and the tentative labels changed if possible, the entire graph is searched for the tentatively labeled node with the smallest value. This node is made permanent and becomes the working node for the next round. Figure 5-7 shows the first six steps of the algorithm.

Flooding

Flooding is a simple routing technique in computer networks where Flooding algorithm makes the decision about path based on local knowledge, not the complete picture of the network. Flooding is the static routing algorithm. **Flooding**, in which every incoming packet is sent out on every outgoing line except the one it arrived on. One major problem of this algorithm is that it generates a large number of duplicate packets on the network. Several measures are takes to stop the duplication of packets. These are:

1. One solution is to include a hop counter in the header of each packet. This counter is decremented at each hop along the path. When this counter reaches zero the packet is discarded. Ideally, the hop counter should become zero at the destination hop, indicating that there are no more intermediate hops and destination is reached. This requires the knowledge of exact number of hops from a source to destination.
2. Another technique is to keep the track of the packed that have been flooded, to avoid sending them a second time. For this, the source router put a sequence number in each packet it receives from its hosts. Each router then needs a list per source router telling which sequence numbers originating at that source have already been seen. If an incoming packet is on the list, it is not flooded.
3. Another solution is to use **selective flooding.** In selective flooding the routers do not send every incoming packet out on every output line. Instead packet is sent only on those lines which are approximately going in the right direction.

Distance Vector Routing

A **distance vector routing** algorithm operates by having each router maintain a table (i.e., a vector) giving the best known distance to each destination and which link to use to get there. These tables are updated by exchanging information with the neighbors. Eventually, every router knows the best link to reach each destination. The distance vector routing algorithm is sometimes called by other names, most commonly the distributed **Bellman-Ford** routing algorithm, after the researchers who developed it. It's a dynamic routing algorithm. It was the original ARPANET routing algorithm and was also used in the Internet under the name RIP. In distance vector routing, each router maintains a routing table known as **vector.** This local routing table containing one entry for each router in the network. This entry has three parts: the destination, an estimate of the distance to that destination and next hop.

How it Works:

Step-1:

Each router prepares its routing table. By their local knowledge. Each router knows about-

- All the Routers present in the network.
- Distance to its neighbor Routers.

Step-2:

- Each router exchanges its distance vector with its neighboring routers.
- Each router prepares a new routing table using the distance vectors it has obtained from its neighbors.
- This step is repeated for (n-1) times if there are n routers in the network.
- After this, routing tables converge / become stable

Distance Vector Routing Example

Consider- There is a network consisting of 4 routers. The weights are mentioned on the edges. Weights could be distances or costs or delays.

Step-1:

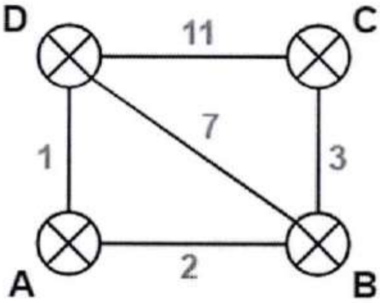
Initially each router prepares its routing table using its local knowledge.

At D

Destination	Distance	Next Hop
A	1	A
B	7	B
C	11	C
D	0	D

At C

Destination	Distance	Next Hop
A	∞	-
B	3	B
C	0	C
D	11	D



At A

Destination	Distance	Next Hop
A	0	A
B	2	B
C	∞	-
D	1	D

At B

Destination	Distance	Next Hop
A	2	A
B	0	B
C	3	C
D	7	D

Step: 2

- Each router exchanges its distance vector obtained in Step-01 with its neighbors.
- After exchanging the distance vectors, each router prepares a new routing table.

At Router A

- Router A receives distance vectors from its neighbors B and D.
- Router A prepares a new routing table as-

From B	From D
2	1
0	7
3	11
7	0

Cost(A→B) = 2 Cost(A→D) = 1

Destination	Distance	Next hop
A	0	A
B		
C		
D		

New Routing Table at Router A

- Cost of reaching destination B from router A = min { 2+0 , 1+7 } = 2 via B.
- Cost of reaching destination C from router A = min { 2+3 , 1+11 } = 5 via B.
- Cost of reaching destination D from router A = min { 2+7 , 1+0 } = 1 via D

Explanation for Destination B

- Router A can reach the destination router B via its neighbor B or neighbor D.
- It chooses the path which gives the minimum cost.
- Cost of reaching router B from router A via neighbor B = Cost (A→B) + Cost (B→B)= **2 + 0** = 2
- Cost of reaching router B from router A via neighbor D = Cost (A→D) + Cost (D→B) = **1 + 7** = 8
- Since the cost is minimum via neighbor B, so router A chooses the path via B.
- It creates an entry (2, B) for destination B in its new routing table.
- Similarly, we calculate the shortest path distance to each destination router at every router.

Thus, the new routing table at router A is-

Destination	Distance	Next Hop
A	0	A
B	2	B
C	5	B
D	1	D

At Router B

- Router B receives distance vectors from its neighbors A, C and D.
- Router B prepares a new routing table as-

From A	From C	From D
0	∞	1
2	3	7
∞	0	11
1	11	0

Cost (B→A) = 2 Cost (B→C) = 3 Cost (B→D) = 7

- Cost of reaching destination A from router B = min { 2+0 , 3+∞ , 7+1 } = 2 via A.
- Cost of reaching destination C from router B = min { 2+∞ , 3+0 , 7+11 } = 3 via C.
- Cost of reaching destination D from router B = min { 2+1 , 3+11 , 7+0 } = 3 via A.

Thus, the new routing table at router B is-

Destination	Distance	Next Hop
A	2	A
B	0	B
C	3	C
D	3	A

At Router C-

- Router C receives distance vectors from its neighbors B and D.
- Router C prepares a new routing table as-

From B	From D
2	1
0	7
3	11
7	0
Cost (C→B) = 3	Cost (C→D) = 11

- Cost of reaching destination A from router C = min { 3+2 , 11+1 } = 5 via B.
- Cost of reaching destination B from router C = min { 3+0 , 11+7 } = 3 via B.
- Cost of reaching destination D from router C = min { 3+7 , 11+0 } = 10 via B.

Thus, the new routing table at router C is

Destination	Distance	Next Hop
A	5	B
B	3	B
C	0	C
D	10	B

At Router D-

- Router D receives distance vectors from its neighbors A, B and C.
- Router D prepares a new routing table as-

From A	From B	From C
0	2	∞
2	0	3
∞	3	0
1	7	11
Cost (D→A) = 1	Cost (D→B) = 7	Cost (D→C) = 11

- Cost of reaching destination A from router D = min { 1+0 , 7+2 , 11+∞ } = 1 via A.
- Cost of reaching destination B from router D = min { 1+2 , 7+0 , 11+3 } = 3 via A.
- Cost of reaching destination C from router D = min { 1+∞ , 7+3 , 11+0 } = 10 via B.

Thus, the new routing table at router D is

Destination	Distance	Next Hop
A	1	A
B	3	A
C	10	B
D	0	D

Step-03:

- Each router exchanges its distance vector obtained in Step-02 with its neighboring routers.
- After exchanging the distance vectors, each router prepares a new routing table.

At Router A

- Router A receives distance vectors from its neighbors B and D.
- Router A prepares a new routing table as-

From B	From D
2	1
0	3
3	10
3	0
Cost(A→B) = 2	Cost(A→D) = 1

- Cost of reaching destination B from router A = min { 2+0 , 1+3 } = 2 via B.
- Cost of reaching destination C from router A = min { 2+3 , 1+10 } = 5 via B.
- Cost of reaching destination D from router A = min { 2+3 , 1+0 } = 1 via D.

Thus, the new routing table at router A is-

Destination	Distance	Next Hop
A	0	A
B	2	B
C	5	B
D	1	D

At Router B-

- Router B receives distance vectors from its neighbors A, C and D.
- Router B prepares a new routing table as-

From A	From C	From D
0	5	1
2	3	3
5	0	10
1	10	0
Cost (B→A) = 2	Cost (B→C) = 3	Cost (B→D) = 3

- Cost of reaching destination A from router B = min { 2+0 , 3+5 , 3+1 } = 2 via A.
- Cost of reaching destination C from router B = min { 2+5 , 3+0 , 3+10 } = 3 via C.
- Cost of reaching destination D from router B = min { 2+1 , 3+10 , 3+0 } = 3 via A.

Thus, the new routing table at router B is-

Destination	Distance	Next Hop
A	2	A
B	0	B
C	3	C
D	3	A

At Router C-

- Router C receives distance vectors from its neighbors B and D.
- Router C prepares a new routing table as-

From B	From D
2	1
0	3
3	10
3	0
Cost (C→B) = 3	Cost (C→D) = 10

- Cost of reaching destination A from router C = min { 3+2 , 10+1 } = 5 via B.
- Cost of reaching destination B from router C = min { 3+0 , 10+3 } = 3 via B.
- Cost of reaching destination D from router C = min { 3+3 , 10+0 } = 6 via B.

Thus, the new routing table at router C is-

Destination	Distance	Next Hop
A	5	B
B	3	B
C	0	C
D	6	B

At Router D-

- Router D receives distance vectors from its neighbors A, B and C.
- Router D prepares a new routing table as-

From A	From B	From C
0	2	5
2	0	3
5	3	0
1	3	10
Cost (D→A) = 1	Cost (D→B) = 3	Cost (D→C) = 10

- Cost of reaching destination A from router D = min { 1+0 , 3+2 , 10+5 } = 1 via A.
- Cost of reaching destination B from router D = min { 1+2 , 3+0 , 10+3 } = 3 via A.
- Cost of reaching destination C from router D = min { 1+5 , 3+3 , 10+0 } = 6 via A.

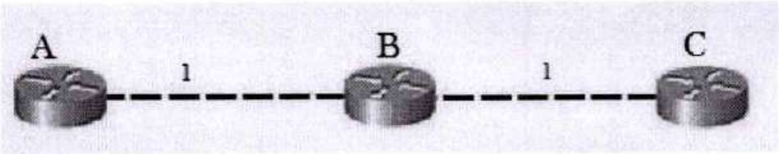
Thus, the new routing table at router D is-

Destination	Distance	Next Hop
A	1	A
B	3	A
C	6	A
D	0	D

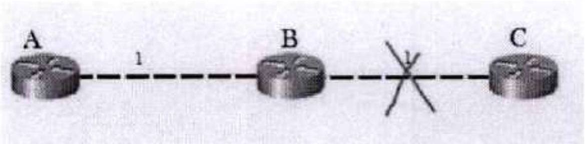
This is how final routing tables will be updated at each router.

The Count-to-Infinity Problem

- One of the important issues in Distance Vector Routing is **County of Infinity Problem.**
- Counting to infinity is just another name for a routing loop.
- In distance vector routing, routing loops usually occur when an interface goes down.
- It can also occur when two routers send updates to each other at the same time.



So in this example, the Bellman-Ford algorithm will converge for each router, they will have entries for each other. B will know that it can get to C at a cost of 1, and A will know that it can get to C via B at a cost of 2.

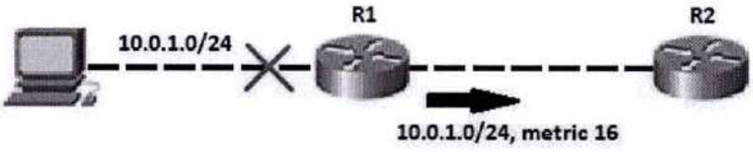


If the link between B and C is disconnected, then B will know that it can no longer get to C via that link and will remove it from it's table. Before it can send any updates it's possible that it will receive an update from A which will be advertising that it can get to C at a cost of 2. B can get to A at a cost of 1, so it will update a route to C via A at a cost of 3. A will then receive updates from B later and update its cost to 4. They will then go on feeding each other bad information toward infinity which is called as **Count to Infinity problem**.

Solution for Count to Infinity problem:-

1. **Route Poisoning**:

When a route fails, distance vector protocols spread the *bad news* about a route failure by poisoning the route. Route poisoning refers to the practice of advertising a route, but with a special metric value called Infinity. Routers consider routes advertised with an infinite metric to have failed. Each distance vector routing protocol uses the concept of an actual metric value that represents infinity. RIP defines infinity as 16. The main disadvantage of poison reverse is that it can significantly increase the size of routing announcements in certain fairly common network topologies.



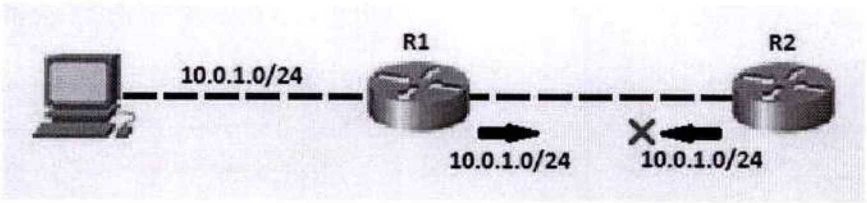
2.Split horizon:

In computer networking, **split-horizon** route advertisement is a method of preventing routing loops in distance-vector routing protocols by prohibiting a router from advertising a route back onto the interface from which it was learned

If the link between B and C goes down, and B had received a route from A , B could end up using that route via A. A would send the packet right back to B, creating a loop. But according to Split - horizon Rule, Node A does not advertise its route for C (namely A to B to C) back to B.

On the surface, this seems redundant since B will never route via node A because the route costs more than the direct route from B to C.

Consider the following network topology showing Split horizon-



Link-State Routing

Link-state routing is an alternative to distance-vector. It is also a dynamic routing algorithm. In distance-vector routing, each node knows a bare minimum of network topology: it knows nothing about links beyond those to its immediate neighbours. In the link-state approach, each node keeps a *maximum* amount of network information: a full map of all nodes and all links. Routes are then computed locally from this map, using the shortest-path-first algorithm. The map also allows calculation of a new route as soon as news of the failure of the existing route arrives; distance-vector protocols on the other hand must wait for news of a new route after an existing route fails.

- Link-state protocols distribute network map information through a modified form of broadcast of the status of each individual link.
- It sends out **link-state packets** (LSPs) that "flood" the network. This broadcast process is called **reliable flooding**.
- The link-state flooding algorithm avoids the usual problems of broadcast in the presence of loops by having each node keep a database of all LSP messages. The originator of each LSP includes its identity, information about the link that has changed status, and also a **sequence number**.
- The next step is to compute routes from the network map, using the shortest-path-first (SPF) algorithm. This algorithm computes shortest paths from a given node.

Link State Routing has two phases:

Reliable Flooding

- **Initial state:** Each node knows the cost of its neighbours.
- **Final state:** Each node knows the entire graph.

Route Calculation

Each node uses Dijkstra's algorithm on the graph to calculate the optimal routes to all nodes.

- The Link state routing algorithm is also known as Dijkstra's algorithm which is used to find the shortest path from one node to every other node in the network.
- The Dijkstra's algorithm is an iterative, and it has the property that after kth iteration of the algorithm, the least cost paths are well known for k destination nodes.

Let's describe some notations:

- **c(i , j):** Link cost from node i to node j. If i and j nodes are not directly linked, then c(i , j) = ∞.
- **D(v):** It defines the cost of the path from source code to destination v that has the least cost currently.
- **P(v):** It defines the previous node (neighbor of v) along with current least cost path from source to v.
- **N:** It is the total number of nodes available in the network.

Algorithm

```
Initialization
N = {A}    // A is a root node.
for all nodes v
    if v adjacent to A
        then D(v) = c(A,v)
        else D(v) = infinity
loop
    find w not in N such that D(w) is a minimum.
    Add w to N
    Update D(v) for all v adjacent to w and not in N:
        D(v) = min(D(v) , D(w) + c(w,v))
Until all nodes in N
```

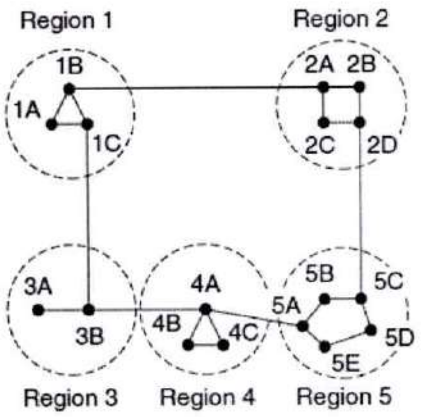
In the above algorithm, an initialization step is followed by the loop. The number of times the loop is executed is equal to the total number of nodes available in the network.

Hierarchical Routing

As networks grow in size, the router routing tables grow proportionally. Not only is router memory consumed by ever-increasing tables, but more CPU time is needed to scan them and more bandwidth is needed to send status reports about them. At a certain point, the network may grow to the point where it is no longer feasible for every router to have an entry for every other router, so the routing will have to be done hierarchically When hierarchical routing is used, the routers are divided into what we will call **regions**. Each router knows all the details about how to route packets to destinations within its own region but knows nothing about the internal structure of other regions. When different networks are interconnected, it is natural to regard each one as a separate region to free the routers in one network from having to know the topological structure of the other ones. For huge networks, a two-level hierarchy may be insufficient; it may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and so on, until we run out of names for aggregations.

The following Figure(5.14) gives a quantitative example of routing in a two-level hierarchy with five regions. The full routing table for router *1A* has 17 entries, as shown in Fig. 5-14(b). When routing is done hierarchically, as in Fig. 5-14(c), there are entries for all the local routers, as before, but all other regions are condensed into a single router, so all traffic for region 2 goes via the *1B-2A* line, but the rest of the remote traffic goes via the *1C-3B* line. Hierarchical routing has reduced the table from 17 to 7 entries. As the ratio of the number of regions to the number of routers per region grows, the savings in table space increase.

Unfortunately, these gains in space are not free. There is a penalty to be paid: increased path length. For example, the best route from *1A* to *5C* is via region 2, but with hierarchical routing all traffic to region 5 goes via region 3, because that is better for most destinations in region 5.



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

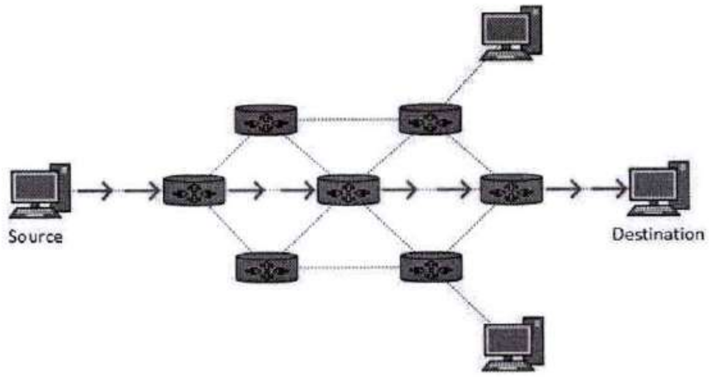
(c)

Fig: Hierarchical routing.

When a single network becomes very large, an interesting question is ''how many levels should the hierarchy have?'' For example, consider a network with 720 routers. If there is no hierarchy, each router needs 720 routing table entries. If the network is partitioned into 24 regions of 30 routers each, each router needs 30 local entries plus 23 remote entries for a total of 53 entries. If a three-level hierarchy is chosen, with 8 clusters each containing 9 regions of 10 routers, each router needs 10 entries for local routers, 8 entries for routing to other regions within its own cluster, and 7 entries for distant clusters, for a total of 25 entries.

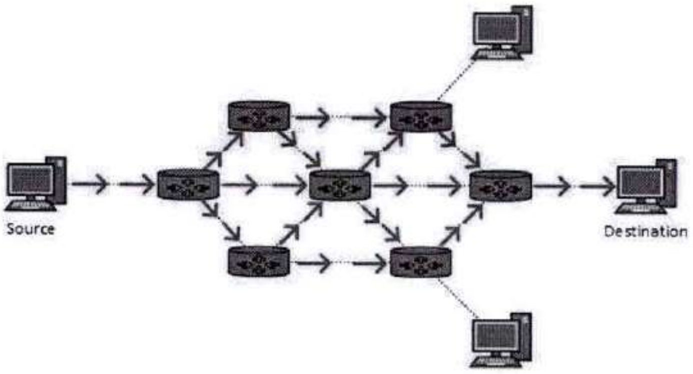
Unicast routing

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop.



Broadcast Routing

Sending a packet to all destinations simultaneously is called **broadcasting**. Various methods have been proposed for doing it.

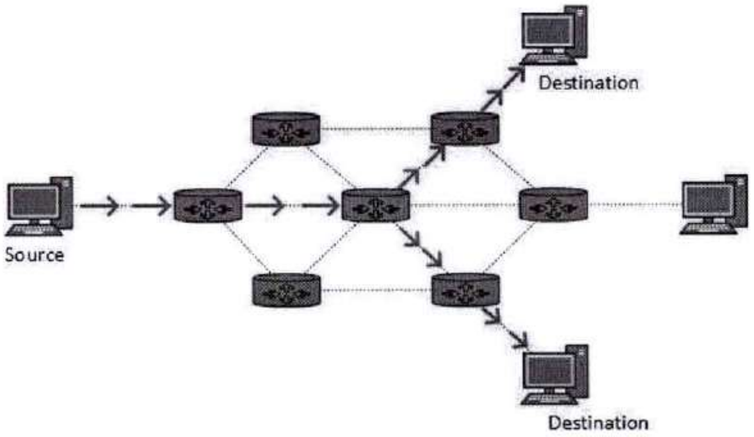


- A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses. All packets are sent as unicast but because they are sent to all, it simulates as if router is broadcasting. This method consumes lots of bandwidth and router must destination address of each node.
- Secondly, when router receives a packet that is to be broadcasted, it simply floods those packets out of all interfaces. All routers are configured in the same way. This method is easy on router's CPU but may cause the problem of duplicate packets received from peer routers. Reverse path forwarding is a technique, in which router knows in advance about its predecessor from where it should receive broadcast. This technique is used to detect and discard duplicates.

The disadvantage with this method is wasteful of bandwidth and slow, but it also requires the source to have a complete list of all destinations. This method is not desirable in practice, even though it is widely applicable. An improvement is **multidestination routing**, in which each packet contains either a list of destinations or a bit map indicating the desired destinations. When a packet arrives at a router, the router checks all the destinations to determine the set of output lines that will be needed. The router generates a new copy of the packet for each output line to be used and includes in each packet only those destinations that are to use the line. In effect, the destination set is partitioned among the output lines. After a sufficient number of hops, each packet will carry only one destination like a normal packet. Multidestination routing is like using separately addressed packets, except that when several packets must follow the same route, one of them pays full fare and the rest ride free. The network bandwidth is therefore used more efficiently. However, this scheme still requires the source to know all the destinations, plus it is as much work for a router to determine where to send one multidestination packet as it is for multiple distinct packets.

Multicast Routing

Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in Multicast routing, the data is sent to only nodes which wants to receive the packets.

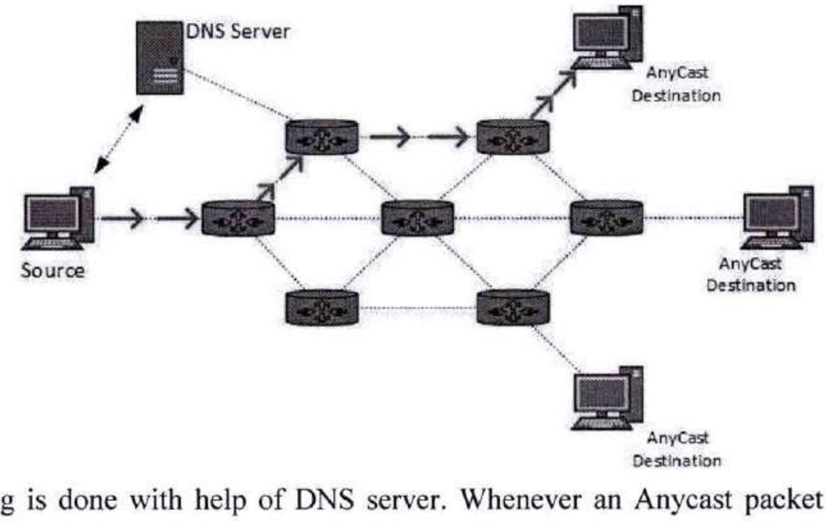


The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping.

Multicast routing also uses reverse path Forwarding technique, to detect and discard duplicates and loops.

Anycast Routing

Anycast packet forwarding is a mechanism where multiple hosts can have same logical address. When a packet destined to this logical address is received, it is sent to the host which is nearest in routing topology.



Anycast routing is done with help of DNS server. Whenever an Anycast packet is received it is enquired with DNS to where to send it. DNS provides the IP address which is the nearest IP configured on it.

CONGESTION

Congestion in a net work may occur if the load on the network is greater than the capacity of a network. If congestion occurs too many packets present in (a part of) the network causes packet delay and loss that degrades performance. This situation is called **congestion.**

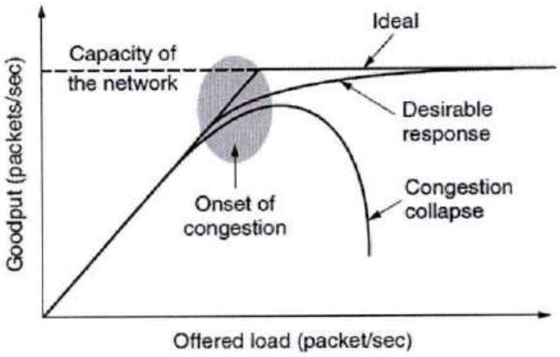
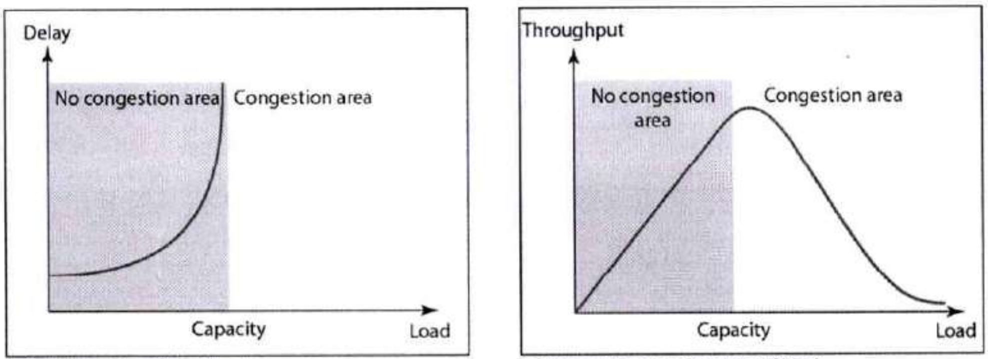


Figure 5-21. With too much traffic, performance drops sharply.

When the number of packets hosts send into the network is well within its carrying capacity, the number delivered is proportional to the number sent. If twice as many are sent, twice as many are delivered. However, as the offered load approaches the carrying capacity, bursts of traffic occasionally fill up the buffers inside routers and some packets are lost. These lost packets consume some of the capacity, so the number of delivered packets falls below the ideal curve. The network is now congested.



a. Delay as a function of load

b. Throughput as a function of load

Fig: Packet delay and throughput as functions of load

Approaches to Congestion Control

The presence of congestion means that the load is (temporarily) greater than the resources (in a part of the network) can handle. Two solutions come to mind: increase the resources or decrease the load. As shown in Fig. 5-22, these solutions are usually applied on different time scales to either prevent congestion or react to it once it has occurred.

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

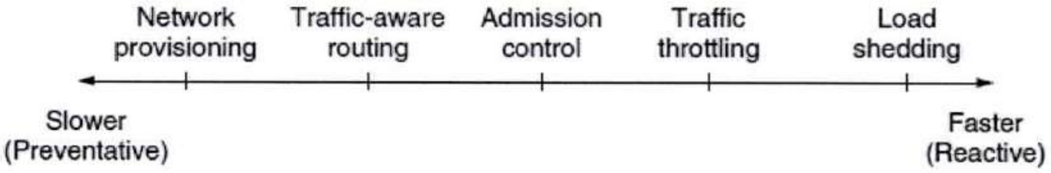


Figure 5-22. Timescales of approaches to congestion control.

- **Network Provisioning:** Is the most basic way to avoid congestion is to build a network that is well matched to the traffic that it carries. Sometimes resources can be added dynamically when there is serious congestion, for example, turning on spare routers or enabling lines that are normally used only as backups or purchasing bandwidth on the open market. More often, links and routers that are regularly heavily utilized are upgraded at the earliest opportunity. This is called **provisioning.**
- **Traffic-aware routing**: Splitting traffic across multiple paths is called traffic-aware routing. To make the most of the existing network capacity, routes can be tailored to traffic patterns that change during the day as network users wake and sleep in different time zones. For example, routes may be changed to shift traffic away from heavily used paths by changing the shortest path weights.
- **Admission control**: However, sometimes it is not possible to increase capacity. The only way then to beat back the congestion is to decrease the load. In a virtual-circuit network, new connections can be refused if they would cause the network to become congested. This is called **admission control**. At a finer granularity, when congestion is imminent the network can deliver feedback to the sources whose traffic flows are responsible for the problem. The network can request these sources to throttle their traffic, or it can slow down the traffic itself.
- **Load shedding:** The process of forcing the network to discard packets that it cannot deliver is generally called as Load Shedding. A good policy for choosing which packets to discard can help to prevent congestion collapse.

- **Traffic Throttling:** In the Internet and many other computer networks, senders adjust their transmissions to send as much traffic as the network can readily deliver. When congestion is imminent, it must tell the senders to throttle back their transmissions and slow down so that congestion can be avoided.

Some approaches to throttling traffic

Each approach must solve two problems.

- First, routers must determine when congestion is approaching, ideally before it has arrived. To do so, each router can continuously monitor the resources it is using. Three possibilities are

✓ The utilization of the output links,

✓ The buffering of queued packets inside the router,

✓ And the number of packets that are lost due to insufficient buffering.

- The second problem is that routers must deliver timely feedback to the senders that are causing the congestion. Congestion is experienced in the network, but relieving congestion requires action on behalf of the senders that are using the network. To deliver feedback, the router must identify the appropriate senders. It must then warn them carefully, without sending many more packets into the already congested network. Different schemes use different feedback mechanisms

a) **Choke Packets:** The most direct way to notify a sender of congestion is to tell it directly. In this approach, the router selects a congested packet and sends a **choke packet** back to the source host, To avoid increasing load on the network during a time of congestion, the router may only send choke packets at a low rate. When the source host gets the choke packet, it is required to reduce the traffic sent to the specified destination, for example, by 50%.

b) **Explicit Congestion Notification:** Instead of generating additional packets to warn of congestion, a router can tag any packet it forwards (by setting a bit in the packet's header) to signal that it is experiencing congestion. When the network delivers the packet, the destination can note that there is congestion and inform the sender when it sends a reply packet. The sender can then throttle its transmissions as before. This design is called **ECN (Explicit Congestion Notification)** and is used in the Internet.

If any of the routers they pass through is congested, that router will then mark the packet as having experienced congestion as it is forwarded. The destination will then echo any marks back to the sender as an explicit congestion signal in its next reply packet. This is shown with a dashed line in the figure to indicate that it happens above the IP level (e.g., in TCP). The sender must then throttle its transmissions, as in the case of choke packets.

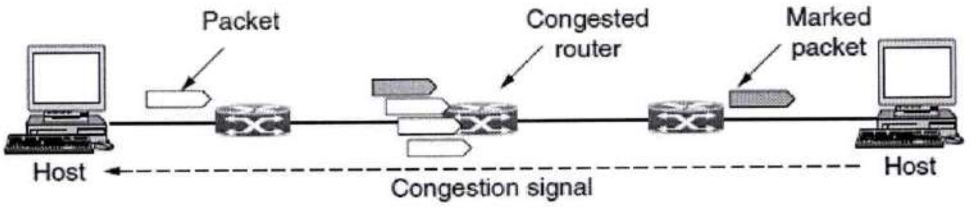


Figure 5-25. Explicit congestion notification

c) **Hop-by-Hop Backpressure** An alternative approach is to have the choke packet take effect at every hop it passes through. As shown in the sequence of Fig. 5-26(b). Here, as soon as the choke packet reaches *F*, *F* is required to reduce the flow to *D*. Doing so will require *F* to devote more buffers to the connection, since the source is still sending away at full blast, but it gives *D* immediate relief, like a headache remedy in a television commercial. In the next step, the choke packet reaches *E*, which tells *E* to reduce the flow to *F*. This action puts a greater demand on *E*'s buffers but gives *F* immediate relief. Finally, the choke packet reaches *A* and the flow genuinely slows down.

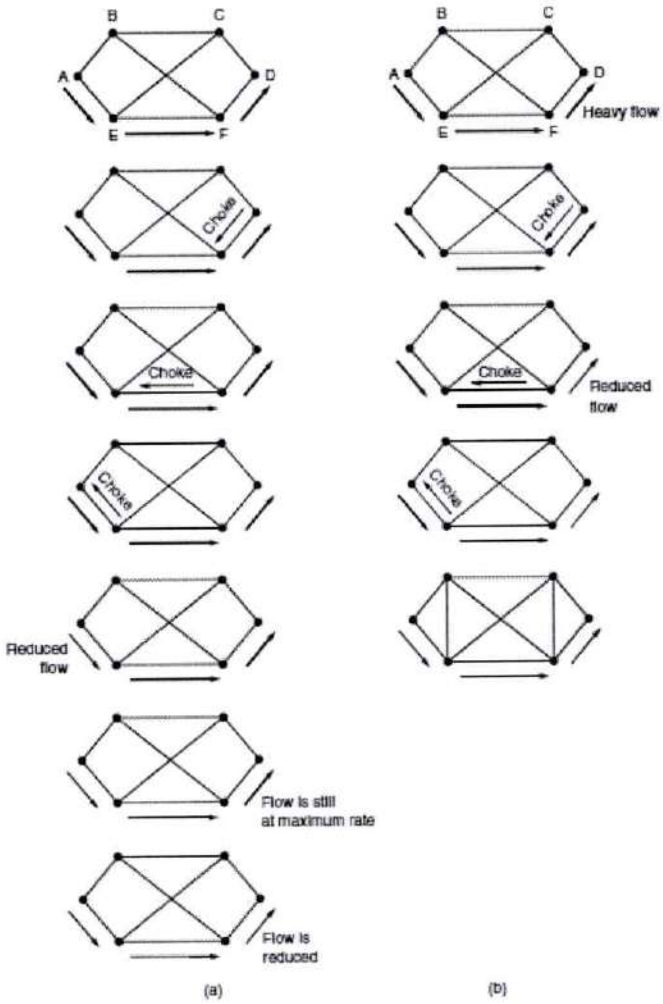


Figure 5-26. (a) A choke packet that affects only the source. (b) A choke packet that affects each hop it passes through.

- **Load Shedding:** Load shedding is a fancy way of saying that when routers are being inundated by packets that they cannot handle, they just throw them away. The term comes from the world of electrical power generation, where it refers to the practice of utilities intentionally blacking out certain areas to save the entire grid from collapsing on hot summer days when the demand for electricity greatly exceeds the supply. The key question for a router drowning in packets is which packets to drop.

  The preferred choice may depend on the type of applications that use the network. For a file transfer, an old packet is worth more than a new one. This is because dropping packet 6 and keeping packets 7 through 10, for example, will only force the receiver to do more work to buffer data that it cannot yet use. In contrast, for real-time media, a new packet is worth more than an old one. This is because packets become useless if they are delayed and miss the time at which they must be played out to the user. The former policy (old is better than new) is often called **wine** and the latter (new is better than old) is often called **milk** because most people would rather drink new milk and old wine than the alternative.

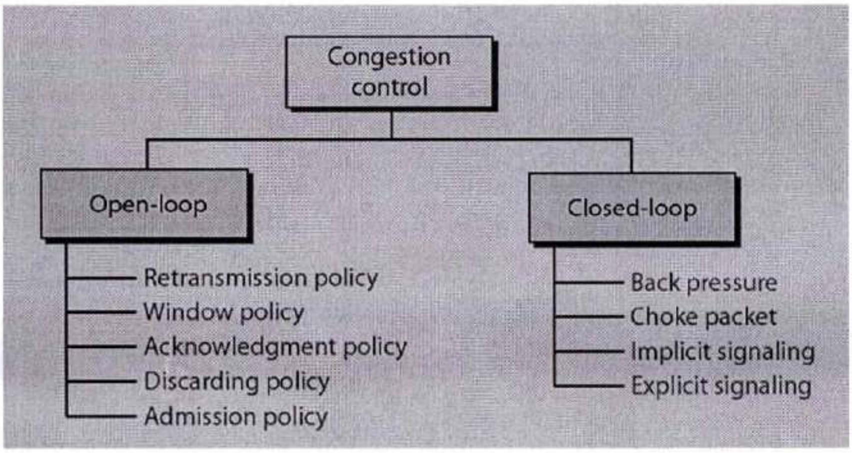
  Random early detection (RED), also known as **random early** discard or **random early** drop is a queuing discipline for a **network** scheduler suited for congestion avoidance

By having routers drop packets early, before the situation has become hopeless, there is time for the source to take action before it is too late. To determine when to start discarding, routers maintain a running average of their queue lengths. When the average queue length on some link exceeds a threshold, the link is said to be congested and a small fraction of the packets are dropped at random. RED routers improve performance compared to routers that drop packets only when their buffers are full. RED is used when hosts cannot receive explicit signals.

Congestion control techniques can be broadly classified into two categories called

1) Open-Loop Congestion Control : Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

2) Closed-Loop Congestion Control: Closed loop congestion control technique is used to treat or alleviate congestion after it happens.



QUALITY OF SERVICE

Quality-of-Service (QoS) refers to traffic control mechanisms that seek to either differentiate performance based on application or network-operator requirements or provide predictable or guaranteed performance to applications, sessions or traffic aggregates. An easy solution to provide good quality of service is to build a network with enough capacity for whatever traffic will be thrown at it. The name for this solution is **overprovisioning**. The resulting network will carry application traffic without significant loss and, assuming a decent routing scheme, will deliver packets with low latency.

Need for QoS –

- Video and audio conferencing require bounded delay and loss rate.
- Video and audio streaming requires bounded packet loss rate, it may not be so sensitive to delay.
- Time-critical applications (real-time control) in which bounded delay is considered to be an important factor.
- Valuable applications should be provided better services than less valuable applications.

QoS requirements for an Application can be specified as:

1. **Delay**: Network delay refers to the amount of time it takes for a packet to go from point A to point B. If Point A is the source and point B is the destination, then the delay is called an end to end delay.
2. **Delay Variation(Jitter)**: It is the variation of the **delays** with which packets travelling on a network connection reach their destination.
3. **Throughput**: **Throughput** is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot.
4. **Error Rate**: The degree of **errors** encountered during data transmission over a communications or **network** connection. The higher the **error rate**, the less reliable the connection or data transfer will be.
5. **Bandwidth** describes the maximum data transfer rate of a network or Internet connection, For **example**, a gigabit Ethernet connection has a **bandwidth** of 1,000 Mbps

For better quality services an application may require less Delay, less jitter, less error rate , more bandwidth and more throughput.

TECHNIQ Q UES TO IMPROVE QoS

Some techniques that can be used to improve the quality of service. The four common methods:

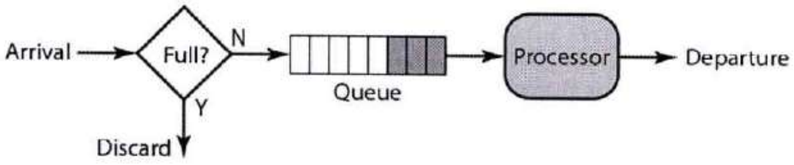
1) Scheduling,
2) Traffic shaping
3) Admission control, and
4) Resource reservation.

1. Scheduling

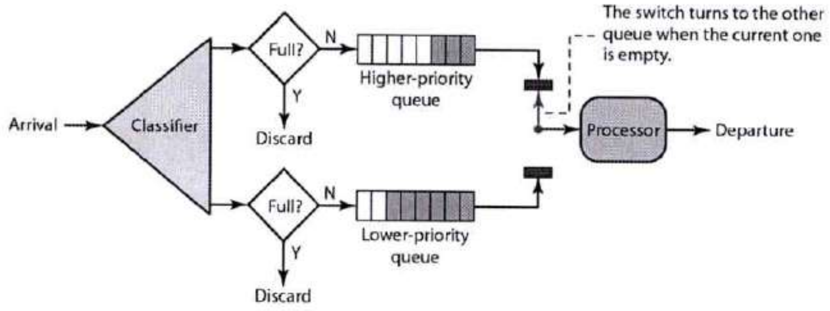
Packets from different flows arrive at a switch or router for processing. A good scheduling technique treats the different flows in a fair and appropriate manner. Several scheduling techniques are designed to improve the quality of service, three of them here are :

a) FIFO queuing
b) Priority queuing, and
c) Weighted fair queuing.

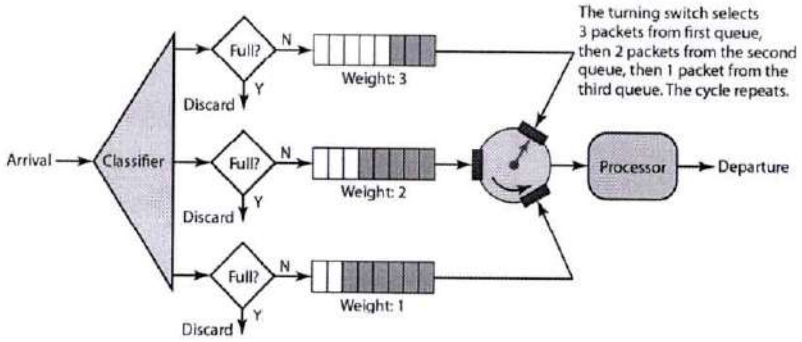
a) **FIFO queuing:** In first-in, first-out (FIFO) queuing, packets wait in a buffer (queue) until the node (router or switch) is ready to process them. If the average arrival rate is higher than the average processing rate, the queue will fill up and new packets will be discarded.



b) **Priority queuing:** In priority queuing, packets are first assigned to a priority class. Each priority class has its own queue. The packets in the highest-priority queue are processed first. Packets in the lowest- priority queue are processed last.A priority queue can provide better QoS than the FIFO queue because higher priority traffic, such as multimedia, can reach the destination with less delay. However, there is a potential drawback. If there is a continuous flow in a high-priority queue, the packets in the lower-priority queues will never have a chance to be processed. This is a condition called starvation



c) **Weighted fair queuing:** A better scheduling method is weighted fair queuing. In this technique, the packets are still assigned to different classes and admitted to different queues. The queues, however, are weighted based on the priority of the queues; higher priority means a higher weight. The system processes packets in each queue in a round-robin fashion with the number of packets selected from each queue based on the corresponding weight. For example, if the weights are 3, 2, and 1, three packets are processed from the first queue, two from the second queue, and one from the third queue. If the system does not impose priority on the classes, all weights can be equal. In this way, we have fair queuing with priority.

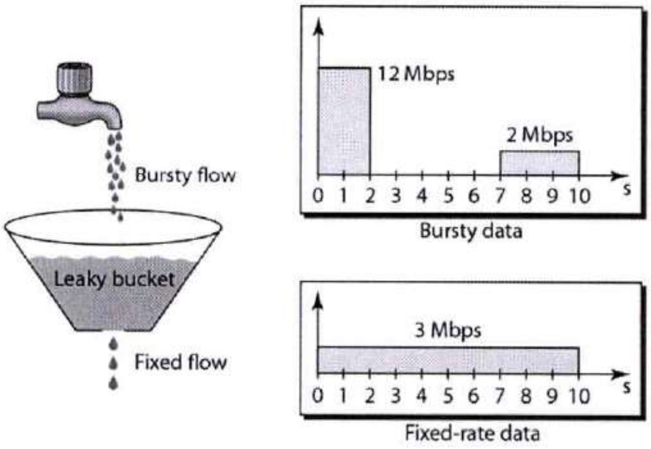

Arrival
Classifier
Full?
N
Y
Discard
Weight: 3
Full?
N
Y
Discard
Weight: 2
Full?
N
Y
Discard
Weight: 1
Processor
Departure
The turning switch selects 3 packets from first queue, then 2 packets from the second queue, then 1 packet from the third queue. The cycle repeats.

2. 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 are:

1) Leaky bucket Algorithm and
2) Token bucket Algorithm

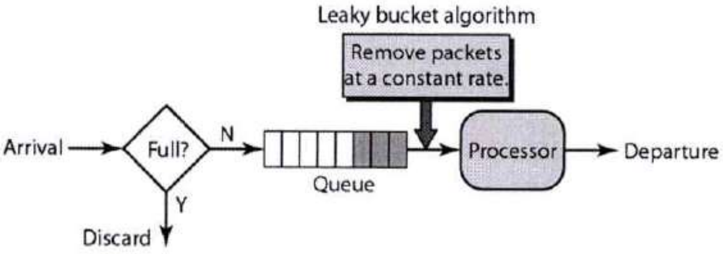
a. Leaky Bucket: If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty. The input rate can vary, but the output rate remains constant. Similarly, in networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an average rate. This can be seen from the below diagram.



In the figure, we assume that the network has committed a bandwidth of 3 Mbps for a host. The use of the leaky bucket shapes the input traffic to make it conform to this commitment. In above Figure, the host sends a burst of data at a rate of 12 Mbps for 2 s, for a total of 24 Mbits of data. The host is silent for 5 s and then sends data at a rate of 2 Mbps for 3 s, for a total of 6 Mbits of data. In all, the host has sent 30 Mbits of data in lOs. The leaky bucket smooth's the traffic by sending out data at a rate of 3 Mbps during the same 10 s.

Leaky bucket implementation

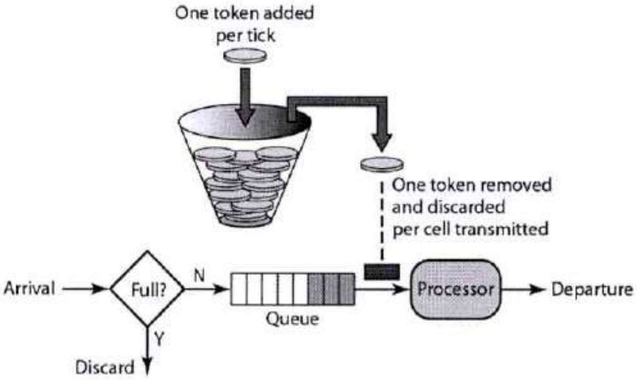
A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.



A FIFO queue holds the packets. If the traffic consists of fixed-size packets (e.g., cells in ATM networks), the process removes a fixed number of packets from the queue at each tick of the clock. If the traffic consists of variable-length packets, the fixed output rate must be based on the number of bytes or bits.

b. Token Bucket: The leaky bucket is very restrictive. It does not credit an idle host. For example, if a host is not sending for a while, its bucket becomes empty. Now if the host has bursty data, the leaky bucket allows only an average rate. The time when the host was idle is not taken into account. On the other hand, the token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) of data sent. For example, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens. The token bucket allows bursty traffic at a regulated maximum rate.

The token bucket can easily be implemented with a counter. The token is initialized to zero. Each time a token is added, the counter is incremented by 1. Each time a unit of data is sent, the counter is decremented by 1. When the counter is zero, the host cannot send data.



3. **Admission Control:** It is a mechanism used by the networking device like router and switches to accept or reject a flow based on predefined parameters called flow specification. Before a router accepts a flow for processing, it checks the flow specification to see if its capacity and its previous commitments to other flows can handle the new flow.

4. **Resource Reservation**: A flow of data needs resource such as buffer bandwidth, CPU time and so on. The QoS is improved if these resources are reserved beforehand.

Internetworking

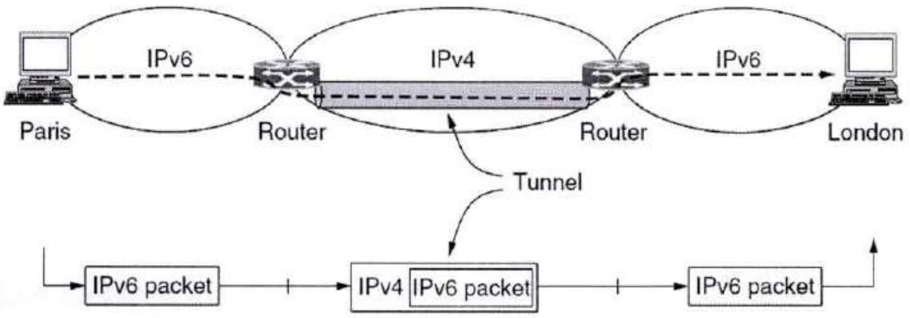
In real world scenario, networks under same administration are generally scattered geographically. There may exist requirement of connecting two different networks of same kind as well as of different kinds. Routing between two networks is called internetworking. Networks can be considered different based on various parameters such as, Protocol, topology and addressing scheme. In internetworking, routers have knowledge of each other's address and addresses beyond them. They can be statically configured go on different network or they can learn by using internetworking routing protocol.

Routing protocols which are used within an organization or administration are called Interior Gateway Protocols or IGP. RIP, OSPF are examples of IGP. Routing between different organizations or administrations may have Exterior Gateway Protocol, and there is only one EGP i.e. Border Gateway Protocol.

Tunneling

A technique of internetworking called **Tunneling** is used when source and destination networks of same type are to be connected through a network of different type. Tunneling is also known as port forwarding .Tunneling is widely used to connect isolated hosts and networks using other networks. The network that results is called an **overlay** since it has effectively been overlaid on the base network. Tunneling involves allowing private network communications to be sent across a public network, such as the Internet, through a process called encapsulation.

For Example : This case is where the source and destination hosts are on the same type of network, but there is a different network in between. As an example, think of an international bank with an IPv6 network in Paris, an IPv6 network in London and connectivity between the offices via the IPv4 Internet. Tunneling a packet from Paris to London can be seen in below fig.



To send an IP packet to a host in the London office, a host in the Paris office constructs the packet containing an IPv6 address in London, and sends it to the multiprotocol router that connects the Paris IPv6 network to the IPv4 Internet. When this router gets the IPv6 packet, it encapsulates the packet with an IPv4 header addressed to the IPv4 side of the multiprotocol router that connects to the London IPv6 network. That is, the router puts a (IPv6) packet inside a (IPv4) packet. When this wrapped packet arrives, the London router removes the original IPv6 packet and sends it onward to the destination host. The path through the IPv4 Internet can be seen as a big tunnel extending from one multiprotocol router to the other. The IPv6 packet just travels from one end of the tunnel to the other, snug in its nice box. It does not have to worry about dealing with IPv4 at all. Neither do the hosts in Paris or London. Only the multiprotocol routers have to understand both IPv4 and IPv6 packets. In effect, the entire trip from one multiprotocol router to the other is like a hop over a single link.

Tunneling is widely used to connect isolated hosts and networks using other networks. The network that results is called an **overlay** since it has effectively been overlaid on the base network.

Packet Fragmentation

Fragmentation is an important function of network layer. It is technique in which gateways break up or divide larger packets into smaller ones called fragments. Each fragment is then sent as a separate internal packet. Each fragment has its separate header and trailer. Sometimes, a fragmented datagram also get fragmented when it encounter a network that handle smaller fragments. Thus, a datagram can be fragmented several times before it reaches final destination. Reverse process of the fragmentation is difficult. Reassembly of fragments is usually done by the destination host because each fragment has become an independent datagram.

There are two different strategies for the recombination or we can say reassembly of fragments : Transparent Fragmentation, and Non-Transparent Fragmentation.

1. **Transparent Fragmentation :**

   This fragmentation is done by one network is made transparent to all other subsequent networks through which packet will pass. Whenever a large packet arrives at a gateway, it breaks packet into smaller fragments as shown in the following figure gateway G1 breaks a packet into smaller fragments.

   After this, each fragment is going to address to same exit gateway. Exist gateway of a network reassembles or recombines all fragments example is shown in the above figure as exit gateway, G2 of network 1 recombines all fragments created by G1 before passing them to network 2. Thus, subsequent network is not aware that fragmentation has occurred. This type of strategy is used by ATM networks. These networks use special hardware that provides transparent fragmentation of packets.

   There are some disadvantages of transparency strategy which are as follows :

   - Exit fragment that recombines fragments in a network must known when it has received all fragments.
   - Some fragments chooses different gateways for exit that results in poor performance.
   - It adds considerable overhead in repeatedly fragmenting and reassembling large packet.

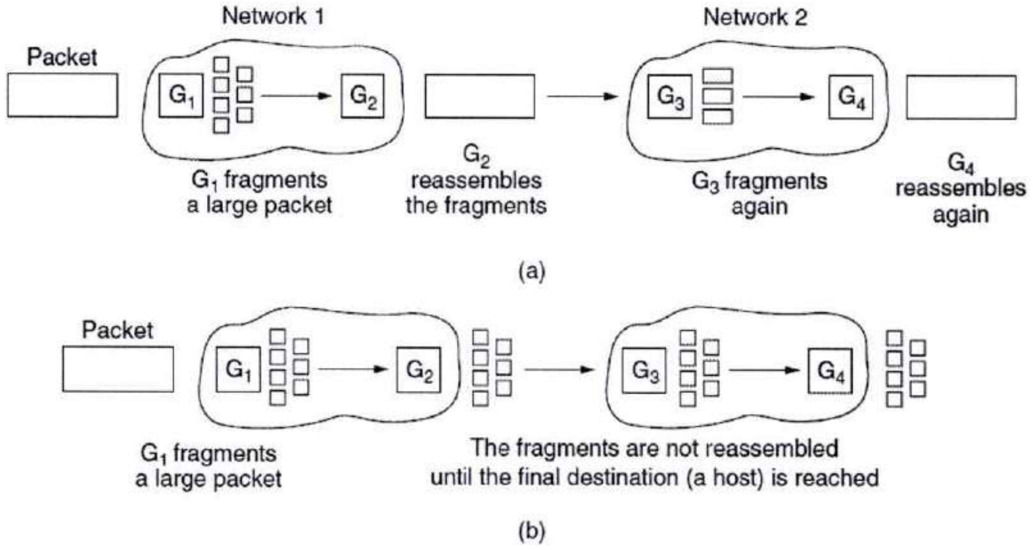

Network 1
Network 2
Packet
G_1
G_2
G_3
G_4
G_1 fragments a large packet
G_2 reassembles the fragments
G_3 fragments again
G_4 reassembles again
(a)
Packet
G_1
G_2
G_3
G_4
G_1 fragments a large packet
The fragments are not reassembled until the final destination (a host) is reached
(b)

Figure 5-42. (a) Transparent fragmentation. (b) Nontransparent fragmentation.

2. **Non-Transparent Fragmentation :**

   This fragmentation is done by one network is non-transparent to the subsequent networks through which a packet passes. Packet fragmented by a gateway of a network is not recombined by exit gateway of same network as shown in the below figure.

   Once a packet is fragmented, each fragment is treated as original packet. All fragments of a packet are passed through exit gateway and recombination of these fragments is done at the destination host.

   Disadvantages of Non-Transparent Fragmentation is as follows :

   - Every host has capability of reassembling fragments.
   - When a packet is fragmented, fragments should be numbered in such a way that the original data stream can be reconstructed.
   - Total overhead increases due to fragmentation as each fragment must have its own header.

THE NETWORK LAYER IN THE INTERNET

In the network layer, the Internet can be viewed as a collection of networks or **ASes** (**Autonomous Systems**) that are interconnected. There is no real structure, but several major backbones exist. These are constructed from high-bandwidth lines and fast routers. The biggest of these backbones, to which everyone else connects to reach the rest of the Internet, are called **Tier 1 networks.** Attached to the backbones are ISPs (Internet Service Providers) that provide Internet access to homes and businesses, data centers and colocation facilities full of server machines, and regional (mid-level) networks. The data centers serve much of the content that is sent over the Internet. Attached to the regional networks are more ISPs, LANs at many universities and companies, and other edge networks.

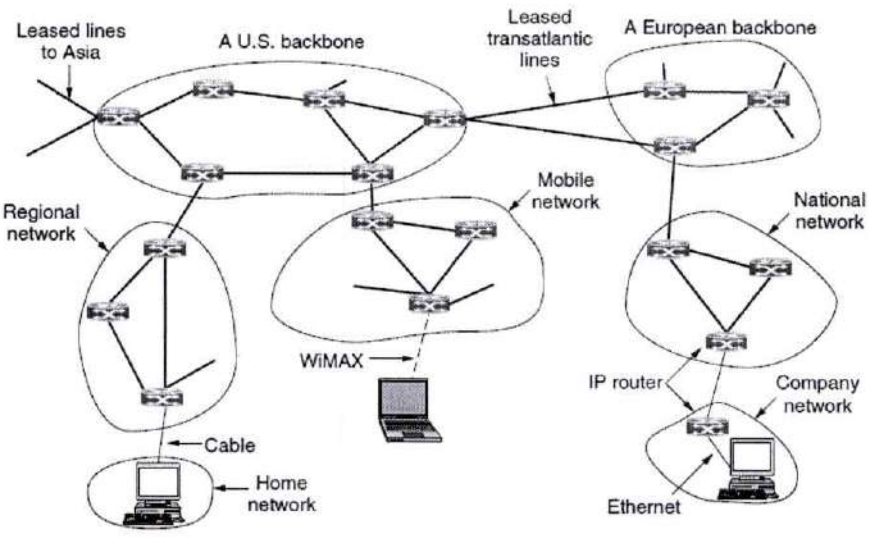


Figure 5-45. The Internet is an interconnected collection of many networks.

The glue that holds the whole Internet together is the network layer protocol, **IP** (**Internet Protocol**).

Communication in the Internet works as follows.

- The transport layer takes data streams and breaks them up so that they may be sent as IP packets. In theory, packets can be up to 64 KB each, but in practice they are usually not more than 1500 bytes.
- IP routers forward each packet through the Internet, along a path from one router to the next, until the destination is reached.
- At the destination, the network layer hands the data to the transport layer, which gives it to the receiving process. When all the pieces finally get to the destination machine, they are reassembled by the network layer into the original datagram.
- This datagram is then handed to the transport layer.

The IP Version 4 Protocol

- IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides a logical connection between network devices by providing identification for each device. There are many ways to configure IPv4 with all kinds of devices – including manual and automatic configurations – depending on the network type.
- IPv4 is defined and specified in IETF publication RFC 791. IPv4 uses 32-bit addresses for Ethernet communication in five classes: A, B, C, D and E. Classes A, B and C have a different bit length for addressing the network host. Class D addresses are reserved for military purposes, while class E addresses are reserved for future use.
- IPv4 uses 32-bit (4 byte) addressing, which gives 2^{32} addresses. IPv4 addresses are written in the dot-decimal notation, which comprises of four octets of the address expressed individually in decimal and separated by periods, for instance, 192.168.1.5.

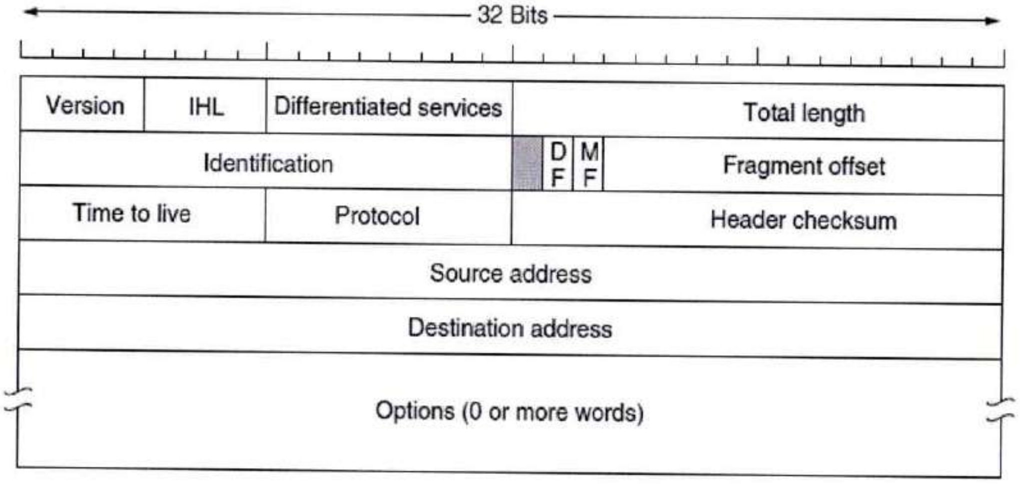


Figure 5-46. The IPv4 (Internet Protocol) header.

- **VERSION**: Version of the IP protocol (4 bits), which is 4 for IPv4
- **HLEN:** IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.
- **Type of service**: Low Delay, High Throughput, Reliability (8 bits)
- **Total Length**: Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.
- **Identification**: Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)
- **Flags:** 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)
- **Fragment Offset**: Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.
- **Time to live**: Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.
- **Protocol**: Name of the protocol to which the data is to be passed (8 bits)
- **Header Checksum**: 16 bits header checksum for checking errors in the datagram header
- **Source IP address**: 32 bits IP address of the sender
- **Destination IP address**: 32 bits IP address of the receiver
- **Option**: Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

Due to the presence of options, the size of the datagram header can be of variable length (20 bytes to 60 bytes).

IP Addresses

An Internet Protocol **address (IP address)** is a numerical label assigned to each device connected to a **computer network** that uses the Internet Protocol for communication. An **IP address** serves two main functions: host or **network** interface identification and location **addressing**.

IP address act as an identifier for a specific machine on a particular network. It also helps you to develop a virtual connection between a destination and a source. The IP address is also called IP number or internet address.

Version of IP address

Two types of IP addresses are 1)IPV4 and 2) IPV6.

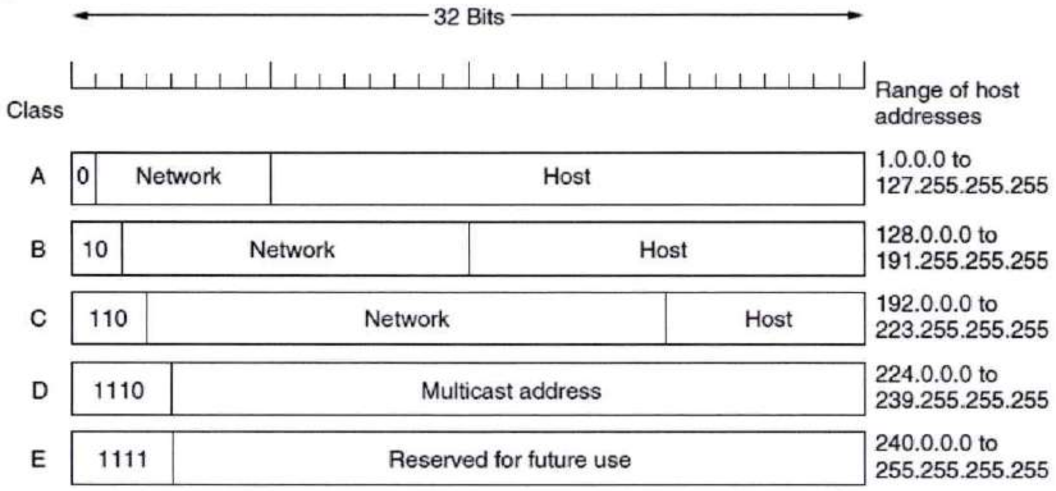
- **IPV4:** IPv4 was the first version of IP. It was deployed for production in the ARPANET in 1983. Today it is the most widely used IP version. It is used to identify devices on a network using an addressing system. The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses, which is more than 4 billion addresses.
- **IPV6:** It is the most recent version of the Internet Protocol. Internet Engineer Taskforce initiated it in early 1994. The design and development of that suite is now called IPv6. This new IP address version is being deployed to fulfill the need for more Internet addresses. It was aimed to resolve issues which are associated with IPv4. With 128-bit address space.

Each IP address consists of two parts. The first part (first three bytes in IP address) specifies the network and second part (last byte of an IP address) specifies the host in the network.

Classful Addressing

An IP address is 32-bit long. An IP address is divided into sub-classes:

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



32 Bits
Class
Range of host addresses
A
0
Network
Host
1.0.0.0 to 127.255.255.255
B
10
Network
Host
128.0.0.0 to 191.255.255.255
C
110
Network
Host
192.0.0.0 to 223.255.255.255
D
1110
Multicast address
224.0.0.0 to 239.255.255.255
E
1111
Reserved for future use
240.0.0.0 to 255.255.255.255

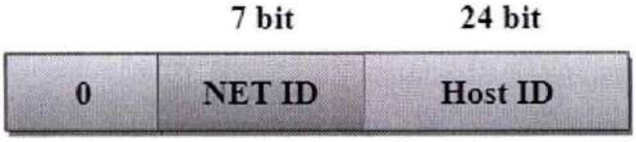
The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

Class A:

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.



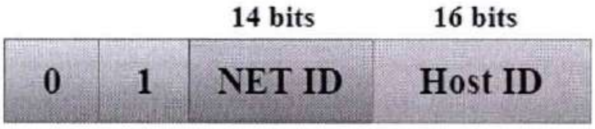
The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address

Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

- The Network ID is 16 bits long.
- The Host ID is 16 bits long.



In Class B, the higher order bits of the first octet is always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

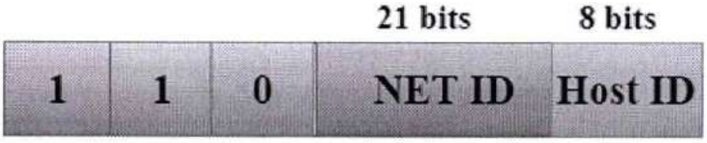
The total number of networks in Class B = 2^{14} = 16384 network address

The total number of hosts in Class B = 2^{16} - 2 = 65534 host address

Class C

In Class C, an IP address is assigned to only small-sized networks.

- The Network ID is 24 bits long.
- The host ID is 8 bits long.



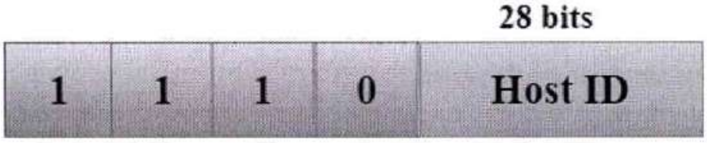
In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks = 2^{21} = 2097152 network address

The total number of hosts = $2^8 - 2 = 254$ host address

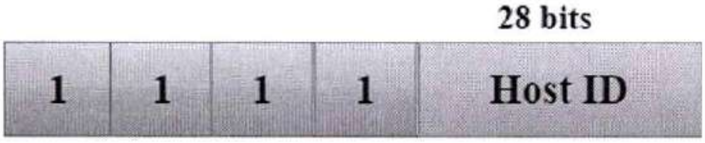
Class D

In Class D, an IP address is reserved for multicast addresses. It does not possess subnetting. The higher order bits of the first octet is always set to 1110, and the remaining bits determines the host ID in any network.



Class E

In Class E, an IP address is used for the future use or for the research and development purposes. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



There are also several other addresses that have special meanings, as shown in Fig. 5-54. The IP address 0.0.0.0, the lowest address, is used by hosts when they are being booted. It means ''this network'' or ''this host.'' IP addresses with 0 as the network number refer to the current network. These addresses allow machines to refer to their own network without knowing its number (but they have to know the network mask to know how many 0s to include).

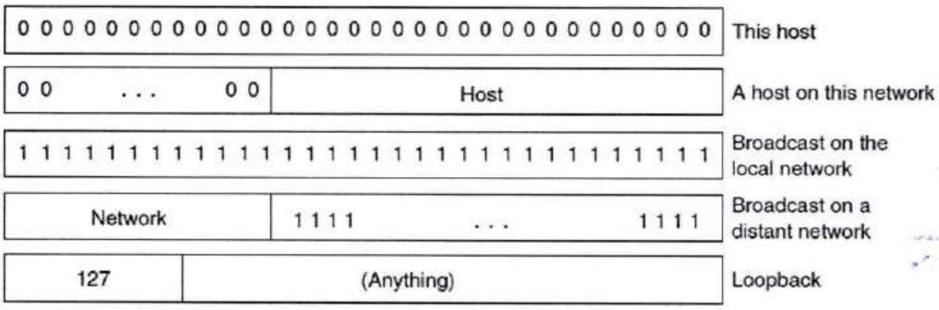


Figure 5-54. Special IP addresses.

The address consisting of all 1s, or 255.255.255.255—the highest address—is used to mean all hosts on the indicated network. It allows broadcasting on the local network, typically a LAN. The addresses with a proper network number and all 1s in the host field allow machines to send broadcast packets to distant LANs anywhere in the Internet. However, many network administrators disable this feature as it is mostly a security hazard. Finally, all addresses of the form 127.*xx*.*yy*.*zz* are reserved for loopback testing. Packets sent to that address are not put out onto the wire; they are processed locally and treated as incoming packets. This allows packets to be sent to the host without the sender knowing its number, which is useful for testing.

What is IPV6

IPv6 is the next generation Internet Protocol (IP) address standard intended to supplement and eventually replace IPv4, the protocol many Internet services still use today. Every computer, mobile phone, home automation component, IoT sensor and any other device connected to the Internet needs a numerical IP address to communicate between other devices. The original IP address scheme, called IPv4, is running out of addresses due to its widespread usage from the proliferation of so many connected devices.

What are the benefits of IPv6?

IPv6 (Internet Protocol version 6) is the sixth revision to the Internet Protocol and the successor to IPv4. It functions similarly to IPv4 in that it provides the unique IP addresses necessary for Internet-enabled devices to communicate. However, it does have one significant difference: it utilizes a 128-bit IP address.

Other Key benefits to IPv6 include:

- No more NAT (Network Address Translation)
- Auto-configuration
- No more private address collisions
- Better multicast routing
- Simpler header format
- Simplified, more efficient routing
- True quality of service (QoS), also called "flow labeling"
- Built-in authentication and privacy support
- Flexible options and extensions
- Easier administration (no more DHCP)

IPv6 utilizes 128-bit Internet addresses. Therefore, it can support 2^128 Internet addresses—340,282,366,920,938,463,463,374,607,431,768,211,456 of them to be exact. The number of IPv6 addresses is 1028 times larger than the number of IPv4 addresses. So there are more than enough IPv6 addresses to allow for Internet devices to expand for a very long time. The text form of the IPv6 address is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where each x is a hexadecimal digit, representing 4 bits.

IPV6 Header

An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow. IPv6 fixed header is 40 bytes long and contains the following information.

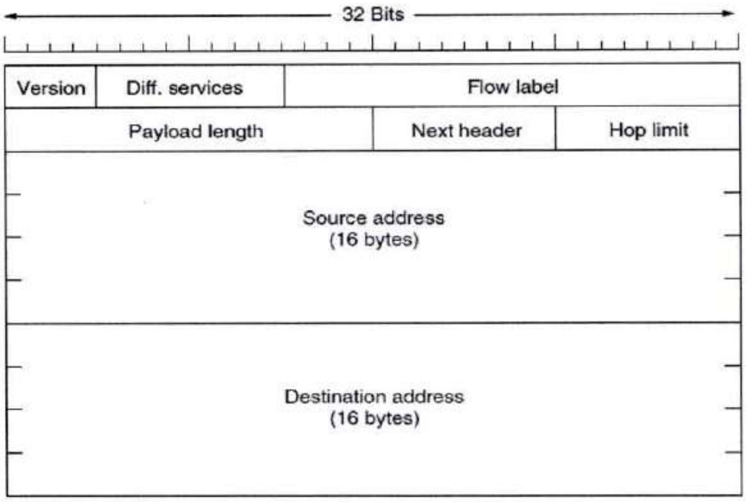


Figure 5-56. The IPv6 fixed header (required).

S.N.	Field & Description
1	**Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.
2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	**Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
4	**Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
5	**Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
6	**Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
7	**Source Address** (128-bits): This field indicates the address of originator of the packet.
8	**Destination Address** (128-bits): This field provides the address of intended recipient of the packet.

Extension Headers

In IPv6, the Fixed Header contains only that much information which is necessary, avoiding those information which is either not required or is rarely used. All such information is put between the Fixed Header and the Upper layer header in the form of Extension Headers. Each Extension Header is identified by a distinct value.

When Extension Headers are used, IPv6 Fixed Header's Next Header field points to the first Extension Header. If there is one more Extension Header, then the first Extension Header's 'Next-Header' field points to the second one, and so on. The last Extension Header's 'Next-Header' field points to the Upper Layer Header. Thus, all the headers points to the next one in a linked list manner.

KEY DIFFERENCES between IPV4 and IPV6

- IPv4 is 32-Bit IP address whereas IPv6 is a 128-Bit IP address.
- IPv4 is a numeric addressing method whereas IPv6 is an alphanumeric addressing method.
- IPv4 binary bits are separated by a dot(.) whereas IPv6 binary bits are separated by a colon(:).
- IPv4 offers 12 header fields whereas IPv6 offers 8 header fields.
- IPv4 supports broadcast whereas IPv6 doesn't support broadcast.
- IPv4 has checksum fields while IPv6 doesn't have checksum fields
- IPv4 supports VLSM (Virtual Length Subnet Mask) whereas IPv6 doesn't support VLSM.
- IPv4 uses ARP (Address Resolution Protocol) to map to MAC address whereas IPv6 uses NDP (Neighbour Discovery Protocol) to map to MAC address.

Questions from Previous Papers

1. Discuss about congestion control in Virtual Circuit subnets.(10M)
2. What is multicast and broadcast(4M)
3. What is channelization?(3M)
4. Explain briefly about the shortest path routing algorithm.
5. What is Count to infinity problem? Explain with suitable example
6. With a suitable example explain Distance Vector Routing algorithm. What is
7. the serious drawback of Distance Vector Routing algorithm? Explain.
8. Describe in detail about the Hierarchical routing.
9. Explain about tunneling
10. Explain about leaky bucket and token bucket algorithms

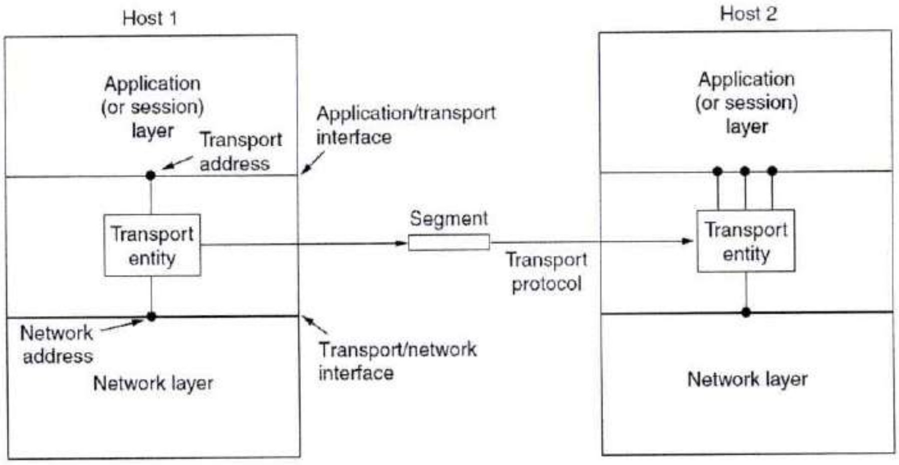
CN-UNIT - IV

(Transport Layer: Transport Services, Elements of Transport protocols, Connection management, TCP and UDP protocols)

THE TRANSPORT SERVICE

a) Services Provided to the Upper Layers:

- The ultimate goal of the transport layer is to provide efficient, reliable, and cost-effective data transmission service to its users, normally processes in the application layer.
- To achieve this, the transport layer makes use of the services provided by the network layer. The software and/or hardware within the transport layer that does the work is called the **transport entity**.
- The transport entity can be located in the operating system kernel, in a library package bound into network applications, in a separate user process, or even on the network interface card.
- There are also two types of transport service, connection oriented and connection less.
- The connection-oriented transport service is similar to the connection-oriented network service in many ways. In both cases, connections have three phases: establishment, data transfer, and release. Addressing and flow control are also similar in both layers.
- Furthermore, the connectionless transport service is also very similar to the connectionless network service. However, note that it can be difficult to provide a connectionless transport service on top of a connection-oriented network service, but it is inefficient. It can be solved by implementing transport layer on top of network layer.
- The (logical) relationship of the network, transport, and application layers is illustrated in Fig.



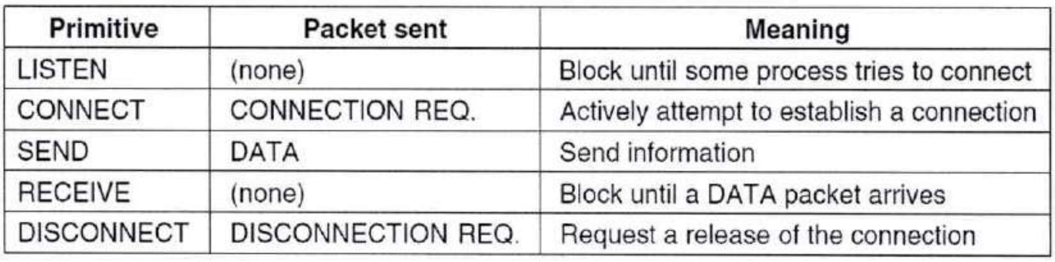
b) Transport Service Primitives:

- To allow users to access the transport service, the transport layer must provide some operations to application programs, that is, a transport service interface. Each transport service has its own interface.
- The transport service is similar to the network service, but there are also some important differences.

- ✓ **The main difference** is that the network service is intended to model the service offered by real networks. Real networks can lose packets, so the network service is generally unreliable. The connection-oriented transport service, in contrast, is reliable. Of course, real networks are not error-free, but that is precisely the purpose of the transport layer—to provide a reliable service on top of an unreliable network. The transport layer can also provide unreliable (datagram) service, ''its datagrams,'', there are some applications, such as client-server computing and streaming multimedia, that build on a connectionless transport service.

- ✓ **A second difference** between the network service and transport service is whom the services are intended for. The network service is used only by the transport entities. Few users write their own transport entities, and thus few users or programs ever see the bare network service. In contrast, many programs see the transport primitives. Consequently, the transport service must be convenient and easy to use.

- To get an idea of what a transport service might be like, consider the five primitives listed in Fig.



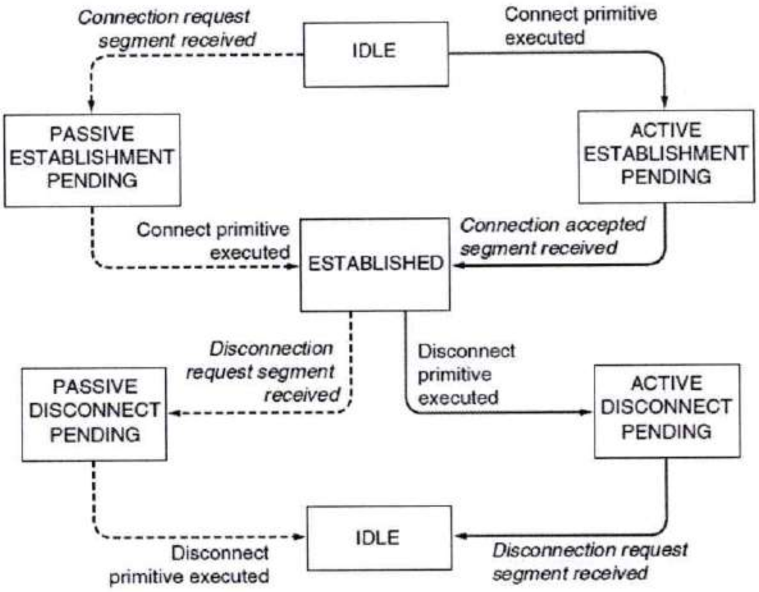
Primitive	Packet sent	Meaning
LISTEN	(none)	Block until some process tries to connect
CONNECT	CONNECTION REQ.	Actively attempt to establish a connection
SEND	DATA	Send information
RECEIVE	(none)	Block until a DATA packet arrives
DISCONNECT	DISCONNECTION REQ.	Request a release of the connection

- This transport interface is truly bare bones, but it gives the essential flavor of what a connection-oriented transport interface has to do. It allows application programs to establish, use, and then release connections, which is sufficient for many applications.

Client-Server Example:
To start with, the server executes a LISTEN primitive, typically by calling a library procedure that makes a system call that blocks the server until a client turns up. When a client wants to talk to the server, it executes a CONNECT primitive. The transport entity carries out this primitive by blocking the caller and sending a packet to the server. Encapsulated in the payload of this packet is a transport layer message for the server's transport entity. A quick note on terminology, we will use the term **segment** for messages sent from transport entity to transport entity. TCP, UDP and other Internet protocols use this term. Some older protocols used the ungainly name **TPDU (Transport Protocol Data Unit**).

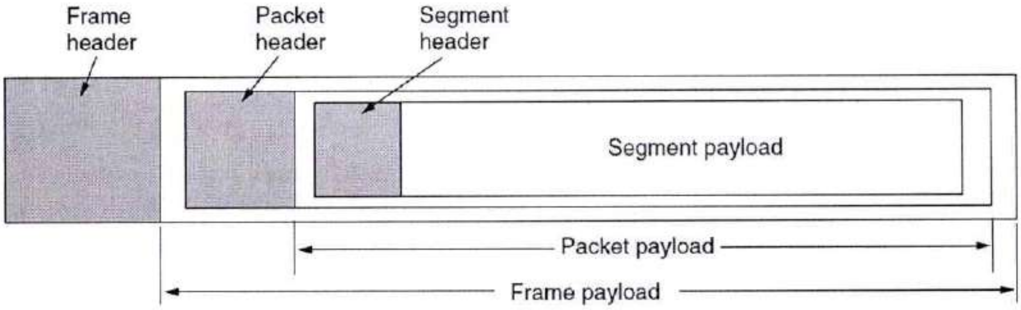
Getting back to our client-server example, the client's CONNECT call causes a CONNECTION REQUEST segment to be sent to the server. When it arrives, the transport entity checks to see that the server is blocked on a LISTEN. If so, it then unblocks the server and sends a CONNECTION ACCEPTED segment back to the client. When this segment arrives, the client is unblocked and the connection is established. Data can now be exchanged using the SEND and RECEIVE primitives. In the simplest form, either party can do a (blocking) RECEIVE to wait for the other party to do a SEND. When the segment arrives, the receiver is unblocked. It can then process the segment and send a reply. As long as both sides can keep track of whose turn it is to send, this scheme works fine. To the transport users, a connection is a reliable bit pipe: one user stuffs bits in and they magically appear in the same order at the other end. This ability to hide complexity is the reason that layered protocols are such a powerful tool. When a connection is no longer needed, it must be released to free up table space within the two transport entities. Disconnection has two variants: asymmetric and symmetric. In the asymmetric variant, either transport user can issue a DISCONNECT primitive, which results in a DISCONNECT segment being sent to the remote transport entity. Upon its arrival, the connection is released. In the symmetric variant, each direction is closed separately, independently of the other one. When one side does a DISCONNECT, that means it has no more data to send but it is still willing to accept data from its partner. In this model, a connection is released when both sides have done a DISCONNECT.

A state diagram for connection establishment and release for these simple primitives is given in Fig below.


IDLE
Connection request segment received
Connect primitive executed
PASSIVE ESTABLISHMENT PENDING
ACTIVE ESTABLISHMENT PENDING
Connect primitive executed
ESTABLISHED
Connection accepted segment received
Disconnection request segment received
Disconnect primitive executed
PASSIVE DISCONNECT PENDING
ACTIVE DISCONNECT PENDING
IDLE
Disconnect primitive executed
Disconnection request segment received

Each transition is triggered by some event, either a primitive executed by the local transport user or an incoming packet. For simplicity, we assume here that each segment is separately acknowledged. We also assume that a symmetric disconnection model is used, with the client going first.

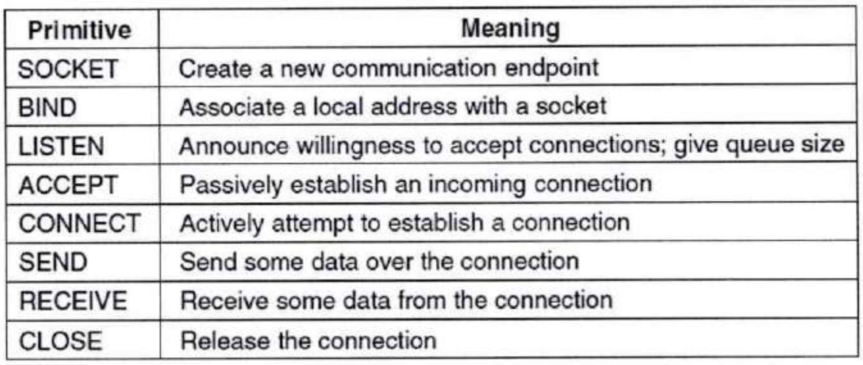
- Thus, segments (exchanged by the transport layer) are contained in packets (exchanged by the network layer). In turn, these packets are contained in frames (exchanged by the data link layer). When a frame arrives, the data link layer processes the frame header and, if the destination address matches for local delivery, passes the contents of the frame payload field up to the network entity. The network entity similarly processes the packet header and then passes the contents of the packet payload up to the transport entity. This nesting is illustrated in Fig below (Nesting of segments, packets, and frames).



PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

c) Berkeley Sockets:

- Another set of transport primitives, the socket primitives as they are used for TCP. Sockets were first released as part of the Berkeley UNIX 4.2BSD software distribution in 1983. They quickly became popular. The primitives are now widely used for Internet programming on many operating systems, especially UNIX-based systems, and there is a socket-style API for Windows called ''winsock.'' The primitives are listed in Fig. 6-5 below.



Primitive	Meaning
SOCKET	Create a new communication endpoint
BIND	Associate a local address with a socket
LISTEN	Announce willingness to accept connections; give queue size
ACCEPT	Passively establish an incoming connection
CONNECT	Actively attempt to establish a connection
SEND	Send some data over the connection
RECEIVE	Receive some data from the connection
CLOSE	Release the connection

The socket primitives for TCP

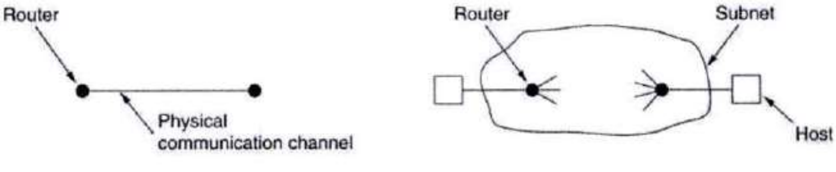
The first four primitives in the list are executed in that order by servers. The SOCKET primitive creates a new endpoint and allocates table space for it within the transport entity. The parameters of the call specify the addressing format to be used, the type of service desired, and the protocol. A successful SOCKET call returns an ordinary file descriptor for use in succeeding calls, the same way an OPEN call on a file does. Newly created sockets do not have network addresses. These are assigned using the BIND primitive. Once a server has bound an address to a socket, remote clients can connect to it. The reason for not having the SOCKET call create an address directly is that some processes care about their addresses, whereas others do not. Next comes the LISTEN call, which allocates space to queue incoming calls for the case that several clients try to connect at the same time. In contrast to LISTEN in our first example, in the socket model LISTEN is not a blocking call. To block waiting for an incoming connection, the server executes an ACCEPT primitive. When a segment asking for a connection arrives, the transport entity creates a new socket with the same properties as the original one and returns a file descriptor for it. The server can then fork off a process or thread to handle the connection on the new socket and go back to waiting for the next connection on the original socket. ACCEPT returns a file descriptor, which can be used for reading and writing in the standard way, the same as for files. Now let us look at the client side. Here, too, a socket must first be created using the SOCKET primitive, but BIND is not required since the address used does not matter to the server. The CONNECT primitive blocks the caller and actively starts the connection process. When it completes, the client process is unblocked and the connection is established. Both sides can now use SEND and RECEIVE to transmit and receive data over the full-duplex connection. The standard UNIX READ and WRITE system calls can also be used if none of the special options of SEND and RECEIVE are required.
Connection release with sockets is symmetric. When both sides have executed a CLOSE primitive, the connection is released. Sockets have proved tremendously popular and are the de-facto standard for abstracting transport services to applications.

- The socket API is often used with the TCP protocol to provide a connection-oriented service called a **reliable byte stream**, which is simply the reliable bit pipe that we described. However, other protocols could be used to implement this service using the same API. It shouldall be the same to the transport service users.

- A strength of the socket API is that is can be used by an application for other transport services. For instance, sockets can be used with a connectionless transport service. In this case, CONNECT sets the address of the remote transport peer and SEND and RECEIVE send and receive datagrams to and from the remote peer.
- Sockets can also be used with transport protocols that provide a message stream rather than a byte stream and that do or do not have congestion control. For example, **DCCP (Datagram Congestion Controlled Protocol**) is a version of UDP with congestion control. It is up to the transport users to understand what service they are getting. However, sockets are not likely to be the final word on transport interfaces. For example, applications often work with a group of related streams, such as a Web browser that requests several objects from the same server. With sockets, the most natural fit is for application programs to use one stream per object. This structure means that congestion control is applied separately for each stream, not across the group, which is suboptimal. It punts to the application the burden of managing the set.
- Newer protocols and interfaces have been devised that support groups of related streams more effectively and simply for the application. Two examples are **SCTP (Stream Control Transmission Protocol**) defined in RFC 4960 and **SST (Structured Stream Transport**). These protocols must change the socket API slightly to get the benefits of groups of related streams, and they also support features such as a mix of connection-oriented and connectionless traffic and even multiple network paths. Time will tell if they are successful.

ELEMENTS OF TRANSPORT PROTOCOLS

The transport service is implemented by a transport protocol used between the two transport entities. Transport protocols as the data link protocols have to deal with error control, sequencing, and flow control. The differences between these protocols are due to major dissimilarities between the environments in which the two protocols operate.



(a) Environment of the data link layer. (b) Environment of the transport layer.

Differences between data link layer and transport layer:

1. At data link layer, two routers communicate directly via a physical channel, whereas at the transport layer, this physical channel is replaced by the entire subnet.

2. In the data link layer, it is not necessary for a router to specify which router it wants to talk to – each outgoing line uniquely specifies a particular router. In the transport layer, explicit addressing of destinations is required.

3. In the data link layer, the process of establishing a connection over the wire is smple: the other end is always there (unless it has crashed, in which case it is not there). In the transport layer, initial connection establishment is more complicated.

4. In the data link layer, when a router sends a frame, it may arrive or lost, but it cannot bounce around for a while, etc. In the transport layer, if the subnet uses datagrams and adaptive routing inside, there is a no negligible probability that a packet may be stored for a number of seconds and then delivered later.

5. A final difference between the data link layer and transport layers is following: Buffering and flow control are needed in both layers, but the presence of a large and dynamically varying number of connections in the transport layer may require a different approach than used in data link layer.

- Addressing
- Connection Establishment
- Connection Release
- Error Control
- Flow Control and Buffering
- Multiplexing
- Crash Recovery

Addressing:

When an application process wishes to set up a connection to a remote application process, it must specify which one to connect to. The method normally used is to define transport addressing to which processes can listen for connection requests. In Internet, these end points are called ports. We will use generic term TSAP, (Transport Service Access Point). The analogous end points in the network layer are then called NSAPs. IP addresses are examples of NSAPs.

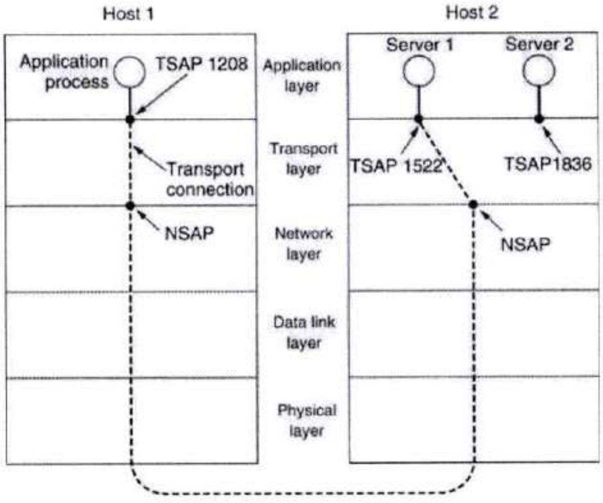


Fig: The relationship between TSAPs, NSAPs and transport connections.

Application processes, both clients and servers, can attach themselves to a TSAP to establish a connection to a remote TSAP. These connections run through NSAPs on each host. The purpose of having TSAPs is that in some networks, each computer has a single NSAP, so some way is needed to distinguish multiple transport end points that share that NSAP.

A possible scenario for a transport connection is as follows.

1) A time of day server process on host 2 attaches itself to TSAP 1522 to wait for an incoming call.
2) An application process on host 1 wants to find out the time-of-day, so it issues a CONNECT request specifying TSAP 1208 as the source and TSAP 1522 as destination

This action ultimately results in a transport connection being established between the application process on host 1 and server 1 on host 2.

3) The application process then sends over a request for the time.
4) The time server process responds with the current time.
5) The transport connection is then released.

Connection Establishment

At first glance, it would seem sufficient for one transport entity to just send a CONNECTION REQUEST TPDU to the destination and wait for a CONNECTION ACCEPTED reply. The problem occurs when the network can lose, store, and duplicate packets. This behaviour causes serious complications. Imagine a subnet that is so congested that acknowledgements hardly ever get back in time and each packet times out is retransmitted two or more times. Suppose that the subnet uses datagrams inside and that every packet follows a different route. Some of the packets might get stuck in a traffic jam inside the subnet and take a long time to arrive, that is, they are stored in the subnet and pop out much later. The crux of the problem is the existence of delayed duplicates; it can be attacked in various ways.

- One way is to use throw-away transport address
- Another possibility is to give each connection a connection identifier, etc

To get around the problem of a machine losing all memory of where it was after a crash, Tomlinson proposed equipping each host with a time-of-day clock. The basic idea is to ensure that two identically numbered TPDUs are never outstanding at the same time.

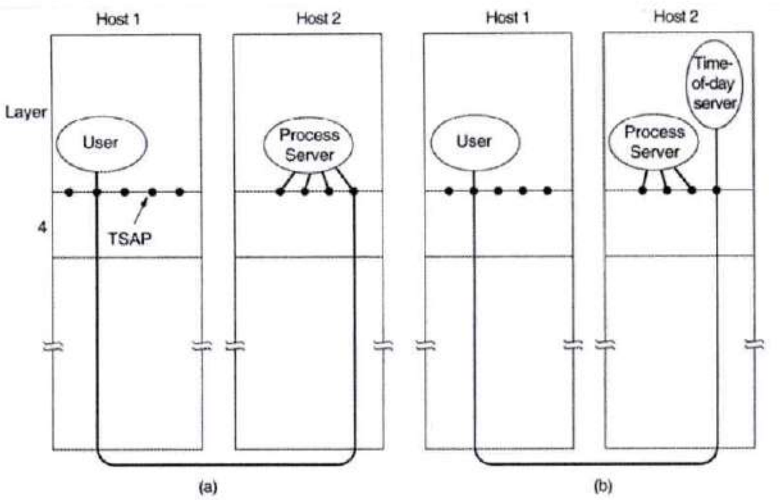


Fig: How a user process in host 1 establishes a connection with a time-of-day server in host 2.

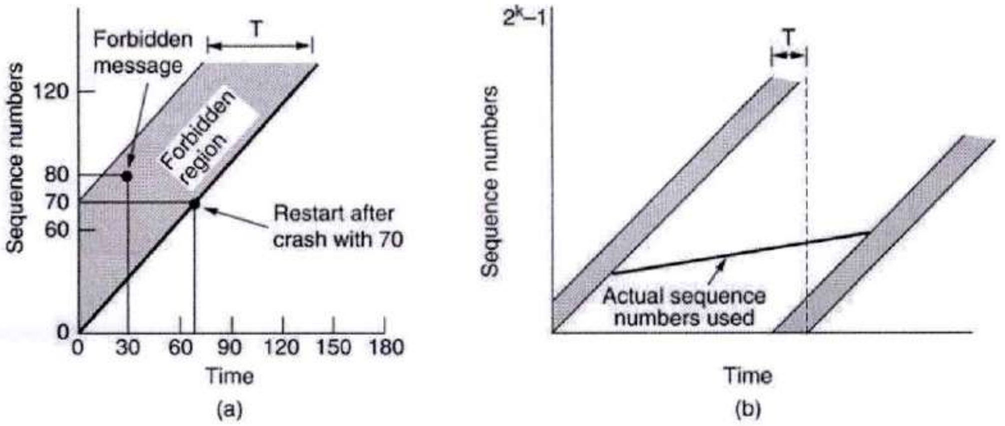
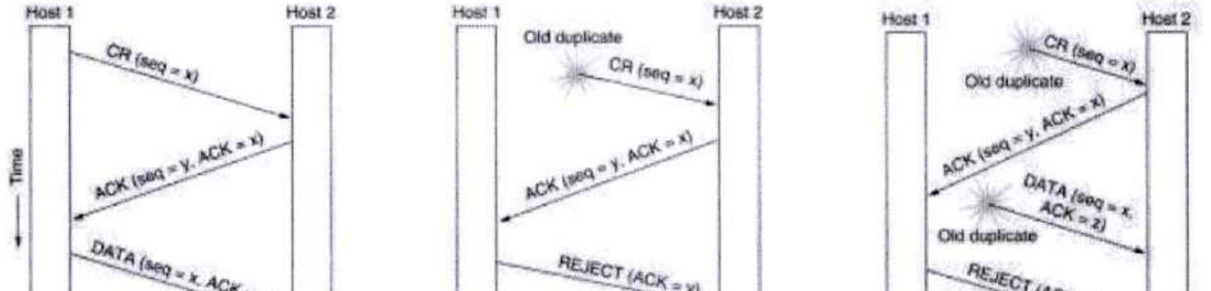


Fig: (a) TPDUs may not enter the forbidden region. (b) The resynchronization problem.



Three protocol scenarios for establishing a connection using a three-way handshake. CR denotes CONNECTION REQUEST.

(a) Normal operation,

(b) Old CONNECTION REQUEST appearing out of nowhere.

(c) Duplicate CONNECTION REQUEST and duplicate ACK.

Connection Release

- Releasing a connection is easier than establishing one.
- There are two styles of terminating a connection: asymmetric release and symmetric release.
- Asymmetric release is abrupt and may result in data loss
- One way to avoid data loss is to use symmetric release, in which each direction is released independently of the other one.
- One can envision a protocol in which host 1 says: I am done. Are you done too? If host 2 responds: I am done too. Goodbye, the connection can be safely released.
- Unfortunately, this protocol does not always work. There is a famous problem that illustrates this issue. It is called the **two-army problem**.

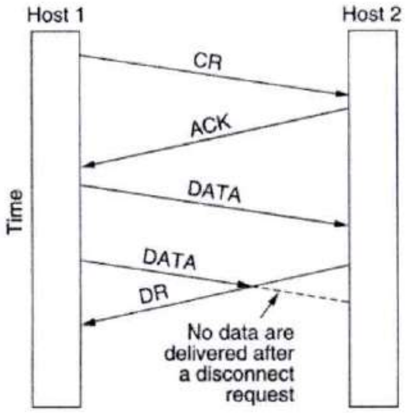


Fig: Abrupt disconnection with loss of data.

Two army problem

White army in valley. Blue arm in hills on either side of valley. White army can defeat either blue army in isolation, but blue armies together can defeat white army. How do the blue armies coordinate an attack on the white army? Their only communication is via messenging through the valley where messengers may be lost (i.e. an unreliable channel).

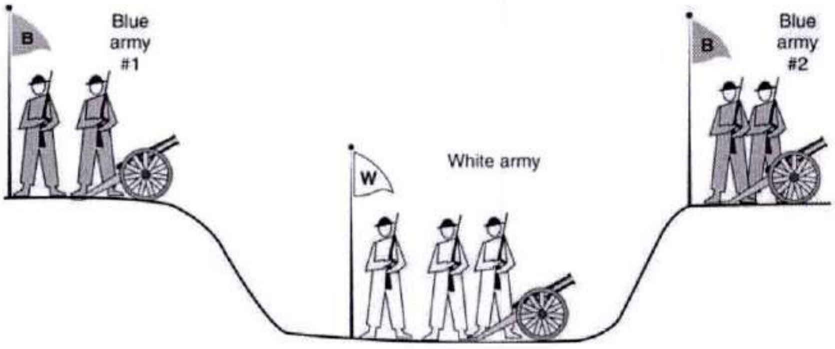


Fig: The two-army problem.

Blue army #1 sends message: attack at time X. Blue army #2 receives this message and sends an acknowledgment to it. Does the attack happen at time X? No, since blue army #2 can't know that it's ack was received. Adding an ack to the ack (three-way handshake) doesn't help, since now blue army #1 doesn't know if his ack to the ack got through, and if it didn't blue army #2 won't attack, so blue army #1 shouldn't attack either.

You can prove that no protocol can solve this problem. Suppose such a protocol existed. The last message sent is either essential or it is not. If it is not, it can be lost or dropped with no adverse affect. Drop all non-essential messages. Now all messages remaining are essential. What if the last message is lost? Since it is essential, the protocol fails. So we have a contradiction. Timers are used in practice to make conclusions about when it is safe to drop connections.

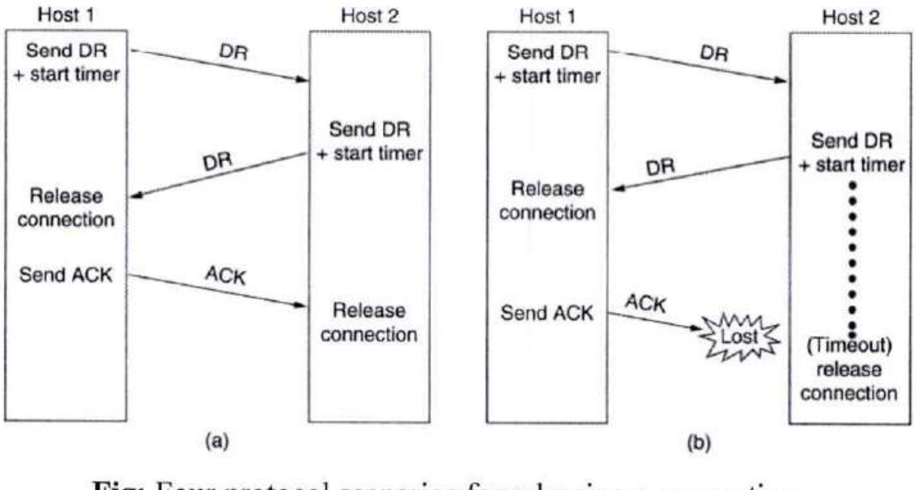


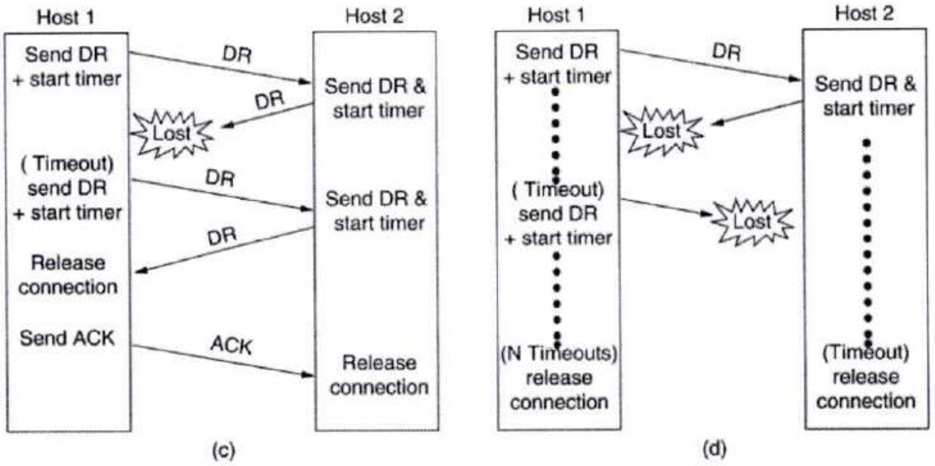
Fig: Four protocol scenarios for releasing a connection.

(a) Normal case of a three-way handshake.

(b) Final ACK lost.

(c) Response lost.

(d) Response lost and subsequent DRs lost.



RD (DISCONNECTION REQUEST)

Error Control, Flow Control and Buffering

Error control is ensuring that the data is delivered with the desired level of reliability, usually that all of the data is delivered without any errors. Flow control is keeping a fast transmitter from overrunning a slow receiver.

1. A frame carries an error-detecting code (e.g., a CRC or checksum) that is used to check if the information was correctly received.
2. A frame carries a sequence number to identify itself and is retransmitted by the sender until it receives an acknowledgement of successful receipt from the receiver. This is called **ARQ (Automatic Repeat reQuest)**.
3. There is a maximum number of frames that the sender will allow to be outstanding at any time, pausing if the receiver is not acknowledging frames quickly enough. If this maximum is one packet the protocol is called **stop-and-wait**. Larger windows enable pipelining and improve performance on long, fast links.
4. The **sliding window** protocol combines these features and is also used to support bidirectional data transfer.

In some ways the flow control problem in the transport layer is the same as in the data link layer, but in other ways it is different. The main difference is that a router usually has relatively few lines, whereas a host may have numerous connections. This difference makes it impractical to implement the data link buffering strategy in the transport layer. If the network service is unreliable, the sender must buffer all TPDUs sent. However, with reliable network service, other trade-off become possible. If the sender knows that the receiver always has buffer size, it need not retain copies of the TPDUs it sends. However, if the receiver cannot guarantee that every incoming TPDU will be accepted, the sender will have to buffer anyway. Even if the receiver has agreed to do the buffering, there still remains the question of the buffer size.

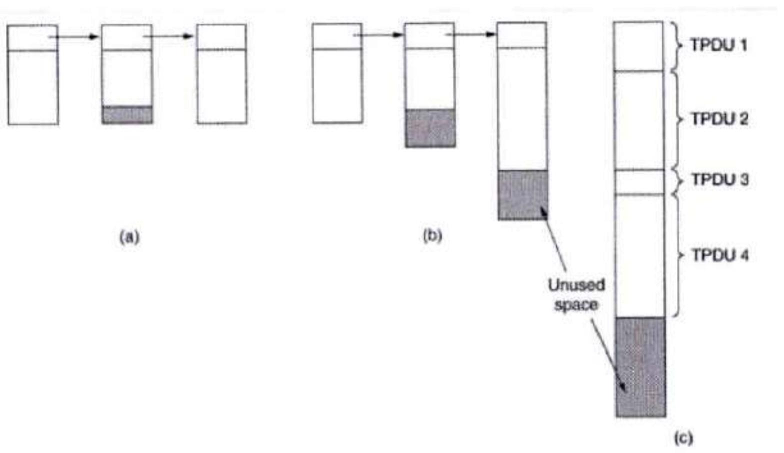
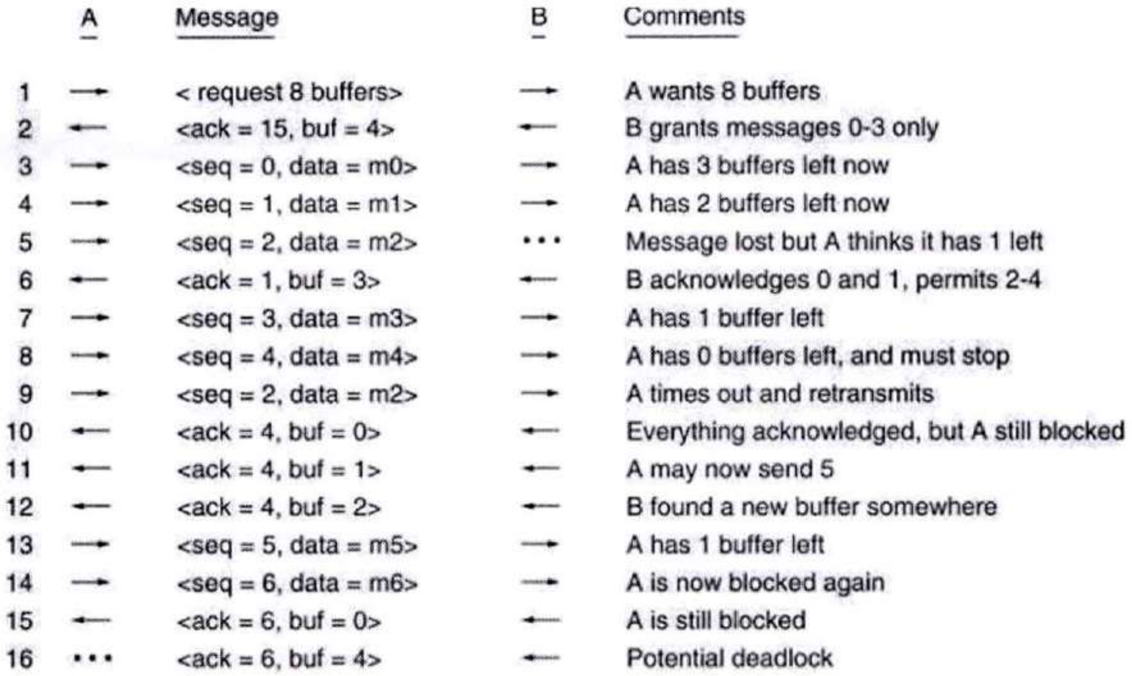


Fig: (a) Chained fixed-size buffers. (b) Chained variable-sized buffers. (c) One large circular buffer per connection.

For low-bandwidth bursty traffic, it is better to buffer at the sender, and for high bandwidth smooth traffic, it is better to buffer at the receiver.

Dynamic buffer management: The sender requests a certain number of buffers, based on its perceived needs. The receiver then grants as many of these as it can afford.



	A	Message	B	Comments
1	→	< request 8 buffers>	→	A wants 8 buffers
2	←	<ack = 15, buf = 4>	←	B grants messages 0-3 only
3	→	<seq = 0, data = m0>	→	A has 3 buffers left now
4	→	<seq = 1, data = m1>	→	A has 2 buffers left now
5	→	<seq = 2, data = m2>	• • •	Message lost but A thinks it has 1 left
6	←	<ack = 1, buf = 3>	←	B acknowledges 0 and 1, permits 2-4
7	→	<seq = 3, data = m3>	→	A has 1 buffer left
8	→	<seq = 4, data = m4>	→	A has 0 buffers left, and must stop
9	→	<seq = 2, data = m2>	→	A times out and retransmits
10	←	<ack = 4, buf = 0>	←	Everything acknowledged, but A still blocked
11	←	<ack = 4, buf = 1>	←	A may now send 5
12	←	<ack = 4, buf = 2>	←	B found a new buffer somewhere
13	→	<seq = 5, data = m5>	→	A has 1 buffer left
14	→	<seq = 6, data = m6>	→	A is now blocked again
15	←	<ack = 6, buf = 0>	←	A is still blocked
16	• • •	<ack = 6, buf = 4>	←	Potential deadlock

Dynamic buffer allocation. The arrows show the direction of transmission. An ellipsis (...) indicates a lost TPDU.

Multiplexing

Multiplexing several conversations onto connections, virtual circuits, and physical links plays a role in several layers of the network architecture. In the transport layer the need for multiplexing can arise in a number of ways. For example, if only one network address is available on a host, all transport connections on that machine have to use it.

For multiplexing the following two main strategies are followed:

1. Upward multiplexing and
2. Downward multiplexing

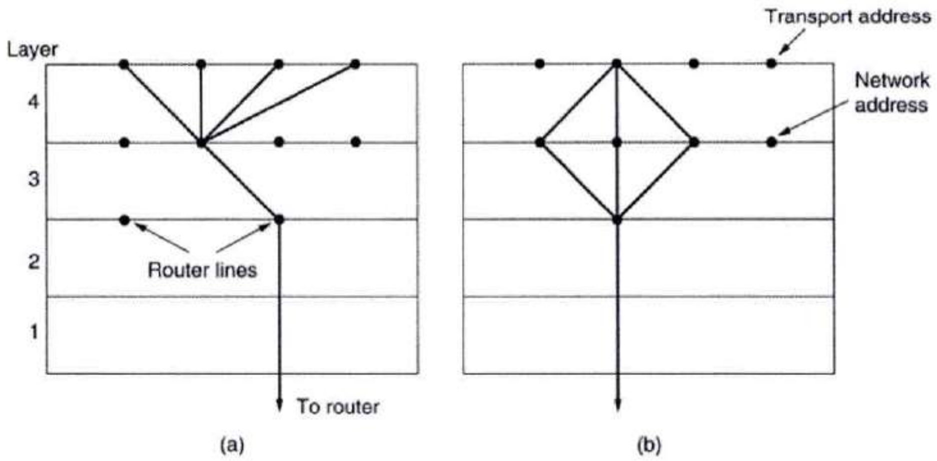


Fig: (a) Upward multiplexing. (b) Downward multiplexing.

Upward Multiplexing

- In upward multiplexing, the different transport connections are multiplexed in to one network connection.
- These transport connections are grouped by the transport layer as per their destinations.
- It then maps the groups with the minimum number of network connections possible.
- The upward multiplexing is quite useful where the network connections come very expensive.

Downward Multiplexing

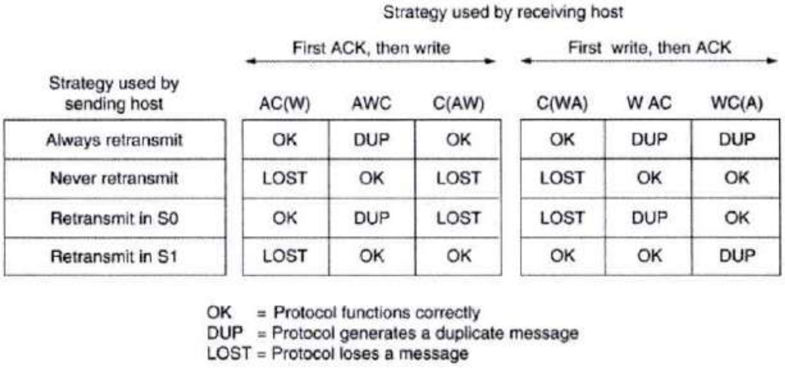
- It is only used when the connections with high bandwidth are required.
- In case of the downward multiplexing, the multiple network connections are opened by the transport layer and the traffic is distributed among them.
- But for using downward multiplexing, it is necessary that this capacity must be handled well by the subnet's data links.

Crash Recovery

If hosts and routers are subject to crashes, recovery from these crashes becomes an issue. If the transport entity is entirely within the hosts, recovery from network and router crashes is straightforward. If the network layer provides datagram service, the transport entities expect lost TPDUs all the time and know how to cope with them. If the network layer provides connection oriented service, then loss of a virtual circuit is handled by establishing a new one and then probing the remote transport entity to ask it which TPDUs it has received and which ones it has not received. The latter ones can be retransmitted. A more troublesome problem is how to recover from host crashes.

Three events are possible at the server: sending an acknowledgement (*A*), writing to the output process (*W*), and crashing (*C*). The three events can occur in six different orderings: *AC*(*W*), *AWC*, *C*(*AW*), *C*(*WA*), *WAC*, and *WC*(*A*), where the parentheses are used to indicate that neither *A* nor *W* can follow *C* (i.e., once it has crashed, it has crashed). Figure 6-18 shows all eight combinations of client and server strategies and the valid event sequences for each one. Notice that for each strategy there is some sequence of events that causes the protocol to fail. For example, if the client always retransmits, the *AWC* event will generate an undetected duplicate, even though the other two events work properly.

Different combinations of client and server strategy



	Strategy used by receiving host					
	First ACK, then write			First write, then ACK		
Strategy used by sending host	AC(W)	AWC	C(AW)	C(WA)	W AC	WC(A)
Always retransmit	OK	DUP	OK	OK	DUP	DUP
Never retransmit	LOST	OK	LOST	LOST	OK	OK
Retransmit in S0	OK	DUP	LOST	LOST	DUP	OK
Retransmit in S1	LOST	OK	OK	OK	OK	DUP

OK = Protocol functions correctly
DUP = Protocol generates a duplicate message
LOST = Protocol loses a message

CONGESTION CONTROL

If the transport entities on many machines send too many packets into the network too quickly, the network will become congested, with performance degraded as packets are delayed and lost. Controlling congestion to avoid this problem is the combined responsibility of the network and transport layers. Congestion occurs at routers, so it is detected at the network layer. However, congestion is ultimately caused by traffic sent into the network by the transport layer. The only effective way to control congestion is for the transport protocols to send packets into the network more slowly. The Internet relies heavily on the transport layer for congestion control, and specific algorithms are built into TCP and other protocols.

1. **Desirable Bandwidth Allocation:** It is to find a good allocation of bandwidth to the transport entities that are using the network. A good allocation will deliver good performance because it uses all the available bandwidth but avoids congestion, it will be fair across competing transport entities, and it will quickly track changes in traffic demands.
   a) **Efficiency and Power:** An efficient allocation of bandwidth across transport entities will use all of the network capacity that is available. However, it is not quite right to think that if there is a 100-Mbps link, five transport entities should get 20 Mbps each. They should usually get less than 20 Mbps for good performance. The reason is that the traffic is often bursty. This curve and a matching curve for the delay as a function of the offered load are given in Fig. below.

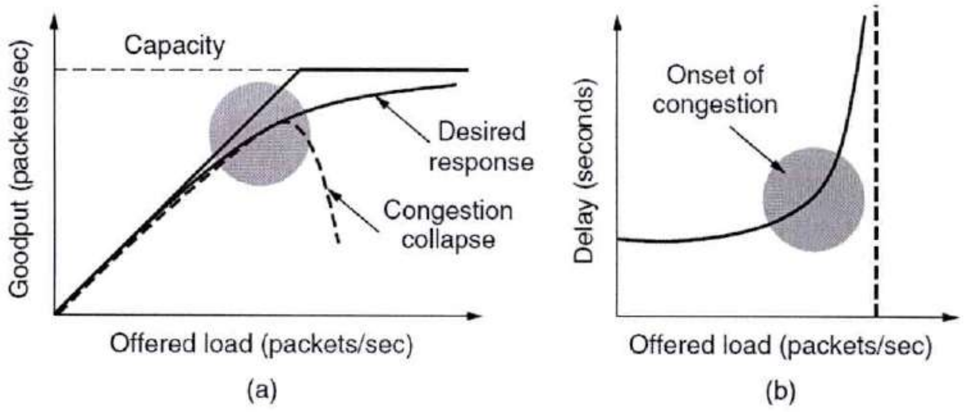


Figure 6-19. (a) Goodput and (b) delay as a function of offered load.

As the load increases in Fig. 6-19(a) goodput initially increases at the same rate, but as the load approaches the capacity, goodput rises more gradually. This falloff is because bursts of traffic can occasionally mount up and cause some losses at buffers inside the network. If the transport protocol is poorly designed and retransmits packets that have been delayed but not lost, the network can enter congestion collapse. In this state, senders are furiously sending packets, but increasingly little useful work is being accomplished.

The corresponding delay is given in Fig. 6-19(b) Initially the delay is fixed, representing the propagation delay across the network. As the load approaches the capacity, the delay rises, slowly at first and then much more rapidly. This is again because of bursts of traffic that tend to mound up at high load. The delay cannot

really go to infinity, except in a model in which the routers have infinite buffers. Instead, packets will be lost after experiencing the maximum buffering delay. For both goodput and delay, performance begins to degrade at the onset of congestion. Intuitively, we will obtain the best performance from the network if we allocate bandwidth up until the delay starts to climb rapidly. This point is below the capacity. To identify it, Kleinrock (1979) proposed the metric of **power**, where

power = load / delay

Power will initially rise with offered load, as delay remains small and roughly constant, but will reach a maximum and fall as delay grows rapidly. The load with the highest power represents an efficient load for the transport entity to place on the network.

b) **Max-Min Fairness:** The form of fairness that is often desired for network usage is **max-min fairness**. An allocation is max-min fair if the bandwidth given to one flow cannot be increased without decreasing the bandwidth given to another flow with an allocation that is no larger. That is, increasing the bandwidth of a flow will only make the situation worse for flows that are less well off.

Let us see an example. A max-min fair allocation is shown for a network with four flows, *A*, *B*, *C*, and *D*, in Fig. 6-20. Each of the links between routers has the same capacity, taken to be 1 unit, though in the general case the links will have different capacities. Three flows compete for the bottom-left link between routers *R4* and *R5*. Each of these flows therefore gets 1/3 of the link. The remaining flow, *A*, competes with *B* on the link from *R2* to *R3*. Since *B* has an allocation of 1/3, *A* gets the remaining 2/3 of the link. Notice that all of the other links have spare capacity. However, this capacity cannot be given to any of the flows without decreasing the capacity of another, lower flow. For example, if more of the bandwidth on the link between *R2* and *R3* is given to flow *B*, there will be less for flow *A*. This is reasonable as flow *A* already has more bandwidth. However, the capacity of flow *C* or *D* (or both) must be decreased to give more bandwidth to *B*, and these flows will have less bandwidth than *B*. Thus, the allocation is max-min fair.

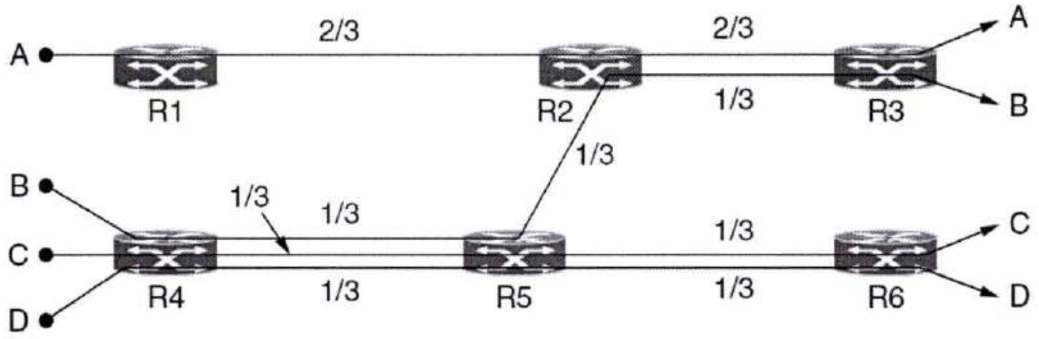


Fig 6.20: Max-min bandwidth allocation for four flows.

c) **Convergence:** A good congestion control algorithm should rapidly converge to the ideal operating point, and it should track that point as it changes over time. If the convergence is too slow, the algorithm will never be close to the changing operating point. If the algorithm is not stable, it may fail to converge to the right point in some cases, or even oscillate round the right point. An example of a bandwidth allocation that changes over time and converges quickly is shown in Fig. 6-21. Initially, flow 1 has all of the bandwidth. One second later, flow 2 starts. It needs bandwidth as well. The allocation quickly changes to give each of these flows half the bandwidth. At 4 seconds, a third flow joins. However, this flow uses only 20% of the bandwidth, which is less than its fair share (which is a third). Flows 1 and 2 quickly adjust, dividing the available bandwidth to each have 40% of the bandwidth. At 9 seconds, the second flow leaves, and the third flow remains unchanged. The first flow quickly captures 80% of the bandwidth. At all times, the total allocated bandwidth is approximately 100%, so that the network is fully used, and competing flows get equal treatment

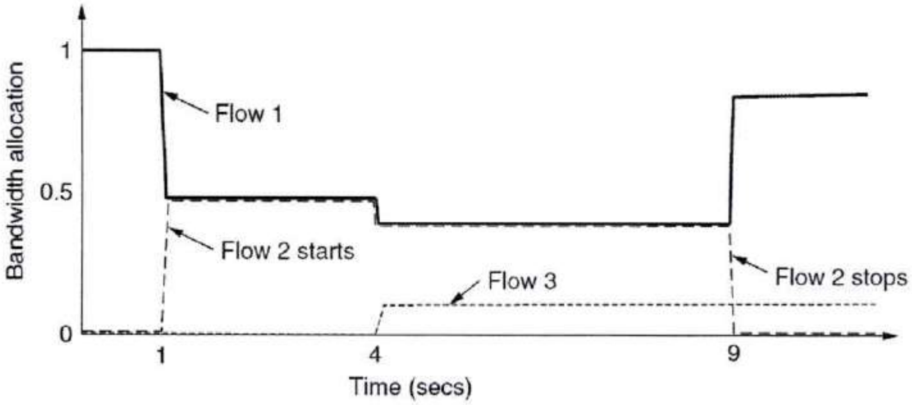


Figure 6-21. Changing bandwidth allocation over time.

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

2. Regulating the Sending Rate: Now it is time for the main course. How do we regulate the sending rates to obtain a desirable bandwidth allocation? The sending rate may be limited by two factors. The first is flow control, in the case that there is insufficient buffering at the receiver. The second is congestion, in the case that there is insufficient capacity in the network.

In Fig. 6-22, we see this problem illustrated hydraulically. In Fig. 6-22(a), we see a thick pipe leading to a small-capacity receiver. This is a flow-control limited situation. As long as the sender does not send more water than the bucket can contain, no water will be lost. In Fig. 6-22(b), the limiting factor is not the bucket capacity, but the internal carrying capacity of the network. If too much water comes in too fast, it will back up and some will be lost (in this case, by overflowing the funnel). These cases may appear similar to the sender, as transmitting too fast causes packets to be lost. However, they have different causes and call for different solutions. We have already talked about a flow-control solution with a variable-sized window. Now we will consider a congestion control solution. Since either of these problems can occur, the transport protocol will in general need to run both solutions and slow down if either problem occurs. The way that a transport protocol should regulate the sending rate depends on the form of the feedback returned by the network. Different network layers may return different kinds of feedback. The feedback may be explicit or implicit, and it may be precise or imprecise. An example of an explicit, precise design is when routers tell the sources the rate at which they may send. Designs in the literature such as XCP (eXplicit Congestion Protocol) operate in this manner. An explicit, imprecise design is the use of ECN (Explicit Congestion Notification) with TCP. In this design, routers set bits on packets that experience congestion to warn the senders to slow down, but they do not tell them how much to slow down.

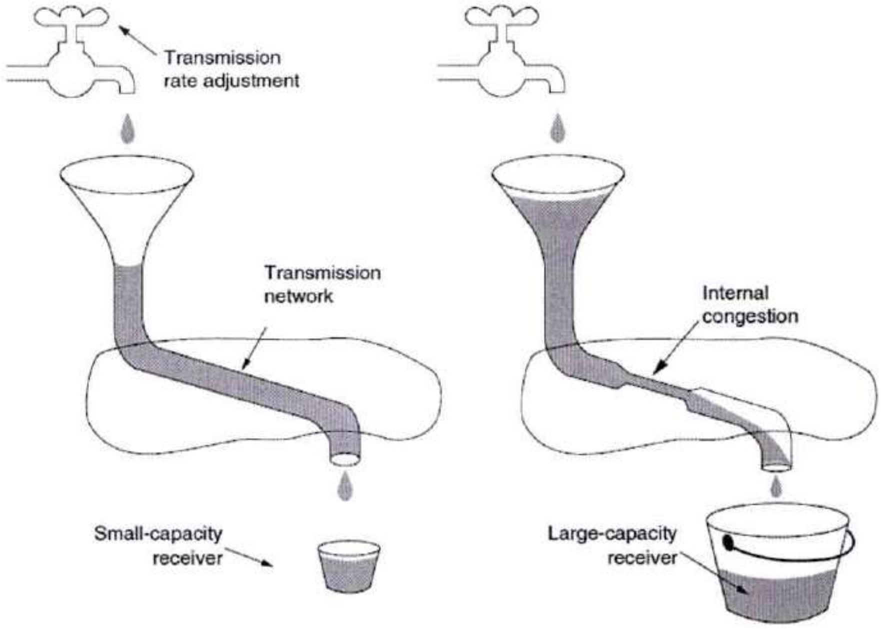


Figure 6-22. (a) A fast network feeding a low-capacity receiver. (b) A slow network feeding a high-capacity receiver.

In other designs, there is no explicit signal. FAST TCP measures the roundtrip delay and uses that metric as a signal to avoid congestion (Wei et al., 2006). Finally, in the form of congestion control most prevalent in the Internet today, TCP with drop-tail or RED routers, packet loss is inferred and used to signal that the network has become congested. There are many variants of this form of TCP, including CUBIC TCP, which is used in Linux (Ha et al., 2008). Combinations are also possible. For example, Windows includes Compound TCP that uses both packet loss and delay as feedback signals (Tan et al., 2006). These designs are summarized in Fig. 6-23. If an explicit and precise signal is given, the transport entity can use that signal to adjust its rate to the new operating point. For example, if XCP tells senders the rate to use, the senders may simply use that rate. In the other cases, however, some guesswork is involved. In the absence of a congestion signal, the senders should decrease their rates. When a congestion signal is given, the senders should decrease their rates. The way in which the rates are increased or decreased is given by a **control law**.

Protocol	Signal	Explicit?	Precise?
XCP	Rate to use	Yes	Yes
TCP with ECN	Congestion warning	Yes	No
FAST TCP	End-to-end delay	No	Yes
Compound TCP	Packet loss & end-to-end delay	No	Yes
CUBIC TCP	Packet loss	No	No
TCP	Packet loss	No	No

Figure 6-23. Signals of some congestion control protocols.

AIMD (Additive Increase Multiplicative Decrease) is the appropriate control law to arrive at the efficient and fair operating point. To argue this case, they constructed a graphical argument for the simple case of two connections competing for the bandwidth of a single link. The graph in Fig. 6-24 shows the bandwidth allocated to user 1 on the x-axis and to user 2 on the y-axis. When the allocation is fair, both users will receive the same amount of bandwidth. This is shown by the dotted fairness line. When the allocations sum to 100%, the capacity of the link, the allocation is efficient. This is shown by the dotted efficiency line. A congestion signal is given by the network to both users when the sum of their allocations crosses this line. The intersection of these lines is the desired operating point, when both users have the same bandwidth and all of the network bandwidth is used.

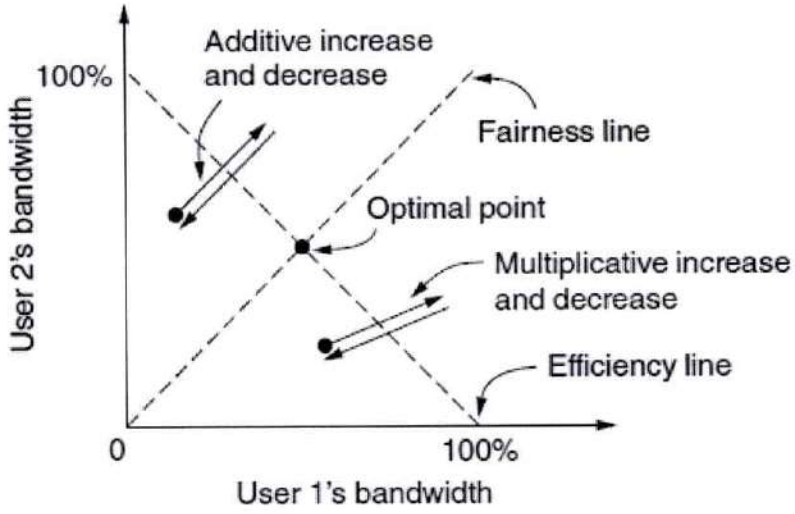


Figure 6-24. Additive and multiplicative bandwidth adjustments.

Consider what happens from some starting allocation if both user 1 and user 2 additively increase their respective bandwidths over time. For example, the users may each increase their sending rate by 1 Mbps every second. Eventually, the operating point crosses the efficiency line and both users receive a congestion signal from the network. At this stage, they must reduce their allocations. However, an additive decrease would simply cause them to oscillate along an additive line. This situation is shown in Fig. 6-24. The behavior will keep the operating point close to efficient, but it will not necessarily be fair. Similarly, consider the case when both users multiplicatively increase their bandwidth over time until they receive a congestion signal. For example, the users may increase their sending rate by 10% every second. If they then multiplicatively decrease their sending rates, the operating point of the users will simply oscillate along a multiplicative line. This behavior is also shown in Fig. 6-24. The multiplicative line has a different slope than the additive line. (It points to the origin, while the additive line has an angle of 45 degrees.) But it is otherwise no better. In neither case will the users converge to the optimal sending rates that are both fair and efficient. Now consider the case that the users additively increase their bandwidth allocations and then multiplicatively decrease them when congestion is signaled. This behavior is the AIMD control law, and it is shown in Fig. 6-25. It can be seen that the path traced by this behavior does converge to the optimal point that is both fair and efficient. This convergence happens no matter what the starting point, making AIMD broadly useful. By the same argument, the only other combination, multiplicative increase and additive decrease, would diverge from the optimal point.

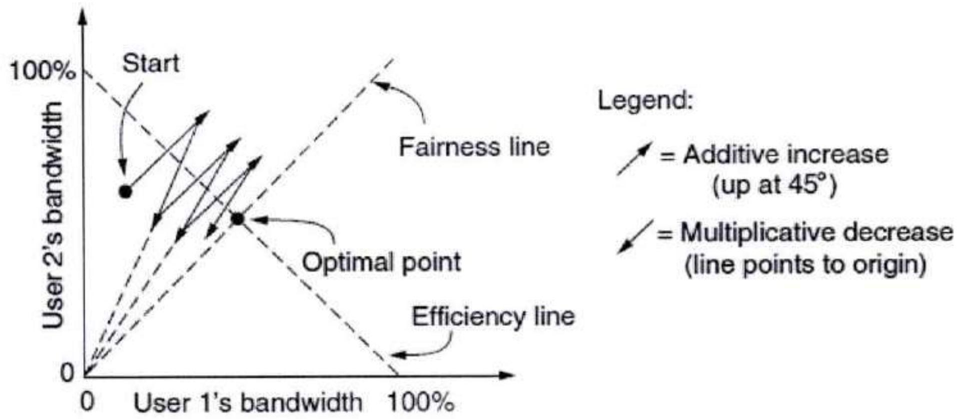


Figure 6-25. Additive Increase Multiplicative Decrease (AIMD) control law.

AIMD is the control law that is used by TCP, based on this argument and another stability argument (that it is easy to drive the network into congestion and difficult to recover, so the increase policy should be gentle and the decrease policy aggressive). It is not quite fair, since TCP connections adjust their window size by a given amount every round-trip time. Different connections will have different round-trip times. This leads to a bias in which connections to closer hosts receive more bandwidth than connections to distant hosts, all else being equal. In Sec. 6.5, we will describe in detail how TCP implements an AIMD control law to adjust the sending rate and provide congestion control. This task is more difficult than it sounds because rates are measured over some interval and traffic is bursty. Instead of adjusting the rate directly, a strategy that is often used in practice is to adjust the size of a sliding window. TCP uses this strategy. If the window size is *W* and the round-trip time is *RTT*, the equivalent rate is *W/RTT*. This strategy is easy to combine with flow control, which already uses a window, and has the advantage that the sender paces packets using acknowledgements and hence slows down in one *RTT* if it stops receiving reports that packets are leaving the network.

Wireless Issues: Transport protocols such as TCP that implement congestion control should be independent of the underlying network and link layer technologies. That is a good theory, but in practice there are issues with wireless networks. The main issue is that packet loss is often used as a congestion signal, including by TCP as we have just discussed. Wireless networks lose packets all the time due to transmission errors. With the AIMD control law, high throughput requires very small levels of packet loss. Analyses by Padhye et al. (1998) show that the throughput goes up as the inverse square-root of the packet loss rate. What this means in practice is that the loss rate for fast TCP connections is very small; 1% is a moderate loss rate, and by the time the loss rate reaches 10% the connection has effectively stopped working. However, for wireless networks such as 802.11 LANs, frame loss rates of at least 10% are common. This difference means that, absent protective measures, congestion control schemes that use packet loss as a signal will unnecessarily

throttle connections that run over wireless links to very low rates. To function well, the only packet losses that the congestion control algorithm should observe are losses due to insufficient bandwidth, not losses due to transmission errors. One solution to this problem is to mask the wireless losses by using retransmissions over the wireless link. For example, 802.11 uses a stop and- wait protocol to deliver each frame, retrying transmissions multiple times if need be before reporting a packet loss to the higher layer. In the normal case, each packet is delivered despite transient transmission errors that are not visible to the higher layers. Fig. 6-26 shows a path with a wired and wireless link for which the masking strategy is used. There are two aspects to note. First, the sender does not necessarily know that the path includes a wireless link, since all it sees is the wired link to which it is attached. Internet paths are heterogeneous and there is no general method for the sender to tell what kind of links comprise the path. This complicates the congestion control problem, as there is no easy way to use one protocol for wireless links and another protocol for wired links.

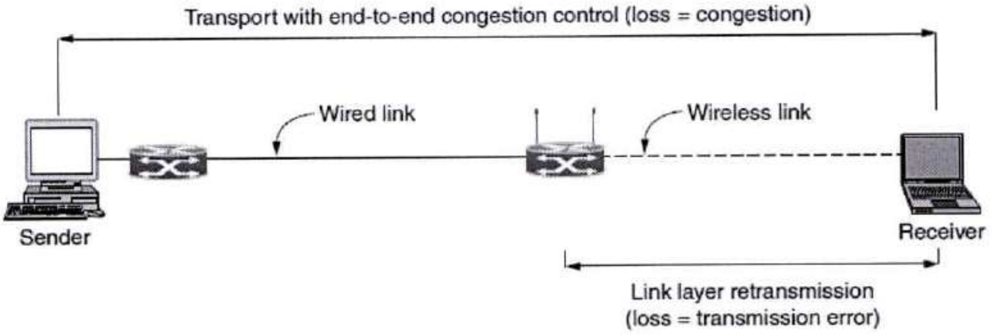

Transport with end-to-end congestion control (loss = congestion)
Wired link
Wireless link
Sender
Receiver
Link layer retransmission
(loss = transmission error)

Figure 6-26. Congestion control over a path with a wireless link.

The figure shows two mechanisms that are driven by loss: link layer frame retransmissions, and transport layer congestion control.

Introduction to UDP

The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism.

In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

Requirement of UDP

A question may arise, why do we need an unreliable protocol to transport the data? We deploy UDP where the acknowledgement packets share significant amount of bandwidth along with the actual data. For example, in case of video streaming, thousands of packets are forwarded towards its users. Acknowledging all the packets is troublesome and may contain huge amount of bandwidth wastage. The best delivery mechanism of underlying IP protocol ensures best efforts to deliver its packets, but even if some packets in video streaming get lost, the impact is not calamitous and can be ignored easily. Loss of few packets in video and voice traffic sometimes goes unnoticed.

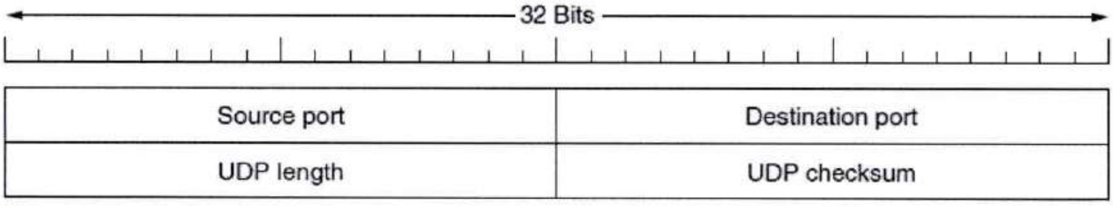
Features

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.

- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

UDP Header

UDP header is as simple as its function. UDP header contains four main parameters:



Source port	Destination port
UDP length	UDP checksum

Figure 6-27. The UDP header.

- **Source Port** - This 16 bits information is used to identify the source port of the packet.
- **Destination Port** - This 16 bits information, is used identify application level service on destination machine.
- **Length** - Length field specifies the entire length of UDP packet (including header). It is 16-bits field and minimum value is 8-byte, i.e. the size of UDP header itself.
- **Checksum** - This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional so when checksum field does not contain any value it is made 0 and all its bits are set to zero.

UDP application

Here are few applications where UDP is used to transmit data:

- Domain Name Services
- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol
- Kerberos

Transmission Control Protocol (TCP)

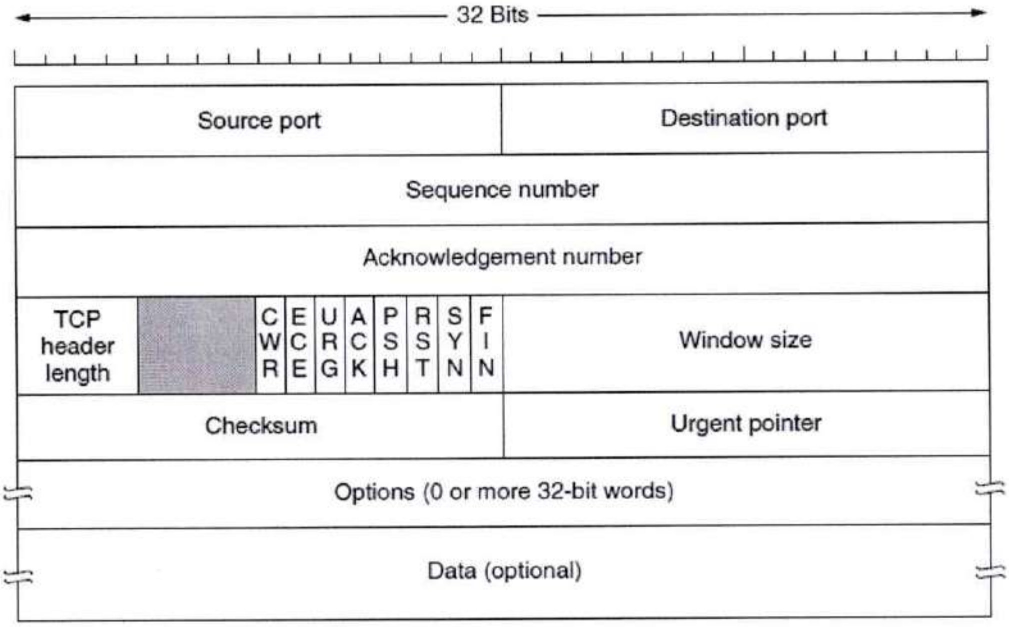
The transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.

Features

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.



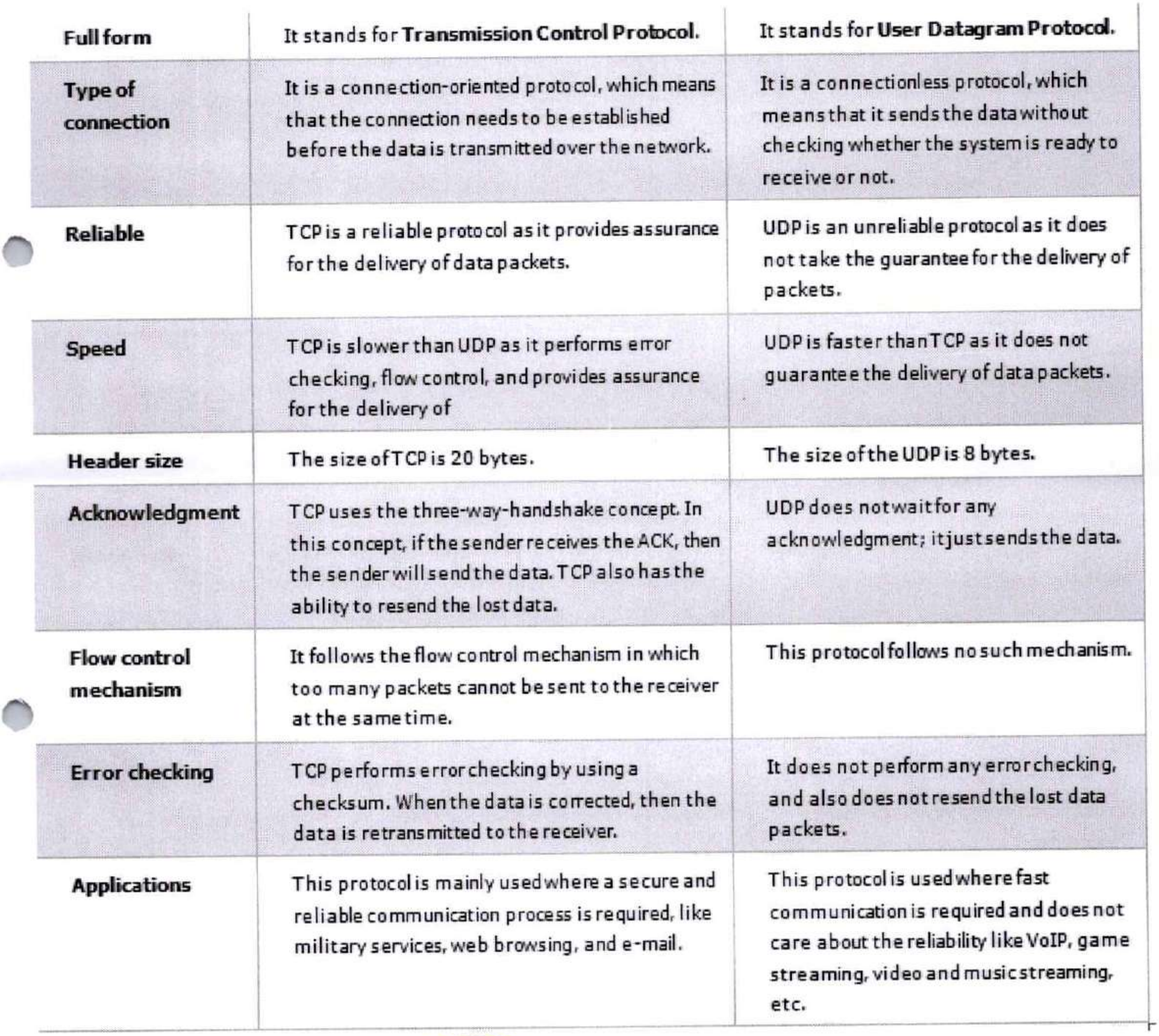
- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.

- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
  - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
  - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
  - **ECE** -It has two meanings:
    - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
    - If SYN bit is set to 1, ECE means that the device is ECT capable.
  - **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
  - **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
  - **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
  - **RST** - Reset flag has the following features:
    - It is used to refuse an incoming connection.
    - It is used to reject a segment.
    - It is used to restart a connection.
  - **SYN** - This flag is used to set up a connection between hosts.
  - **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.
- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.

- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

Difference between TCP and UDP

TCP **UDP**



Full form	It stands for **Transmission Control Protocol.**	It stands for **User Datagram Protocol.**
Type of connection	It is a connection-oriented protocol, which means that the connection needs to be established before the data is transmitted over the network.	It is a connectionless protocol, which means that it sends the data without checking whether the system is ready to receive or not.
Reliable	TCP is a reliable protocol as it provides assurance for the delivery of data packets.	UDP is an unreliable protocol as it does not take the guarantee for the delivery of packets.
Speed	TCP is slower than UDP as it performs error checking, flow control, and provides assurance for the delivery of	UDP is faster than TCP as it does not guarantee the delivery of data packets.
Header size	The size of TCP is 20 bytes.	The size of the UDP is 8 bytes.
Acknowledgment	TCP uses the three-way-handshake concept. In this concept, if the sender receives the ACK, then the sender will send the data. TCP also has the ability to resend the lost data.	UDP does not wait for any acknowledgment; it just sends the data.
Flow control mechanism	It follows the flow control mechanism in which too many packets cannot be sent to the receiver at the same time.	This protocol follows no such mechanism.
Error checking	TCP performs error checking by using a checksum. When the data is corrected, then the data is retransmitted to the receiver.	It does not perform any error checking, and also does not resend the lost data packets.
Applications	This protocol is mainly used where a secure and reliable communication process is required, like military services, web browsing, and e-mail.	This protocol is used where fast communication is required and does not care about the reliability like VoIP, game streaming, video and music streaming, etc.

TCP Connection Establishment (Three-way handshake)

Connections are established in TCP by means of the three-way handshake.

- To establish a connection, one side, say, the server passively waits for an incoming connection by executing the LISTEN and ACCEPTS primitives in that order, either specifying a specific source or nobody in particular.
- The other side, say, the client, executes a CONNECT primitive, specifying the IP address and port to which it wants to connect, the maximum TCP segment size it is willing to accept, and optionally some user data (e.g., a password).
- The CONNECT primitive sends a TCP segment with the *SYN* bit on and *ACK* bit off and waits for a response. When this segment arrives at the destination, the TCP entity there checks to see if there is a process that has done a LISTEN on the port given in the *Destination port* field. If not, it sends a reply with the *RST* bit on to reject the connection.
- If some process is listening to the port, that process is given the incoming TCP segment. It can either accept or reject the connection. If it accepts, an acknowledgement segment is sent back. The sequence of TCP segments sent in the normal case is shown in Fig. 6-37(a).

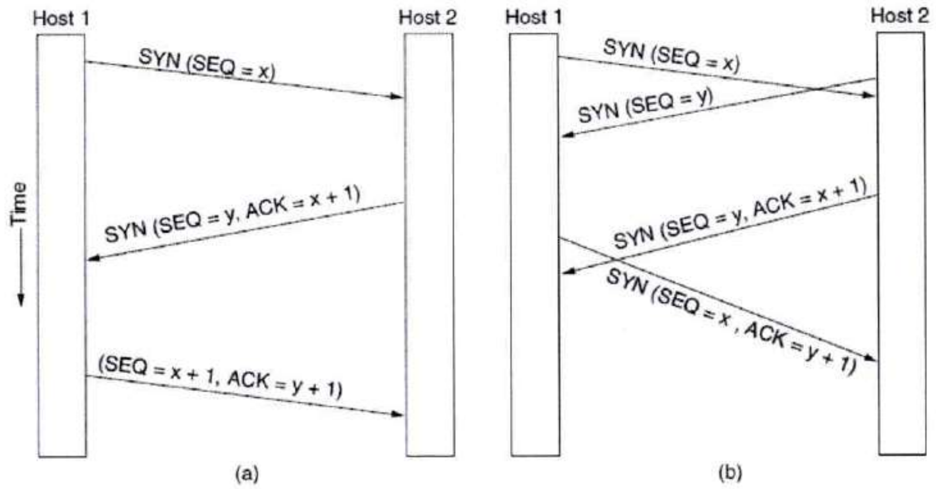

Host 1
Host 2
Host 1
Host 2
SYN (SEQ = x)
SYN (SEQ = y, ACK = x + 1)
(SEQ = x + 1, ACK = y + 1)
Time
SYN (SEQ = x)
SYN (SEQ = y)
SYN (SEQ = y, ACK = x + 1)
SYN (SEQ = x, ACK = y + 1)
(a)
(b)

Figure 6-37. (a) TCP connection establishment in the normal case. (b) Simultaneous connection establishment on both sides.

In the event that two hosts simultaneously attempt to establish a connection between the same two sockets, the sequence of events is as illustrated in Fig. 6- 37(b). The result of these events is that just one connection is established, not two, because connections are identified by their end points. If the first setup results in a connection identified by (*x*, *y*) and the second one does too, only one table entry is made, namely, for (*x*, *y*).

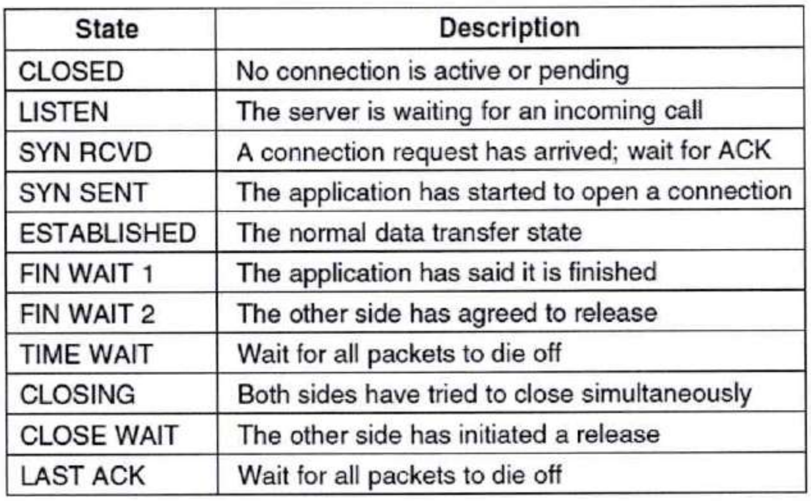
TCP Connection Release

Although TCP connections are full duplex, to understand how connections are released it is best to think of them as a pair of simplex connections. Each simplex connection is released independently of its sibling. To release a connection, either party can send a TCP segment with the *FIN* bit set, which means that it has no more data to transmit. When the *FIN* is acknowledged, that direction is shut down for new data. Data may continue to flow indefinitely in the other direction, however. When both directions have been shut down, the connection is released.

Normally, four TCP segments are needed to release a connection: one *FIN* and one *ACK* for each direction. However, it is possible for the first *ACK* and the second *FIN* to be contained in the same segment, reducing the total count to three. Just as with telephone calls in which both people say goodbye and hang up the phone simultaneously, both ends of a TCP connection may send *FIN* segments at the same time. These are each acknowledged in the usual way, and the connection is shut down. There is, in fact, no essential difference between the two hosts releasing sequentially or simultaneously.

TCP Connection Management Modeling

The steps required establishing and release connections can be represented in a finite state machine with the 11 states listed in Fig. 6-38. In each state, certain events are legal. When a legal event happens, some action may be taken. If some other event happens, an error is reported. Each connection starts in the *CLOSED* state. It leaves that state when it does either a passive open (LISTEN) or an active open (CONNECT). If the other side does the opposite one, a connection is established and the state becomes *ESTABLISHED*. Connection release can be initiated by either side. When it is complete, the state returns to *CLOSED*. The finite state machine itself is shown in Fig. 6-39. The common case of a client actively connecting to a passive server is shown with heavy lines—solid for the client, dotted for the server. The lightface lines are unusual event sequences.



State	Description
CLOSED	No connection is active or pending
LISTEN	The server is waiting for an incoming call
SYN RCVD	A connection request has arrived; wait for ACK
SYN SENT	The application has started to open a connection
ESTABLISHED	The normal data transfer state
FIN WAIT 1	The application has said it is finished
FIN WAIT 2	The other side has agreed to release
TIME WAIT	Wait for all packets to die off
CLOSING	Both sides have tried to close simultaneously
CLOSE WAIT	The other side has initiated a release
LAST ACK	Wait for all packets to die off

Figure 6-38. The states used in the TCP connection management finite state machine.

Each line in Fig. 6-39 is marked by an *event/action* pair. The event can either be a user-initiated system call (CONNECT, LISTEN, SEND, or CLOSE), a segment arrival (*SYN*, *FIN*, *ACK*, or *RST*), or, in one case, a timeout of twice the maximum packet lifetime. The action is the sending of a control segment (*SYN*, *FIN*, or *RST*) or nothing, indicated by —. Comments are shown in parentheses. One can best understand the diagram by first following the path of a client (the heavy solid line), then later following the path of a server (the heavy dashed line). When an application program on the client machine issues a CONNECT request, the local TCP entity creates a connection record, marks it as being in the *SYN SENT* state, and shoots off a *SYN* segment. Note that many connections may be open (or being opened) at the same time on behalf of multiple applications, so the state is per connection and recorded in the connection record. When the *SYN+ACK* arrives, TCP sends the final *ACK* of the three-way handshake and switches into the *ESTABLISHED* state.

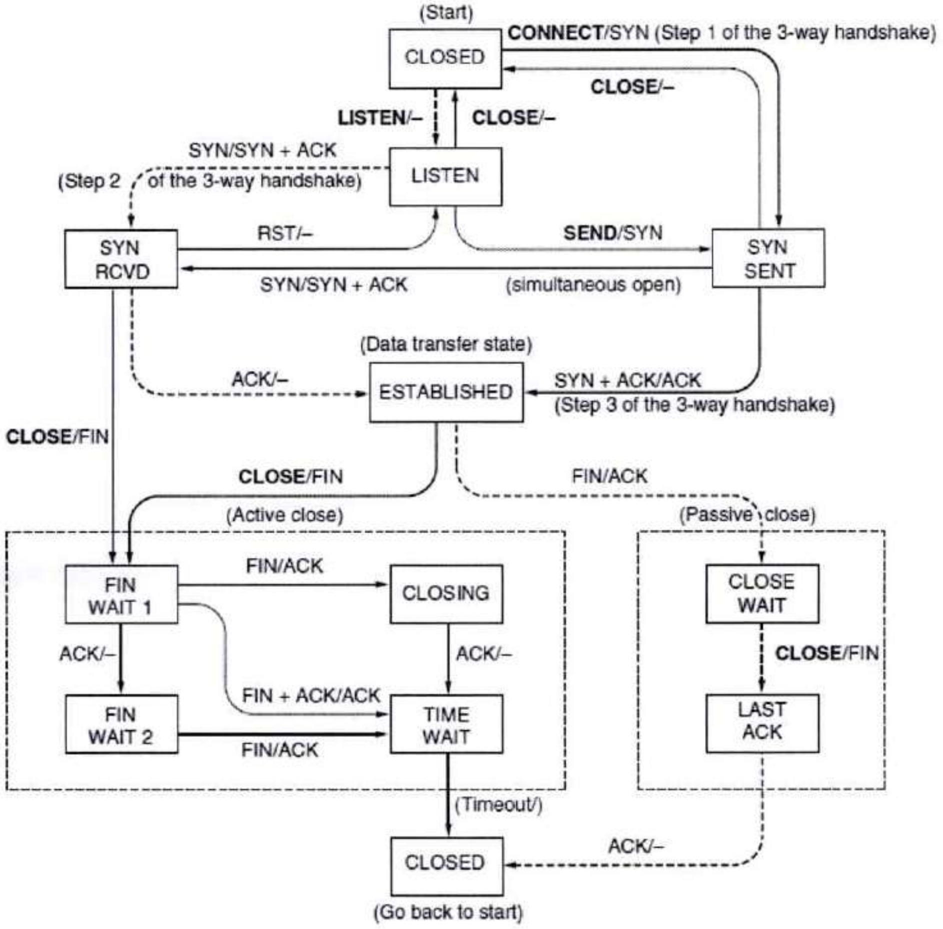
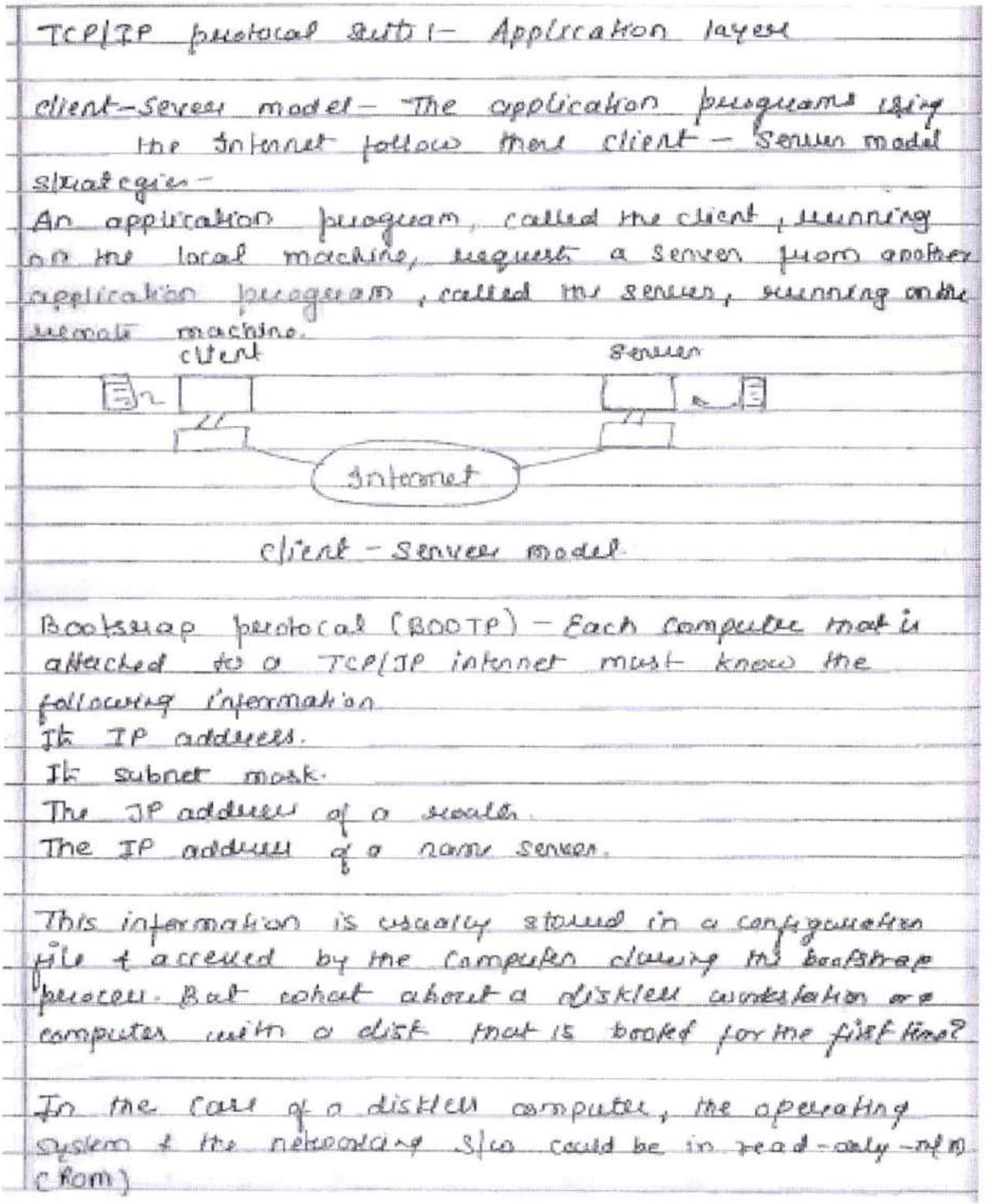


Figure 6-39. TCP connection management finite state machine. The heavy solid line is the normal path for a client. The heavy dashed line is the normal path for a server. The light lines are unusual events. Each transition is labeled with the event causing it and the action resulting from it, separated by a slash.

Data can now be sent and received. When an application is finished, it executes a CLOSE primitive, which causes the local TCP entity to send a *FIN* segment and wait for the corresponding *ACK* (dashed box marked ''active close''). When the *ACK* arrives, a transition is made to the state *FIN WAIT 2* and one direction of the connection is closed. When the other side closes, too, a *FIN* comes in, which is acknowledged. Now both sides are closed, but TCP waits a time equal to twice the maximum packet lifetime to guarantee that all packets from the connection have died off, just in case the acknowledgement was lost. When the timer goes off, TCP deletes the connection record. Now let us examine connection management from the server's viewpoint. The server does a LISTEN and settles down to see who turns up. When a *SYN* comes in, it is acknowledged and the server goes to the *SYN RCVD* state. When the server's *SYN* is itself acknowledged, the three-way handshake is complete and the server goes to the *ESTABLISHED* state. Data transfer can now occur. When the client is done transmitting its data, it does a CLOSE, which causes a *FIN* to arrive at the server (dashed box marked ''passive close''). The server is then signaled. When it, too, does a CLOSE, a *FIN* is sent to the client. When the client's acknowledgement shows up, the server releases the connection and deletes the connection record.

THE END

Application Layer :



TCP/IP protocal suit :- Application layer

client-server model - The application programs using the Internet follow these client - Server model strategies -

An application program, called the client, running on the local machine, request a server from another application program, called the server, running on the remote machine.

client
Server
Internet

client - server model

Bootsrap protocal (BOOTP) - Each computer that is attached to a TCP/IP internet must know the following information

Its IP address.

Its subnet mask.

The IP address of a router.

The IP address of a name server.

This information is usually stored in a configuration file & accessed by the computer during the bootstrap process. But what about a diskless workstation or a computer with a disk that is booted for the first time?

In the case of a diskless computer, the operating system & the networking s/w could be in read-only-mem (Rom)

BOOTP is a client-Server protocal designed to provide the four previously mentioned pieces of information for a diskless computer or a computer that is booted for the first time. If we use BOOTP, we do not need RARP.

Dynamic Host configuration protocal (DHCP):- BOOTP is not a dynamic configuration protocal. When a client request is IP address, the BOOTP server searches a table that matches the physical address of the client with its IP address. This implies that the binding b/w the physical address & the IP address of the client should already exist. The binding is predetermined.

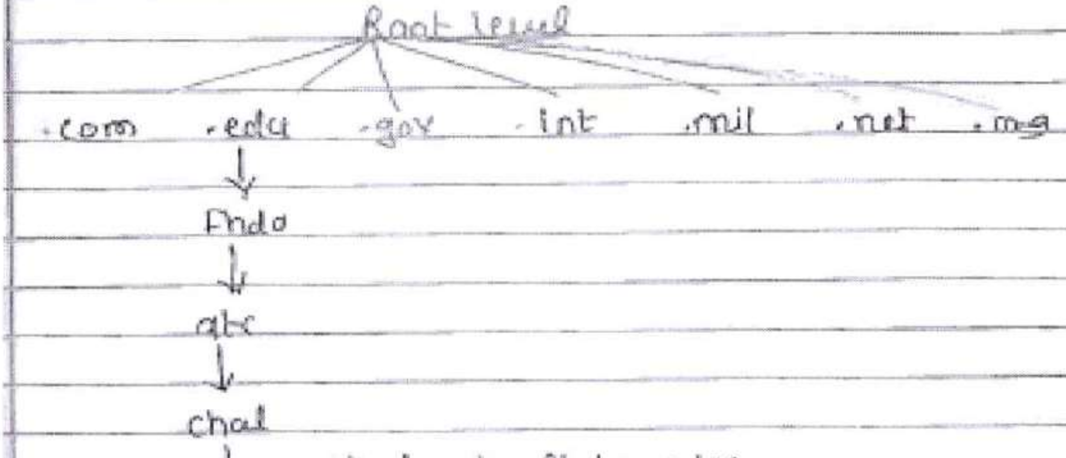
DHCP has been devised to provide dynamic configuration. It is an extension to BOOTP. It provides temporary IP addresses for a limited period of time.

Domain Name System:- To identify an entity, TCP/IP protocols use the IP address, which uniquely identifies the connection of a host to the Internet. However, people prefer to use names instead of addresses.

DNS is a protocol that ~~the~~ can be used in different platforms. It is divided into three different sections:- generic domains, country domains & inverse domains.

Generic domains:- define registered host according to their generic behavior. Each node in the tree defines a domain, which is an index to the domain name space database.

It allow three-character labels.



↳ chal.atc.fhda.edu
Index to address.

Generic domain labels -

Label	Descriptions
com	commercial organizations
edu	Educational institutions
gov	Government institutions
int	International organizations
mil	Military groups
net	Network support centers
org	Non-profit organizations

proposed generic domain labels

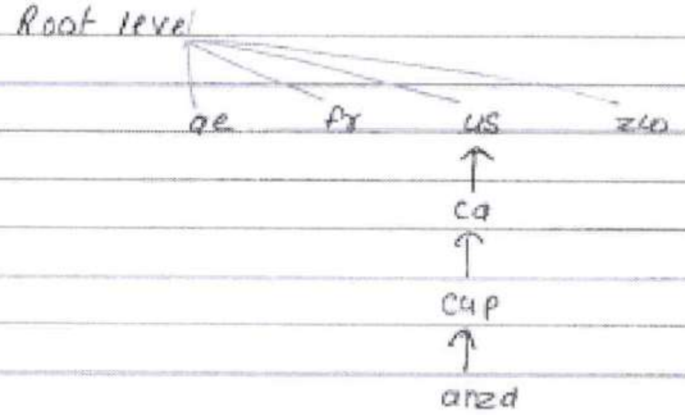
Label	Descriptions
arts	cultural organizations
firm	Businesses or firms
info	Information service providers
nom	Personal nomenclatures
rec	Recreation / entertainment organizations
store	Business offering goods to purchase
web	web-related organizations

Vignan's Institute of Management & Technology For Women
Kondapur (V), Ghatkesar (M), Medchal Malkajgiri (Dt.) Pin-501301 (T.S.)

PRINCIPAL
Vignan's Institute of Management & Technology For Women
Kondapur(V),Ghatkesar(M),Medchal-Malkajgiri(Dt)-501301
Telangana State

country Domains - follows the same format as the generic domains but uses two-charactere country abbreviations. In place of three charactere organizational abbreviations at the first level

country domains -

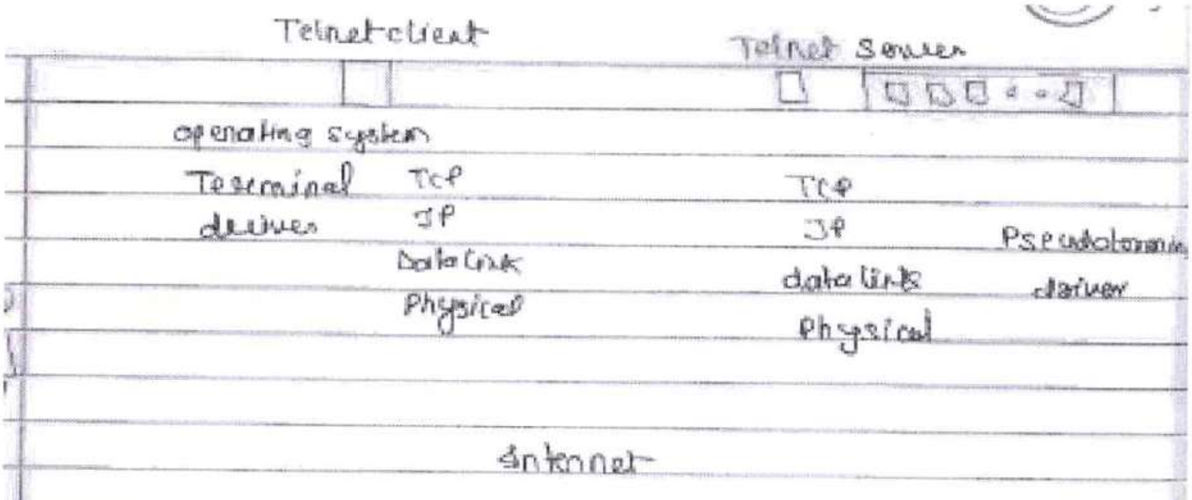


anza. cup. ca. us
Index to address.

Inverse domain - used to map an address to a name

Example - when a Server has received a request from a client to do a task. whereas the Server has a file that contains a list of authorized clients, the server lists only the IP address of the client. To determine, if the client is on the authorize list, it can send a query to the DNS Server & ask for a mapping of address to name.

Telnet - is a general - purpose client - Server application program. It enables the establishment of a connection & to a remote system in such a way that the local terminal appears to be a terminal at the remote system.

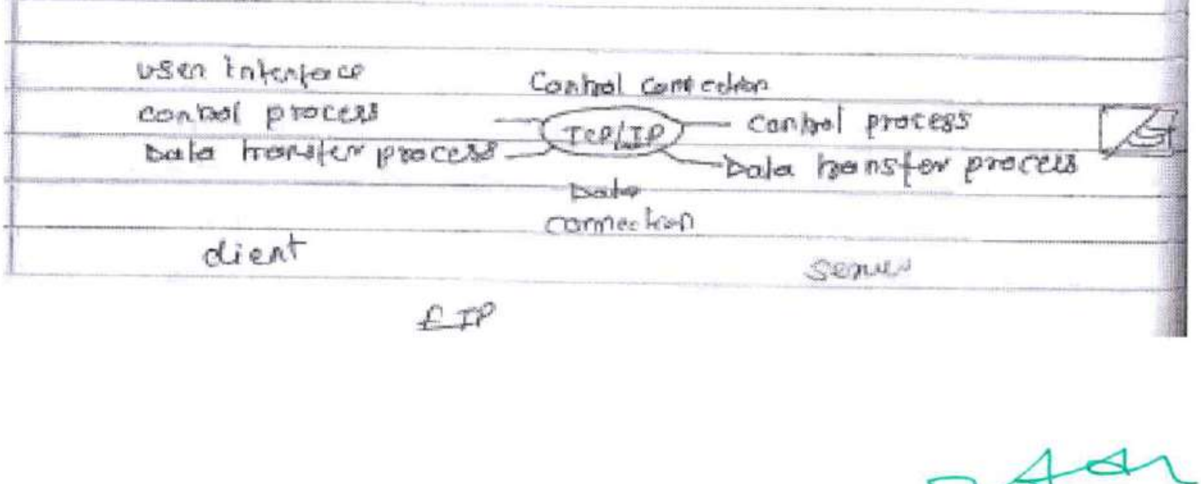


Remote login

File Transfer protocol (FTP):- is the standard mechanism provided by TCP/IP for copying a file from one host to another

Example:- Two systems may use different file name conventions, or may have different ways to represent text & data, or may have different directory structures. All of these problems have been solved by FTP in a very simple & elegant approach.

FTP differs from other-client-server applications in that it establishes two connection between the hosts. one connection is used for data transfer, the other for control information (commands + responses)



FTP

Trivial File Transfer Protocol - There are occasions when we need to simply copy a file without the need for all of the functionalities of the FTP protocol. It is designed for these types of file transfer. It is so simple that the software package can fit into the read-only mem of a diskless workstation. It can be used at bootstrap time It can read or write a file for the client.

Reading means copying a file from the server site to the client site.
Writing means copying a file from the client site to the server site

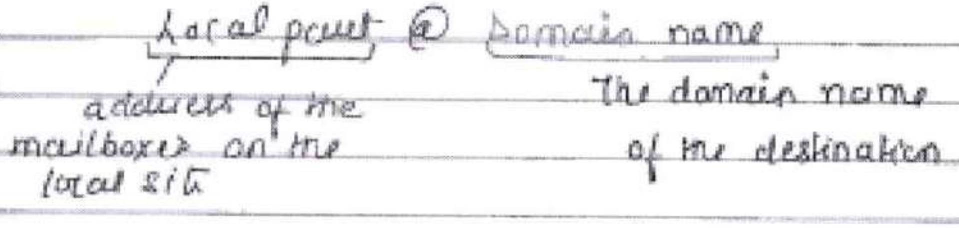
Example - when a diskless workstation or a router is booted, we need to download the bootstrap & configuration files. here we do not need all the sophistication provided in FTP, just need a protocol that quickly copies the files

Simple mail transfer protocol (SMTP):- One of the most popular network services is electronic mail (e-mail)
SMTP is a system for sending messages to other computer users based on e-mail addresses. It provides for mail exchange ~~based~~ between users on the same/ different computers & supports

Sending a single message to one or more recipients.
Sending messages that include text, voice, video or graphics
Sending messages to users on networks outside the Internet.

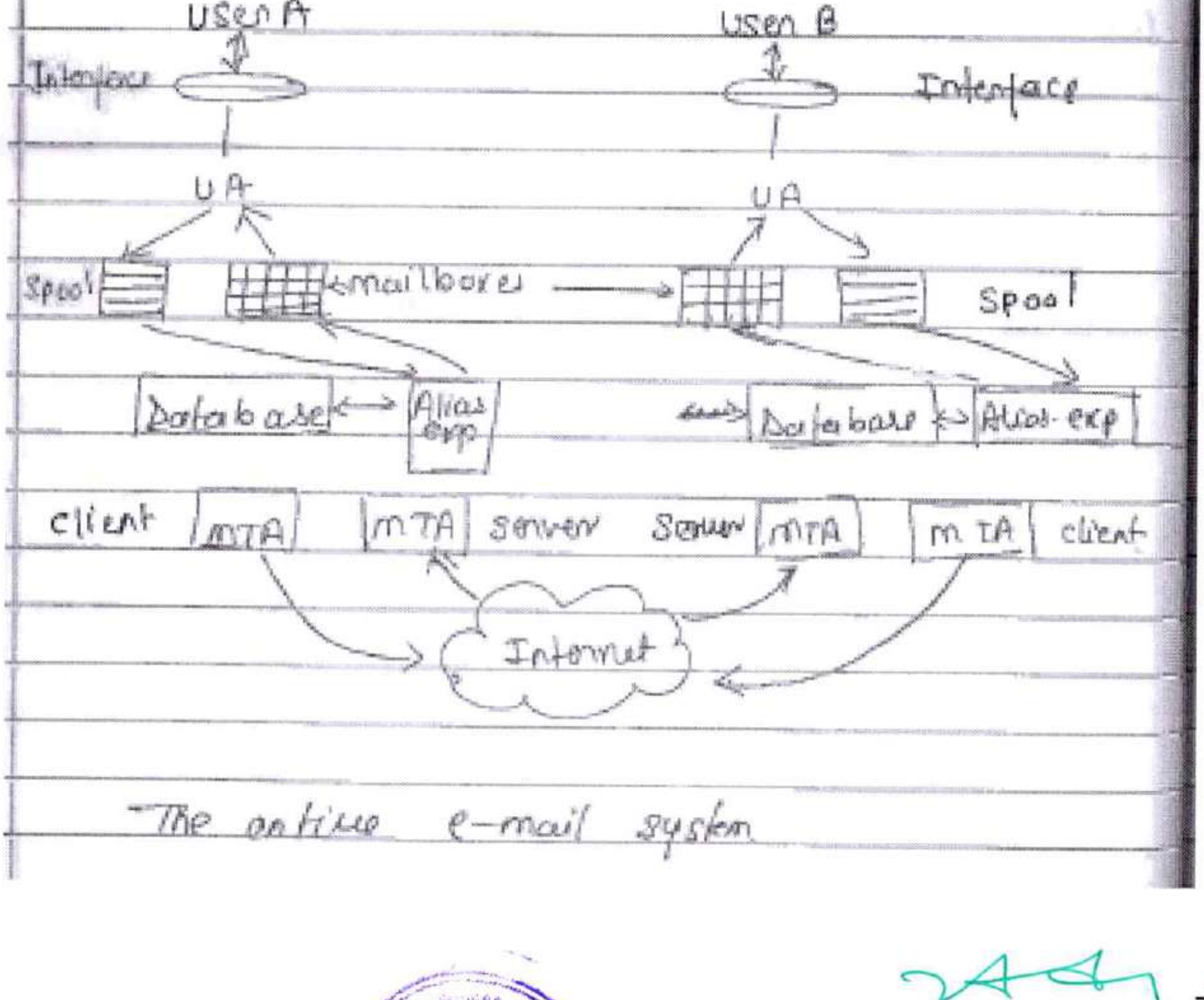
SMTP client and server into two components :- UA & MTA or user agent & mail transfer agent

User Agent (UA) is normally a program used to send & receive mail.



Local part @ Domain name
address of the mailboxes on the local site
The domain name of the destination

Mail transfer Agent :- The actual mail Transfer is done through mail transfer agents (MTAs). To send mail, a system must have a client MTA, and to receive mail, a system must have a server MTA



The entire e-mail system

Multipurpose Internet mail Extension :- SMTP is a simple mail transfer protocol. SMTP can send messages only in NVT seven-bit ASCII format.

Example - It can't be used for languages that are not supported by 7-bit ASCII character (such as French, German, Hebrew, Russian, chinese & Japanese). Also, it can't be used to binary files or to send video or ~~au~~ audio data.

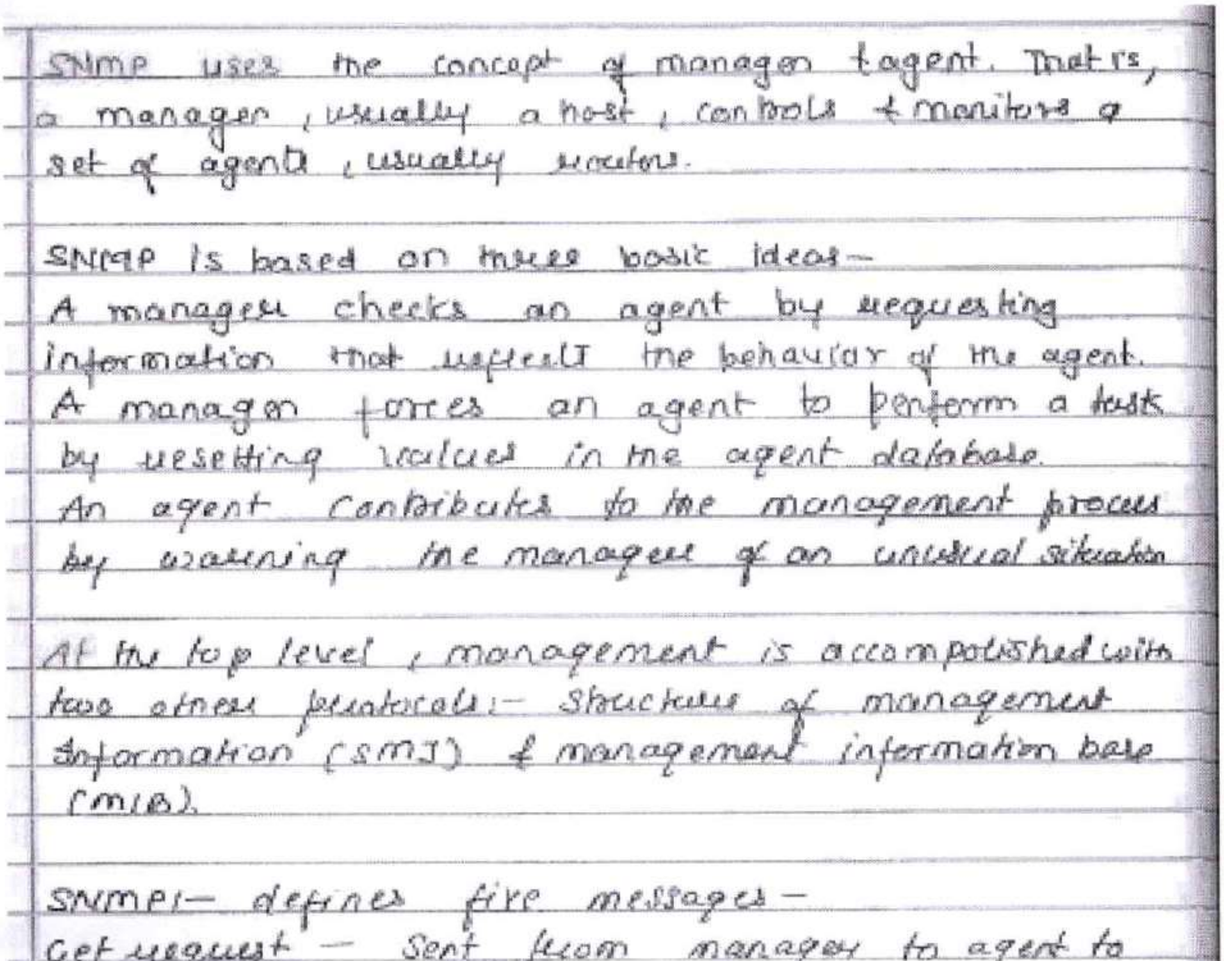
- MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME is not a mail protocol & can't replace SMTP, it is only an extension to SMTP

Post office protocol (POP) :- SMTP expects the destination host, the mail server receiving the mail, to be on-line all the time, otherwise, a TCP connection can't be established.

For this reason, it is not practical to establish an SMTP session with a desktop computer b/c desktop computers are usually powered down at the end of the day

In many organizations, mail is received by an SMTP server that is always on-line. This SMTP server provides a mail-drop service. The server receives the mail on behalf of every host in the organization. Workstations interact with the SMTP host to ~~receive~~ retrieve messages by using a client-server protocol such as Post-office-protocol (POP) version 3 (POP3)

SNMP :- Simple Network management protocol is a framework for managing devices in an internet using the TCP/IP protocol suite. It provides a set of fundamental operations for monitoring & maintaining an internet.



SNMP uses the concept of manager & agent. That is, a manager, usually a host, controls & monitors a set of agents, usually routers.

SNMP is based on three basic ideas—
A manager checks an agent by requesting information that reflect the behavior of the agent.
A manager forces an agent to perform a task by resetting values in the agent database.
An agent contributes to the management process by warning the manager of an unusual situation

At the top level, management is accomplished with two other protocols:— Structure of management Information (SMI) & management information base (MIB).

SNMP— defines five messages—
Get request — Sent from manager to agent to retrieve the value of a variable
GetNextRequest — Sent from manager to agent to retrieve the value of a variable. (The retrieved value is the value of the object following the defined object in the message)
Get Response — Sent from an agent to a manager in response to Get request & getnext response
Set request — Sent from manager to the agent to set (store) a value in a variable.
Trap — is sent from the agent to the manager to report an event.
example — If the agent is rebooted, it informs the manager & reports the time of rebooting.

THE END