NEHRU COLLEGE OF ENGINEERING AND RESEARCH CENTRE
(NAAC Accredited)
(Approved by AICTE, Affiliated to APJ Abdul Kalam Technological University, Kerala)

Moulding True Citizen
Since 1968

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

COURSE MATERIAL

CS 306 COMPUTER NETWORKS

VISION OF THE INSTITUTION

To mould true citizens who are millennium leaders and catalysts of change through excellence in education.

MISSION OF THE INSTITUTION

NCERC is committed to transform itself into a center of excellence in Learning and Research in Engineering and Frontier Technology and to impart quality education to mould technically competent citizens with moral integrity, social commitment and ethical values.

We intend to facilitate our students to assimilate the latest technological know-how and to imbibe discipline, culture and spiritually, and to mould them in to technological giants, dedicated research scientists and intellectual leaders of the country who can spread the beams of light and happiness among the poor and the underprivileged.

ABOUT DEPARTMENT

- Established in: 2002
- Courses offered : B.Tech in Computer Science and Engineering

  M.Tech in Computer Science and Engineering

  M.Tech in Cyber Security
- Approved by AICTE New Delhi and Accredited by NAAC
- Affiliated to the A P J Abdul Kalam Technological University.

DEPARTMENT VISION

Producing Highly Competent, Innovative and Ethical Computer Science and Engineering Professionals to facilitate continuous technological advancement.

DEPARTMENT MISSION

1. To Impart Quality Education by creative Teaching Learning Process
2. To Promote cutting-edge Research and Development Process to solve real world problems with emerging technologies.
3. To Inculcate Entrepreneurship Skills among Students.
4. To cultivate Moral and Ethical Values in their Profession.

PROGRAMME EDUCATIONAL OBJECTIVES

PEO1: Graduates will be able to Work and Contribute in the domains of Computer Science and Engineering through lifelong learning.

PEO2: Graduates will be able to Analyse, design and development of novel Software Packages, Web Services, System Tools and Components as per needs and specifications.

PEO3: Graduates will be able to demonstrate their ability to adapt to a rapidly changing environment by learning and applying new technologies.

PEO4: Graduates will be able to adopt ethical attitudes, exhibit effective communication skills, Teamworkand leadership qualities.

PROGRAM OUTCOMES (POS)

Engineering Graduates will be able to:

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.

COURSE OUTCOMES

SUBJECT CODE: C213	
COURSE OUTCOMES	
C208.1	Define, explain and illustrate the fundamental concepts of databases.
C208.2	Construct an E-R model from specifications to perform the transformation of the conceptual model into corresponding logical data structures.
C208.3	Model and design a relational database following the design principles.
C208.4	Develop queries for relational database in the context of practical applications.
C208.5	Define, explain and illustrate fundamental principles of data organization, query optimization and concurrent transaction processing.
C208.6	Acquire knowledge about the latest trends in databases.

PROGRAM SPECIFIC OUTCOMES (PSO)

PSO1: Ability to Formulate and Simulate Innovative Ideas to provide software solutions for Real-time Problems and to investigate for its future scope.

PSO2: Ability to learn and apply various methodologies for facilitating development of high quality System Software Tools and Efficient Web Design Models with a focus on performance optimization.

PSO3: Ability to inculcate the Knowledge for developing Codes and integrating hardware/software
products in the domains of Big Data Analytics, Web Applications and Mobile Apps to create innovative career path and for the socially relevant issues.

CO PO MAPPING

Note: H-Highly correlated=3, M-Medium correlated=2, L-Less correlated=1

CO'S	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
C208.1		3	3	3	3							
C208.2	3	3	3									
C208.3	3	3	3	3	3							
C208.4	3	3	3	3	2							
C208.5	3	2	2	2	2				2			
C208.6	3	2	2	2	3							
C208	3	2.67	2.67	2.16	2.16				2			

CO PSO MAPPING

CO'S	PSO1	PSO2	PSO3
C208.1	3	3	3
C208.2		3	3
C208.3	3		
C208.4		3	3
C208.5	3		
C208.6			2
C208	3	3	2.75

APPENDIX 1

CONTENT BEYOND THE SYLLABUS

S:NO;	TOPIC	PAGE NO:
1	**Cellular networks**	178
2	**Multimedia Networking**	179

Course code	Course Name	L-T-P - Credits	Year of Introduction
CS306	Computer Networks	3-0-0-3	2016

Prerequisite: Nil

Course Objectives

- To build an understanding of the fundamental concepts of computer networking.
- To introduce the basic taxonomy and terminology of computer networking.
- To introduce advanced networking concepts.

Syllabus

Concept of layering, LAN technologies (Ethernet), Flow and error control techniques, switching, IPv4/IPv6, routers and routing algorithms (distance vector, link state), TCP/UDP and sockets, congestion control, Application layer protocols.

Expected Outcome

The students will be able to

i. Visualise the different aspects of networks, protocols and network design models.
ii. Examine various Data Link layer design issues and Data Link protocols.
iii. Analyse and compare different LAN protocols.
iv. Compare and select appropriate routing algorithms for a network.
v. Examine the important aspects and functions of network layer, transport layer and application layer in internetworking.

Text Books

1. Andrew S. Tanenbaum, Computer Networks, 4/e, PHI.
2. Behrouz A. Forouzan, Data Communications and Networking, 4/e, Tata McGraw Hill.
3. Larry L. Peterson & Bruce S. Dave, Computer Networks-A Systems Approach, 5/e, Morgan Kaufmann, 2011.

References

1. Fred Halsall, Computer Networking and the Internet, 5/e.
2. James F. Kurose, Keith W. Ross, Computer Networking: A Top-Down Approach, 6/e.
3. Keshav, An Engineering Approach to Computer Networks, Addison Wesley, 1998.
4. Request for Comments (RFC) Pages - IETF -https://www.ietf.org/rfc.html
5. W. Richard Stevens. TCP/IP Illustrated volume 1, Addison-Wesley, 2005.
6. William Stallings, Computer Networking with Internet Protocols, Prentice-Hall, 2004.

Course Plan

Module	Contents	Hours	End Sem. Exam Marks
I	Introduction – Uses – Network Hardware – LAN –MAN – WAN, Internetworks – Network Software – Protocol hierarchies – Design issues for the layers – Interface & Service – Service Primitives. Reference models – OSI – TCP/IP.	07	15%
II	Data Link layer Design Issues – Flow Control and ARQ techniques. Data link Protocols – HDLC. DLL in Internet. MAC Sub layer – IEEE 802 FOR LANs & MANs, IEEE 802.3, 802.4, 802.5. Bridges - Switches – High Speed LANs - Gigabit Ethernet. Wireless LANs - 802.11 a/b/g/n, 802.15.PPP	08	15%
FIRST INTERNAL EXAMINATION			

III	Network layer – Routing – Shortest path routing, Flooding, Distance Vector Routing, Link State Routing, RIP, OSPF, Routing for mobile hosts.	**07**	**15%**
IV	Congestion control algorithms – QoS. Internetworking – Network layer in internet. IPv4 - IP Addressing – Classless and Classfull Addressing. Sub-netting.	**07**	**15%**
SECOND INTERNAL EXAMINATION			
V	Internet Control Protocols – ICMP, ARP, RARP, BOOTP. Internet Multicasting – IGMP, Exterior Routing Protocols – BGP. IPv6 – Addressing – Issues, ICMPv6.	**07**	**20%**
VI	Transport Layer – TCP & UDP. Application layer –FTP, DNS, Electronic mail, MIME, SNMP. Introduction to World Wide Web.	**07**	**20%**
END SEMESTER EXAM			

Question Paper Pattern

1. There will be *five* parts in the question paper – A, B, C, D, E
2. Part A
   a. Total marks : 12
   b. *Four* questions each having *3* marks, uniformly covering modules I and II;All*four* questions have to be answered.
3. Part B
   a. Total marks : 18
   b. *Three* questions each having *9* marks, uniformly covering modules I and II; *Two* questions have to be answered. Each question can have a maximum of three subparts.
4. Part C
   a. Total marks : 12
   b. *Four* questions each having *3* marks, uniformly covering modules III and IV; All*four* questions have to be answered.
5. Part D
   a. Total marks : 18
   b. *Three* questions each having *9* marks, uniformly covering modules III and IV; *Two* questions have to be answered. Each question can have a maximum of three subparts
6. Part E
   a. Total Marks: 40
   b. *Six* questions each carrying 10 marks, uniformly covering modules V and VI; *four* questions have to be answered.
   c. A question can have a maximum of three sub-parts.

7. There should be at least 60% analytical/numerical questions.

MODULE NOTES & QUESTION BANK

MODULE I				
Q:NO:	**QUESTIONS**	**CO**	**KL**	**PAGE NO:**
1	Briefly explain about different uses of networks.	CO1	K5	4
2	Briefly describe about point to point links and broad cast links.	CO1	K2	6
3	Briefly explain the terms: a) LAN b) MAN c) WAN	CO1	K2	8
4	Briefly describe about internetworks.	CO1	K2	9
5	Explain about different design issues for the layers.	CO1	K2	10
6	Write short notes on a) Service b) Interface	CO1	K5	12
7	Define service Primitive? Explain about different	CO1	K2	12
8	Explain the different steps involved in client-server	CO1	K5	11
9	Explain about the OSI Reference model with the	CO1	K5	17
10	Write notes on functions of : a) Transport layer b) Data link layer	CO1	K4	25
11	Briefly describe about TCP/IP model.	CO1	K3	26
12	Differentiate between OSI and TCP/IP model.	CO1	K4	27
MODULE II				
1	Define framing and the reason for its need.	CO2	K2	63
2	Explain Data Link Layer design Issues.	CO2	K5	64
3	Compare Go Back N ARQ protocol with Selective Repeat ARQ.	CO2	K4	78
4	Differentiate between Flow Control and Error Control.	CO2	K3	65
5	Explain about HDLC Protocol	CO2	K5	82
6	Discuss Protocols in internet Layer	CO2	K3	87
MODULE III				
1	Describe the network layer design issues.	CO3	K3	63

2	Define datagram and Virtual circuit networks.	CO3	K2	64
3	Compare Virtual Circuit and Datagram networks	CO3	K4	78
4	Define routing algorithm? Name its two types.	CO3	K2	65
5	Write a note on the shortest path algorithm.	CO3	K5	82
6	Write a note on different performance metrics used in network?	CO3	K5	87
7	Explain the flooding technique used in networks?	CO3	K5	89
8	Describe distance vector algorithm with an example.	CO3	K3	91
9	Define count to infinity problem?	CO3	K2	89
10	Define Link state routing? Explain its steps.	CO3	K2	95
11	Justify routing is done in mobile hosts.	CO3	K4	102
12	Define care of address and tunnelling.	CO3	K2	103

13	Write a note on OSPF Protocol.	CO3	K5	101
	MODULE IV			
1	Explain Distance Vector Routing Algorithm with example.	CO4	K2	106
2	Write short notes on Open loop Congestion Control	CO4	K3	107
3	Write short notes on Closed loop Congestion Control.	CO4	K3	108
4	What are four general techniques to improve QoS?	CO4	K5	110
5	Differentiate between Backpressure and Choke Packet.	CO4	K4	111
6	List out main factors that measure the performance of a network	CO4	K2	113
	MODULE V			
1	Compare ARP and RARP	CO5	K4	132
2	With neat diagram ,explain ICMPv6.	CO5	K2	143
3	Write short notes on IGMP.	CO5	K3	133
4	Briefly explain Internet Multicasting.	CO5	K2	136
5	With neat sketch explain the MIME.	CO5	K2	139
6	Investigate in detail about Exterior Routing Protocol	CO5	K5	141
7	Explain in detail about BGP.	CO5	K2	142
8	Explain BOOTP.	CO5	K2	141
	MODULE VI			
1	Compare TCP and UDP	CO5	K4	160
2	With neat diagram ,explain FTP.	CO5	K2	167
3	Write short notes on DNS.	CO5	K3	176
4	Briefly explain Email.	CO5	K2	173
5	With neat sketch explain the MIME.	CO5	K2	174
6	Investigate in detail about basic structure of URL	CO5	K5	183
7	Explain in detail about SNMP.	CO5	K2	175

8	Explain FTP transmission modes.	CO5	K2	168

MODULE I

Introduction.

→ Uses 1

→ N/w Hardware 2
- * LAN
- * MAN
- * WAN
- * Internetworks

→ Network S/w 3
- * Protocol Hierarchies
- * Design Issues for the Layers 4
- * Interface & Service 5
- * Service Primitives

→ Reference Models
- * OSI 6
- * TCP/IP 7

Questions:

1. What are the 2 reasons for using Layered Protocols.?
2. What is the diffs. b/w Connless & connⁿ oriented commⁿ?
3. List 2 ways in which the OSI & TCP/IP model are the same.
   List " " they differ.
4. What is the main diffs. b/w TCP & UDP?

April 2018

1. How are computer n/ws classified on the basis of physical size?
2. Define the terms protocol & interface?
3. What are the reasons for using Layered Architecture in Computer Networks.?
4. What are the OSI primitives for connⁿ oriented service?
5. List the key design issues that occur in Computer N/ws.
6. Describe ISO/OSI layered architecture with the help of diagram.

Module I

Computer Network is a collection of autonomous computers interconnected by a single technology. - They are able to exchange information.

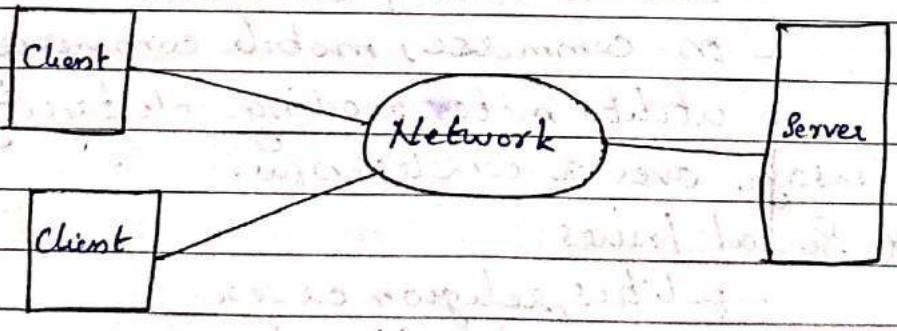
→ Uses of Computer Networks:

→ * Business Applications: eg: monitor production, keep track of inventories & pay roll:- worked at in isolation from others, but mgmt may have to connect them to be extract & correlate info about the company.

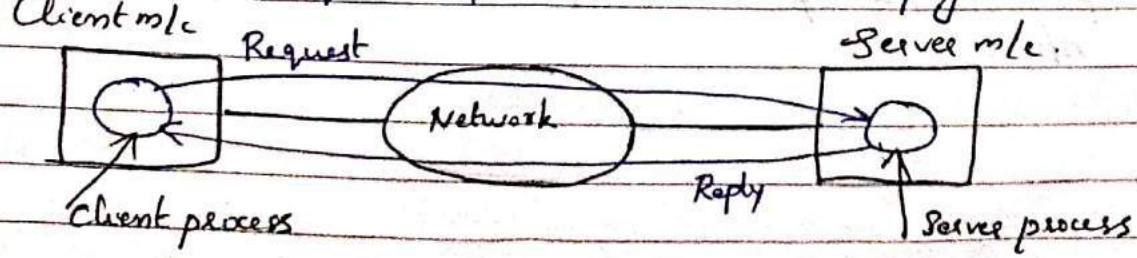
- Resource sharing: All pgms, equipment & data available to anyone connected on the n/w.

Eg: sharing phy. resources-as printers, scanners & CD burners.

- Client-Server Model: Data stored on servers - employees have simpler m/cs - clients with which they access remote data.



- Client-Server Model with request-reply: Client sends a rqst msg & waits for reply msg. Server processes the request & sends back a reply.



* Communication medium among employees: e-mail.
- video conferencing - hold meeting, seeing & hearing each other & even writing on virtual board.
* Online shopping:- Manufacturers can place orders reduces need for large inventories. & enhances efficiency.
* E commerce: shopping from home.

→* Home Applications:
1. Access to remote Inf^n
2. Person to person comm^n (peer to peer)
3. Interactive entertainment
4. Electronic commerce.

* Instant msging - multiperson version - chat room.

→* Mobile Users:
- ~~comme~~ Connected to home base even when away from home. through wireless n/ws.
- wireless PDAs & cell phones.
- m-commerce, mobile commerce.
- utility meter reading - electricity, gas, water report usage over a wireless n/w.

→* Social Issues:
- politics, religion or sex.
- Views posted to such groups may ~~not~~ be deeply offensive to some people. High resolution photographs & video clips can be transmitted over comp. n/ws.

→ Network Hardware:

— Two dimensions: transmission technology & scale.

There are two types of transmn technology as follows:

1. Broadcast links 2. Point to pt. links.

1. Broadcast links n/ws: single comm^n channel that is shared by all the m/cs on the n/w. Short msgs, called pkts sent by any m/c are received by all others. An address field within the pkt specifies the intended recipient. Receiving m/c checks the ~~pkt~~ address field, if the pkt is intended for the receiving m/c, that m/c processes the pkt; if the pkt is intended for some other m/c, it is just ignored.

— It uses special code in the address field for addressing a pkt to all destinations. When a pkt with this code is transmitted, it is received & processed by every m/c on the n/w. This mode of opn is called broadcasting.

Some broadcast s/ms support transmn to a subset of the m/cs — multicasting. ⇒ reserve one bit to indicate multicasting. Remaining n-1 address bits can hold a group no. When a pkt is sent to certain group, it is delivered to all m/cs subscribing to that group.

2. Point-to-point n/ws: many connections b/w individual pairs of m/cs. With one sender & one receiver is called unicasting.

~~An alterna~~

Scale: An alternative criterion for classifying n/ws is their scale. ie; by their physical size.

Personal Area N/w: n/ws that are meant for one person. For eg: a wireless n/w connecting a comp. with its mouse, keyboard & printer is a personal area N/w.

Classific^{n} of interconnected processors by scale.

Interprocessor distance	Processors located in same	Example
1m	Sq. mtr.	Personal Area N/w
10m	Room	Local Area N/w
100m	Building	
1km	Campus	
10 km	City	
100 km	Country	Wide Area N/w
1000 km	Continent	
10,000 km	Planet	The Internet.

* Local Area Networks:

→ privately owned n/ws within a single building or campus of upto few kms. in size.

Eg: Connecting personal Computers & workstations in offices.

Characteristics of LAN

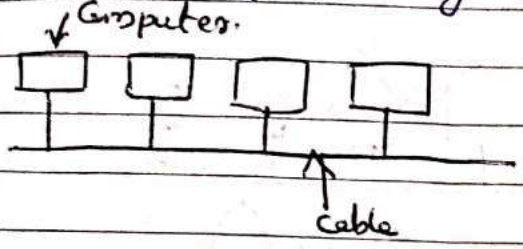
* → Size * → transm^{n} technology * → topology.

Size:— Restricted size ✓
— Simple n/w mgmt. ✓

Transmission technology:
— cable to which all the m/cs are attached. ✓
— speed 10 Mbps – 100 Mbps. ✓

Topology:—
└ broadcast LANs.
— Bus & Ring topology
— In a bus (i.e; linear cable) n/w, at any instant at most one m/c is the master & is allowed to transmit. An arbitration mechanism is needed to resolve conflicts when two/more m/cs want to transmit simultaneously.

Eg: IEEE 802.3 ⇒ Ethernet.; can transmit whenever they want to; if 2 or more plts collide, each comp. just waits random time & tries again later.



— Ring topology: In a ring, each bit propagates around on its own, not waiting for the rest of the plt to which it belongs. ⇒ Each bit ~~bag~~ navigates the entire ring in the time it takes to transmit a few bits.

Eg: IEEE 802.5 token ring.

Further classific"

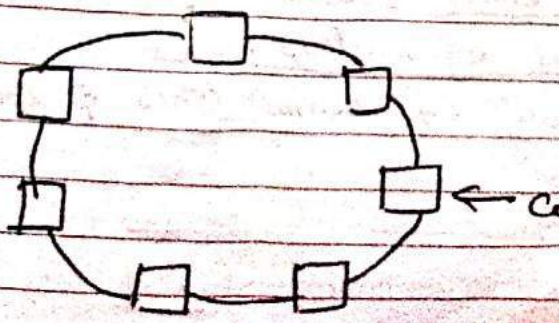
→ Broadcast nlws → static
→ dynamic. } depending on how the channel is allocated.

* Static Allocation: Divide time into discrete intervals & use a R-R algm, allowing each m/c to broadcast only when its time slot comes up. static allocation wastes channel capacity when a m/c has nothing to say during its allocated slot, so most slms allocate the channel dynamically.

* Dynamic allocation → centralized
→ decentralized.

— Centralized — A single entity, eg: bus ol arbitration unit, which determines who goes next.

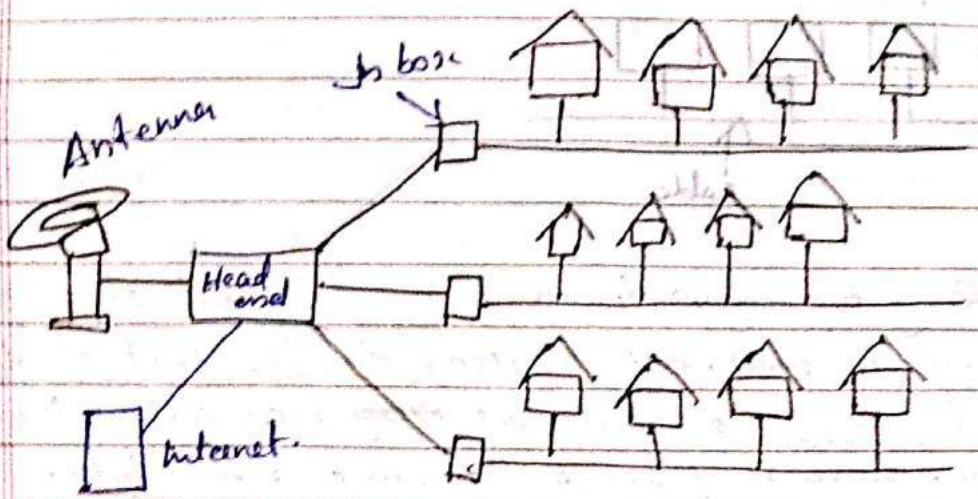
— Decentralized — no central entity, each m/c decide itself to transmit.



↳ * Metropolitan Area Networks: (MAN)

— covers a city.

— Eg: cable TV n/w.



Both TV s/ls & internet being fed into the centralized head end for subseq. distribution to people's homes.

↳ * Wide Area Networks (WAN).

— Large geographical area, country.

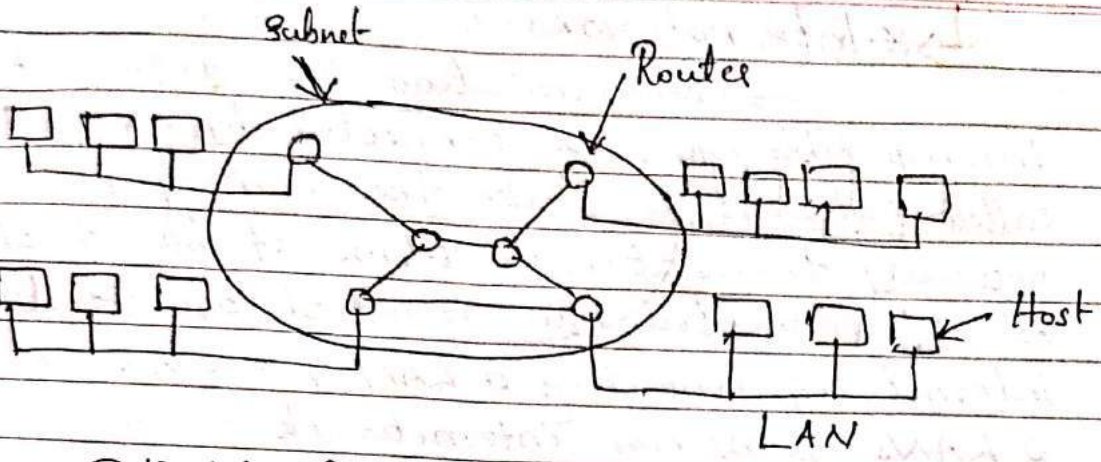
— Contains a coll^n of m/cs intended for running user pgms. m/cs ⇒ hosts. are connected by a comm^n subnet. Hosts owned by the customers (PCs) & comm^n subnet is owned by telephone company/Internet Service Provider. Duty Subnet is to carry msgs from host to host

Subnet — 2 components → Transm^n lines
↳ Switching elmts.

Transm^n lines: move bits b/w m/cs. made of Copper wire optical fiber or radio links.

Switching elmts: computers that connect 3 or more transm^n lines. eg: routers.

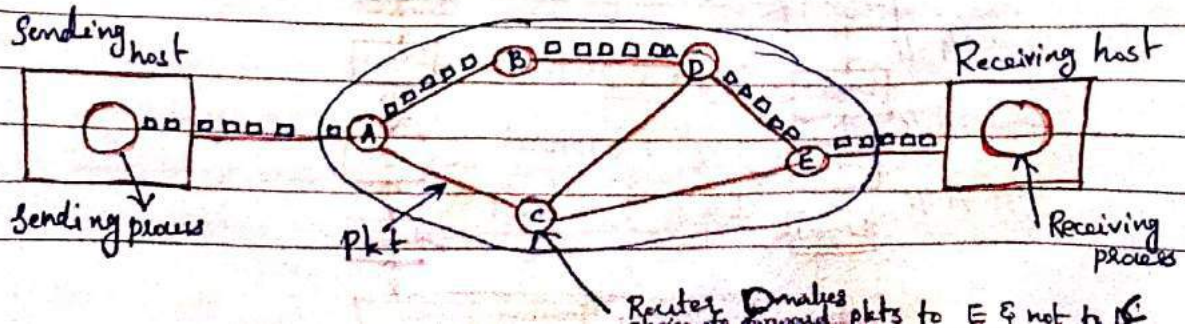
The coll^n of comm^n lines & routers form the subnet



Rel' b/w hosts on LANs & the subnet.

The n/w contains numerous transm^n lines, each one connecting a pair of routers. When a pkt is sent from one router to another via one or more intermediate routers, the pkt is received at each intermediate router in its entirety, stored there until the required o/p line is free & then forwarded. Such subnet is called store and forward or pkt switched subnet.

When a process on some host has a msg to be ~~send~~ sent to a process on some other host, the sending host first cuts the msg into pkts, each one bearing its no. in the sequence. These packets are entered into the n/w one at a time in quick succession. The pkts are transported individually over the n/w & deposited at the receiving host; They are reassembled into the original msg & delivered to the receiving process.



* Internetworks:

→ Communication b/w different n/ws. Incompatible n/ws be connected by means of nodes called gateways to make the conn° & provide the necessary translation in terms of h/w & s/w. A coll° of interconnected n/ws is called an internetwork or internet. Eg: connecting a LAN & a WAN or connecting 2 LANs forms an internetwork

Network Software

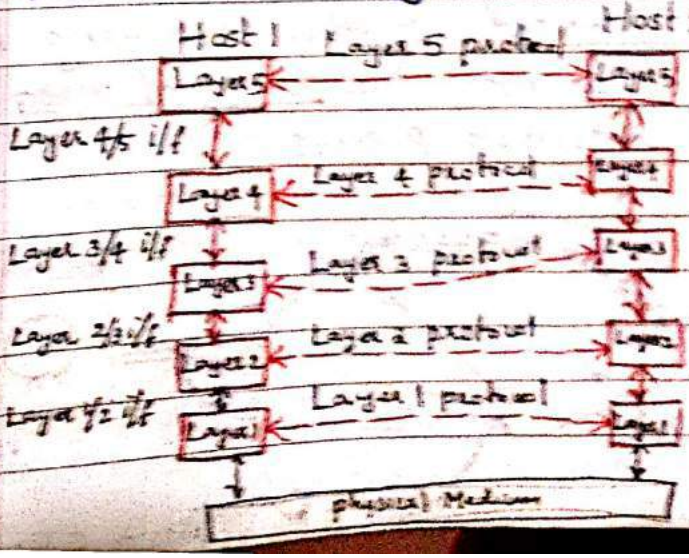
→ highly structured.

structuring technique

* → Protocol Hierarchies:

— n/ws are organized as stack of layers or levels. — each one built upon the one below it. The no., name, conts. & function of each layer differ from n/w to n/w. The purpose of each layer is to offer certain services to the higher layers.

Layer n on one m/c carries on a conversation with layer n on another m/c. The rules & conventions used in this conversation are collectively known as the layer n protocol. A protocol is an agreement b/w the communicating parties on how comm° is to proceed



No data are directly transferred from layer n on one m/c to layer n on another m/c. Each layer passes data & ctrl inf^n to the layer immediately below it, until lowest layer is reached. Below layer 1 is the phy. medium through which actual comm^n occurs. Virtual comm^n is shown by dotted lines & phy. comm^n by solid lines.

Between each pair of adjacent layers is an i/f. The i/f defines which primitive op's & services the lower layer makes available to the upper one.

A set of layers & protocols is called n/w architecture. Neither the details of the implementation nor the specifi^n of the i/fs is part of the architecture. b/c these are hidden away inside the m/cs & not visible from outside. A list of protocols used by a certain s/m, one protocol per layer is called a protocol stack.

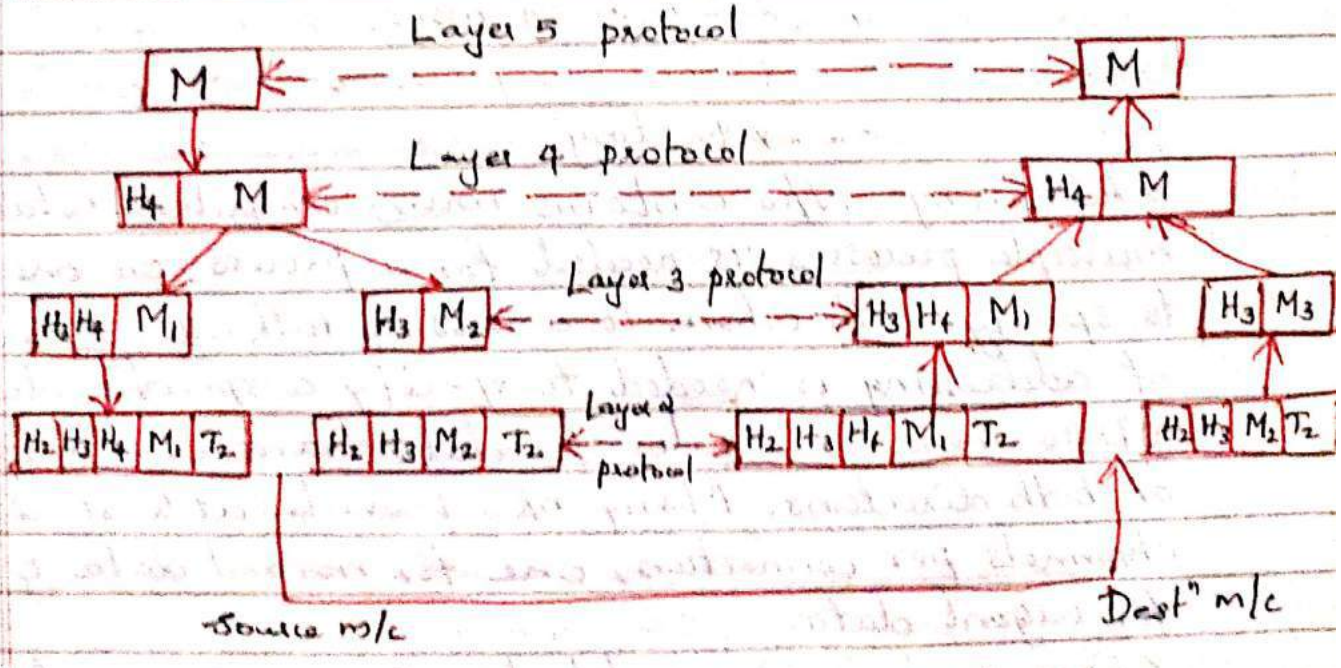


Fig: shows how to provide comm^n to the top layer of the 5 layer n/w. A msg M is produced by the appl^n process running in layer 5 & given to layer 4. Layer 4 puts a header to identify the msg & passes the result to layer 3. The header includes ctrl inf^n such as

seq. no.s to allow layer 4 on the dest^n m/c to deliver msgs in the right order. (size, time & other ctrl fields).

Layer 3 break up the incoming msgs into smaller units, pkts adding layer 3 header to each pkt. In fig. M → M_1, M_2 Layer 2 adds a header & a trailer & gives resulting units to layer 1 for phy. transmn. At the receiving m/c, the msg moves upward, from layer to layer with headers stripped off & it progresses.

↳ * Design Issues for the Layers:

* Addressing
* rules for data transfer
* Error ctrl
* sequencing
* Flow ctrl
* Length of msgs.
* Conn^n b/w processes
* Routing

* Addressing: N/w contains many computers which have multiple processes, is needed for a process on one m/c to specify with whom it wants to talk. ie; some form of addressing is needed to specify a specific dest^n.

* Data transfer: — rules for data transfer — in one direction or both directions. Many n/ws provide at least 2 logical channels per connection, one for normal data & one for urgent data.

* Error Control: Error detecting & correcting codes are there but both ends of the conn^n must agree on which one being used.

* Sequencing: Comm^n channels preserve the order of msgs sent on them. Number the pieces of msgs to reassemble properly.

* Flow control: How to keep a fast sender from a slow receiver with data. – feedback from the receiver to the sender directly or indirectly.
* Length of msgs: Inability of all processes to accept long msgs. This leads to disassembling, transmitting & then reassembling msgs.
* Conn^n b/w processes: Separate connection for each pair of communicating processes, expensive. It can be used for multiple, unrelated conversations. Multiplexing & demultiplexing can be used by any layer.
* Routing: There are multiple paths b/w source & dest^n, a route must be chosen. – select one of the available ckts based on the current traffic load.

→ * Services & Interfaces:

Layers can offer 2 diff. types of service to the layers above them: — Connection Oriented
— Connectionless

Connection oriented service: the service user first establishes conn^n, uses the conn^n & releases the conn^n.
When a conn^n is established, the sender, receiver & subnet conduct a negotiation about parameters to be used, such as max. msg size, quality of service required & other issues. Eg: telephone s/m.
Conn^n less Service: Eg: postal s/m.

Each msg carries the full dest^n address, & each one is routed through the s/m independent of all the others.
Quality of Service: Some services are reliable in the sense that they never lose data. A reliable service is implemented by having the receiver acknowledge the receipt of each msg so the sender is sure that it arrived.

* Diff. types of Services.

	Service	Example
Connection oriented	Reliable msg stream	seq. of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connectionless	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

* → Service Primitives:
→ primitives
→ LISTEN, CONNECT, RECIEVE, SEND & DISCONNECT.

A service is formally specified by a set of primitives or op^n's available to a user process to access the service. These primitives tell the service to perform some action taken by a peer entity. The primitives are normally s/m calls. These calls cause a trap to kernel mode, which then turns the ctrl of the m/c over to the O.S to send the necessary pkts.

Primitive	Meaning
LISTEN :	Blk waiting for an incoming conn^n ✓
CONNECT :	Establish a conn^n with a waiting peer ✓
RECIEVE :	Blk waiting for an incoming msg ✓
SEND :	Send a msg to the peer ✓
DISCONNECT :	Terminate a conn^n ✓

→ service primitives for implementing a simple conn^n oriented service.

1. Server executes LISTEN to indicate that it is prepared to accept incoming conn^n's. After executing the primitive, the server process is blked until a rqst for conn^n appears.

2. The client process executes CONNECT to establish a connⁿ with the server. The CONNECT call needs to specify who to connect to, so it might have a parameter giving the server's address. The O.S then typically sends a pkt to the peer asking to connect. When the pkt arrives at the server, it is processed by the O.S there. The s/m checks to see if there is a listener. If so 2 things.

- unlocks the listener ✓
- sends back ACK. ✓

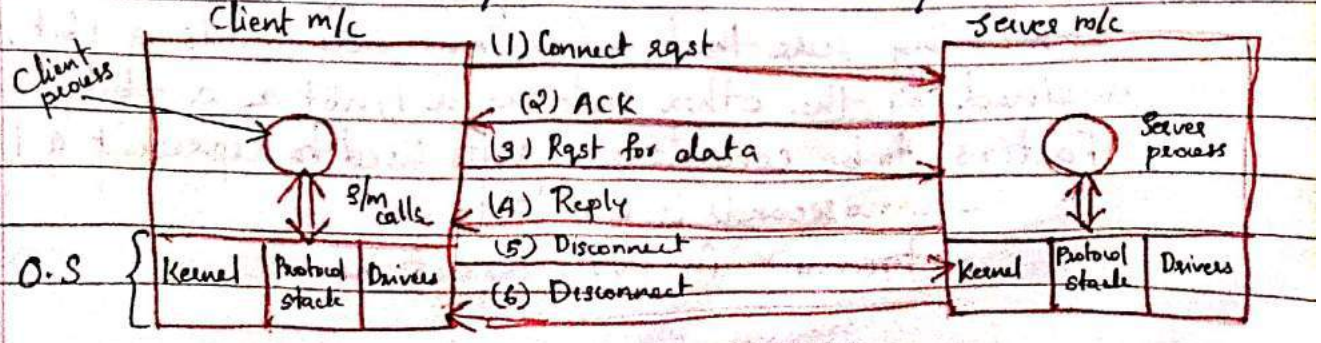
If the connⁿ rqst arrives & there is no listner, the result is undefined.

3. Server execute RECIEVE to prepare to accept the 1st rqst. Server does this immediately upon being released from the LISTEN, before the ~~ac~~ ACK can get back to the client. The RECEIVE call blks the server.

4. The client executes SEND to transmit its rqst(3) followed by the exⁿ of RECIEVE to get the reply. The arrival of the rqst pkt unblocks ~~se~~ server process so it can process the rqst.

5. The server uses SEND to return the answer to the client. The arrival of this pkt unblocks the client, which can now inspect the answer.

6. If it is done, it can use DISCONNECT to terminate the connⁿ. An initial DISCONNECT is a blking call, suspending the client & sending a pkt to the server saying that the connⁿ is no longer needed(5). When the server's pkt (6) gets back to the client m/c, the client process is released & connⁿ is broken.

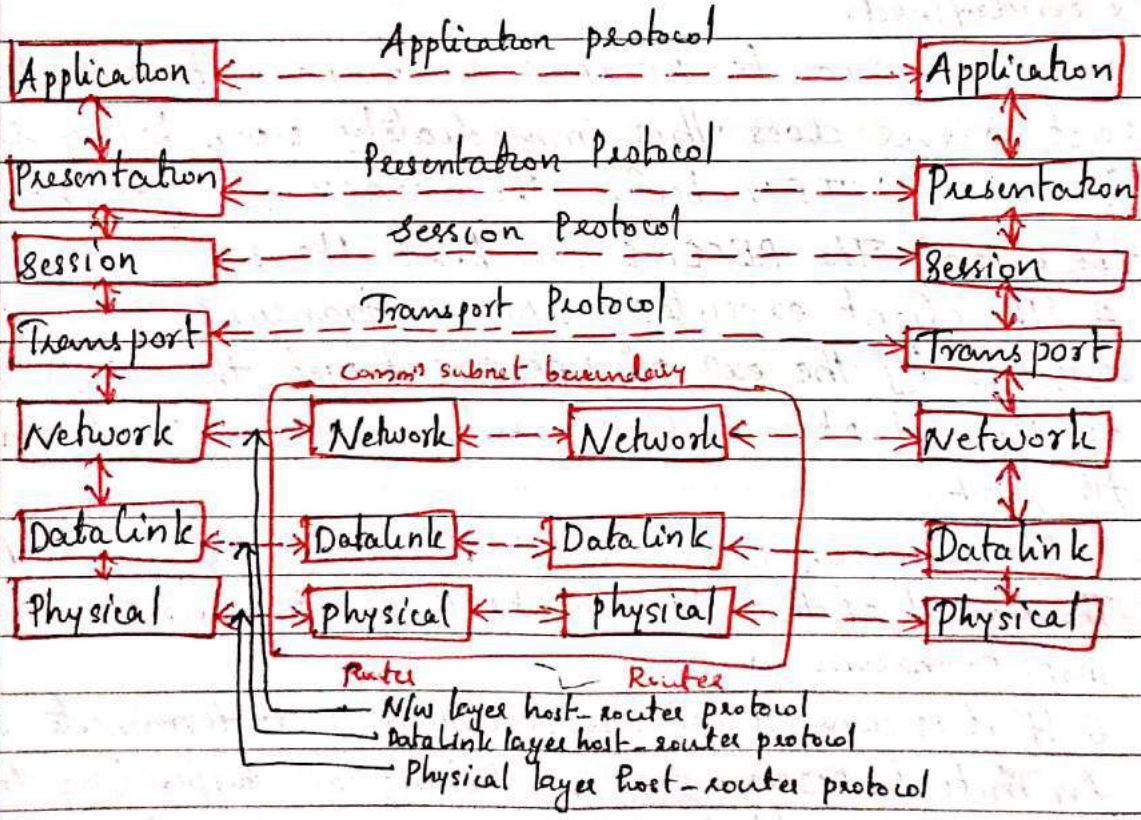


→ REFERENCE MODELS
- → OSI
- → TCP/IP

The OSI Reference Model: (ISO OSI Model)

ISO — International Standards Org^n.
OSI — Open S/ms Interconnection.

Open s/ms — that are open for comm^n with other s/ms.
OSI Model has 7 layers:



The Physical Layer:

— transmitting raw bits over a comm^n channel.
— making sure that when one side sends a 1 bit, it is received by the other side as a 1, not as a 0 bit.
Factors to be considered: volts used to represent a 1 & a 0.
- nano seconds a bit lasts
- transm^n in both directions.

The Data Link Layer:

- transform a raw transmn facility into a line that appears free of undetected transmn errors to the n/w layer. Sender break up the i/p data into data frames & transmit the frames sequentially. If the service is reliable the receiver confirms correct receipt of each frame.
- Flow regulation mechanism.
- Broadcast n/ws have an additional issue in the DLL: how to ctrl access to the shared channel. So DLL has sublayer Medium access control sublayer.

The N/w Layer:

- determines how pkts are routed from source to destn. Routes are based on static routing tables.
- Congestion control, if too many pkts are present in the subnet at the same time.
- Network layer addresses the issues such as;
  * addressing used by second n/w may be diff. from first one.
  * Too large size of pkt.
  * Protocols may differ.

  Here network layer allow heterogenous n/ws to be interconnected.

The Transport Layer:

- accept data from above, split it up into smaller units, pass these to n/w layer & ensure that the pieces all arrive correctly at the other end.
- transporting of isolated msgs, with no guarantee about the order of delivery.
- broadcasting of msgs to multiple destns.

The Session Layer:

allows users on diff. m/cs to establish sessions b/w them. Sessions offer various services:

- dialog ctrl: keeping track of whose turn it is to transmit.
- token mgmt: preventing 2 parties from attempting the same critical opn at the same time.
- synchronization: checkpointing long transm^n to allow them to continue where they were after a crash.

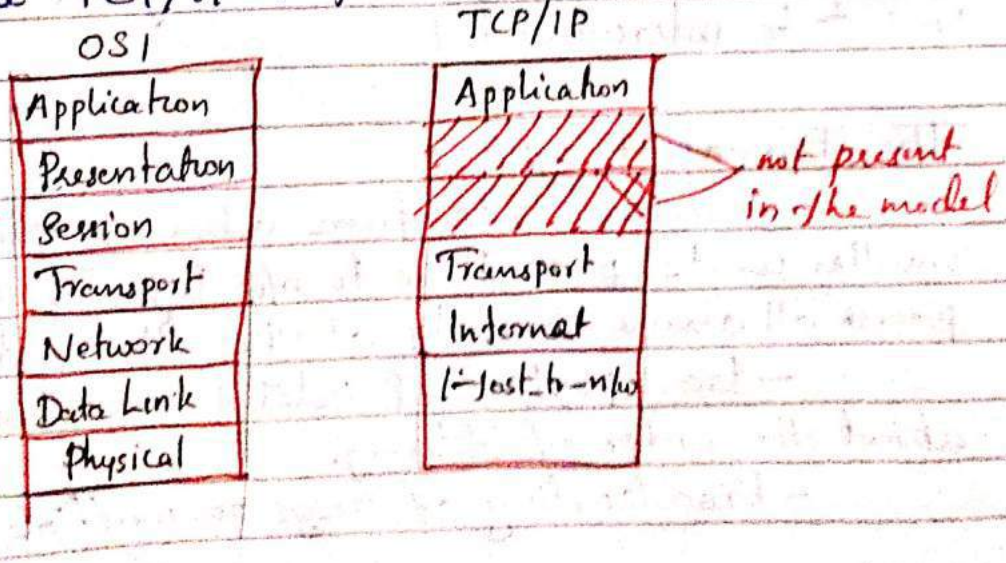
The Presentation Layer:

- is concerned with syntax & semantics of the info transmitted.
- manage diff. data representations, data structures to be exchanged.

The Application Layer:

- Variety of protocols such as HTTP for WWW.
- Protocols for file transfer, e-mail & n/w.

→ The TCP/IP Reference Model



The Internet Layer:

- It permit hosts to inject pkts into any n/w & have them travel independently to the dest^n. The internet layer defines an official pkt format & protocol called "Internet Protocol"
- It delivers IP pkts where they are supposed to go. It is
- It is similar to n/w layer in OSI model.

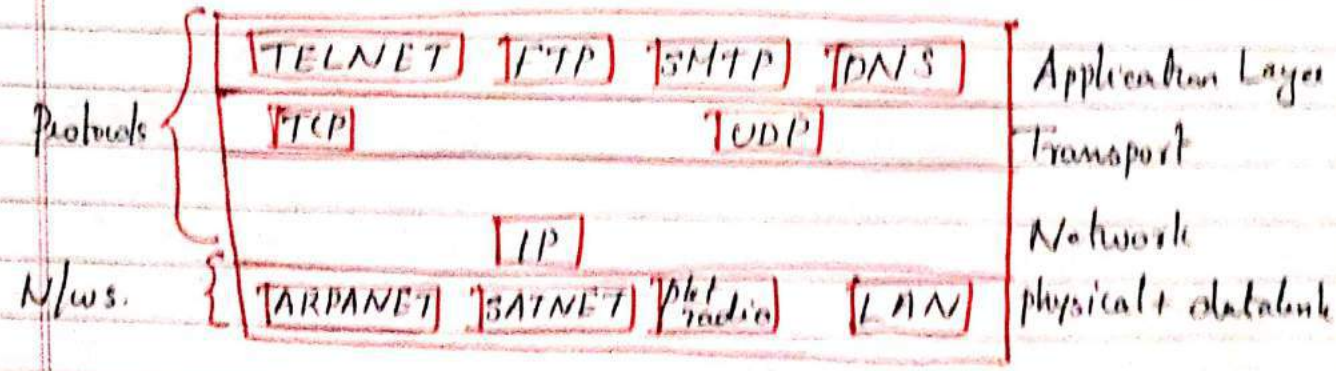
The Transport Layer:

- It allows peer entities on the source & dest^n hosts to carry on a conversation, just as OSI transport layer.

Two protocols are defined: TCP & UDP.

* TCP: Transmission Ctrl Protocol: conn^n oriented protocol that allows a byte stream originating on one m/c to be delivered without error on any other m/c in the internet. It fragments byte stream into discrete msgs & passes each one on to the internet layer. At the dest^n, the receiving TCP process reassembles the received msgs into the o/p stream. TCP handles flow ctrl.

* UDP: User Datagram Protocol: unreliable, connⁿless protocol, no flow ctrl & sequencing. used in client server, request-reply queries.



The Application Layer:

It contains all the higher level protocols: TELNET, FTP & SMTP. The virtual terminal protocol allows a user to on one m/c to log on to a distant m/c & work there.
DNS: mapping host names onto their n/w addresses.

The Host to N/w Layer:

Host has to connect to the n/w using some protocol so it can send IP pkts to it. This protocol is not defined & varies from host to host & n/w to n/w.

Assignment Questions:

1. Comparison b/w ISO OSI & TCP/IP models.
2. Relationship of Services to Protocols.
3. Short notes on 1. Wireless N/ws 2. Home N/ws
4. Basic principles for 7 layers in the OSI model.
5

MODULE II

> Datalink layer Design Issues
  * Flow Control
  * ARQ Techniques.
> Data Link Protocols
  * HDLC
  * DLL in Internet
> MAC Sub layer
  * IEEE 802 for LANs & MANs
  * IEEE 802.3, 802.4, 802.5
  * Bridges, Switches
> High Speed LANs
  * Gigabit Ethernet.
  * ~~High Speed~~
> Wireless LANs
  * 802.11a/b/g/n,
  * 802.15.PPP

Questions:

1. The follo. character encoding is used in a datalink protocol: A: 01000111; B: 11100011; FLAG: 01111110; ESC: 11100000 Show the bit sequence transmitted for the 4 char. frame: A B ESC FLAG when each of the follo. framing methods are used.
   a) Character count b) Flag bytes with byte stuffing
   c) Starting & end flag bytes with bit stuffing.
2. The following data fragment occurs in the middle of the data stream for which the byte stuffing algm is used: A B ESC C ESC FLAG FLAG D. What is the o/p after stuffing?
4. A bit string 0111101111101111110 needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing?

5. Data link protocols almost always put the CRC in a trailer rather than in a header. Why?
6. What is the baud rate of the standard 10Mbps - Ethernet?
7. How many frames/sec can gigabit Ethernet Handle?.
8. Compare a piconet & scatternet
9. What is the access method used by wireless LANs?
10. What is the diffs. b/w BSS & ESS?
11. Match the layers in Bluetooth & the Internet model.
12. What are the 2 types of links b/w a Bluetooth primary & a Bluetooth secondary?
13. How is OFDM diff. from FDM?.
14. Discuss 3 types of mobility in a wireless LAN

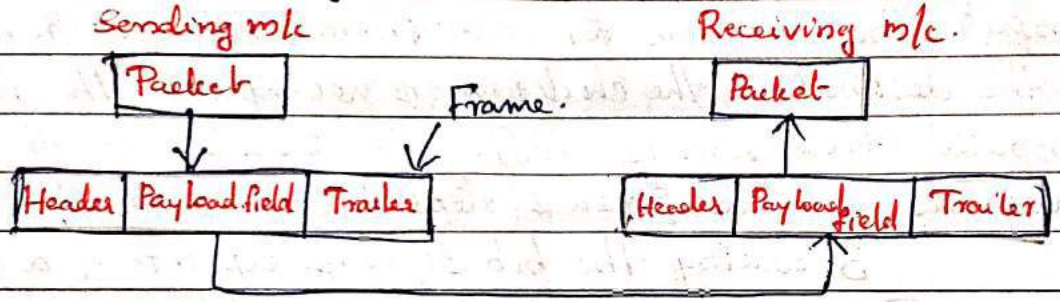
April 2018

1. Differentiate b/w normal & asynchronous balanced mode of op^n's in HDLC.
2. Draw & Explain the frame format for Ethernet.
3. Explain the phases in a PPP conn^n with the help of a trans^n diagrams.
4. How collisions is avoided in CSMA/CA? Describe diff. strategies used for this.
5. Write notes on IEEE 802.5 frame format.

> Data Link layer Design Issues:

1. Providing a well-defined service i/f to the n/w layer.
2. Dealing with transm^n errors.
3. Regulating the flow of data so that slow receivers are not swamped by fast senders.

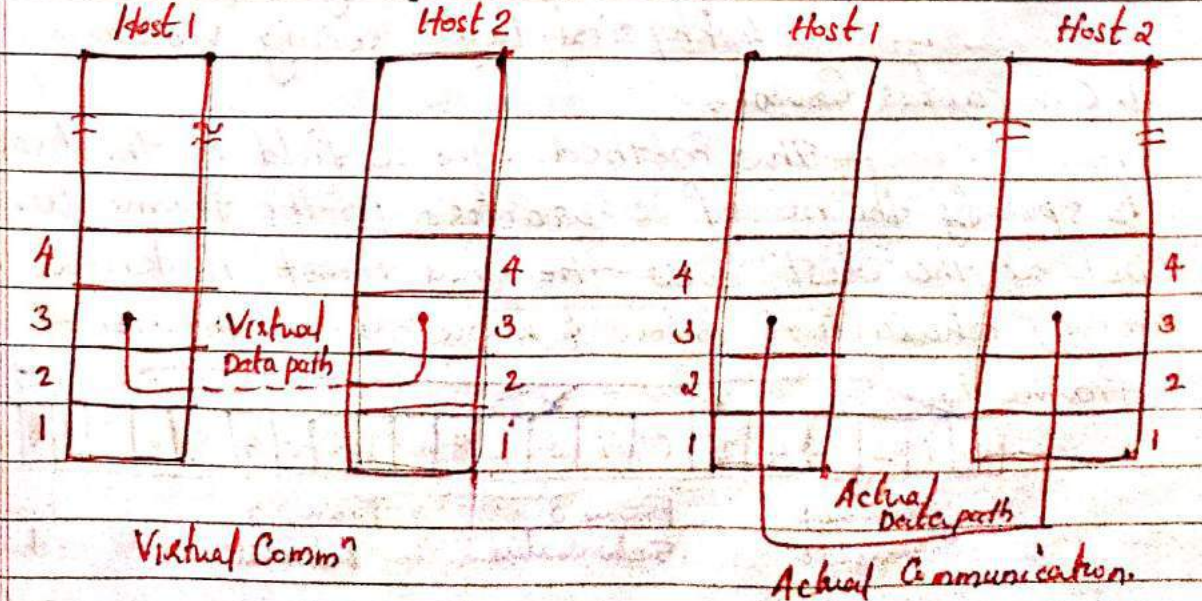
To accomplish these goals, the DLL takes the pkts it gets from the n/w layer & encapsulates them into frames for transm^n. Each frame contains a frame header, a payload field for holding the pkt, & frame trailer.



Rel^{n}ship b/w packets & frames.

1. Services provided to the N/w Layer:

— transferring data from the n/w layer on the source m/c to the n/w layer on the dest^n m/c.



The job of the data link layer is to transmit the bits to the dest^{n} m/c so they can be handed over to the n/w layer there.

The DLL can be designed to offer various services. The actual services offered can vary from s/m to s/m. Three reasonable possibilities that are commonly provided are

1. Unacknowledged connless service
2. Acknowledged connless service
3. Acknowledged conn^{n} oriented service.

2. Framing:

Break up bit streams into discrete frames & compute the checksum for each frame. When a frame arrives at the destination, the checksum is recomputed. The newly computed checksum is diff., the DLL knows that an error has occured & takes steps to deal with it.

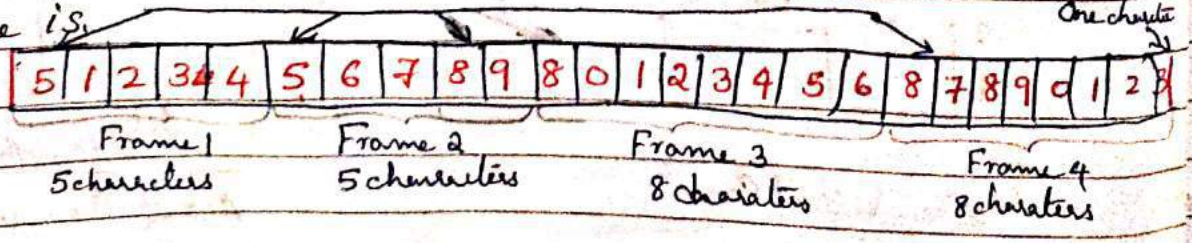
Breaking the bit stream up into frames is ~~more~~ Framing. – insert time gaps blw frames, much like the spaces blw words in ordenary text.

Four methods:

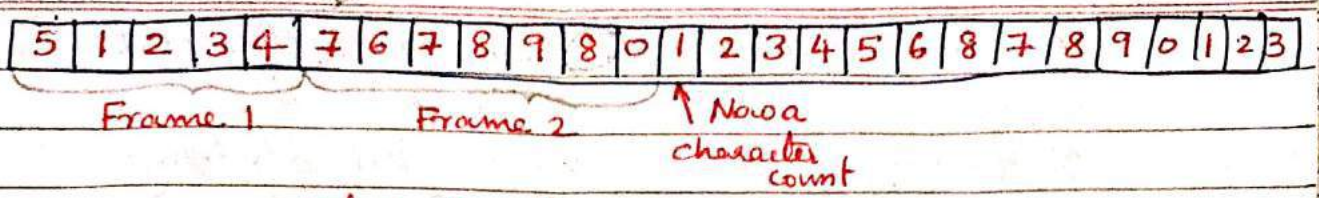
1. Character count
2. Flag bytes with byte stuffing
3. Starting & ending flags, with bit stuffing
4. Physical layer coding violation.

1. Character Count:

– This method uses a field in the header to specify the no. of characters in the frame. When the DLL at the dest^{n} sees the char. count, it knows how many characters follow & hence where the end of the frame is.



A character stream – without errors

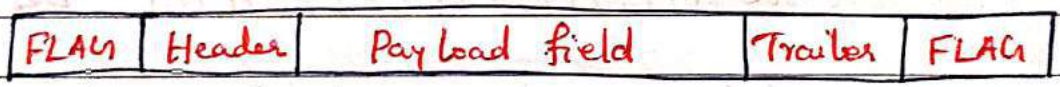


Character stream with one error.

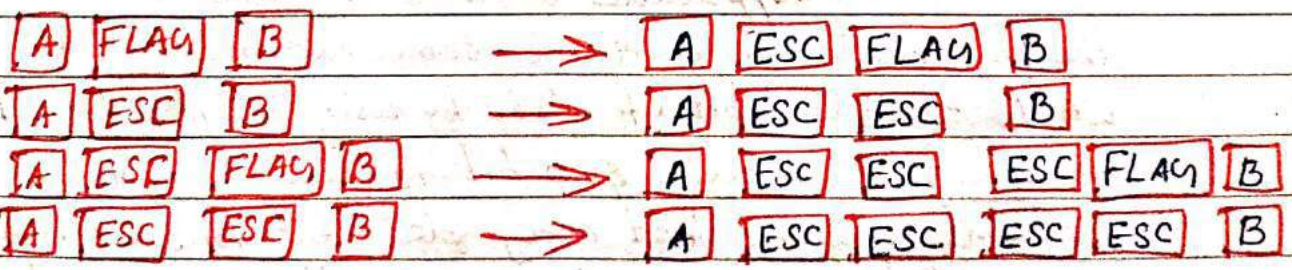
The trouble with this is that the count can be garbled by a transm^n error. For eg: the char. count 5 in the second frame becomes a 7, the dest^n will get out of synchronization & will be unable to locate the start of the next frame.

2. Flag bytes with byte stuffing:

For starting & ending same byte is used, called flag byte as delimiter. If the receiver ever loses synchronization, it can just search for the flag byte to find the end of the current frame. Two consecutive flag bytes indicate the end of one frame & start of the next one.



Original Characters → After stuffing



A serious pblm occurs with this method when binary data, such as obj pgms or floating pt. no.s are being transmitted. It may easily happen that flag byte's bit pattern occurs in the data. One way to solve this pblm is to have the sender's DLL insert a special escape byte (ESC) just before accidental flag byte in the data. The DLL on the receiving end removes the escape byte before the data are given to the n/w layer. This technique is called byte stuffing or character stuffing. A framing flag byte

can be distinguished from one in the data by the absence or presence of an escape byte before it.

3. Starting & Ending flags, Bit stuffing:

—allows data frames to contain an arbitrary no. of bits/character. Each frame begins & ends with a special bit pattern, 01111110. Whenever the sender's DLL encounters 5 consecutive 1s in the data it automatically stuffs a 0 into the outgoing bit stream. This is bit stuffing. When the receiver sees 5 consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs the 0 bit.

a) 01101111111111111111110010 original data

01101111101111101111010010 bit stuffed data

(stuffed bits)

01101111111111111111010010 Destuffed data

4. Physical layer coding Violation:

—Applicable to nlws in which the encoding on the phy. medium contains some redundancy. For eg: some LANs encode 1 bit of data by using 2 phy. bits. A 1 bit is a high-low pair & 0 bit is low-high pair. The scheme means that every data bit has a transition in the middle, making it easy for the receiver to locate the bit boundaries.

3. Error Control:

→ proper order. ✓

→ timer for ack. ✓

→ Error control is both error detection & error correction. It allows the receiver to inform the sender of any frames lost or damaged in transm^n & coordinates retransm^n of those frames by the sender. Error ctrl in the DLL is implemented simply: Any time an error is detected in an exchange, specified

frames are retransmitted. This process is called Automatic Repeat ReQuest (ARQ)

4. Flow Control:

A sender systematically wants to transmit frames faster than the receiver can accept them. Even if transmn is error free, at a certain point the receiver will simply be unable to handle the frames as they arrive & will start to lose some.

Flow ctrl coordinates the amnt of data that can be sent before receiving an ACK. Flow ctrl is a set of procedures that tells the sender how much data it can transmit before it must wait for an ACK from the receiver. Each receiving device has a block of memory called buffer, reserved for storing incoming data until they are processed.

Two approaches used: → Feed back based flow ctrl.
→ rate based flow ctrl.

Feed back based flow ctrl: The receiver sends back inf^n to the sender giving it permission to send more data.

Rate based flow ctrl: limits the rate at which senders may transmit data without using feedback from the receiver.

* ARQ Techniques:

→ Stop and wait ARQ
→ Go back N ARQ
→ Selective_Reject_ARQ

Data Link Protocols:

The widely used data link protocols are HDLC le; common in X.25 & many other nlws. And also data link protocols used in the Internet.

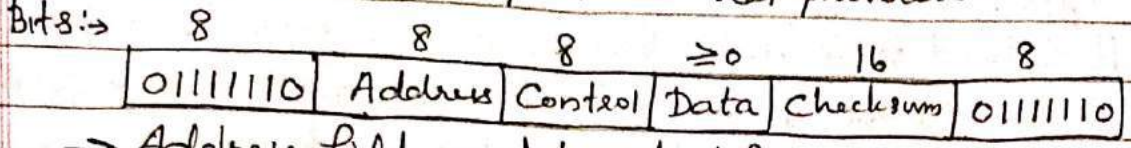
HDLC – High Level Data Link Control:

The Synchronous Data Link Control (SDLC) protocol developed by IBM is an example of a bit oriented protocol; SDLC was later standardized by the ISO as the High-Level Data Link Control (HDLC) protocol.

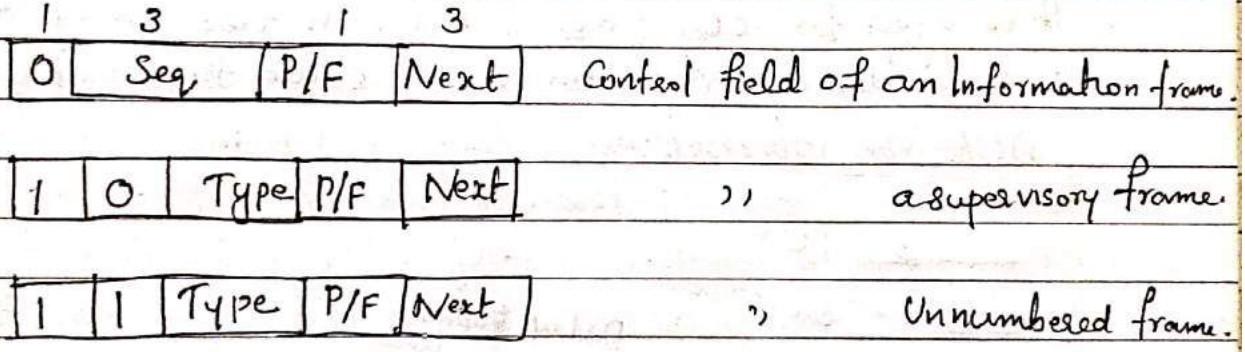
HDLC denotes both the begining & the end of a frame with the distinguished sequence 01111110. This sequence is also transmitted during any times that the link is idle so that the sender & receiver can keep their clocks synchronized.

Bit stuffing in the HDLC protocol works as follows. On the sending side, any time 5 consecutive 1s have been transmitted from the body of the msg, the sender inserts a 0 before transmitting the next bit. On the receiving side, should five consecutive 1s arrive the receiver makes its decision based on the next bit it sees. If the

Frame structure of bit oriented protocols:



→ Address field used to identify one of the terminals.
→ Control field is used for sequence no.s, acknowledgments, & other purposes.
→ The data field may contain any inf^n
→ The Checksum field for error control.
→ The minimum frame contains 3 fields & totals 32 brts, excluding the flags on either end.
There are 3 kinds of frames:- Information, Supervisory & unnumbered.



→ The Seq field - frame sequence number.
→ The Next field - piggy-backed ACK.
→ The P/F bit stands for Poll/Final: It is used when a computer is polling a group of terminals. When used as P, the computer is inviting the terminal to send data. All the frames sent by the terminal, except the final one, have the P/F bit set to P. The final one is set to F.
→ The various kinds of Supervisory frames are distinguished by the Type field.
Type 0 is an acknowledgement frame used to indicate the next frame expected. This frame is used when there is no reverse traffic to use for piggybacking.

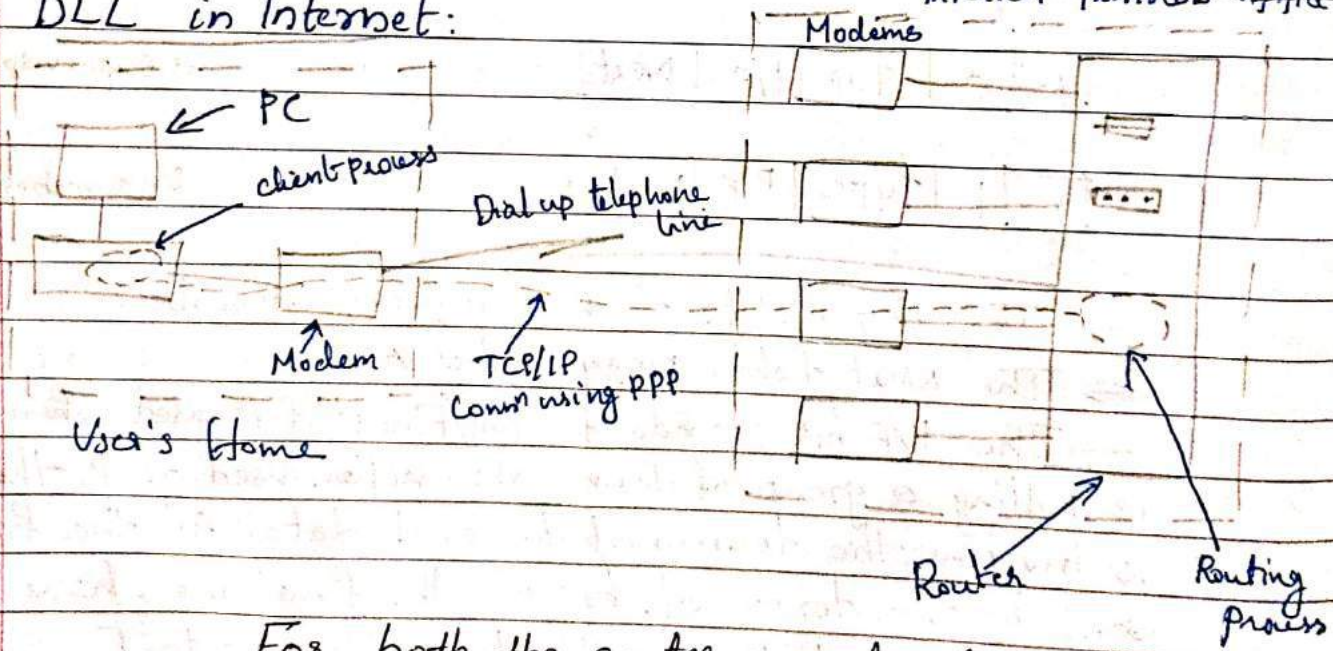
Type 1 is negative ack. frame (officially called REJECT) It is used to indicate that a transmn error has been detected. The Next field indicates the first frame in sequence not received correctly. (ie; frame to be retransmitted) The sender is required to retransmit all outstanding frames starting at Next.

Type 2 - RECIEVE NOT READY - It acknowledges all frames up to but not including Next, just as RECIEVE READY but it tells the sender to stop sending.

Type 3 - SELECTIVE REJECT. It calls for retransmn of only the frame specified.

The third class of frame is the Unnumbered frame. It is used for ctrl purposes but can also carry data when unreliable connless service is called for.

DLL in Internet:



For both the router - router leased line connn & the dial up host router connn, some pt. to pt. datalink protocol is required on the line framing, error ctrl & other DLL fns. The one used in the Internet is called PPP.

PPP- The Point-to-Point Protocol:

→ for router-to-router traffic & home user-to ISP traffic.

PPP provides 3 features:

1. A framing method delineates the end of the frame & the start of the next one. The frame format also handles error detection.

2. Link Control Protocol (LCP) is responsible for establishing, maintaining, configuring & terminating links. It supports synch. & asynch. dets & byte oriented & bit oriented encodings.

3. A way to negotiate n/w layer options in a way that is independant of the n/w layer protocol to be used. The method chosen is to have a different NCP (Network Control Protocol) for each n/w layer supported.

PPP provides several services:

→ PPP defines the format of the frame to be exchanged b/w devices.

→ defines how two devices can negotiate the establishment of the link and the exchange of data.

→ defines how n/w layer data encapsulated in the data link frame.

→ defines how 2 devices can authenticate each other.

→ provides multiple n/w layer services supporting a variety of n/w layer protocols.

→ provides conn^n^s over multiple links.

→ PPP provides n/w address configuration.

PPP — several services are missing:

→ doesn't provide flow control.

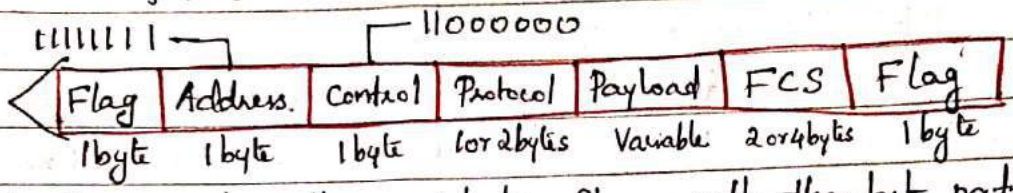
→ simple mechanism for error control — CRC field.

→ doesn't provide addressing mechanism to handle frames in a multipoint configuration.

Framing:

→ byte oriented protocol

Frame format:



Flag: starts & end with a 1 byte flag with the bit pattern 01111110.

Address: (omit this byte) — constant value & set to 11111111 (broadcast address)

Control: This field is set to the constant value 11000000

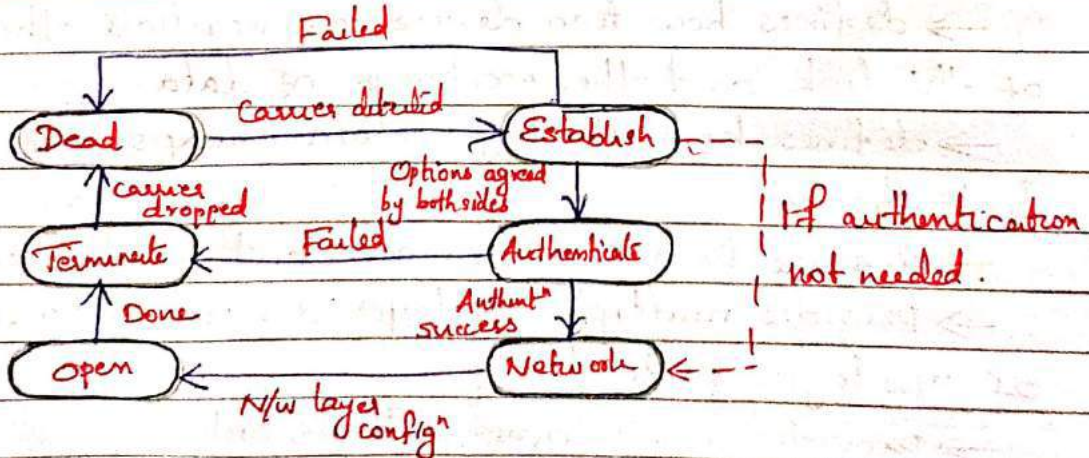
PPP doesn't provide flow ctrl & provides only error ctrl. This field is not needed. (Omit this byte)

Protocol: defines what is being carried in data field.

Payload field: This field carries either the user data or other inf^n. The data field is a sequence of bytes with the default of maximum of 1500 bytes.

FCS: is a 2 byte or 4 byte standard CRC.

Transition Phases:



Dead: The link is not being used. There is no active carrier & the line is quiet.

Establish: When one of the nodes starts the comm^n, the comm^n goes into this phase. If the options agreed, the s/m goes to the authentication phase.

Authenticate: The authentication phase is optional; the 2 nodes may decide, during the establishment phase. If they decide to proceed with authentication, they send several authentication pkts, If the result is successful, the conn^n goes to the n/w phase else it goes to the termination phase.

Network: In this phase, negotiation for the n/w layer protocols takes place. PPP specifies that 2 nodes establish a n/w layer agreement before data at the n/w layer can be exchanged.

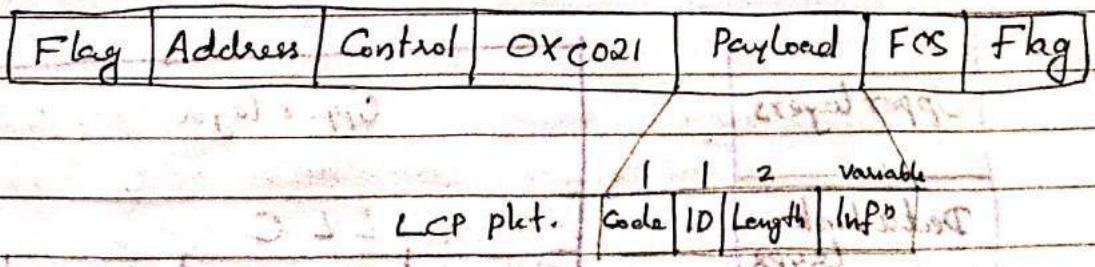
Open: Data transfer takes place. When a connection reaches this phase, the exchange of data pkts can be started.

Terminate: connection is terminated. Several pkts are xchanged b/w the 2 ends for house cleaning & closing the link.

PPP - protocols:

- Link Control Protocol (LCP)
- Authentication Protocol (AP)
- Network Control Protocol (NCP)

LCP: responsible for establishing, maintaining, configuring & terminating links.



AP: Eg: Password Authentication Protocol (PAP)

→ 2 step process: 1. The user wants to access s/m sends an authentication ~~procedure with~~ identification & a password.

2. The s/m checks the validity of the identifi^n & pswd & either accepts or denies connection.

Preamble: 7 bytes of alternating 0s & 1s that alerts the receiving s/m to the coming frame & enables it to synchronize its i/p timing. The preamble is actually added at the phy. layer & is not part of the frame.

Start frame delimiter(SFD): signals the begining of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2bits is 11 & alerts the receiver that the next field is the dest^n address.

Destination Address: is 6 bytes & contains the physical address of the dest^n station to receive the pkt.

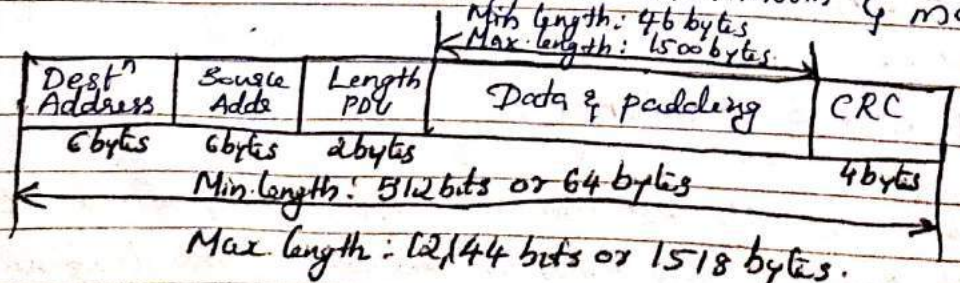
Source Address: The SA field is also 6 bytes & contains the phy. address of the sender of the pkt.

Length or type: The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE std used it as the length field to define the no. of bytes in the data field.

Data: This field carries data encapsulated from upper layer protocols. It is a minimum of 46 & a max. of 500 bytes.

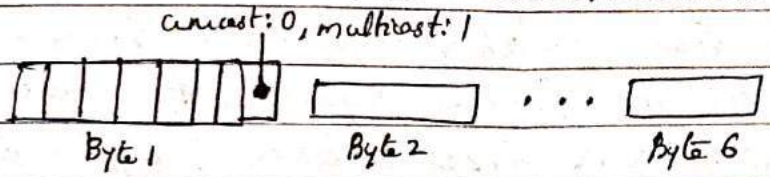
CRC: Error detection inf^n.

Frame Length: Minimum & max. length



Addressing: Each station on an Ethernet network has its own Network I/f card (NIC). The NIC fits inside the station & provides the station with a 6 byte physical address.

Unicast, Multicast & Broadcast Address: A source address is always unicast Address - the frame comes from only one station. The dest^{n} address can be unicast, multicast or broadcast



The least significant bit of the first byte defines the type of address. If the bit is 0, the addr. is unicast; otherwise, it is multicast.

The broadcast dest^{n} addr. is a special type of the multicast address in which all bits are 1s.

Eg: Define the type of the follo. Dest^{n} Address.

a) 4A:30:10:21:10:1A

Ans: Byte 1 $\Rightarrow$ 4A $\xrightarrow{(LSB)}$ A $\Rightarrow$ 1010 ↑ unicast.

b) 47:20:1B:2E:08:EE

Ans: Byte 1 $\Rightarrow$ 47 $\xrightarrow{(LSB)}$ 7 $\Rightarrow$ 0111 ↑ multicast

c) FF:FF:FF:FF:FF:FF

Ans: Byte 1 $\Rightarrow$ FF $\xrightarrow{(LSB)}$ F $\Rightarrow$ 1111 ↑ broadcast.

Access Method: ~~CS~~ CSMA/CD

classmate
Date
Page

IEEE 802.5 ⇒ Token Ring Media Access Control:

→ is based on the use of a small frame called a token, that circulates when all stations are idle. A station wishing to transmit must wait until it detects a token passing by. It then seizes the token by changing one bit in the token which transforms it from a token into a start of the frame sequence for a data frame.

When a station seizes a token & begins to transmit a data frame, there is no token on the ring, so other stations wishing to transmit must wait. The transmitting station will insert a new token on the ring. when the station has completed transmn of its frame.

1byte	1	1	2or6	2or6	≥0	4	1	1
SD	AC	FC	DA	SA	Data Unit	FCS	ED	FS

SD – Starting Delimiter DA – Destination Address
AC – Access Control SA – Source Address
FC – Frame Control FCS – Frame Check Sequence.
ED – Ending Delimiter FS – Frame Status.

AC field:

P P P	T	M	R R R

PPP – priority bits M – monitor bit
T – token bit RRR – reservation bit

FC field.

F F	Z Z Z Z Z Z

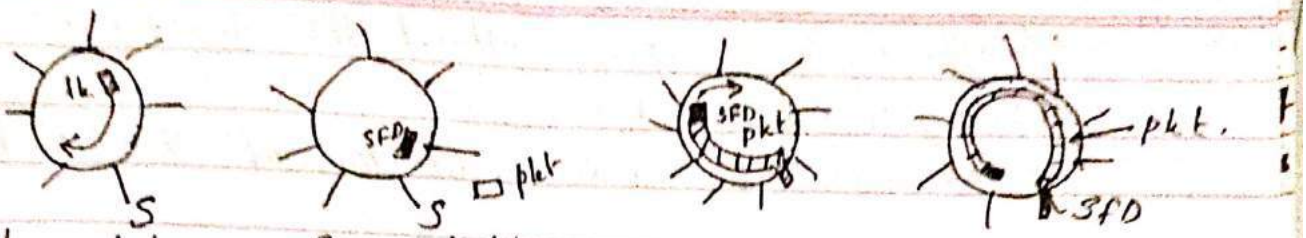
F – frame type bits
Z – Control bits.

FS field

A	C	r r	A	C	r r

A – Address recognized bit
sets when sees intended recipient
rr – Reserved C – frame copied bit : sets when frame is copied into adaptor.

A	C	Significance
0	0	Destn not present or not powered up.
1	0	Destn present but frame not accepted.
1	1	Destn present & frame copied.



Token rotates around the ring | S converts token into SFD | S then releases the token.

Token release earlier: The sender can insert token back onto the ring immediately follo the frame.
Token release delayed: After frame it transmits has gone all the way around & ~~been~~ been removed.

Token Ring Maintenance: Each token ring has one station designated as monitor. Monitor's job is to ensure the health of the ring. eg: the token is not lost.
Any station on the ring can become the monitor & there are defined procedures by which monitor is elected when the ring is first connected or on the failure of the current monitor.

A healthy monitor periodically announces its presence with a special ctrl msg; if a station fails to see such a msg for some period of time, it will assume that the monitor has failed & will try to become the monitor. When a station decides that a new monitor is needed, it transmits a "claim token" frame announcing its intent to become a new monitor. If that token circulates back to the sender, it can assume that it is ok for it to become the monitor. If some other station is also trying to become the monitor at the same instant the sender might see a claim token msg from other station. In this case it will be necessary to break the using some well defined rule like "highest addr. wins".

Max. possible token rotation time = NumStations × THT + Ring Latency.

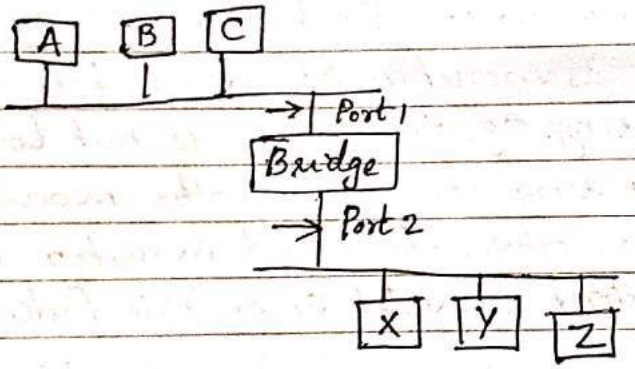
If the timer expires without the monitor seeing a token, it creates a new one.
Addnal fn of monitor – detection of dead stations.

24/1/18

IEEE 802.4 Token Bus.

Bridges:

is a node b/w 2 n/ws (eg: Ethernet) & have the node forward frames from one Ethernet to the other. This node will be accepting all frames transmitted on either of Ethernets, so it could forward them to the other. This node is called Bridges.



whenever the bridge receives a frame on port 1 that is addressed to host A, it would not forward the frame out on port 2. Anytime a frame addressed to host A was received on port 2, the bridge would forward the frame out on port 1.

Forwarding table maintained by a bridge

Host	Port
A	1
B	1
C	1
X	2
Y	2
Z	2

Bridge uses the datagram model of forwarding.

For creating this table, bridge inspect the source address in all the frames it receives.

Eg: When host A sends a frame to a host on either side of the bridge, the bridge receives this frame & records the fact that a frame from host A was just received on port 1.

When a bridge first boots, this table is empty; entries are added on time.

Spanning Tree Algorithm:

Bridges handles loops using Spanning tree Algm. The nlw of nlw can be formed in a cyclic graph. Spanning tree is a subgraph of this cyclic graph that covers all vertices. But it throws out some of the edges.

Algorithm:

For bridges, to select the ports over which they will forward frames. The algm selects ports as follows:

* Each bridge has unique identifier B_1, B_2, B_3....
* The algm first selects the bridge with the smallest ID as root of Spanning tree.
* The root bridge always forwards frames out over all of its ports.
* Each bridge computes the shortest path to the root & notes which of its ports on this path.
* This port is also selected as the bridges' preferred path to the root.
* Finally, all the bridges connected to a given LAN elect a single designated bridge that will be responsible for forwarding frames toward the root bridge.
* Each LAN's designated bridge is one that is closest to the root & if 2 or more bridges are equally close to the root, then the smallest ID wins.

The bridges have to exchange config msgs with each other & then decide whether they are the root or a designated bridge based on these msgs.

Config msg contains:

1) ID for the bridge that is sending msg.
2) ID for the what the sending bridge believes to be the root bridge.
3) The distance measured in hops, from the sending bridge to the root bridge.

Source Routing Bridges:

A transparent bridge's duties include filtering frames, forwarding & blocking. In a n/w that has source routing bridges, these duties are performed by the source station & to some extent, the dest^n station.

In source routing, a sending station defines the bridges that the frame must visit. The addresses of these bridges are included in the frame. The frame contains the source & dest^n addresses & addresses of all bridges to be visited.

Bridges Connecting Diff. LANs:

There are many issues to be considered.

* Frame format * Max data size. * Data rate * Latency * Security * Multimedia support.

Switches:

Switches operate at the DLL or 2nd layer. Switches are intelligent hubs. Switches can remember which ports are connected to which devices. When a switch receives a pkt (data), it resends that pkt directly to the correct port. For eg:, host A sends out a msg through port 1. The switch records into its switch table that host A is on port 1. When host B decides to send a pkt to host A, the switch first

checks its switch table. If port A is registered in the switch table, it will resend the pkt directly to port A instead of sending it to all the ports. This also means that switching gives dedicated bandwidth. A private phone call is like a switch. The phone no. that is entered is looked up in the table and the correct telephone rings at the other end.

Stand alone Ethernet switch devices were commonly used on home nlws. High performance nlw switches are still widely used in corporate nlws & data centers.

→ Its a multiport nlw bridge that uses hlw addr. to process & forward data at the DLL of the OSI model. ~~Some~~ ie; layer 2 switches.

→ Some switches can also process data at the nlw layer by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

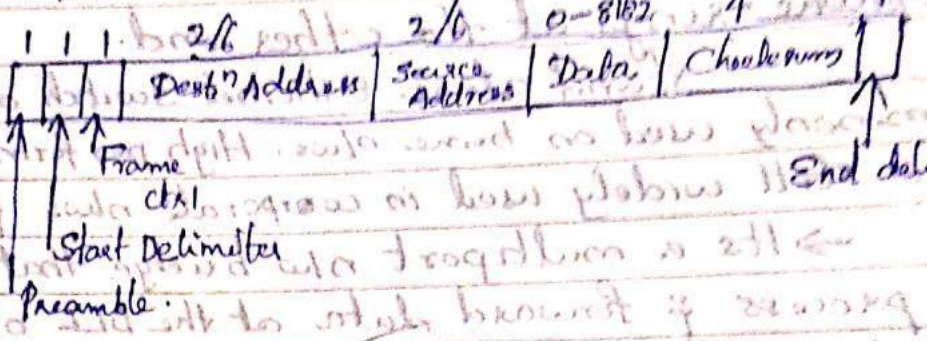
Switches manage the flow of data across a nlw by transmitting a received nlw pkt only to the one or more devices for which the pkt is intended.

High Speed LANs

IEEE 802.4 Token Bus

In a token bus LAN, the physical media is a bus & a logical ring. The token is passed from one station to other in a sequence, described in the logical ring.

Frame Format



Preamble: synchronize the receiver's clock, may be short as 1 byte.

SD & ED: frame boundaries

Frame ctrl: distinguish data frame & ctrl frames

Data frames, it carries frame's priority. The token bus defines 4 priority classes 0, 2, 4 & 6 for traffic, with 0 the lowest & 6 the highest. To understand priority classes, each station can be thought of being internally divided into 4 sub stations, one at each priority level.

When a token comes into the station over the cable, it is passed internal to the priority 6 substation which may begin transmitting frames, if it has any. When it is done, or when its timer expires, the token is passed internally to the priority 4 substation & so on to priority 0, so 4 token timers used to control the internal flow of token at a station.

For ctrol frames, frame ctrl field is used to specify the frame types, which include, token passing & various ring maintenance frames.

The data field may be upto 8182 bytes long, when 2 byte addresses are used upto 8174 bytes long when 6 byte addresses are used. The checksum is used to detect transm^n errors, which uses the same polynomial algm as in 802.3

Token Bus Maintenance.

High Speed LAN

The IEEE 802.2 802.3 and 802.5 LANs having data transfer rate in the range of 10 Mb/s to 16 Mb/s. High Speed LANs with 100 Mb/s.

They can be categorized into 3 types based on token passing, successors of Ethernet & based on switching Technology. In the first category FDDI & its variations. & high speed token ring. In the second category fast Ethernet & Gigabit Ethernet. Third category ATM, fiber channel & ethernet switches.

FDDI – Fibre Distributed Data Interface

– It is a LAN protocol. It uses optical fibre as medium

Access Method: Token Passing

The access is limited by time. A station may send many frames as it can within its allotted access period.

FDDI defines 2 types of data frames:

synchronous & asynchronous data frames. These frames

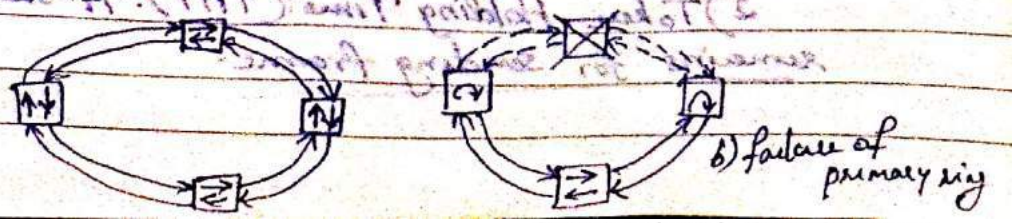
↓ real time ↓ not real time

are called S-frames & A-frames.

Each station that captures token is requisred to send S-frames first.

FDDI n/w consists of dual rings

→ 2 independant rings that transmit data in opposite directions.



a) normal op^n

b) failure of primary ring

The second is not used during normal opⁿ but takes over data flow only if the primary ring fails. The ring loop back on the secondary fiber to form a complete ring. FDDI also is able to tolerate a single break in the cable or the failure of one station.

Time Registers: FDDI defines 3 time registers to control the token & distribute the access opportunities among the nodes equitably.
Values are set when the ring is initialized & do not vary in the course of opⁿ.

Registers are:

⇒ Synchronous Allocation (SA) - at the time of Ring initialization; the reg. indicates length of the time allowed each station for sending data. Length of the time allowed for S frames diff for each station.

⇒ Target Token Rotation Time - indicates the avg time required for a token to circulate around the ring exactly once. The actual time of any rotation may be less than or greater than this value.

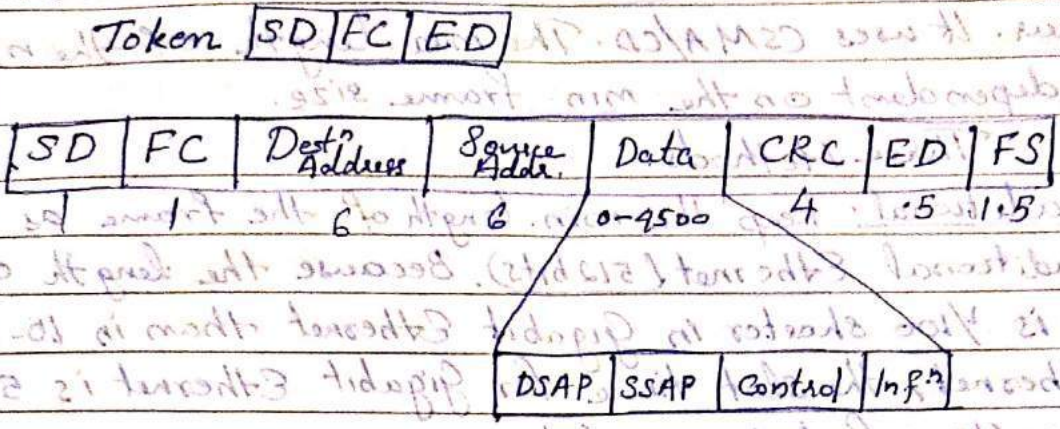
⇒ Absolute Max Time (AMT): indicates value equal to twice of TTRT. A token may not take longer than this time to make one rotation of the ring. If it does ring must be initialized.

Timers: Each station contain a set of timers that enables to compare actual timings with the values contained in the registers.

1) Token rotation timer (TRT): runs continuously & measure the actual time taken by the token to complete a cycle.

2) Token Holding Time (THT): It shows how much time remains for sending frames.

FDDI Frame Format:



GIGABIT ETHERNET

→ Higher data rate; 1000 Mbps.

The goals: 1. Upgrade the data rate to 1Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48 bit address.
4. Use the same frame format.
5. Keep the same min & max. frame lengths.
6. To support autonegotiation as defined in Fast Ethernet.

MAC Sublayer: Gigabit Ethernet has 2 distinctive approaches for medium access.

→ Half duplex & full duplex

All Implementations of Gigabit Ethernet follow the full-duplex approach.

Full Duplex Mode: There is a central switch connected to all computers or other switches. In this mode, each switch has buffers for each i/p port in which data are stored until they are transmitted. There is no collision in this mode; CSMA/CD is not used. Lack of collision implies that the max. length of the cable is determined by the s/l attenuation in the cable, not by collision detection process.

Half-Duplex Mode: A switch can be replaced by a hub which act as the common cable in which a collision might occur. It uses CSMA/CD. The max. length of the n/w is dependent on the min. frame size.

Three Methods:

Traditional: keep the min. length of the frame as in the traditional Ethernet (512 bits). Because the length of a bit is 1/100 shorter in Gigabit Ethernet than in 10-Mbps Ethernet, the slot time for Gigabit Ethernet is 512bits x 1/1000 μs, which is equal to 512 μs.

Carrier Extension: To allow for a longer n/w, increase the min. frame length. This method defines the min. length of a frame as 512 bytes. This method forces a station to add extension bits to any frame that is less than 4096 bits. The max. length of n/w can be increased 8 times to a length of 200m. This allows a length of 100 m from the hub to the station. Since this padding is added by the sending h/w & removed by the receiving h/w, the s/w is unaware of it. ie; no changes are needed to existing s/w.

Frame Bursting:

Carrier extension is inefficient if we have a series of short frames to send; each frame carries redundent data.

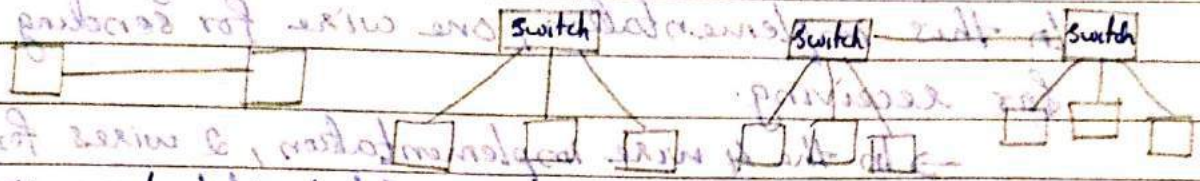
Instead of adding an extension to each frame multiple frames are sent. To make multiple frames look like one frame, padding is added b/w the frames so that the channel is not idle.

Physical Layer:

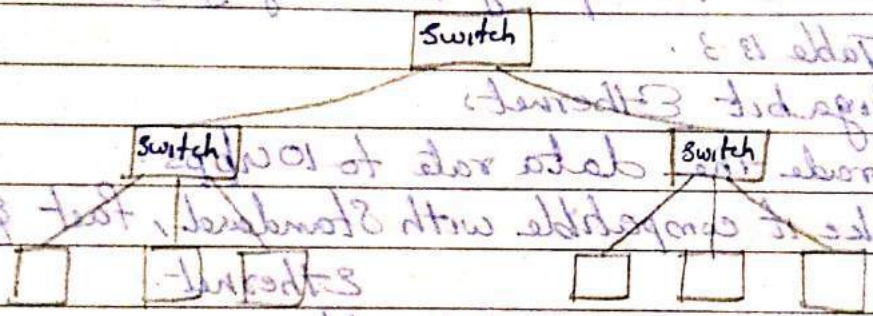
- Features of this layer:

Topology: If there are two stations, they can be connected point-to-point. Three or more stations need to be connected in a star topology with a hub or a switch at the center.

a. Point to pt. b. Star c. Two stars

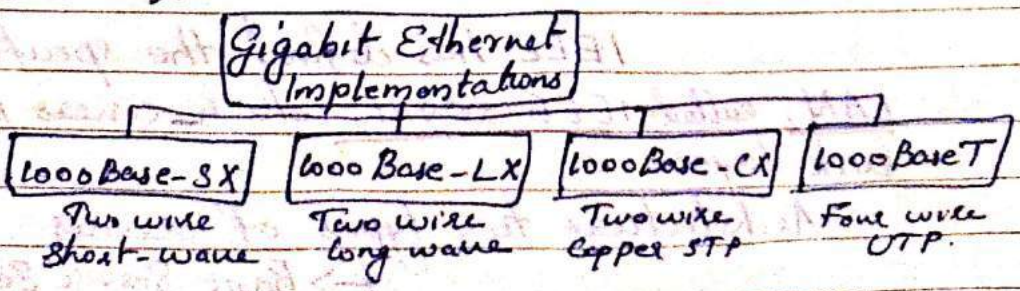


d. Hierarchy of stars:



Implementation: — categorized as either a 2 wire or a four wire implementation. The 2 wire implementations use fibre-optic cable (1000 Base-SX, short wave or 1000 Base LX, long wave) or STP (1000 Base-CX).

- The 4 wire version uses category 5 twisted pair cable (1000 Base T).



Encoding:

→ Gigabit Ethernet cannot use the Manchester encoding scheme b/c it involves a very high bandwidth. The 2 wire implementations use an NRZ scheme, but NRZ does not self synchronize properly.

→ This block encoding prevents long sequences of 0s or 1s in the stream, but the resulting stream is 1.25 Gbps. In this implementation, one wire for sending & one for receiving.

→ In the 4 wire implementation, 2 wires for i/p & 2 for o/p, bc each wire would need to carry 500 Mbps, which exceeds the capacity for category 5 UTP.

Table 13-3.

Ten Gigabit Ethernet:

1. Upgrade the data rate to 10 Gbps.
2. Make it compatible with Standard, Fast & Gigabit Ethernet.
3. Use the same 48 bit address.
4. Use the same frame format.
5. Keep the same min & max frame lengths.
6. Allow interconn^n of existing LANs into a metropolitan area Network (MAN) or WAN.

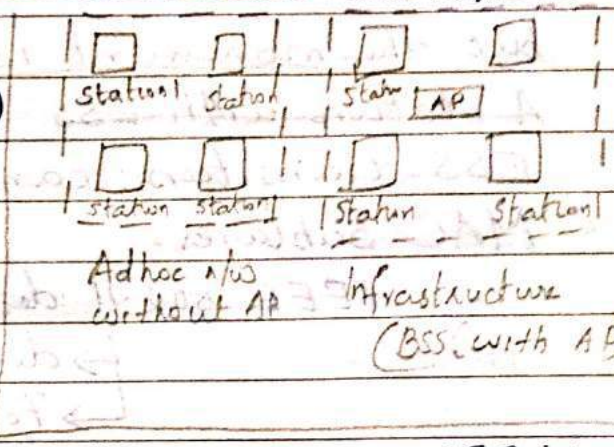
802.11 a/b/g/n

IEEE has defined the specifics for a wireless LAN, called IEEE 802.11, which covers physical & data link layers.

Architecture: two types of services
- → Basic Service Set (BSS) ✓
- → Extended Service Set (ESS) ✓

Basic Service Set:

IEEE 802.11 defines the BSS as the building blk of wireless LAN. It is made of stationery or mobile wireless stations and an optional central base station, known as access point. The BSS without an AP is a stand-alone s/w and cannot send data to other BSSs. It is called an adhoc architecture. A BSS with an AP is called an infrastructure n/w.

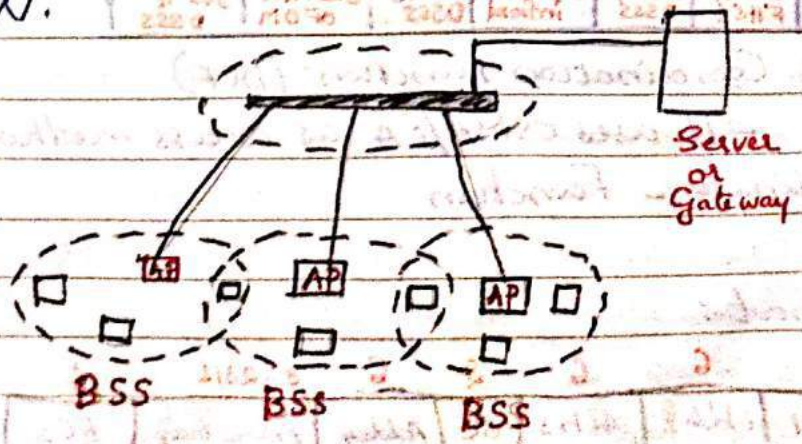


Extended Service Set: (ESS)

→ is made of 2 or more BSSs with APs. The BSSs are connected through a distribution s/m, i.e; wired LAN. The distribution s/m connects the APs in the BSSs. It can be any IEEE LAN as an Ethernet. ESS uses 2 types of stations:

→ mobile
→ stationary.

The mobile stations are normal stations inside a BSS. The stationary stations are AP station that are part of a wired LAN.

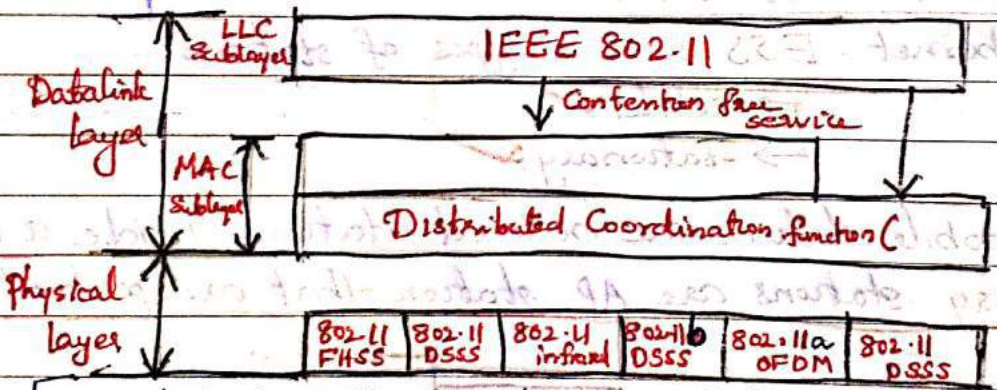


When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. Comm? b/w 2 stations in 2 diff. BSSs occurs via 2 APs.

Station Types: 3 types based on mobility
- no-transition
- BSS-transition
- ESS-transition.

no-transition: A station with no transition mobility is either stationary or moving only inside a BSS. A BSS-transition: can move from one BSS to another but the movement is confined inside one ESS.
~~A station with ESS~~
ESS-transition: can move from one ESS to another.

MAC Sublayer:
IEEE 802.11 defines 2 MAC sublayers:
- distributed Coordination Function
- Point Coordination Function.

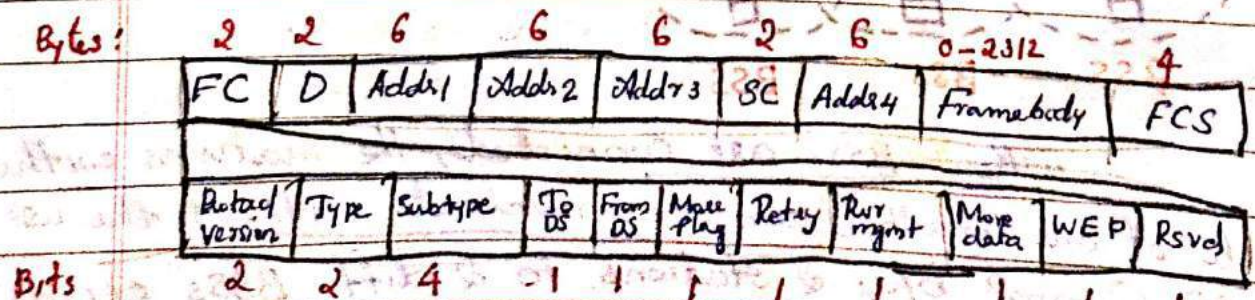


Assignment

Distributed Coordination Function: (DCF)
- It uses CSMA/CA as access method.

Point Coordination Function

Frame Format:



FC fields

Version: Current version is 0

Type: Type of inf^n; mgmt (00), ctrl (01), or data (10)

subtype: 1011 → Request to send (RTS)

1100 → clear to send (CTS)

1101 → Acknowledgement (ACK)

To DS: Defined later From DS: defined later.

Morefrag: when set to 1, means more fragments

Retry: when set to 1, means retransmitted frame.

Pwrmgmt: when set to 1, station is in power mgmt mode

More data: station has more data to send.

WEP: Wired Equivalent privacy (encryption implemented)

Rsvd: Reserved

D: defines duration of the transm^n

Addresses: 4 addresses - depends on To DS & From DS subfields.

Sequence Ctrl (SC): defines seq no of the frame to be used in flow c

Frame body: b/w 0 & 2312 bytes.

FCS: CRC

Frame Types: 3 categories:

- Mgmt frames
- Ctrl frames
- Data frames

Mgmt frames: are used for the initial comm^n b/w stations & access pts

Ctrl frames: used for accessing the channel & acknowledging fram

FC	D	Addr1	Addr2	FCS

RTS

FC	D	Addr1	FCS

CTS or ACK

Data frames: used for carrying data & ctrl information.

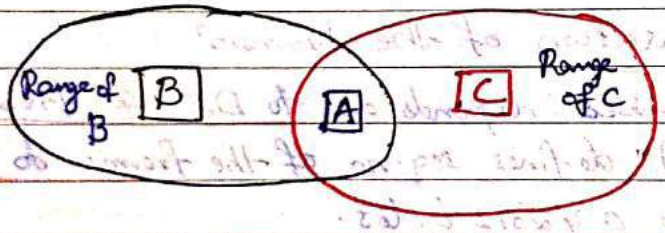
Addressing Mechanisms:

—specifies 4 cases, defined by the value of the 2 flags in the FC field, To DS and from DS.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destn	Source	BSSID	NA
0	1	Destn	sending AP	Source	NA
1	0	Receiving AP	Source	Destn	NA
1	1	Receiving AP	sending AP	Destn	Source

Hidden & Exposed Station Problems:

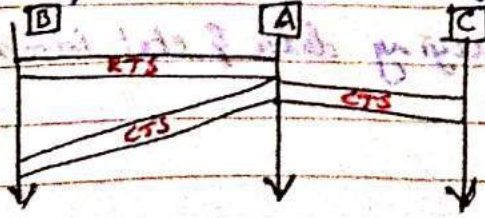
Hidden Station Problem:



B & C are hidden from each other with r.to A.

Station B has a transmn range shown by the left oval; every station in this range can hear any s/l transmitted by station B. Station C has a transmn range shown by the right oval; every station located in this range can hear any s/l transmitted by C. Station C is outside the transmn range of B; station B is outside the transmn range of C. Station A, is in the area covered by both B & C; it can hear any s/l transmitted by B or C.

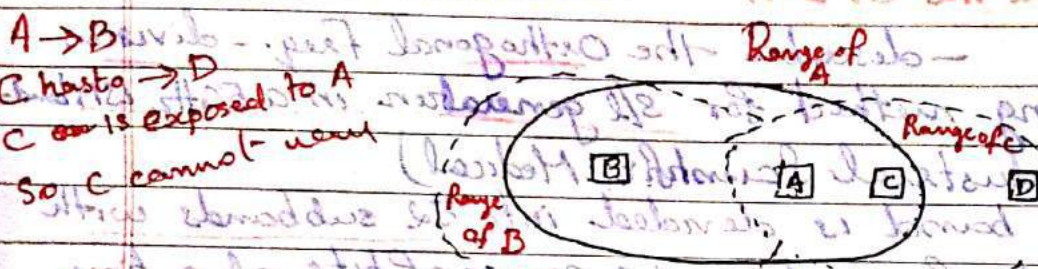
The soln to the hidden station pblm is the use of the handshake frames (RTS & CTS).



The RTS msg from B reaches A, but not C. B/c both B & C are within the range of A, the CTS msg, which contains the duration of data transmission from B to A reaches C. Station C knows that some hidden station is using the channel & refrains from transmiting until that duration is over.

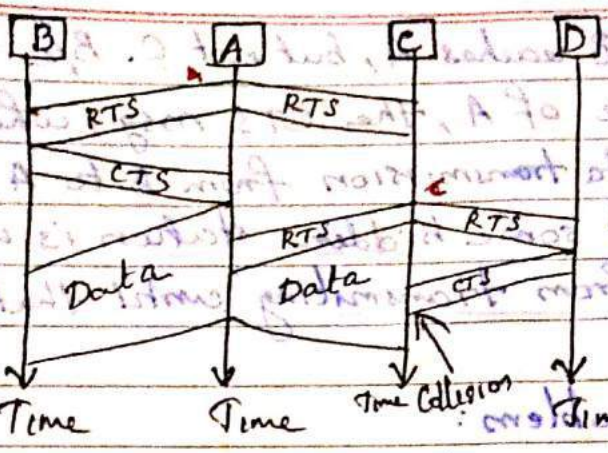
Exposed Station Problem:

A station refrains from using a channel when it is available.



Station A is transmitting to station B. Station C has some data to send to station D which can be sent without interfering with the transmn from A to B. Station C is exposed to transmn from A; it hears what A is sending & thus refrains from sending. C wastes capacity of channel.

The handshaking msgs RTS & CTS cannot help in this case. Station C hears the RTS from A, but does not hear the CTS from B. Station C, after hearing the RTS from A, can wait for a time so that CTS from B reaches. It then sends an RTS to D to show that it needs to communicate with D. Both stations B & A may hear this RTS, but station A is in sending state, not the receiving state. Station D responds with a CTS. The pblm is here. If station A has started sending its data, station C cannot hear the CTS from D b/c of collision; It cannot send its data to D.



IEEE 802.11a OFDM:

– describes the Orthogonal Freq.-division multiplexing method for s/l generation in a 5GHz ISM band. (ISM – Industrial Scientific Medical)

The band is devided into 52 subbands with 48 subbands for sending 48 groups of bits at a time & 4 subbands for ctrl info. OFDM uses PSK & QAM for modulation. Datarate 18 Mbps (PSK) & 54 Mbps (QAM).

IEEE 802.11b DSSS:

– describes the High rate direct seq. spread Spectrum (HR-DSSS) method for s/l generation in the 2.4 GHz ISM band. Complementary Code keying (CCK) encodes 4 or 8 bits to one CCK symbol.

Datarates: 1/2, 5.5, & 11 Mbps.
↓ BPSK ↓ QPSK

IEEE 802.11g:

– defines forward error correction & OFDM using the 2.4 GHz ISM band. Datarate: 22 or 54 Mbps. It is backward compatible with 802.11b. Modulation is OFDM.

IEEE 802.15 BLUETOOTH

—is a wireless technology designed to connect devices of diff. fns such as telephones, computers etc.

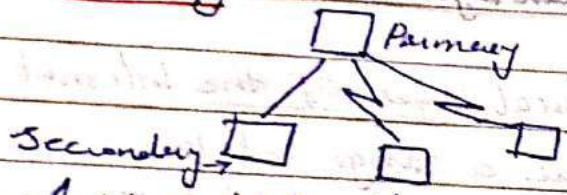
Architecture:

Two types of Networks:

- piconet
- Scatternet

Piconets:

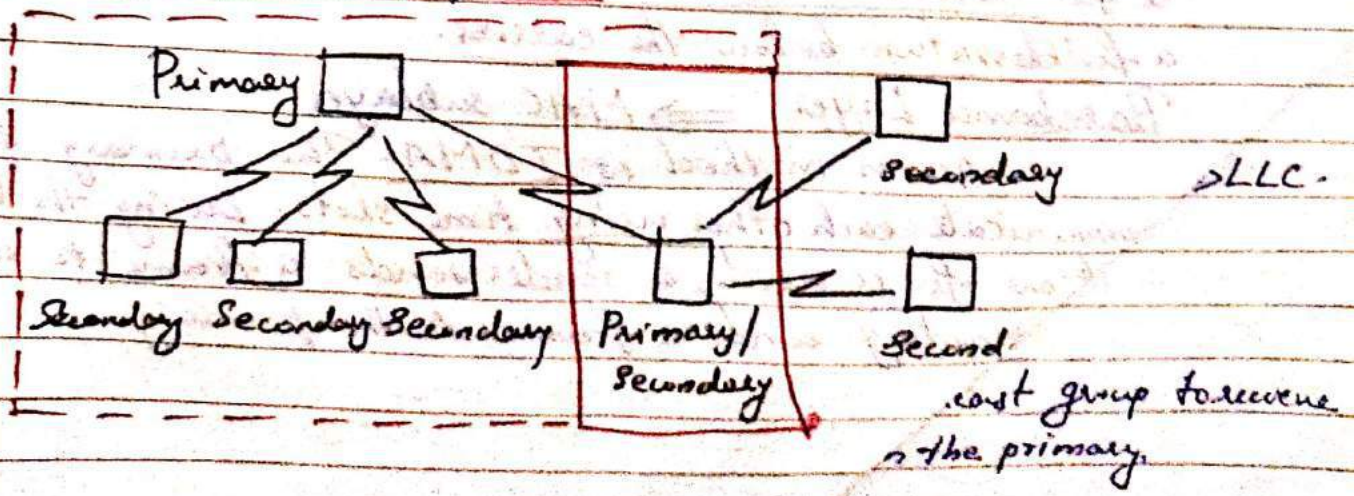
—small nets can have upto 8 stations, one of which is called the primary, the rest are called secondaries. The comm^n b/w the primary & secondary can be one to one or one to many.



A piconet can have a max. of 7 secondaries. An additional 8 secondaries can be in the parked state. A secondary in a parked state is synchronised with the primary, but cannot take part in comm^n until it is moved from the parked state.

Scatternet:

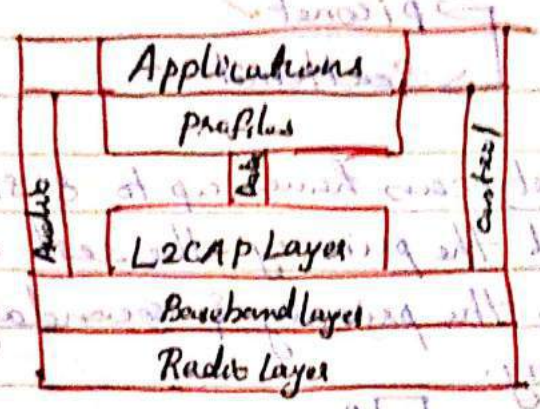
— Piconets can be combined to form what is called a scatternet. A secondary station in one piconet can be the primary in another piconet.



Bluetooth Devices:

A Bluetooth device has built-in short-range radio transmitter. The current data rate is 1Mbps with 2.4GHz bandwidth.

Bluetooth Layers:



Radio Layer: ⟹ physical layer of the Internet model.
- low-power & have a range of 10m.

Band: 2.4GHz ISM band devided into 79 channels of 1MHz each.

FHSS: Frequency Hoping Spread Speclurum:
- to avoid interference from other devices or other n/ws. A device uses a fr. for only 625μs (1/1600s) before it hops to another fr.

Modulation: - uses GFSK - Gaus Gaussian bandwidth filtering. GFSK has a carrier fr. Bit 1 is represented by a fr. deviation above the carrier; bit 0 is represented by a fr. deviation below the carrier.

Baseband Layer: ⟹ MAC sublayer.
- Access method is TDMA. The primary & secondary communicate each other using time slots. During the time that one fr. is used, a sender sends a frame to a secondary or a secondary sends a frame to the primary.

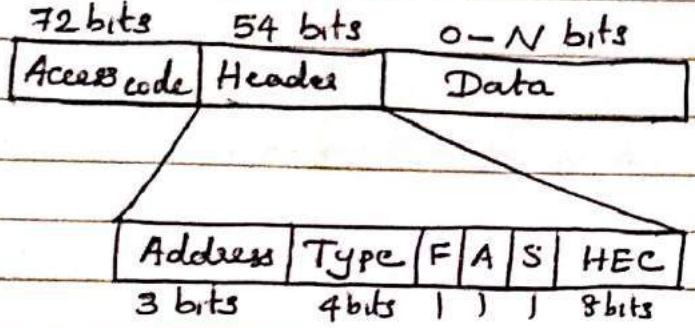
TDMA: Bluetooth uses TDD-TDMA (time division duplex TDMA). is a kind of half duplex comm^n in which the 2° & receiver send & receive data but not same time.

Two types of comm^n → Single Secondary comm^n ✓
→ Multiple Secondary comm^n. ✓

Physical Links:

2 types of links → Synch. connection Oriented link
→ ASynch. connectionless link.

Frame Format



N = 240 for 1 slot frame
N = 1490 for 3 slot frame
N = 2740 for 5 slot frame.

Access Code: 2 Synchronization bits & identifier of the primary to distinguish the frame of one piconet from another.

Header — Address: defines upto 7 secondaries. If the addr. is zero, it is used for broadcast comm^n from primary to all secondaries.

Type — type of data coming from the upper layers.
F — flow control ✓
A — Acknowledgement ✓
S - Sequence Number. ✓
HEC - error correction field. ✓

Payload: 0 - 2740 bits long.

L2CAP: Logical Link Control & Adaptation Protocol ⇒ LLC.

duties:
- multiplexing ✓
- segmentation & reassembly ✓
- QoS. ✓
- Group Management. ✓ multicast group to receive from the primary.

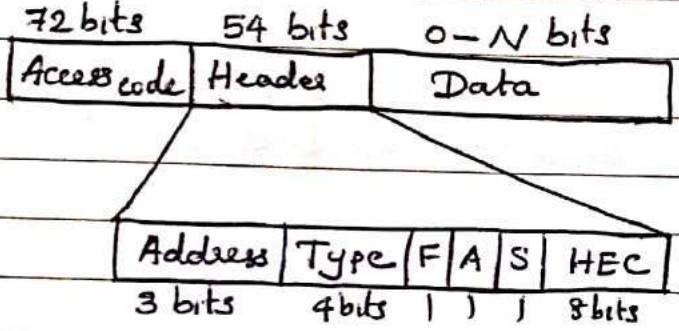
TDMA: Bluetooth uses TDD-TDMA (time division duplex TDMA). is a kind of half duplex comm^n in which the 2^o & receiver send & receive data but not same time.

Two types of comm^n → Single Secondary comm^n ✓
→ Multiple Secondary comm^n. ✓

Physical links:

2 types of links: → Synch. connection Oriented link
→ ASynch. connectionless link.

Frame Format



N = 240 for 1 slot frame
N = 1490 for 3 slot frame
N = 2740 for 5 slot frame

Access Code: of Synchronization bits & identifier of the primary to distinguish the frame of one piconet from another.

Header — Address: defines upto 7 secondaries. If the addr is zero, it is used for broadcast comm^n from primary to all secondaries.

Type — type of data coming from the upper layers
F — flow control ✓
A — Acknowledgement ✓
S — Sequence Number. ✓
HEC — error correction field. ✓

Payload: 0 — 2740 bits long.

L2CAP: Logical Link Control & Adaptation Protocol ⇒ LLC.

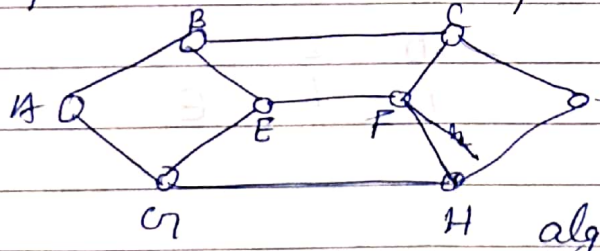
duties: → multiplexing ✓
→ segmentation & reassembly ✓
→ QoS. ✓
→ Group Management. — multicast group to receive from the primary.

MODULE III
Network Layer:

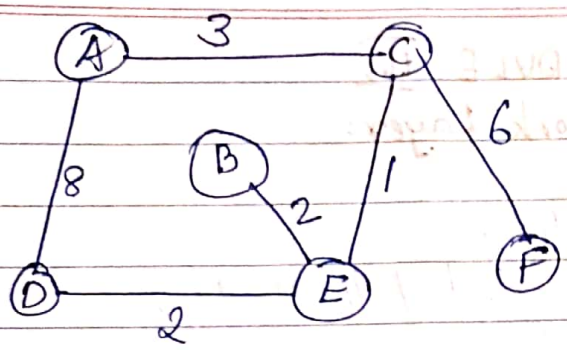
→ Routing
* Shortest Path Routing
* Flooding
* Distance Vector Routing
* Link State Routing
* RIP
* OSPF
* Routing for Mobile Hosts.

Assignment: Two node Instability & 3 node Instability.

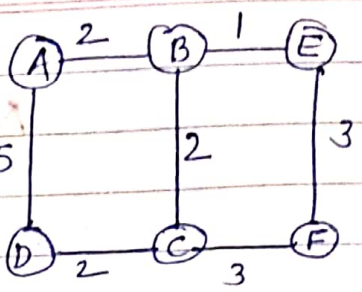
Questions:

1. Give 2 eg: computer appl^{n}s for which conn^n oriented service is appropriate - 2 eg: for conn^{n}less service.
2. Are there any circumstances when conn^n oriented service will deliver pkts out of order? Explain.
3. 

Suppose that it uses flooding as the routing algm. If pkt A to D has a max. hop count of 3, list all the routes it will take. Also tell how many hops worth of bandwidth it consumes.
4. How does the hop count limit alleviate RIP's pblms?
5. What is the basis of classific^n for the 4 types of links defined by OSPF?
6. For n/w given in fig, Give global distance vector tables when
   a) Each node knows only the distances to its immediate neighbors.
   b) Each node has reported the inf^n it had in the preceding step to its immediate neighbors.



(a)



(b)

7 Given 2 forwarding tables. for nodes A & F in a n/w where all links have cost 1. Give diagram of smallest n/w consistent with tables.

(1)

Node	Cost	Nxt
A→ B	1	B
C	2	B
D	1	D
E	2	B
F	3	D

F→		
A	3	E
B	2	C
C	1	C
D	2	E
E	1	E

(2)

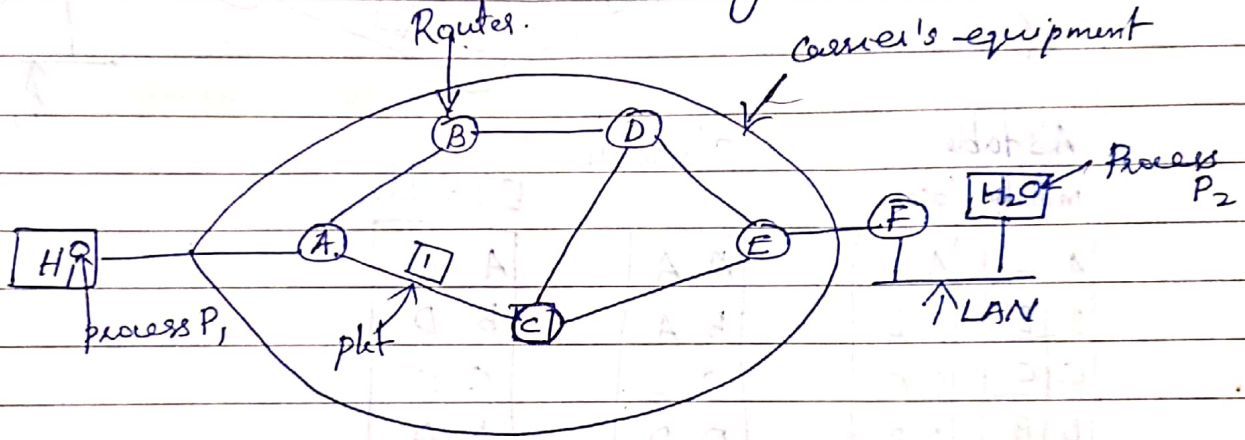
A→		
B	1	B
C	1	C
D	2	B
E	3	C
F	2	C

F→		
A	2	C
B	3	C
C	1	C
D	2	C
E	1	E

Network Layer Design Issues:

1. Store & forward Packet Switching
2. Services Provided to the Transport Layer
3. Implementation of Connectionless Service.
4. " Connection Oriented Service.
5. Comparison of VC & Datagram Subnets.

1. Store and forward Packet Switching:



A host with a pkt to send transmits it to the nearest router, either on its own LAN or over pt-to-pt link to the carrier. The pkt is stored there until it has fully arrived so the checksum can be verified. The it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is store & forward pkt switching.

2. Services provided to the Transport Layer.

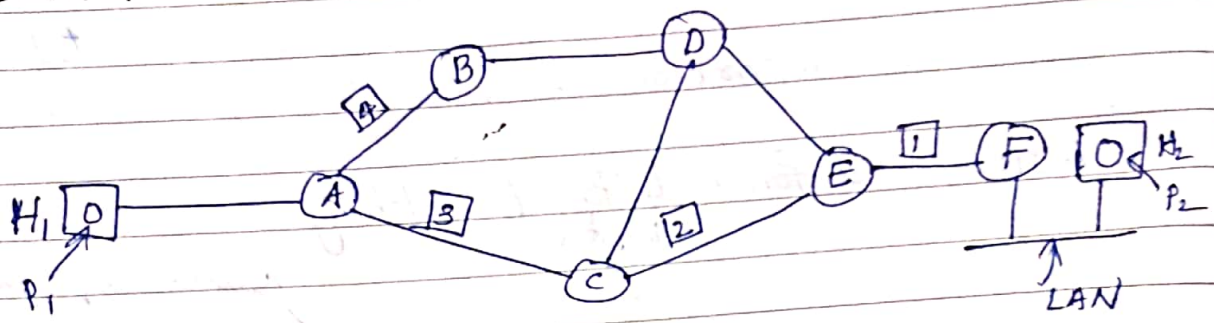
→ The services should be independent of the routers technology.

→ The transport layer should be shielded from the no; type & topology of the routers present.

→ The n/w addresses made available to the transport layer should use a uniform numbering plan.

3. Implementation of Connectionless Service:

If connⁿ less service is offered, pkts are injected into the subnet individually & routed independently of each other. No advance set up is needed. The pkts are called datagrams & the subnet is called datagram subnet.



A's table

	initially	later
A	–	A –
B	B	B B
C	C	C C
D	B	D B
E	C	E B
F	C	F B

Dest. Line

C's table

A	A
B	A
C	–
D	D
E	E
F	E

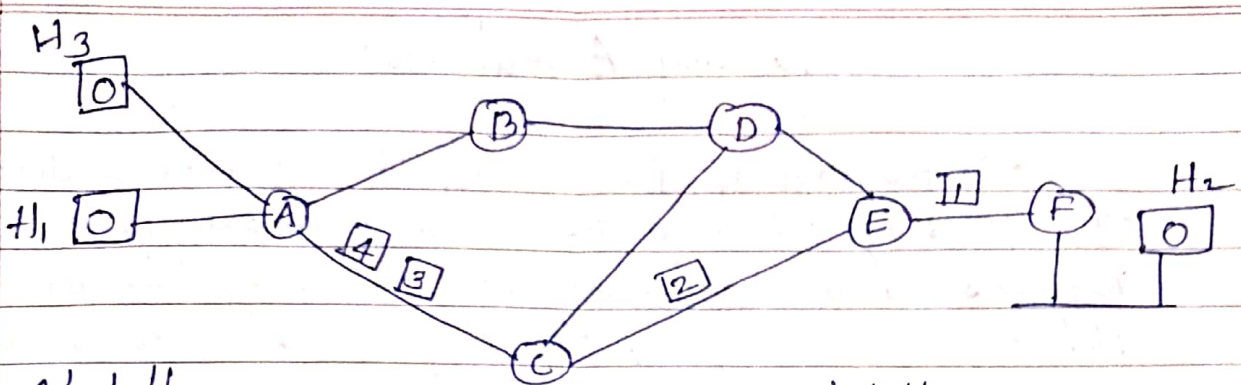
E's table

A	C
B	D
C	C
D	D
~~E~~	~~D~~
E	F

As they arrived at A, pkts 1, 2, 3 were stored briefly. Then each was forwarded to C acc. to A's table. When pkt 4 got to A it was sent to router B, even though it is also destined for F. (traffic)
The algm that manages & makes routing decisions is called the routing algm.

4. Implementation of Connection Oriented Service:

If connⁿ oriented service is used, a path from source router to the destⁿ routes must be established before any data pkt can be sent. This connⁿ is called Virtual Circuit (subnet VC subnet).



A's table

H_1	1	C	1
H_3	2	C	2
in		out	

C's table

A	1	E	1
A	2	E	2
in		out	

E's table

C	1	F	1
C	2	F	2

1, 2 - connection identifiers.

H_3 chooses connection identifier 1 b/c it is initiating the connⁿ & tells the subnet to establish the virtual circuit. A can easily distinguish connⁿ 1 from H_1 from connⁿ 1 pkts from H_3, C cannot do this. ∴ A assigns a diff. connⁿ identifiers to the outgoing traffic for the 2nd connⁿ(2)

5. Comparison of VC & Datagram Subnets:

Issue	Datagram Subnet	Virtual Circuit Subnet.
Ckt. Setup	Not needed	Required.
Addressing	Full source & Destⁿ Address	a short VC Number.
State Infⁿ	Do not hold	requires router table space per connection.
Routing	routed independently	Route is chosen when VC is setup; all pkts follow.
Effect of Router failures	None	All VCs that passed through the failed router are terminated.
QoS	Difficult	Easy if enough resources can be allocated in advance for each VC.
Congestion ctrl	Difficult	Easy "

Routing Algorithms:

→ Routing & forwarding: Routing is making the decision which routes to use & forwarding is what happens when a pkt arrives. Forwarding handles each pkt arrives, looking up the outgoing line to use for it in the routing tables.

Properties of Routing:

* Correctness * Simplicity * robustness * stability * fairness & * Optimality.

Routing Algorithms → non adaptive
→ Adaptive.

Non adaptive algms: do not base their routing decisions on measurements or estimates of the current traffic and topology. The choice of the route to use to get from I to J is computed in advance, offline & downloaded to the routers when the n/w is booted. This procedure is called static routing.

Adaptive Algms: change their routing decisions to reflect changes in the topology & the traffic. They differ in where they get their inf", when they change the routes & what metric is used for optimization.

The Optimality Principle:

It states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.

To see this, call the part of the route I to J r_1 & rest of the route r_2. If a route better than r_2 existed from J to K, it could be concatenated with r_1 to improve the route from I to K, contradicting our stmt $r_1 r_2$ is optimal.

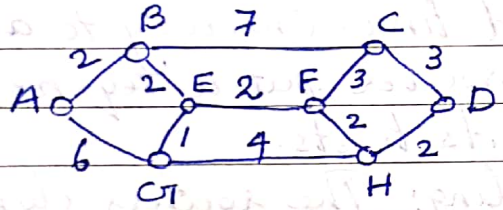
As a direct consequence of the optimality

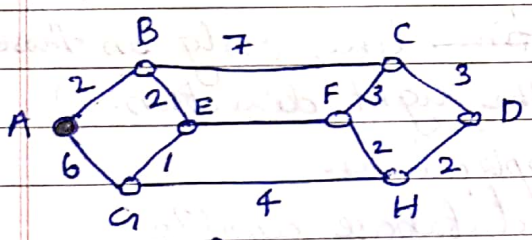
principle, the set of optimal routes from all sources to a given dest^n form a tree rooted at the dest^n. Such a tree is called a sink tree.

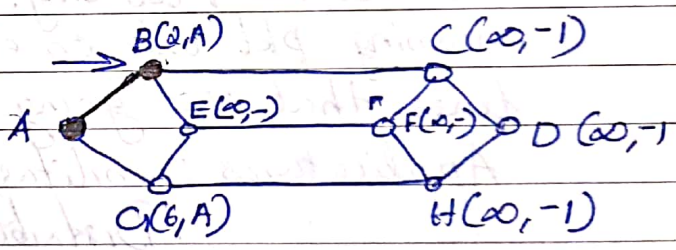
* Shortest Path Routing:

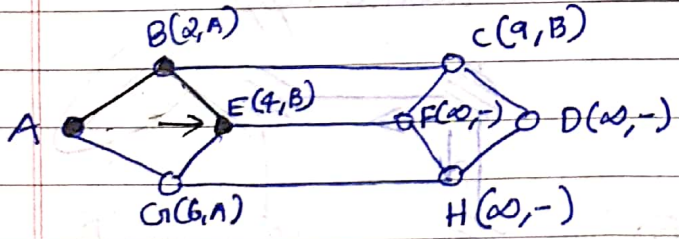
→ One way of measuring path length is the no. of hops. The labels on the arcs could be computed as fn. of the distance, bandwidth, avg traffic comm^n cost, measured delay & other factors. Algm compute the 'shortest' path measured acc. to any one of a no. of criteria or to a comb^n of criteria.

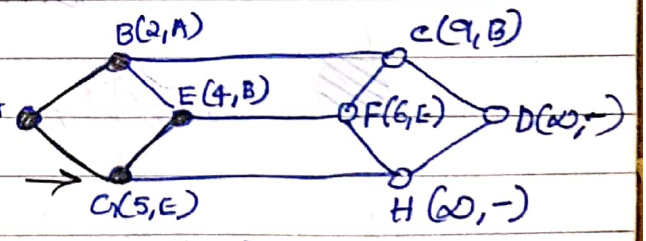
Dijkstra's Algm:

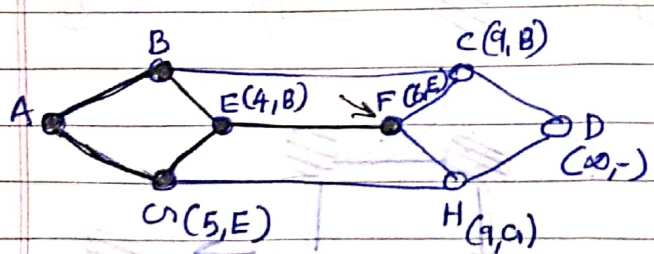


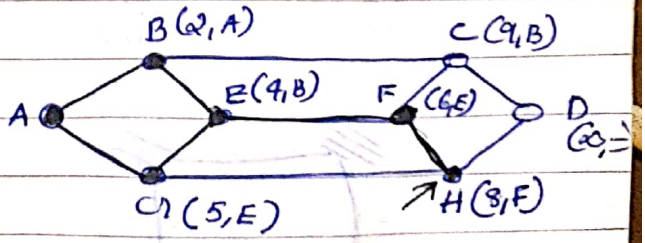












*Flooding:

→ Static Algm: Every incoming pkt is sent out on every outgoing line except the one it arrived on. Flooding generates vast no. of duplicate pkts.

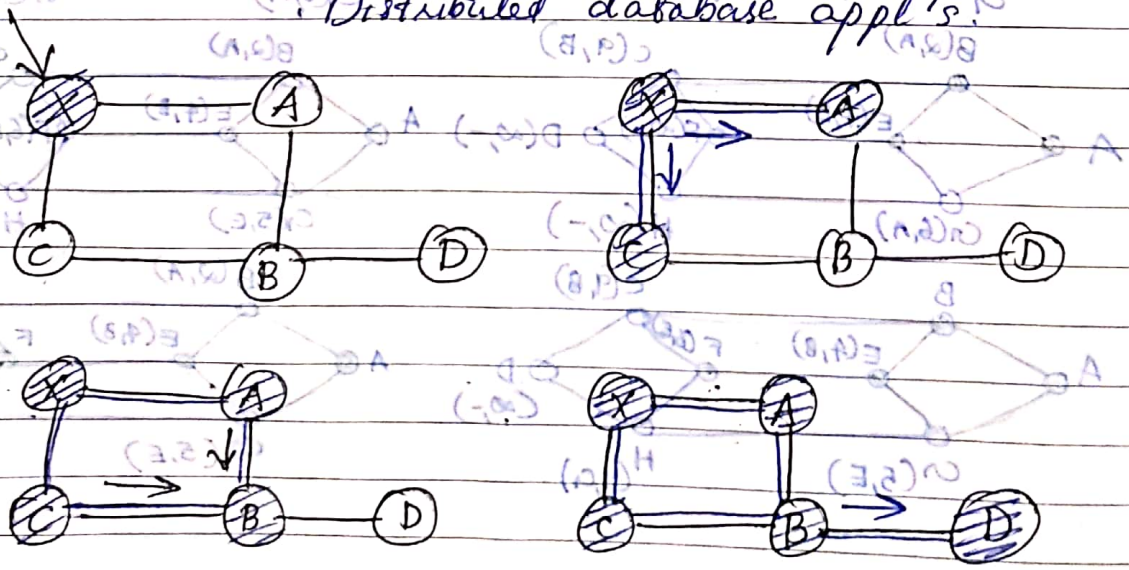
→ Measure is to have a hop counter contained in the header of each pkt, which is decremented ~~by~~ at each hop, with the pkt being discarded when the counter reaches zero. The hop counter should be initialised to the length of the path from source to destn.

→ Alternative measure is to keep track of which pkts have been flooded, to avoid sending them out a second time. One way to achieve is to have the source router put a seq-no in each pkt it receives from its hosts.

Selective Flooding: The routers do not send every incoming pkt out on every ~~line~~ line, only on those lines that are going in the right direction.

Applications: military applications.

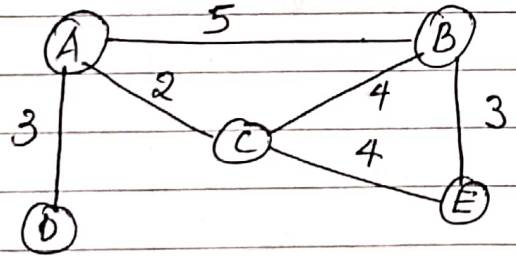
Distributed database appl^ns:



A node X that receives a copy of pkt that originated at some other node Y. Y may be any other router as X. X checks to see if it has already stored a copy of pkt from Y. If not it stores. Else it compares seq. no.s if it has larger seq. no it is assumed to be more recent, that pkt is stored. A smaller seqno means older than stored one, so it would be discarded & no further action. If the received pkt was newer, X sends a copy of that pkt to all of its neighbours. All its neighbours do the same thing eventually reaches all nodes.

* Distance Vector Routing:

In distance vector routing, the least cost route b/w any 2 nodes is the route with min. distance. Each node maintains a vector(table) of min. distances to every node. The table at each node also guides the pkts to the desired node by showing the next stop in the route.



Initialization of tables in distance vector routing:

Each node can know only the distance b/w itself and its immediate neighbours, those directly connected to it.

A's table

To	Cost	Next
A	0	-
B	5	-
C	2	-
D	3	-
E	∞	

B's table

To	cost	Nxt
A	5	-
B	0	-
C	4	-
D	∞	
E	3	-

C's table

To	Cost	Nxt
A	2	-
B	4	-
C	0	-
D	∞	
E	4	-

D's table

To	Cost	Nxt
A	3	-
B	∞	
C	∞	
D	0	-
E	∞	

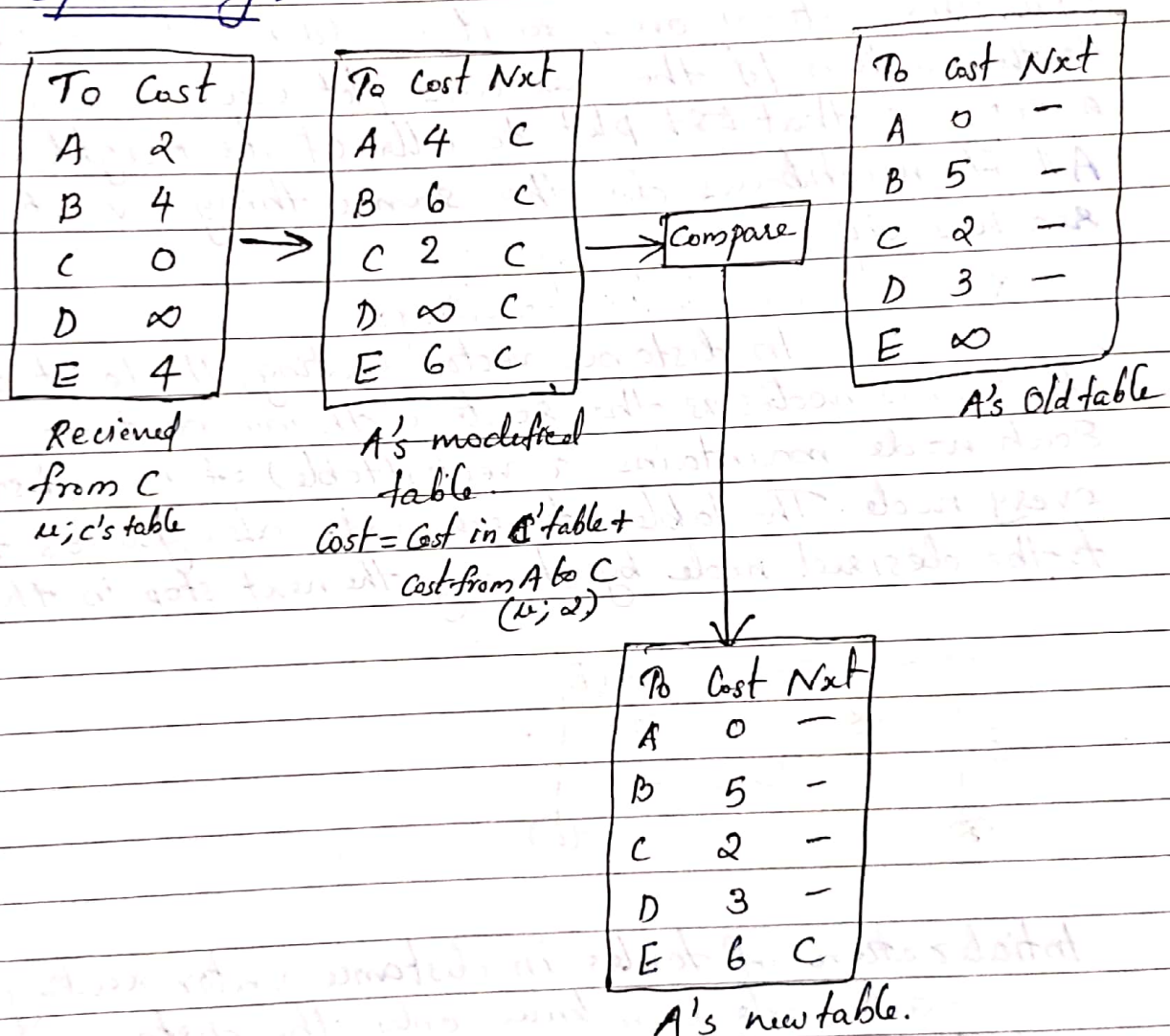
E's table

To	Cost	Nxt
A	∞	
B	3	B
C	4	C
D	∞	
E	0	D

Sharing

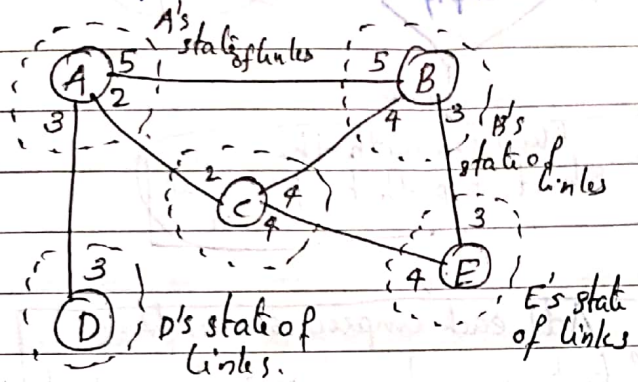
– Sharing of info b/w neighbours.
Although node A doesn't know about node E, node C does. So if node C shares its routing table with A, node A can also know how to reach node E.

Updating:



* Link State Routing:

Each node knows link to its neighbours & cost of each link. Every node knows how to reach its directly connected neighbors & is forwarded to every node. Then every node will have enough knowledge of the n/w to build up complete map.



Link state knowledge.

Building Routing Tables:

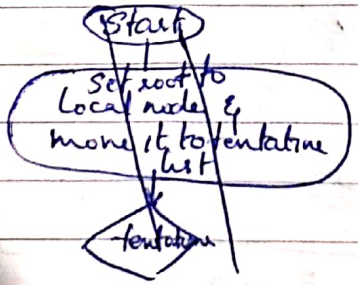
In link state Routing, 4 sets of actions are rqd to ensure that each node has the routing table

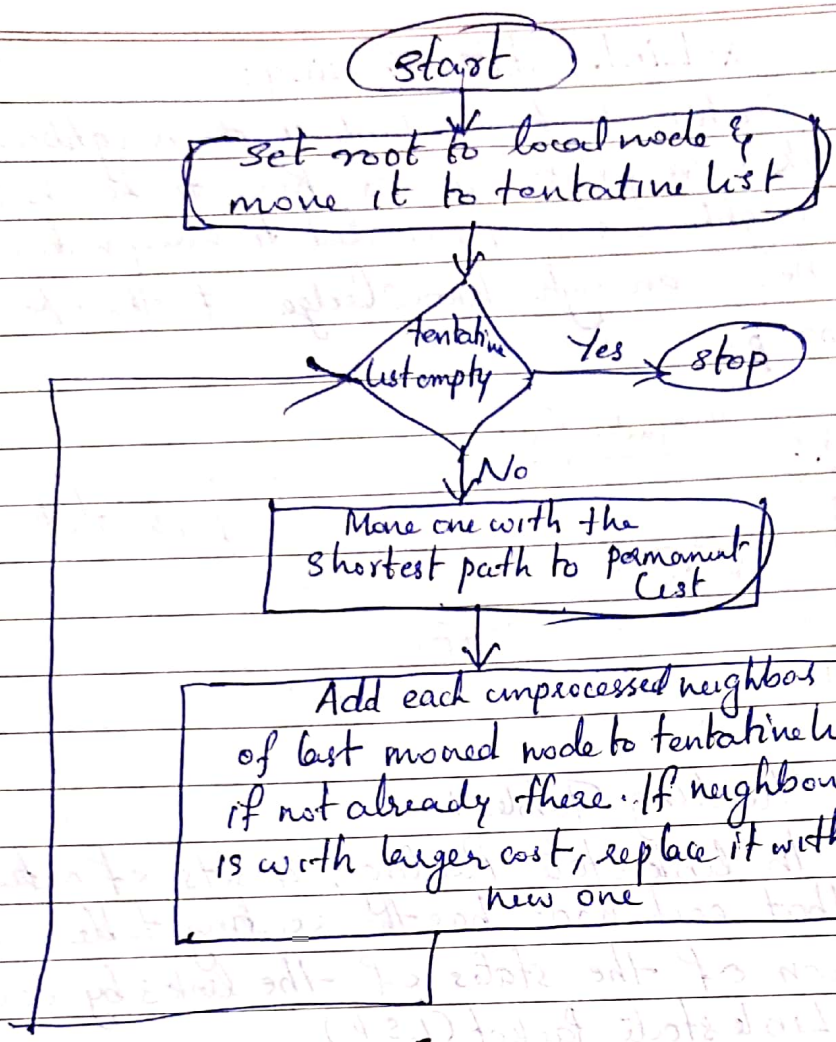
1. Creation of the states of the links by each node, called Link state Packet (LSP)

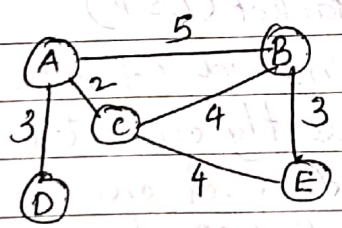
LSP contains id of the node that created LSP, a list of directly connected neighbours with the cost of the link to each one.

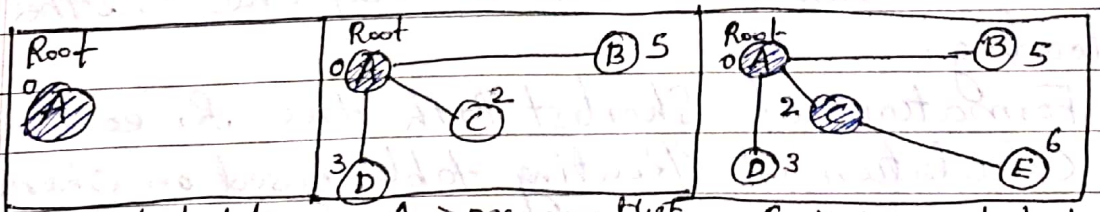
2. Dissemination of LSPs to every one another called flooding.
3. Formation of Shortest Path tree for each node.
4. Calculation of Routing table based on Shortest Path tree.

Formation of Shortest Path Tree: Dykstra's Algm.





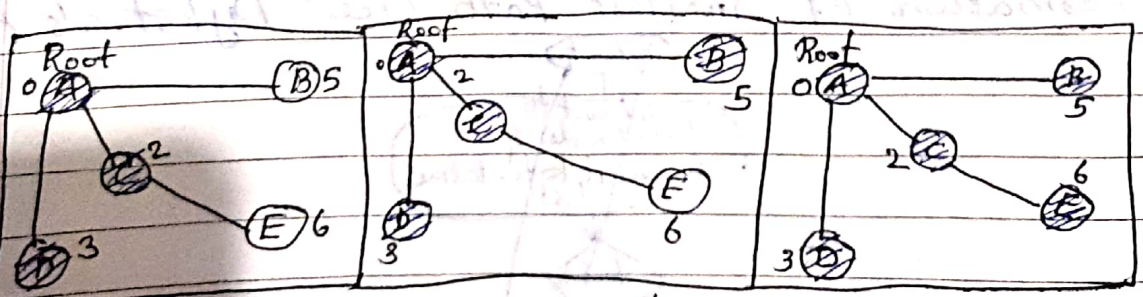




Root A to tentative list

A → permanent list
B, C & D → tentative list

C → permanent list
E → tentative list



D to permanent list

B → permanent list

E → permanent list.

Steps:

1. Permanent list: Empty ; Tentative list : A(0)
2. Move A to permanant list & neighbours to tentative list
   Permanent list: A(0) ; Tentative list: B(5), C(2), D(3)
3. Node C has shortest cost ; So C is moved to permanent list. And A also C has neighbours A, B & E. A Res already processed. B & E are unprocessed neighbours. B is already in tentative list. & move E to tentative list.
   Permanent list: A(0), C(2) ; tentative list: B(5), E(6), D(3)
4. Node D with minimum cost 3 is moved to permanent list. Node D has no unprocessed list.
   Permanent list: A(0), C(2), D(3) tentative list: B(5), E(6)
5. Node B has minimum cost 5 is moved to permanent list & it has ~~xxx unprocess~~ neighbors A, C, & E. A & C in permanent list. E(6) in tentative list. Cost from A to E through B is 8 which is greater than E(6).
   Permanent list: A(0), C(2), D(3), B(5) tentative list E(6).
6. E has shortest cost of 6. & it has no unprocessed neighbors. So E is moved to permanent list & tentative list empty.
   Permanent list: A(0), C(2), D(3), B(5), E(6); tentative list: empty.

Calculation of Routing Table from Shortest Path Tree:

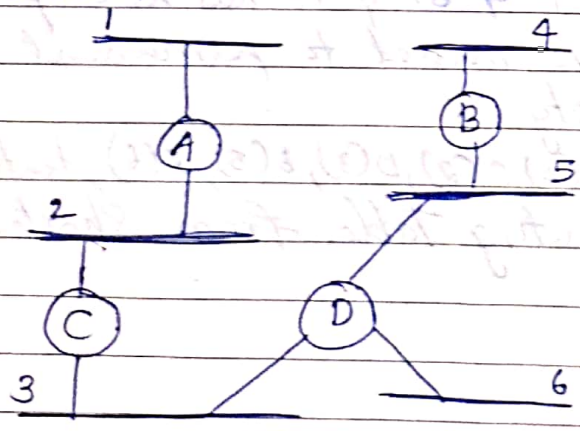
Node	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

* Routing Information Protocol: (RIP)

— is an intradomain routing protocol used inside an autonomous s/m. It is based on distance vector routing.

Considerations:

1. Dealing with routers & networks. The routers have routing tables; n/ws do not.
2. The dest^n in a routing table is a n/w which means 1st column defines n/w address.
3. The distance is defined as the no. of n/ws to reach the dest^n. The metric in RIP is called a hop count.
4. Infinity is defined as 16, which means that any route in an autonomous s/m using RIP cannot have more than 15 hops.
5. The next node ~~et~~ column defines the addr. of the router to which the pkt is to be sent to reach its dest^n.



→ The routers advertise the cost of reaching networks. For eg: router C would advertise to router A that it can reach n/ws 2 & 3 (directly connected) at a cost of 0; n/ws 5 & 6 at cost 1 & n/w 4 at cost 2.

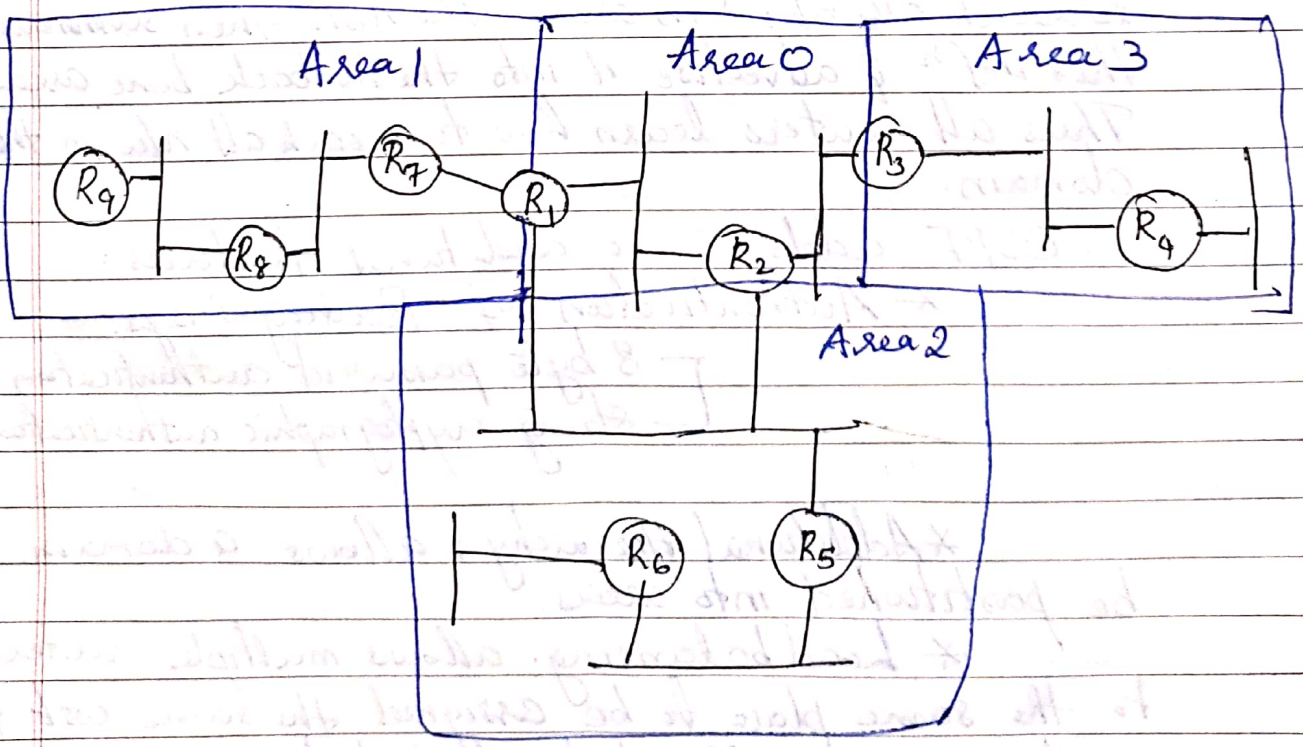
If a router A learns from B router B that n/w X can be reached at a lower cost via B than the existing next hop in the routing table, A updates the cost & next hop info for the n/w.

Routers running RIP send their advertisements every 30 seconds; a router also sends in update msg whenever an update from another router causes it to change its routing table.

* Open Shortest Path First protocol (OSPF)

(Implement" of Link state routing Protocol)

OSPF is an Intradomain routing protocol. OSPF divides an autonomous s/m into areas. An area is a set of routers that are configured to exchange link state info" with each other. There is one special area the backbone area also known as area 0..



A router that is member of the backbone area & a non backbone area is an area border routers. All routers in the area send and link state advertisements to each other. The link state advertisements of routers that are not ABR dont leave the area in which they originated. For eg: R_1 in area3 will never see a link state advertisement from R_8 in area1.

First it travels from its source n/w to backbone area, then it crosses the backbone, then it travels from backbone to the dest^n n/w.

For eg: R_1 receives link state advertisement s from all routers in area1 & can thus determine the cost of reaching any n/w in area1. When area1 sends link state advertisements into area0, it advertises the cost of reaching the n/ws in area1. This enables to reach all n/w in area1. The ABR then summarizes this info^n & advertise it into the nonbackbone areas. Thus all routers learn how to reach all n/w in the domain.

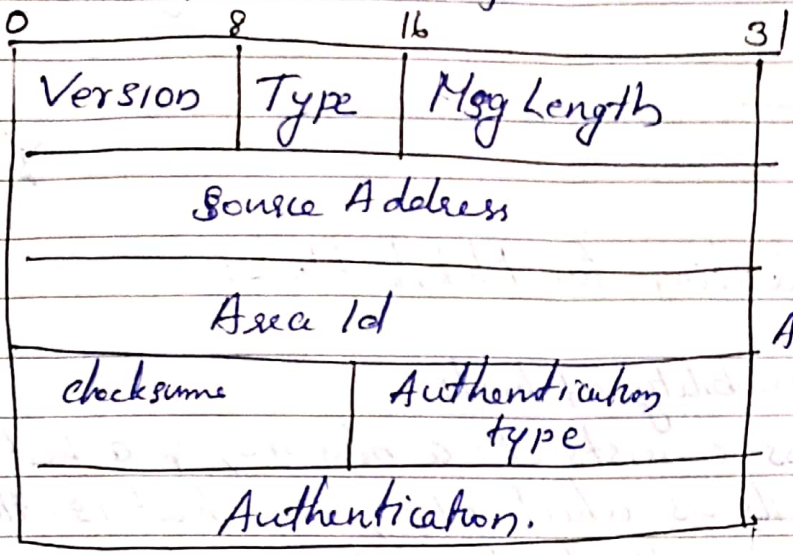
OSPF adds some additional features:

* Authentication of Routing Msgs:
  - 8 byte password authentication
  - strong cryptographic authentication

* Additional Hierarchy: allows a domain to be partitioned into areas.

* Load balancing: allows multiple routers to the same place to be assigned the same cost & will cause traffic to be distributed.

OSPF Header format



Version - currently 2
Type ⇒ 1 - 5
Msg length - length

Authentication type:
0 - no authentication
1 - Simple authentication
2 - Cryptographic "

Authentication field: pswd or crypto. pswd.

Type 1 - Hello msg, remaining ⇒ rqst, send, advertisement or acknowledgement.

Metrics: - link cost

- Queue length: no. of pkts that were queued waiting to be transmitted on each link.

- Latency: Each incoming pkt was timestamped with its time of arrival at the router (Arrival time) its departure time from the router (Depart time) was also recorded.

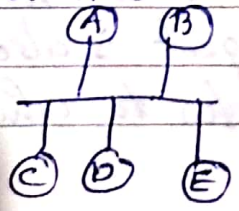
Delay = (Depart time - Arrival time) + Transm^n time + Latency.

Transm^n time & latency depends on link's bandwidth.

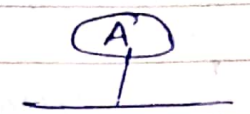
Types of Links:

Point to point link: connects 2 routers without any other host or router in b/w.

Transient link: n/w with several routers attached to it.



Stub Link: is a n/w connected to only one router.



* Routing for Mobile Hosts:

→ mobility of hosts.

A host address consists of a n/w no, & a host part. ~~Net~~ N/w no. tells us which n/w, the host is attached to. In some cases the host is disconnected from one n/w & connected to another. In such cases, if we do not change the n/w no, then the host would become unreachable. Any pkt destined for this host would be sent to the n/w that has the appropriate n/w no. but that n/w tried to deliver the pkt to the host, the host would not be there to receive it.

Solution is to provide the host with a new addr. when attaches to a new n/w.

- Home agent of the mobile node.

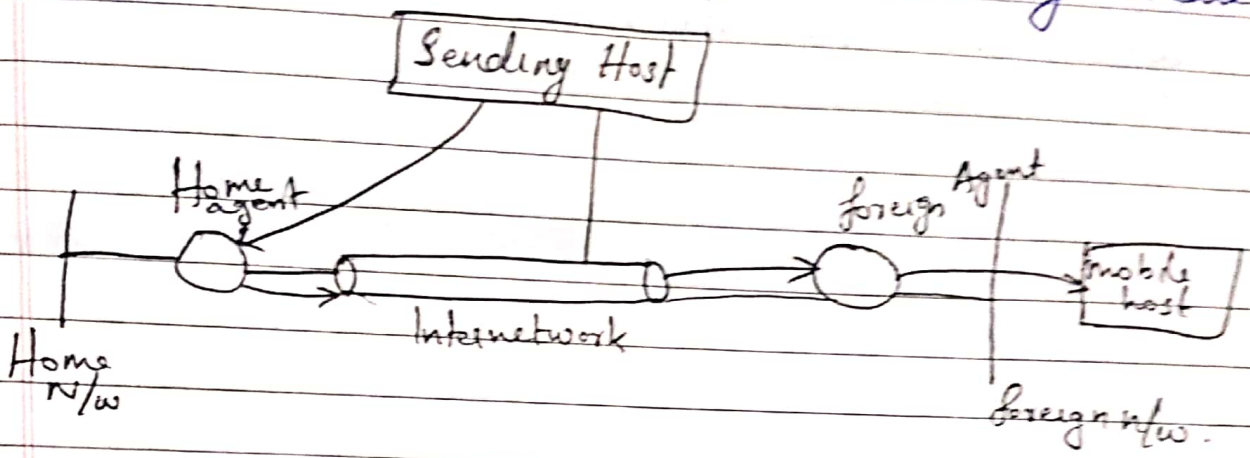
This routes is located on the 'home' n/w of the mobile host. The mobile host is assumed to have a permanent host address, called home address.

Home address has a n/w no. equal to that of home n/w & thus of home agent. This is the addr. that will be used by other hosts when they send pkts to the mobile host, since it doesn't change, it can be used by long lived appl^{n}s.

In many cases, a 2nd routes with enhanced fnality, the foreign agent is also required. This routes is located on a n/w to which the mobile

node attaches itself when it is away from its home n/w. Both home & foreign agent periodically announce their's presence on the n/ws to which they are attached using advertisement msgs.

When the mobile host attaches to a foreign n/w, it hears an advertisement from a foreign agent then it contacts the home agent, providing a care of address.



MODULE IV

Congestion Control Algorithms.

→ QoS
→ Internetworking
→ N/w Layer in the Internet
→ IPv4
→ IP Addressing
→ Classless & Classful Addressing
→ Subnetting.

1. What is the no. of bits in an IPv4 address?
2. Explain why most of the addresses in class A are wasted.
3. What is the n/w address in a blk of addresses? How can we find the n/w address if one of the addresses in a blk is given?.
4. What is NAT?. How can NAT help in address depletion?.
5. What are the differences b/w classful addressing & classless addressing in IPv4?.
6. What is mask in IPv4 addressing?.
7. Change the follo. IP addresses from binary notation to dotted decimal notation.
   a) 01111111 11110000 01100111 11111001
   b) 10101111 11000111 11111000 00011101
   c) 11011111 10110000 00011111 01011101
   d) 11100000 11110111 11000111 01111101
8. Find the netid & the hostid of the follo. IP addresses.
   a) 117.34.3.8 b) 132.57.8.6 c) 207.3.54.12
9. An ISP is granted a blk of addresses starting with 120.60.4.0/22. The ISP wants to distribute these blks to 100 org's with each org^n recieving just 8 addresses. Design the subblks & give the slash notation for each subblock. Find out how many

addresses are still available after these allocations?

10. In a blk of addresses, the IP address of one host is 182.44.82.16/26. What are the first address & last address in this block?

11. ~~Show in hexadecimal colon notation~~

Change Write the follo. masks in slash notation(/n)

a) 255.0.0.0 b) 255.255.224.0 c) 255.255.255.0

d) 255.255.240.0.

12. An ISP is granted a blk of addresses starting with 150.80.0.0/16. The ISP wants to distribute these blks to 2600 customers as follows:

a) The first group has 200 customers; each needs 16 addresses.

b) The 2nd " 400 " ; " 8 addresses

c) 3rd " 2000 " " 4 addresses.

Design subblocks & give slash notation for each subblocks. Find out how many addresses are still available after these allocations.

13. An ISP has a blk of 1024 addresses. It needs to divide the addresses among 1024 customers. Does it need subnetting? Explain.

14. Find the range of the addresses in the follo. blks.

a) 200.17.21.128/27 b) 200.17.21.128/27 c) 17.34.16.0/23

d) 123.56.77.32/29.

15. An orgn is granted the blk 211.17.180.0/24. The admin wants to create 32 subnets.

a) Find the subnet mask b) Find the no. of addresses in each subnet

c) Find the first & last addresses in subnet 1.

d) " " subnet 32.

16. An orgn is granted the blk 130.56.0.0/16. The admin wants to create 1024 subnets

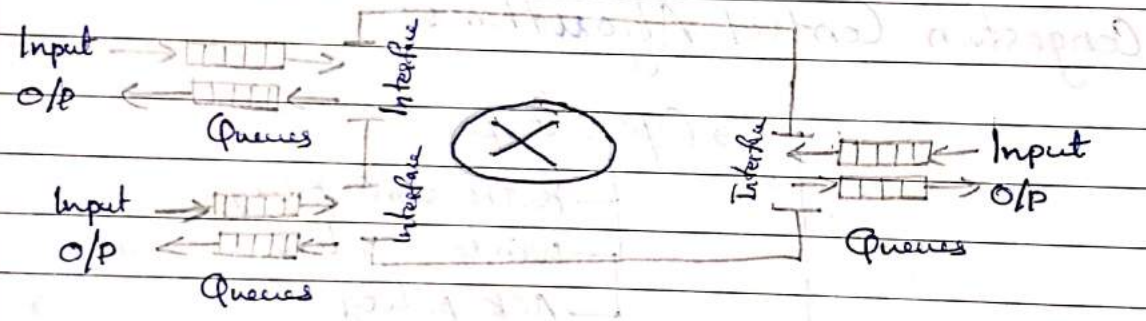
a) 15.a, 15.b, 15.c, 15.d

classmate
Date
Page

Congestion Control:

Congestion in a n/w may occur if the load on the n/w – the no. of pkts sent to the n/w – is greater than the capacity of the n/w – the no. of pkts a n/w can handle. Congestion ctrl refers to the mechanisms & techniques to ctrl the congestion & keep the load below the capacity. Congestion in a n/w or internetwork occurs b/w routers & switches have queues.

A router has an ~~its~~ i/p queue and an o/p queue for each i/f. when a packet arrives at the incoming i/f, it undergoes 3 steps before departing.

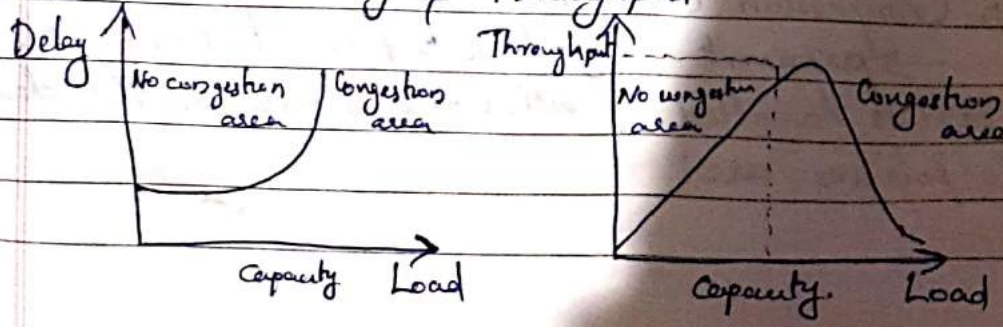


1. The pkt is put at the end of the i/p queue while waiting to be checked.

2. The processing module of the router removes the pkt from the i/p queue once it reaches the front of the queue & uses its routing table & the dest^n address to find the route.

3. The pkt is put in the appropriate o/p queue & waits its turn to be sent.

Congestion ctrl involves 2 factors that measure the performance of a n/w.: delay & throughput.



Delay versus Load

→ ~~load~~ When load is much less than the capacity of the n/w, the delay is at a minimum. This minimum delay is composed of propagation delay & processing delay. When the load reach n/w capacity, the delay increases sharply. Delay becomes infinite when the load is greater than the capacity.

Throughput versus Load:

→ When the load is below the capacity of the n/w, the throughput increases proportionally with the load. When load becomes greater than capacity throughput decreases sharply.

Congestion Control Algorithms:

- Open loop
  - Retransmn policy
  - Window policy
  - ACK policy
  - Discarding policy
  - Admission policy
- Closed loop
  - Back pressure
  - Choke packet
  - Implicit signalling
  - Explicit signalling

Open loop Congestion Control

→ prevent congestion before it happens. Congestion ctrl is handled by either the source or the destn. The diff. policies are:

Retransmission Policy:

In general Retransmission may increase congestion in the n/w. The retransmission policy and the retransm^n timers must be designed to optimize efficiency and at the same time prevent congestion. Eg: retransmission policy used by TCP.

Window Policy:

The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-back-N window for congestion control. In the Go-Back-N window, when the timer for a pkt times out, several pkts may be resent; The Selective Repeat window tries to send the specific pkts that have been lost/corrupted.

Acknowledgement Policy:

If the reciever doesn't acknowledge every pkt it recieves, it may slow down the sender & help prevent congestion. Several approaches are used in this case.

→ A reciever may send an ack only if it has a pkt to be sent or a special timer expires.

→ A reciever may decide to acknowledge only N pkts at a time.

Sending fewer ack. means imposing less load on the n/w.

Discarding Policy:

A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transm^n.

Eg: audio transm^n – qlty of sound is preserved.

Admission Policy: in virtual ckt n/ws. Switches in a flow first check the resource rqmt of a flow before admitting it to the n/w. A router can deny establishing a virtual ckt conn^n if there is congestion in the n/w or if there is possibility of future congestion.

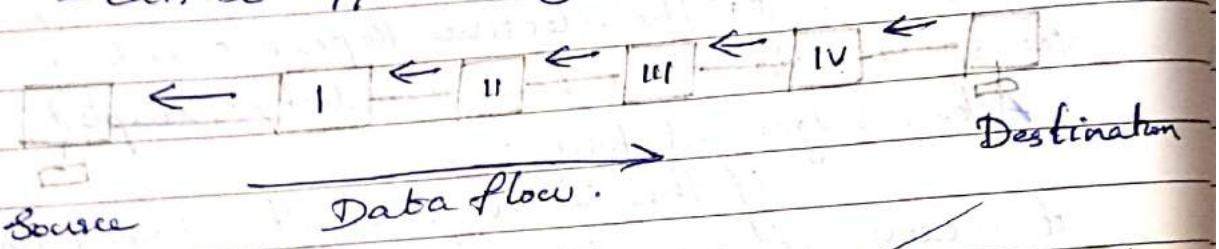
Closed Loop Congestion Control:

→ alleviate congestion after it happens.

* Backpressure: (Warning Bit)

- congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node or nodes to become congested. & they in turn, reject data from their upstream nodes & so on. Backpressure is a node to node congestion ctrl that starts with a node & propagates, in the opposite direction of data flow, to the source.

- can be applied only to virtual ckt nlw.

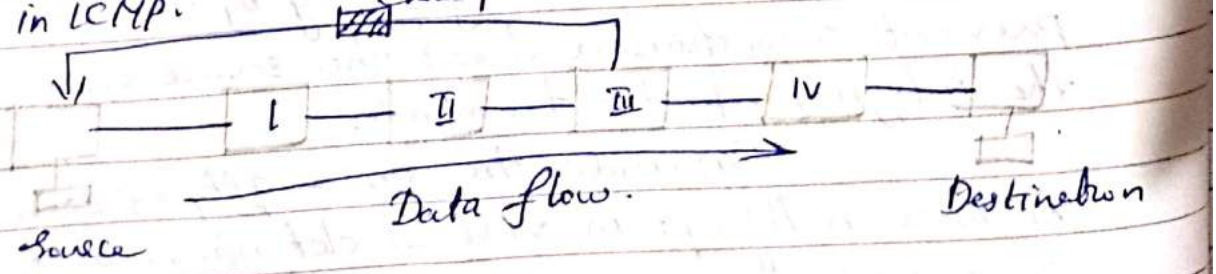


* Choke Packet:

is a pkt sent by a node to the source to inform it of congestion. In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station.

In choke pkt method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes are not warned.

Eg: in ICMP.



* Implicit Signalling:

There is no comm^n b/w the congested node or nodes & the source.

The source guesses that there is a congestion somewhere in the n/w from other symptoms. For eg: when a source sends several pkts & there is no ack for a while, one assumption is that the n/w is congested. The delay in recieving an ack is interpreted as congestion in the n/w; the source should slow down.

* Explicit Signalling:

The node that experiences congestion can explicitly send a s/l to the sr source or destn. In choke pkt method separate pkt is used for this purpose; in the explicit signalling method, the s/l is included in the pkt that carry data. Eg: Frame Relay Congestion Control.

- Backward Signaling: A bit can be set in a pkt moving in the direction opposite to the congestion. This bit can warn the source that there is congestion & that it needs to slow down to avoid the discarding of pkts.

- Forward Signaling: A bit can be set in a pkt moving in the direction of the congestion. This bit can warn the destination that there is congestion.

QoS - Quality of Services:

QoS is an internetworking issue that a flow seeks to attain. There are 4 types of characteristics are attributed to flow: 1-Reliability 2. Delay 3. Jitter 4. Bandwidth

1. Reliability: Lack of reliability means losing a pkt or ack which causes retransmn. Eg: E-mail, File transfer etc have high reliability. But telephony or audio conferencing have less reliability.

2. Delay: ie; source to destination delay. Telephony, & audio, video conferencing need minimum delay, while in file transfer or email is less important.

3. Jitter: is the variation in delay for pkts belonging to the same flow.

For eg: 4 pkts depart at times 0, 1, 2, 3 & arrive at 20, 21, 22, 23 all have the same delay, 20 units of time. On the other hand, if the above 4 pkts arrive at 21, 23, 21 & 28, they will have diff. delays: 21, 22, 19 & 24.

High jitter means the diff. b/w delays is large; low jitter means the ~~diff~~ variation is small.

4. Bandwidth: Diff. appl^{n}s need diff. bandwidths. In video conferencing we need to send millions of bits per second to refresh a color screen while the total no. of bits in an e-mail may not reach even a million.

Techniques to Improve QoS:

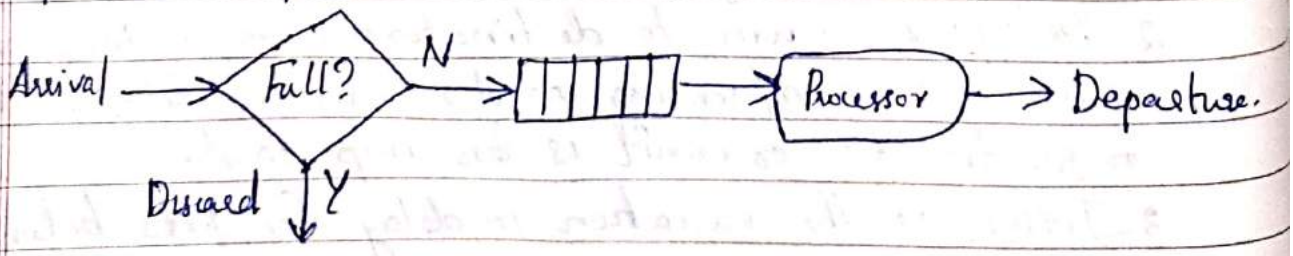
1. Scheduling 2. Traffic shaping 3. Admission Control 4. Resource reservation.

Scheduling:

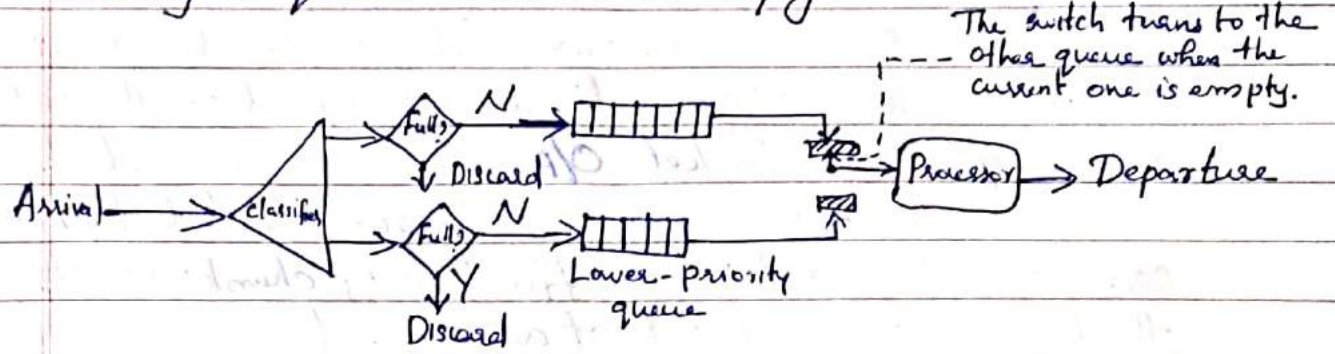
Packets from diff. flows arrive at a switch or router for processing. A good scheduling technique treats the diff. flows in a fair & appropriate manner.

Diff. scheduling techniques are
- FIFO queuing
- priority queuing
- weighted fair queuing

FIFO Queuing: packets wait in a buffer (queue) until the node is ready to process them. If the avg arrival rate is higher than the avg processing rate, the queue will fill up and new pkts will be discarded.

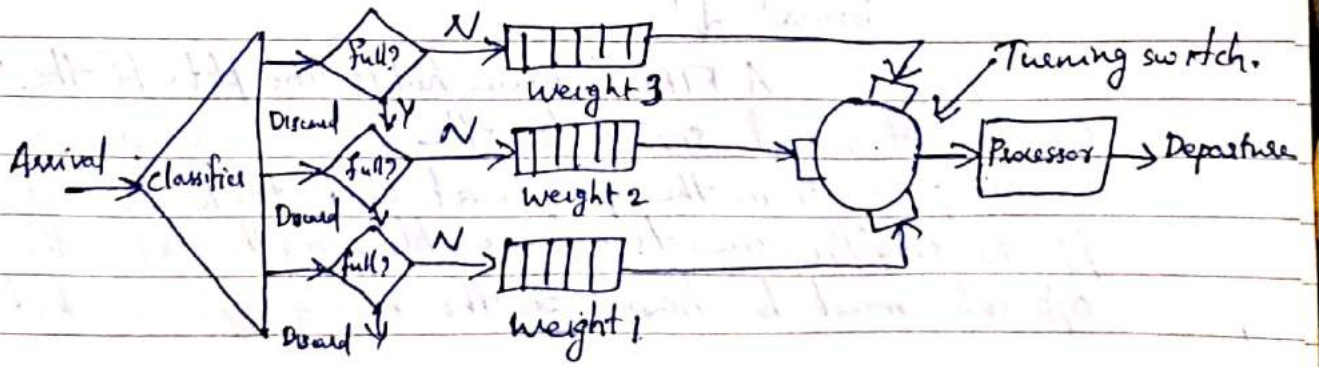


Priority Queuing: Pkts are first assigned to a priority class. Each priority class has its own queue. The pkts in the highest-priority queue are processed first. Pkts in the lowest priority queue are processed last. The s/m doesn't stop serving a queue until it is empty.



A priority queue can provide better QoS than the FIFO queue b/c higher priority traffic, such as multimedia, can reach the dest^n with less delay. If there is a continuous flow in a high-priority queue, the pkts in the lower-priority queues will never have a chance to be processed. This is a condition called starvation.

Weighted Fair Queuing: Pkts are still assigned to diff. classes and admitted to deff. queues. The queues are weighted based on the priority of the queues. Higher priority means a higher weight. The ~~pro~~ s/m processes pkts in each queue based on the corres. wt. for eg: If the weights are 3, 2, 1, 3 pkts are processed from the first queue, 2 from second queue & one from the 3rd queue. If the s/m doesn't impose priority on classes, all weights can be equal.



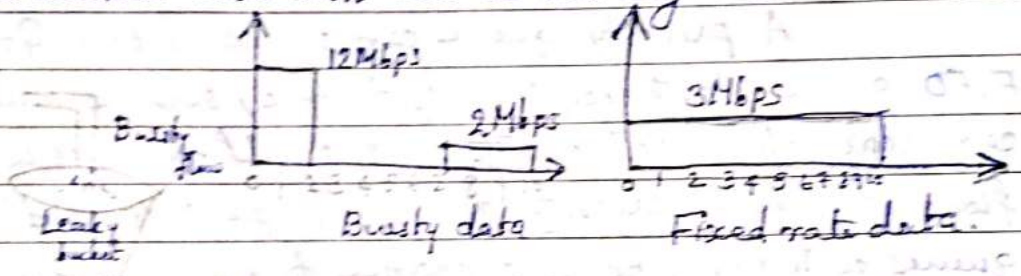
Traffic Shaping:

→ mechanism to ctrl the amnt and the rate of the traffic sent to the nw. Two techniques are used: Leaky bucket and token bucket.

Leaky Bucket:

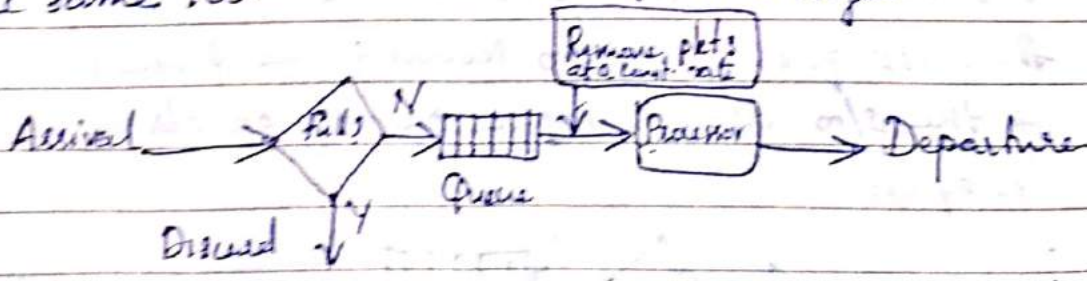
Bucket with small hole - water leaks at constant rate. Leakage rate doesn't depend on the rate at which i/p to the bucket. O/p rate remains constant.

In networking, a technique called leaky bucket can smooth out bursty traffic. Bursty chunks are stored in the bucket and sent out at an avg rate.



The host sends a burst of data at a rate of 12Mbps for 2s, for a total of 24 Mbits of data. The host is silent for 5s and sends data at a rate of 2 Mbps for 3s for a total of 6 Mbits of data. The leaky bucket smooths the traffic by sending out data at a rate of 3 Mbps during the same 10s.

Leaky bucket algo



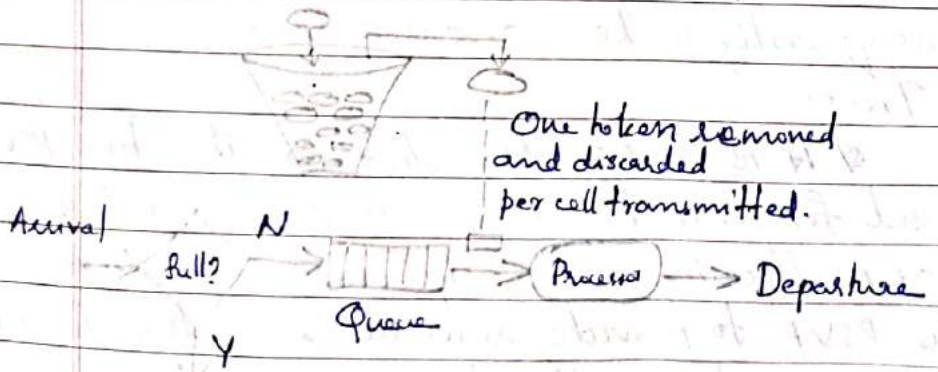
A FIFO Queue holds the pkts. If the traffic consists of fixed-size pkts; the process removes a fixed no. of pkts from the queue at each tick of the clock. If the traffic consists of variable-length pkts, the fixed o/p rate must be based on the no. of bytes or bits.

1. Initialize a counter to n at the tick of the clock.
2. If n is greater than the size of the pkt, send the pkt & decrement the counter by the pkt size. Repeat this step until n is smaller than the pkt size.
3. Reset the counter & go to step 1.

Token Bucket:

In Leaky bucket Algm, if the host has bursty data, the leaky bucket allows only an avg rate. The time when the host was idle is not taken into account.

The token bucket algm allows idle hosts to accumulate credit for the future in the form of tokens. For each tick of the clock, the s/m sends n tokens to the bucket. The s/m removes one token for every cell of data sent. For eg:, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens. Now the host can consume all these tokens in one tick with 10,000 cells, or the host takes 1000 ticks with 10 cells per tick. The token bucket can easily be implemented with a counter. The token is initialised 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.



The two techniques can be combined to credit an idle host and at the same time regulate the traffic.

~~Resource Reservation:~~

Resource Reservation:

A flow of data needs resources such as a buffer, bandwidth, CPU time, and so on. The QoS is improved if these resources are reserved.

Admission Control:

- mechanism used by a router, or a switch to accept or reject a flow based on predefined parameters called flow specifications. Before a router accepts a flow for processing, it checks the flow specific^{n}s to see if its capacity & previous commitments to other flows can handle the new flow.

⟹ Models for QoS:

- Integrated Services
- Differentiated Services.

Integrated Services:

- Sometimes called IntServ, is a flow-based QoS model, which means that a user needs to create a flow, a kind of virtual ckt, from the source to the dest^{n} & inform all routers of the resource rqmt.

Resource Reservation Protocol:

It is a signalling protocol to help IP create a flow and consequently make a resource reservation.

Multicast Trees:

It is a signalling s/m for multicasting. RSVP can be also used for unicasting b/c unicasting is just a special case of multicasting with only one member in each group. Enable RSVP to provide resource reservations for all kinds of traffic including multimedia.

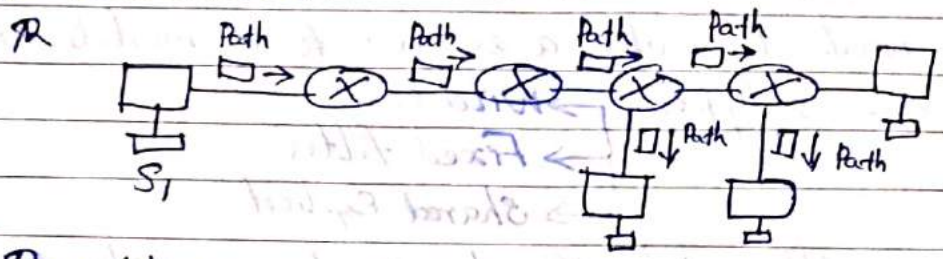
Receiver-Based Reservation:

Receivers make reservation.

RSVP messages: several type of msgs
- Path & Resv.

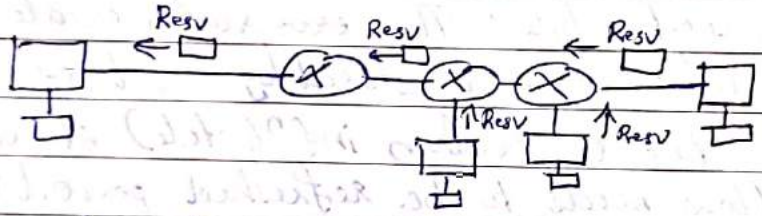
Path Messages:

The path is needed for reservation. The recievers do not know the path traveled by pkts before the reservation is made. To solve the pblm RSVP uses path msgs. A path msg travels from the sender & reaches all recieners in the multicast path. On the way, a Path msg stores the necessary info for the recieners.



Resv Messages:

After a reciever a Path msg, it sends a Resv msg. The Resv msg travels toward the sender & makes a resource reservation on the routers that support RSVP. If a router doesn't support RSVP on the path, it routes the pkt based on the best-effort delivery methods.

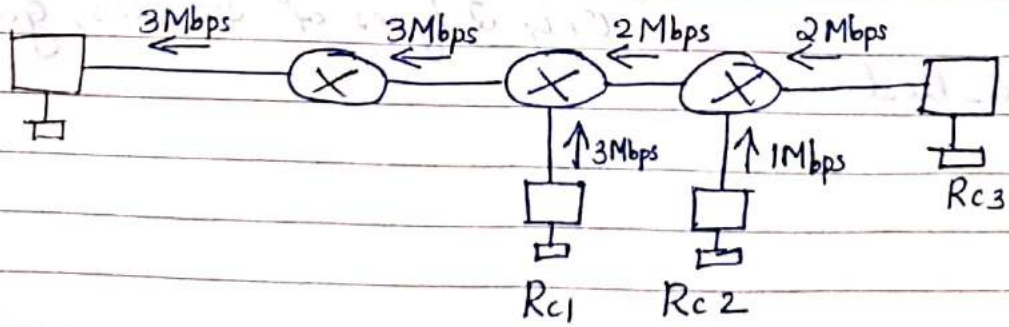


Integrated Services: Differentiated Services:

→ class based QoS model designed for IP.

Reservation Merging:

- the resources are not reserved for each reciever in a flow; the reservation is merged.



Rc3 requests a 2 Mbps bandwidth while Rc2 rqsts a 1 Mbps bandwidth. Router R3, which needs to make a bandwidth reservation, merges the two rqsts. The reserv'n made for 2 Mbps, the larger of the 2, b/c a 2 Mbps i/p reservation can handle both rqsts.

Reservation Styles:

When there is more than one flow, the router needs to make a reserv'n to accomodate all of the

There are 3 types:
- Wild card
- Fixed filter
- Shared Explicit

Wild Card Filter Style: Router creates a single reservation for all senders. The reservation is based on the largest request.

Fixed Filter Style: Router creates distinct reservation for each flow. This means that if there are n flows n diff. reservations are made.

Shared Explicit Style: The ~~router~~ router creates a single reservation which can be shared by a set of flows.

Soft State: The reservation inf'n (state) stored in every node for a flow needs to be refreshed periodically. This is referred to as a soft state.

Problems with Integrated Services:

→ Scalability - Each router keep inf'n for each flow. As internet is growing every day, this is a pblm

→ Service type Limitation.

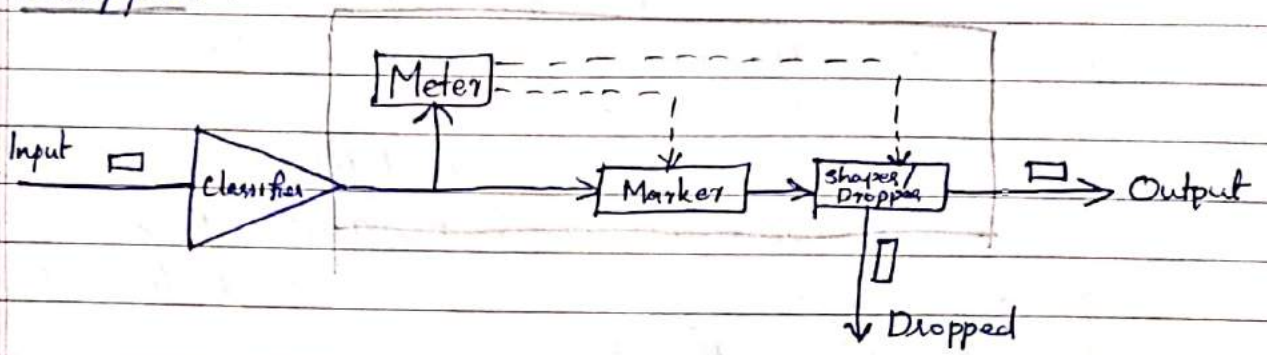
- Only 2 types of services, guaranteed ctrl_load.

Differentiated Services: (DS)

introduced by IETF (Internet Engg. Task Force)

Traffic Conditioner (Assured Forwarding)

→ such To implement these services, DS node uses traffic conditioners such as meters, markers, shapers & droppers.



Meters: The meter checks to see if the incoming flow matches the negotiated traffic profile. The meter sends this result to other components.

Marker: A marker can remark a pkt that is using best effort delivery (DSCP-000000) or down-mark a pkt based on info received from the meter. Down marking occurs if the flow doesn't match the profile. A marker doesn't upmark a pkt.

Shaper: A shaper uses the info received from the meter to reshape the traffic if it is not compliant with the negotiated profile.

Dropper: A dropper, which works as shaper with no buffer, discards pkts if the flow severely violates the negotiated.

23/12/16

Network Layer in the Internet

IPv4, IP Addressing – Classless & Classful Addressing, Subnetting

IPv4 Addresses:

is a 32 bit address that uniquely & universally defines conn^n of a device (for eg: a comp. or a router) to the Internet.

Two devices on the Internet can never have the same address at the same time. If a device operating at the n/w layer has m conn^n's to the Internet, it needs to have m addresses.

Address Space: is the total no. of addresses used by the protocol. If a protocol uses N bits to define an address, the adds. space is 2^N b/c each bit can have 2 diff. values (0 or 1) & N bits can have 2^N values.

IPv4 uses 32 bit addresses, ie; the address space is 2^{32} or 4,294,967,296. If there were no restrictions more than 4 billion devices could be connected to the Internet.

Notations

Two types of notations: → Binary notation
→ dotted decimal notation.

Binary Notation:

IPv4 address is displayed as 32 bits. Each octet is referred to as a byte.

Eg: 01110101 10010101 00011101 00000010

Dotted-Decimal Notation:

Eg: 117.149.29.2

B/c each byte (octet) is 8 bits, each no. in dotted decimal notation is a value ranging from 0–255.

10000000 00001011 00000011 00011111

128 . 11 . 3 . 31

Dotted decimal notation & binary notation for an IPv4 addres.

Example.

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

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Ans: Replace each group of 8 bits with its equivalent decimal no. & add dots for separation.

a. 129.11.11.239 b) 193.131.27.255.

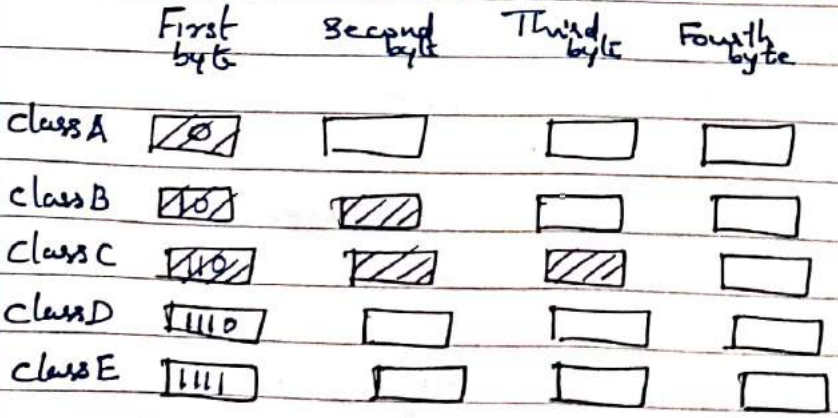
2. Change the follo. IPv4 addresses from dotted-decimal notation to binary equivalent

a. 111. 56 . 45. 78 b) 221. 34. 7 . 82

Classful Addressing:

IPv4 addressing used concept of classes. This architecture is called classful addressing.

The address space is devided into five classes: A, B, C, D, E. If the address is given in binary notation, the first few bits defines class of address. If the address is given in decimal-dotted notation, the first byte defines the class.



Binary Notation:

Example

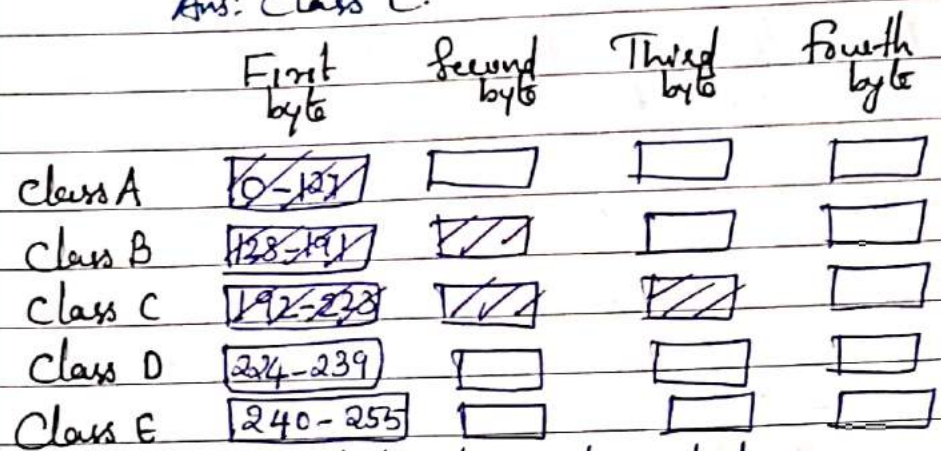
1. Find the class of each address

a. 00000001 00001011 00001011 11101111

Ans: class A

b. 11000001 10000011 00011011 11111111

Ans: Class C.



Dotted-decimal notation.

c. 14.23.120.8

Ans: Class A

d. 252.5.15.111

Ans: class E.

Classes and Blocks:

Each class is devided into a fixed no. of blks with each blk having a fixed size.

Class	No. of blks	Blk size	Application.
A	128	16,777,216	Unicast
B	16384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Multicast.

Class A - large Org^n's. Large no. of hosts or routers attached

Class B-addresses – midsize Org^n with 100's of 1000 of attached hosts.

Class C – small Org^n with a small no. of attached hosts.

Drawback:

A blk in class A is too large for any org^n. ie; most of the addresses in class A were wasted and were not used. A block in class B is also very large. A blk in class C is too small for many org^{n}s. Class D addresses were designed for multicasting. Class E addresses were ~~wasted~~ reserved for future use.

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

Netid & Hostid:

An IP address in class A, B, or C is divided into netid & hostid. These parts are of varying lengths depending on the class of the address.

In class A N.H.H.H (2^{24} for Host)
B N.N.H.H (2^{16} for host)
C N.N.N.H (2^8 for host)

Mask

Although the length of the netid & hostid (in bits) is predetermined in classfull addressing, we can also use a mask. It is a 32 bit number made of contiguous 1s followed by contiguous 0s.

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

The mask can help us to find the netid & host id. For eg: the mask for a class A address has 8 1s which means first 8 bits of any address in class A define the netid; next 24 bits define the hostid. The CIDR column in the table shows the mask in the form /n where n can be 8, 16, 24 in classful addressing.

This notation is also called slash notation or Classless Interdomain Routing (CIDR).

Subnetting:

If an organization was a large blk in class A or B, it could devide the addresses into several contiguous groups & assign each group to smaller n/ws called subnets. Subnetting increases the no. of 1s in the mask.

Supernetting:

— Midsize blocks. The size of a class C blk with a max. no. of 256 addresses didn't satisfy the needs of most org^ns. Midsize org^n needed more addresses. One solution was supernetting. In supernetting an org^n can combine several class C blks to create larger range of addresses. i.e; several n/ws can be combined to create supernetwork or supernet.

Classless Addressing

To give more org^ns access to the Internet classless addressing was designed & implemented. There are no classes, but the addresses are still granted in blks.

Address Blocks:

In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a blk of addresses. The size of blk (no. of addresses) varies based on the nature & size of the entity. For eg: A household may be given only 2 addresses. A large org^n may be given 1000s of addresses.

To simplify the handling of addresses, the Internet authorities impose 3 restrictions on classless address blks:

1. The addresses in a blk must be contiguous, one after another.
2. The no. of addresses in a blk must be a power of 2.
3. The first address must be evenly divisible by no. of addresses.

Example: A blk of 16 addresses granted to a small org^n.

a. Decimal

Block	
First →	205.16.37.32
	205.16.37.33
	⋮
Last →	205.16.37.47

b) Binary

Block			
11001101	00010000	00100101	00100000
11001101	00010000	00100101	00100001
⋮			
11001101	00010000	00100101	00101111

→ satisfies 3 restrictions.

Mask

Mask is a 32 bit no in which the n leftmost bits are 1s & the 32−n right most bits are 0s. In classless addressing the mask for a block can take any value from 0-32.

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

The address & the /n defines the whole blk (the first address & the no. of addresses).

The first address in the blk can be found by setting 32−n right most bits in the binary notation of address to 0s.

Example:

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

Ans: Binary: 11001101 00010000 00100101 00100111. If we set 32-28 rightmost bits to 0, we get 11001101 00010000 00100101 00100000 or 205.16.37.32.

Last Address: The last address in the block can be found by setting the 32-n right most bits in the binary notation of the address to 1s.

Example:

Find the last address for the block 205.16.37.39/28.

Ans: Binary: 11001101 00010000 00100101 00100111.

32-28 rightmost bits to 1 → 11001101 00010000 00100101 00101111 or

→ 205.16.37.47.

Number of Addresses: is the difference b/w the last addr & first address. It can easily be found using the formula 2^{32-n}.

Example

Find the no. of addresses in the above eg:

Ans: n = 28

no. of addresses = $2^{32-28} = 2^4 = 16$

Another way to find first, last, no. of Addresses.

Example: mask: /28 can be represented as 11111111 11111111 11111111 11110000 (28 1s & 4 0s). Find a) First Address b) The last address c) no. of Addresses.

a) First Address ⇒ Given address AND Mask.

Given Address: 11001101 00010000 00100101 00100111

Mask: 11111111 11111111 11111111 11110000

First Address: 11001101 00010000 00100101 00100000

b) Last Address ⇒ Given Address OR (Mask)'

Given Address: 11001101 00010000 00100101 00100111

(Mask)': 00000000 00000000 00000000 00001111

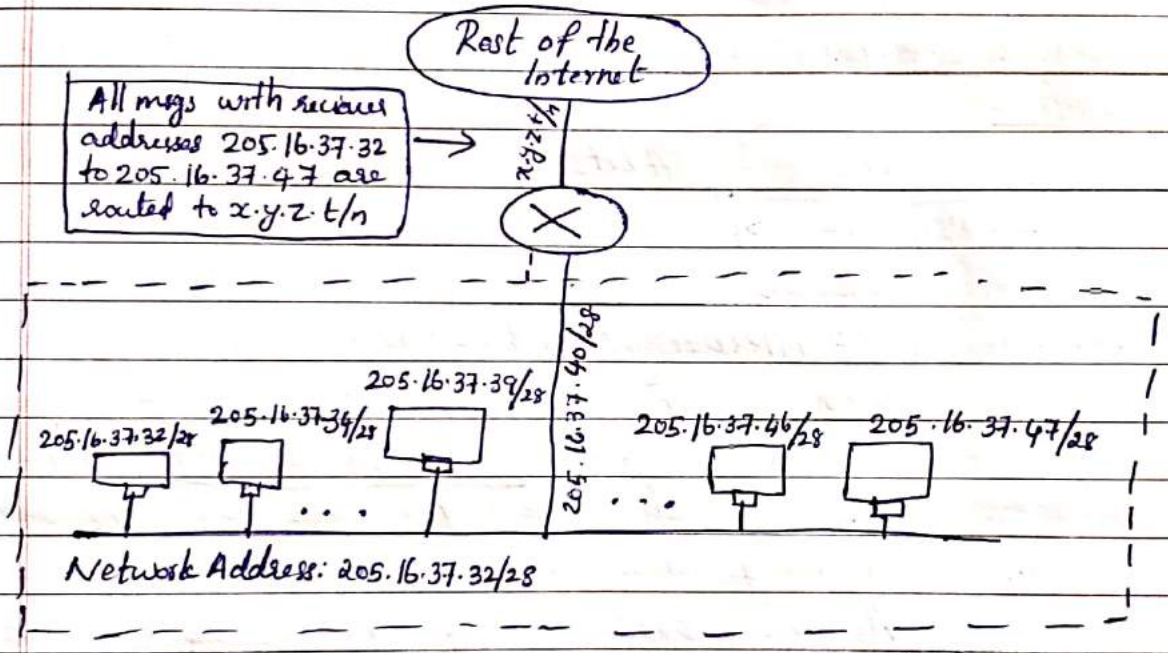
Last Address: 11001101 00010000 00100101 00101111

c) No. of Addresses = (Mask)' → Decimal + 1

Mask Complement: 00000000 00000000 00000000 00001111
No. of Addresses = 15+1 = 16

Network Address

When an orgn is given a blk of addresses, the orgn is free to allocate the devices that need to be connected to the Internet. The first address is called the n/w address & is used by the routers to direct msg sent to the orgn from outside.



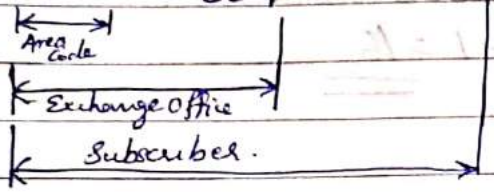
The Orgn n/w is connected to the Internet via router. The router has 2 addresses. One belongs to the granted blk & the other belongs to the n/w that is at the other side of the router. The second address is x.y.z.t/~~32~~ 28. All msgs destined for addresses in the orgn blk (205.16.37.32 to 205.16.37.47) are sent directly or indirectly to x.y.z.t/n.

The first address in a blk is normally not assigned to any device; it is used as the n/w address that represents the orgn to the rest of the world.

Hierarchy:

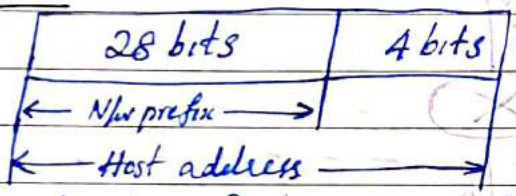
IP addresses have levels of hierarchy. Eg: Telephone n/w in America has 3 levels of Hierarchy.

Eg: 408 - 864 - 8902



Two level Hierarchy: No Subnetting:

The n leftmost bits of the address x.y.z.t/n define the n/w; The 32 − n right most bits define the particular host to the n/w. The part of the address that defines the n/w is called prefix; the part that defines the host is called the suffix.



Three levels of Hierarchy: Subnetting:

An org^n that is granted a large blk of addresses may want to create clusters of n/ws (called subnets) & divide the addresses b/w the diff. subnets. Externally the org^n as one entity; internally there are several subnets.

All msgs are sent to the router address that connects the org^n to the rest of the Internet; the router routes the msg to the appropriate subnets. The org^n has its own mask; each subnet has its own.

Eg: An org^n is given the blk 17.12.14.0/26 which contains 64 addresses. The org^n has to devide the addresses into 3 subblocks of 32, 16 & 16 addresses.

1. Suppose the mask for the 1st subnet is n_1, then 2^{32-n_1} must be 32 which means $n_1 = 27$

i.e; no. of addresses $= 2^{32-n_1} = 32$

$\therefore n_1 = 27$

2. Suppose the mask for the 2nd subnet is n_2

$$2^{32-n_2} = 16$$

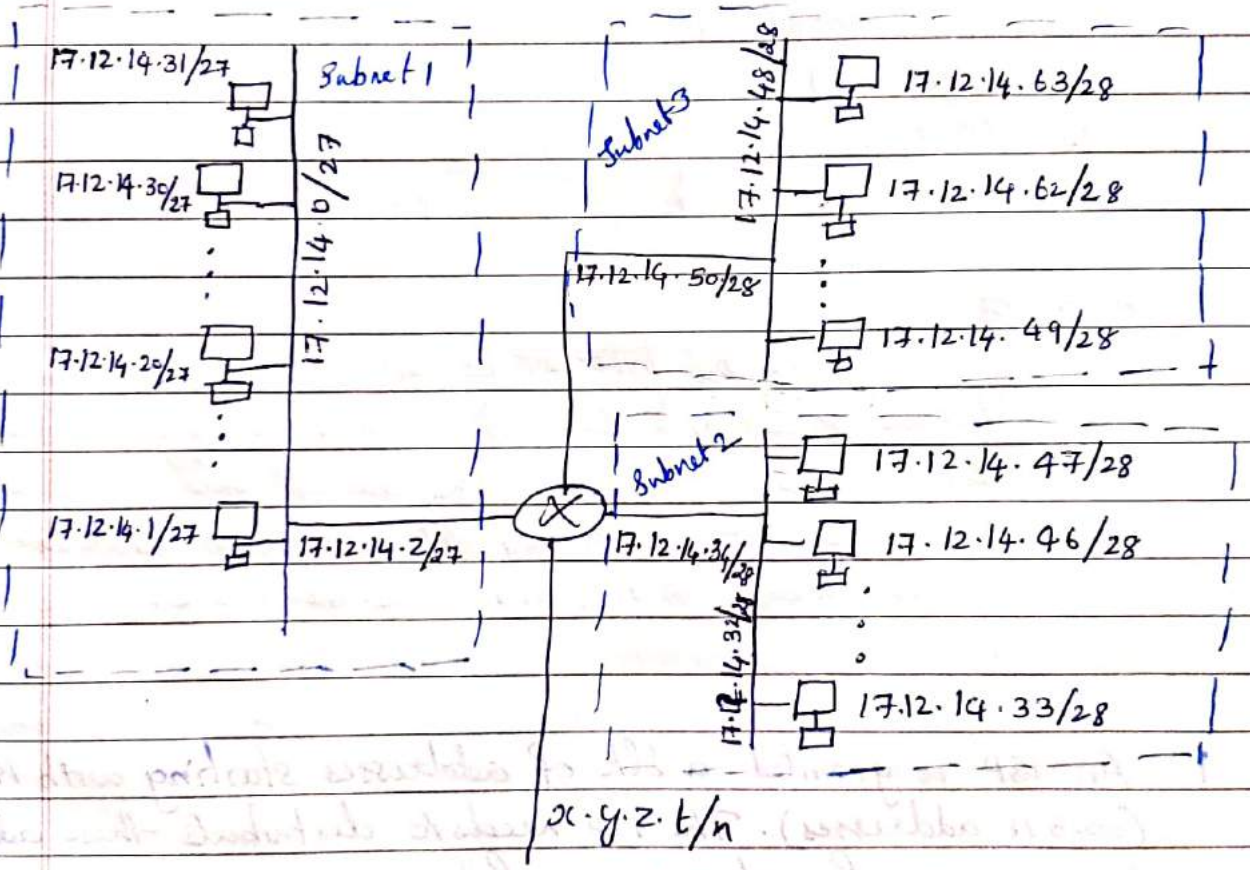
$$\therefore n_2 = 28$$

3. The mask for 3rd subnet is n_3

$$2^{32-n_3} = 16$$

$$\therefore n_3 = 28$$

Organization mask: 26.



a. In subnet1, the address 17.12.14.29/27 can give us the subnet address if we use the mask: /27.

Host: 00010001 00001100 00001110 00011101

Mask: /27;

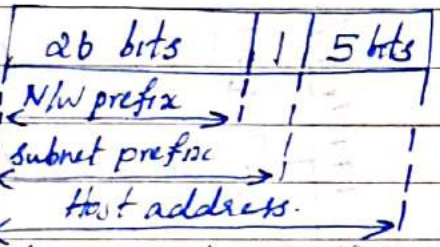
32 − 27 = 5 bits → zero.

Subnet: 00010001 00001100 00001110 00000000 → 17.12.14.0

b) In subnet2, the address 17.12.14.45/28; mask /28

Host: 00010000 00001100 00001110 00101101
Mask: /28 32-28 = 4 bits → 0
Subnet: 00010000 00001100 00001110 00100000 → 17.12.14.32.
c) In ~~sub nt~~ subnet 3, address 17.12.14.50/28
Host: 00010000 00001100 00001110 00110010
Mask: /28 32-28 = 4 bits
Subnet: 00010000 00001100 00001110 00110000 → 17.12.14.48

Subnet 1

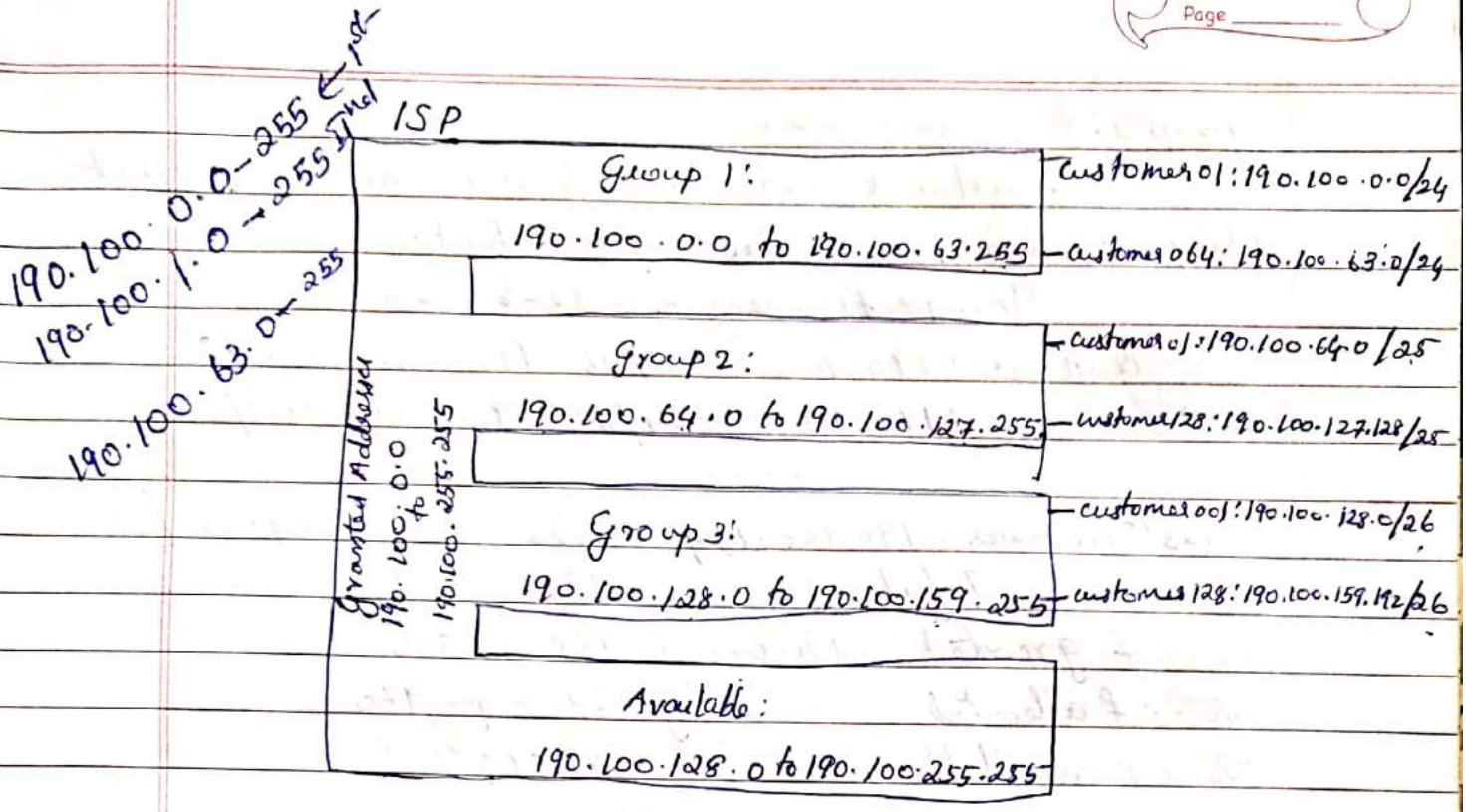


Address Allocation:

is done by Internet Corporation for Assigned Names and Addresses (ICANN) doesn't normally allocate addresses to individual org's. It assigns large blk of addresses to an ISP. Each ISP, divides its assigned blk into smaller subblocks & grants the subblks to its customers. This is called address aggregation.

1. An ISP is granted a blk of addresses starting with 190.100.0.0 (65,536 addresses). The ISP needs to distribute these addresses to 3 groups of customers as follows:
   a) 1st group – 64 customers; each needs 256 addresses.
   b) IInd group – 128 customers; " 128 addresses
   c) IIIrd " – 128 " " 64 addresses.

Design the subblks & find out how many addresses are still available after these allocns.



a. Group 1

- Each customer needs 256 addresses.
  i.e; 8 bits ($\log_2 256$) to define each host.
  prefix length/network address length = 32 − 8 = 24

The addresses are

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

Total = 64 × 256 = 16,384.

Group 2.

- Each customer needs 128 addresses.
  i.e; 7 bits; prefix length = 32 − 7 = 25 bits

1st customer : 190.100.64.0/25 190.100.64.127/25
and 190.100.64.128/25 190.100.64.255/25
. . .
128th customer 190.100.127.128/25 190.100.127.255/25

Total = 128 × 128 = 16,384

Group 3:

Each customer needs 64 addresses. This means that 6 ($\log_2 64$) bits are needed to each host.

The prefix length = 32 − 6 = 26

1st Customer : 190.100.128.0/26 190.100.128.63/26

2nd " : 190.100.128.64/26 190.100.128.127/26.

....

128th customer : 190.100.159.192/26 190.100.159.255/26

Total = 128 × 64 = 8192

No. of granted addresses to ISP: 65536

No. of allocated " by ISP : 40,960

No. of available " = 24,576

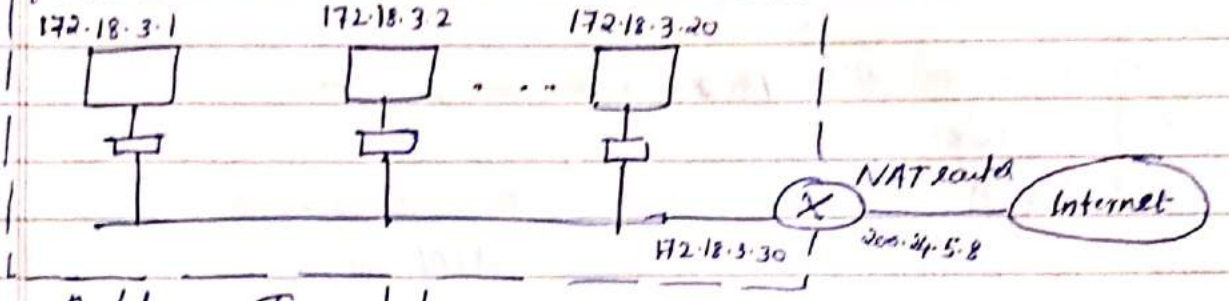
Network Address Translation

Today, Home users & small businesses can be connected by an ~~ISP~~ cable modem. Many have created small nlws with several hosts & need an IP address for each host. With the shortage of addresses, this is a serious pblm. Sol^n to this pblm is called network address translation (NAT) - NAT enables a user to have a large set of addresses internally & one address or a small set of addresses externally.

To separate the addresses used inside the home or business and the ones used for the Internet, the Internet authorities have reserved 3 sets of addresses as private addresses.

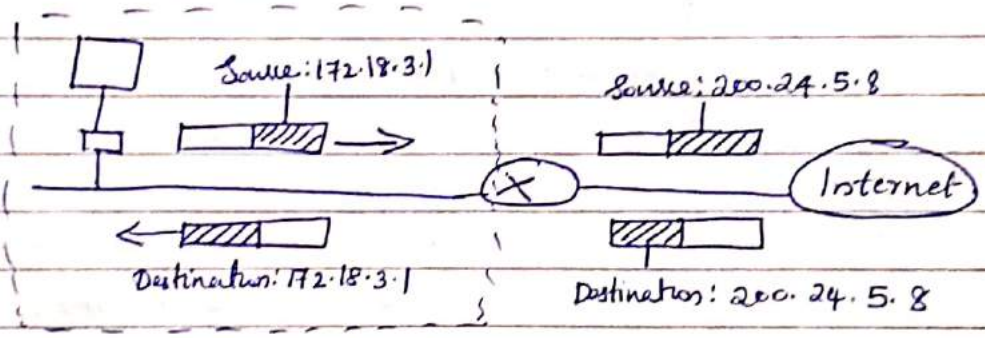
Range			Total
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.16.0.0	to	192.168.255.255	2^{16}

Any Org^n can use an address out of this set without permission from the internet authorities.



Address Translation:

All the outgoing pkts go through the NAT router, which replaces the source address in the pkt with the global NAT address. All incoming pkts also pass through the NAT router, which replaces the dest^n address in the pkt with the appropriate private address.



Translation Table:

Translation table has only 2 columns: the private address & the external address. When the router translates the source address of outgoing pkt, it also makes a note of the destination address where the pkt going. When the response comes back from the destination the router uses the source address of the pkt to find the private address of the pkt.

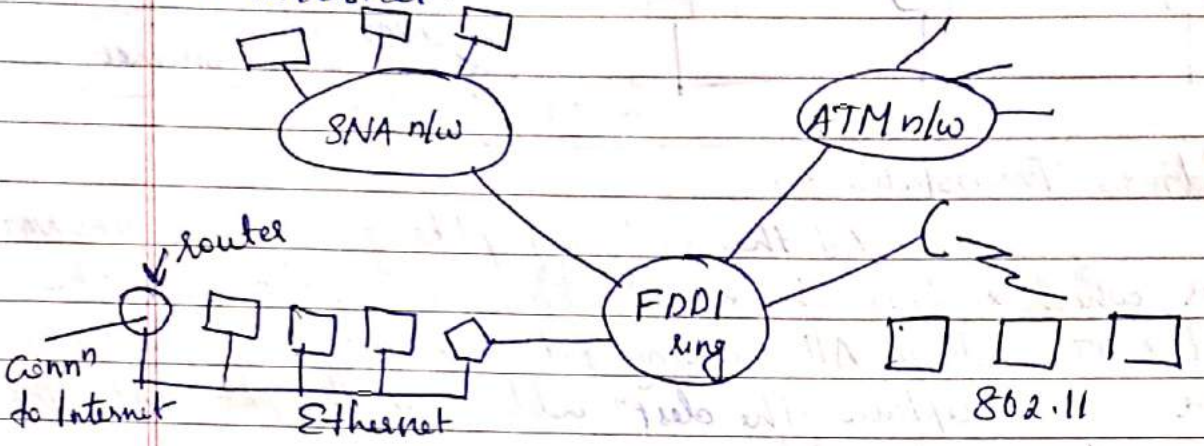
Pool of IP Addresses.

Instead of using only one global address the NAT router can use 4 addresses. In this case 4 private n/w hosts can communicate with same external host

at the same time.

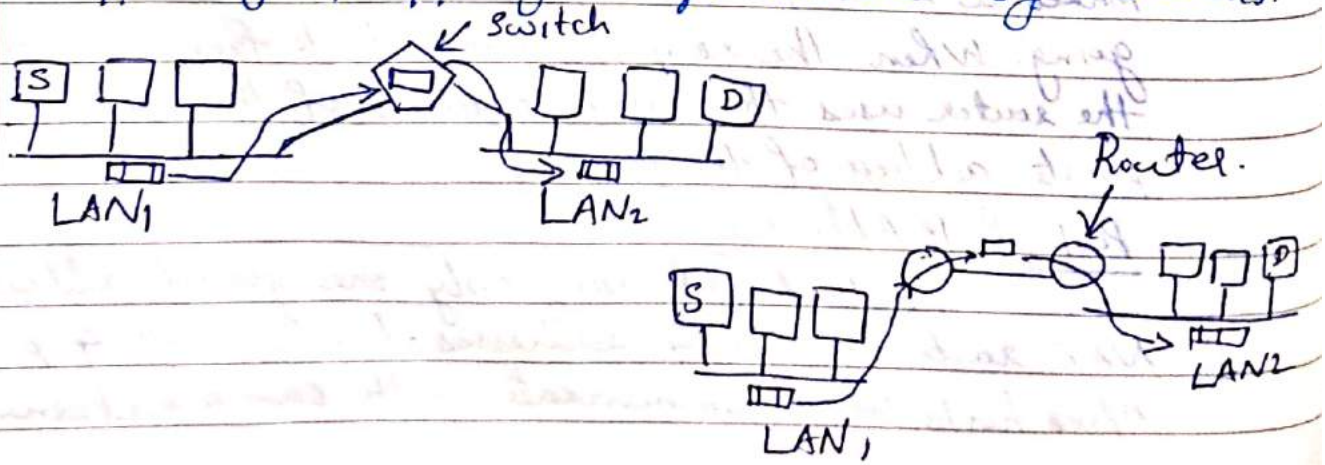
Internetworking

Two or more n/ws are connected to form an internet.



Networks can differ in many ways: such as diff. modulation techniques or frame formats.

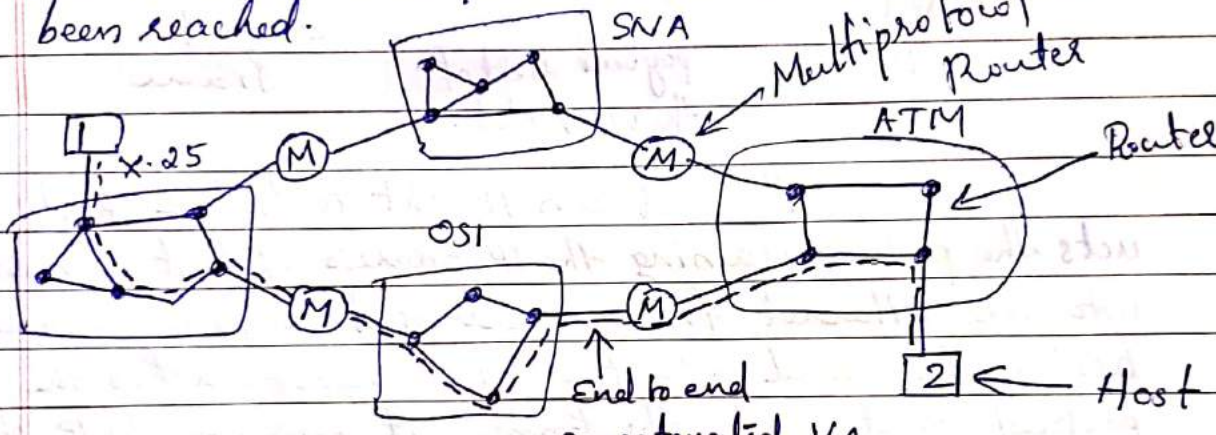
Networks can be interconnected by diff. devices. In phy layer, n/w can be connected by repeaters or hubs, which just move the bits from one n/w to an identical n/w. In d' DLL, bridges & switches are used. They can accept frames, MAC addresses & forward. In n/w layer, Routers are used. Routers may be able to translate b/w the pkt formats. A router can handle multiprotocols is called a multiprotocol router. In transport layer, Gateways are used, which can interface b/w 2 transport connⁿs. In applⁿ layer, applⁿ gateways translate msg semantics.



Internetworking using concatenated virtual circuits:

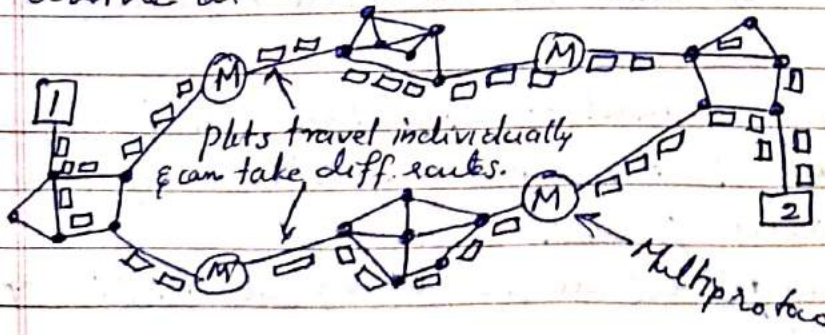
Two styles: a conn^n oriented concatenation of VC subnets
↳ Datagram style.

In VC model, conn^n to a host in a distant n/w is set up in a way similar to the way conn^n's are established. The subnet sees that the dest^n is remote & builds a VC to the router to an external gateway (multiprotocol router). This gateway records the existence of the VC in its tables & proceeds to build another VC to a router in the next subnet. This process continues until dest^n host has been reached.



Connectionless Internetworking

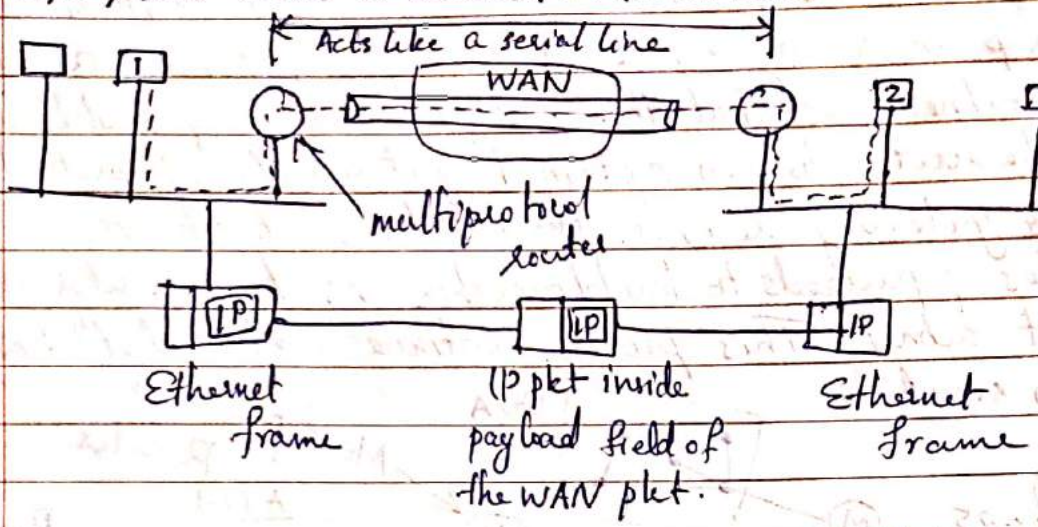
Datagrams from host 1 to host 2 are taking diff. routes through the internetwork. A routing decision is made separately for each packet, possibly depending on the traffic at the moment the pkt is sent. This strategy can use multiple routes & thus achieve higher bandwidth than the VC. model. There is no guarantee that pkts arrive at the dest^n in order.



classmate
Date
Page

Tunnelling

→ Source & dest^n hosts are on the same type of n/w, but there is a diff. n/w in blw.



To send an IP pkt to host 2, host 1 constructs the pkt containing the IP address of host 2, inserts it into an Ethernet frame addressed to Paris (eg) multiprotocol router, and puts it on the Ethernet. When the multiprotocol router gets the frame, it removes the IP pkt, inserts in the payload field of the WAN n/w layer pkt & addresses to the WAN address of London multiprotocol router. When it gets there, the London router removes the IP pkt & sends it to host 2 inside the an Ethernet frame.

Internetwork Routing

→ 2 level routing Algm: within each n/w an interior Gateway protocol is used.
: b/w the n/ws: an exterior gateway protocol

April 2018

1. List & explain any 3 closed loop congestion ctrl techniques.
2. Describe the format of IPv4 datagram with the help of diagram, highlight significant field of each.
3. Define Subnetting? What are the adv. of subnetting? Explain with an eg

Name	Jeffi
Reg. No.	7 c E 1 5 c s 2 0 5

NEHRU COLLEGE OF ENGINEERING & RESEARCH CENTRE

PAMPADY, THIRUVILWAMALA, THRISSUR, KERALA – 680 588

SERIES TEST – II

CS306: Computer Networks

emester & Branch: VI/ S6 B. Tech. **Computer Science and Engineering**

y Name: Arun . K **Exam Date:7/3/2018**

60 Min **Max. Marks: 20**

Answer All Questions (2 Marks ×3 = 6 Marks)

Define routing algorithm and its types?
What is flooding in networks?
What is the use of RSVP protocol?

PART –B

Answer All Questions (2×7 Marks = 14 Marks)

. Explain about the Shortest path algorithm in detail (3)
i. Briefly explain about Routing in mobile hosts. (4)

(OR)

Write a short note on OSPF protocol. (4)
. Explain about Link state routing protocol (3)

xplain about Congestion control protocols in detail (7)

(OR)

Write a short note on Quality of Service. (4)
. Briefly describe Leaky Bucket Algorithm. (3)

4) Discuss the common techniques to improve QoS.

MODULE V

Internet Control Protocols

→ ICMP, ARP, RARP, BOOTP
→ Internet Multicasting
  * IGMP
  * Exterior Routing Protocols
  * BGP
  * IPv6 – Addressing Issues.
→ ICMPv6

Questions

1. Why is there a restriction on the generation of an ICMPv4 msg in response to a failed ICMPv4 error msg?
2. What is the purpose of including the IPv4 ~~pkt~~ header and the first 8 bytes of datagram data in the error reporting ICMPv4 msgs?
3. What is the min-size of an ARP pkt when the protocol is IPv4 and the h/w is Ethernet?
4. Give an eg: of a situation in which a host would never receive a redirection msg?

April 2018.

1. Write notes on the msgs & msg formats used in ICMP.
2. Describe BOOTP & DHCP
4. Explain how routing is done using BGP.
5. What is the use of ARP? Explain ARP op^n & pkt format.
6. Draw & explain the diagram format for IPv6.
7. List & explain the diff. types of error reporting msgs used by ICMP.

classmate
Date
Page

Internet Control Protocols:

— used for data transfer. & the protocols are
* ICMP * ARP * RARP * BOOTP

* Internet Control Message Protocol

The IP protocol lacks a mechanism for host & mgmt queries. A host needs to determine if a router or another host alive.

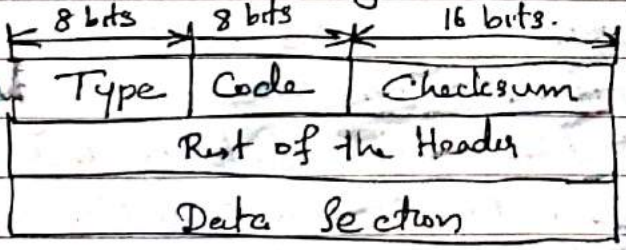
Types of Messages:

→ Two broad categories:
- → error reporting msgs
- → Query msgs.

Error-reporting msgs report pblms that a router or a host may encounter when it processes an IP pkt.
The Query msgs, which occur in pairs, help a host or n/w mngr get specific info from a router or another host.
For eg: nodes can discover their neighbors.

Message Format

→ 8 byte header & a variable size data section.



Code field the reason for particular msg type.

Error Reporting →
- Destination unreachable (Type 3)
- Source quench (Type 4).
- Time exceeded (Type 11)
- Parameter Problems (Type 12)
- Redirection (Type 5).

Destination Unreachable: When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded & the router or host sends a dest^n unreachable msg back to the source host that initiated the datagram.

Source Quench: (Choke packet)

—to add a kind of flow ctrl to the IP. ~~The source quench msg~~ When a router/host discards a datagram due to congestion, it sends source quench msg to the sender of the datagram. This msg has 2 purposes → It informs the source that the datagram has been discarded.
→ It warns the source that there is congestion somewhere in the path & that the source should slow down the sending process.

Time Exceeded:

Routers use routing tables to find the next hop(router) that must receive the pkt. If there are errors in one or more routing tables, a pkt can travel in a loop or a cycle going from one router to the next or visiting a series of routers endlessly.

Each datagram contains a field called time to live that ctrls this situation. When a datagram visits a router, the value of this field is decremented by 1. When the time to live value reaches 0, after decrementing, the router discards the datagram. When the datagram is discarded, a time-exceeded msg must be sent by the router to the original source.

A time exceeded msg is also generated when not all fragments that make up a msg arrive at the dest^n host within a certain time limit.

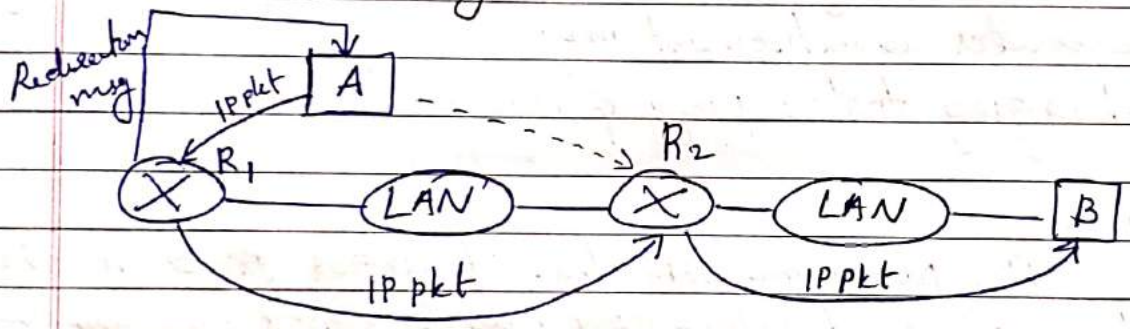
Parameter Problem:

Any ambiguity in the header part of a datagram

can create serious pblms as the datagram travels through the Internet. Then it discards the datagram & sends a parameter-pblm msg back to the source.

Redirection:

When a host comes up, its routing table has a limited no. of entries. It usually knows the IP address of only one router, the default router. For this reason, the host may send a datagram, which is destined for another n/w, to the wrong ~~number~~ router. ~~To update~~ The router that receives the datagram will forward the datagram to the correct router. To update the routing table of the host, it sends the redirection msg to the host.



→ Query Messages
- → Echo rqst & Reply
- → Timestamp rqst & Reply
- → Address mask rqst & Reply
- → Router solicitation & advertisement.

— Diagnose some n/w pblms.

Echo Request and Reply: The combination of echo-rqst and echo-reply msgs determines whether a s/ms can communicate with each other.

Timestamp Request & Reply: To determine the round-trip time needed for an IP datagram to travel b/w ~~them~~ a m/cs. It can also be used to synchronize the clks in a m/cs.

Address Mask Rqst and Reply: A host may know its IP address, but it may not know the corres. mask. To obtain its mask, a host sends an address-mask-rqst msg to a router on the LAN. The router receiving the address-mask request msg responds with an address-mask-reply msg, providing the necessary mask for the host.

Router Solicitation & Advertisement:

~~Router~~ used to know if the routers are alive & functioning. ~~The router~~ A host can broadcast a router-solicitation msg. The routers that receive the solicitation msg broadcast their routing info using the router advertisement msg.

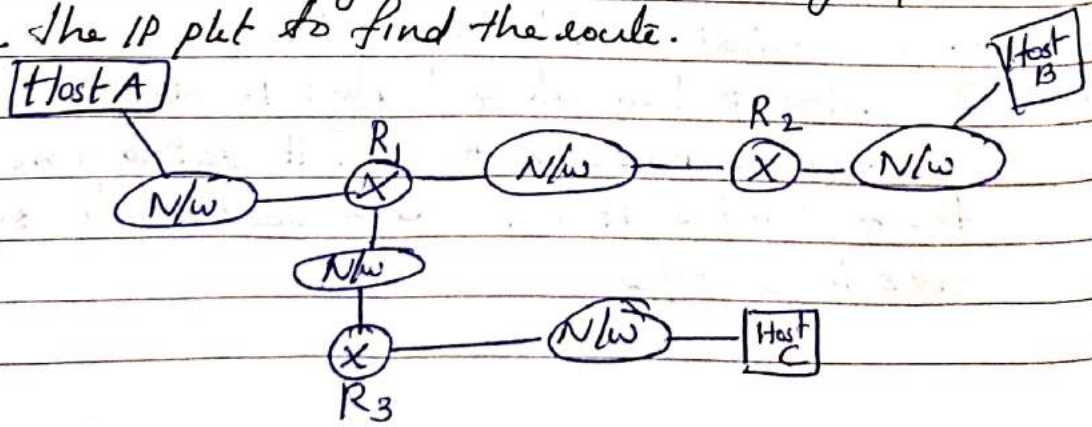
Debugging tools: ping & traceroute.

Ping:

The program sets the identifier field in the echo-rqst and echo-reply msg & starts the seq. no from 0; this no. is incremented by 1 each time a new msg is sent. Ping can calculate the round trip time. It inserts the sending time in the data section of the msg. When the pkt arrives, it subtracts the arrival time from the departure time to get the round trip time (RTT)

Traceroute:

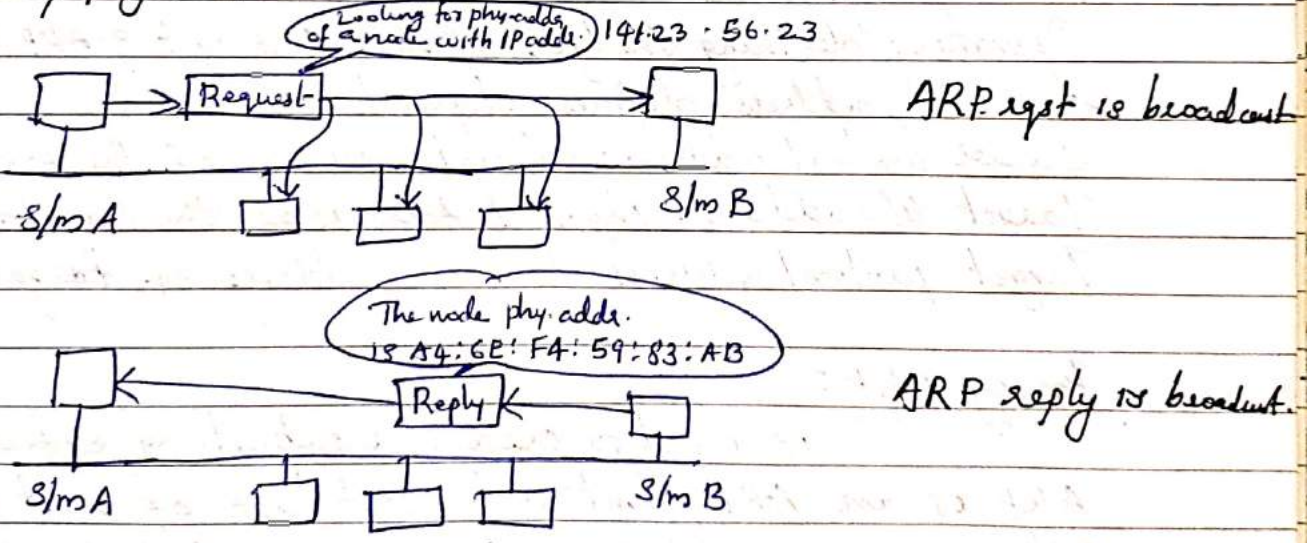
used to trace the route of a pkt from source to destn. Traceroute pgm uses the ICMP msgs & the TTL field in the IP pkt to find the route.



* Address Resolution Protocol

Mapping Logical to Physical Address (ARP)

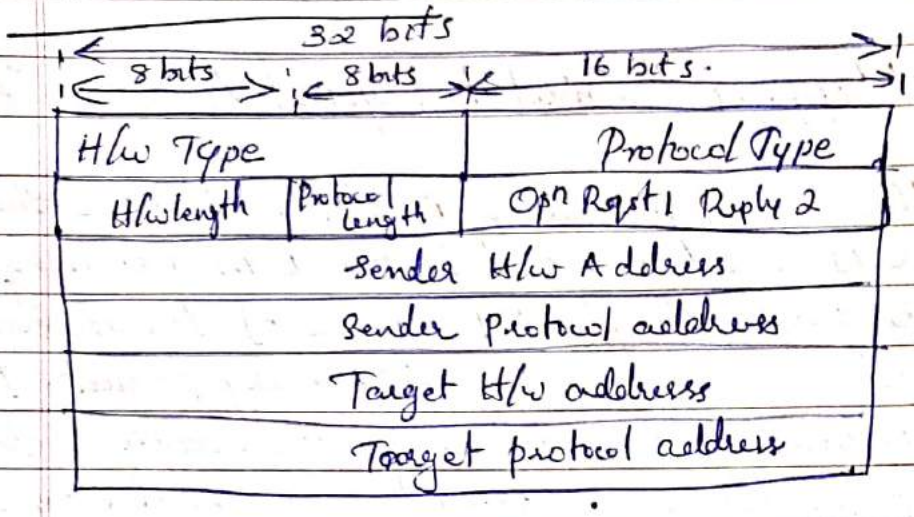
The logical IP address is obtained from the DNS if the sender is the host or it is found in a routing table. But the sender needs the physical address of the receiver. The host or the router sends an ARP query packet. The pkt includes the physical & IP addresses of the sender & the IP address of the receiver. Every host or router on the n/w receives & processes the ARP query pkt, but only the intended recipient recognizes its IP address & sends back an ARP response pkt. The response pkt contains the recipient's IP & physical addresses.



Cache Memory:

Using ARP is inefficient if S/m A needs to broadcast an ARP rqst for each IP. pkt it needs to send to s/m B. A s/m that receives an ARP reply stores the mapping in the cache memory & keeps it for 30 minutes unless the space in the cache is exhausted. Before sending an ARP rqst, the s/m first checks its cache to see if it can find the mapping.

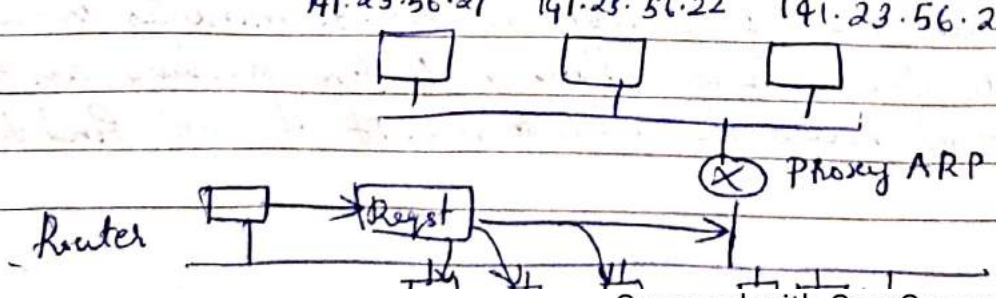
Packet Format:



H/w Type : defines type of n/w on which ARP is running.
Protocol Type: defines protocol - Eg : 0800 for IPv4.
H/w length: length of phy. address.
Protocol length: length of logical address.
Operation: defining the type of pkt: ARP rqst & ARP reply.
Sender h/w address: defines physical addr of the sender.
Sender protocol address: logical address of the sender
Target H/w address: physical Address of the target.
Target protocol address: logical address of target

Proxy ARP:

is used to create a subnetting effect. A proxy ARP is an ARP that acts on behalf of a set of hosts. Whenever a router running a proxy ARP receives an ARP rqst looking for the IP addr. of one of these hosts, the router sends an ARP reply announcing its own phy. addr. After the router receives the actual IP pkt, it sends the pkt to the appropriate host or router.



Four cases ARP can be used:
1. A host has a pkt to send to another host on the same n/w.
2. A host wants to send a pkt to another host on another n/w. It must first delivered to a router.
3. A router receives a pkt to be sent to a host on another n/w. It must first be delivered to the appropriate router.
4. A router receives a pkt to be sent to a host on the same n/w.

Mapping Physical to Logical Address:

* RARP: Reverse Address Resolution Protocol:

—finds the logical address for a m/c that knows only its physical address. Each host/router is assigned one or more logical addresses, which are unique & independent of the phy. address of the m/c. To create an IP datagram, a host or router needs to know its own IP address or addresses. The IP address of a m/c is usually read from its config. file stored on a disk file.

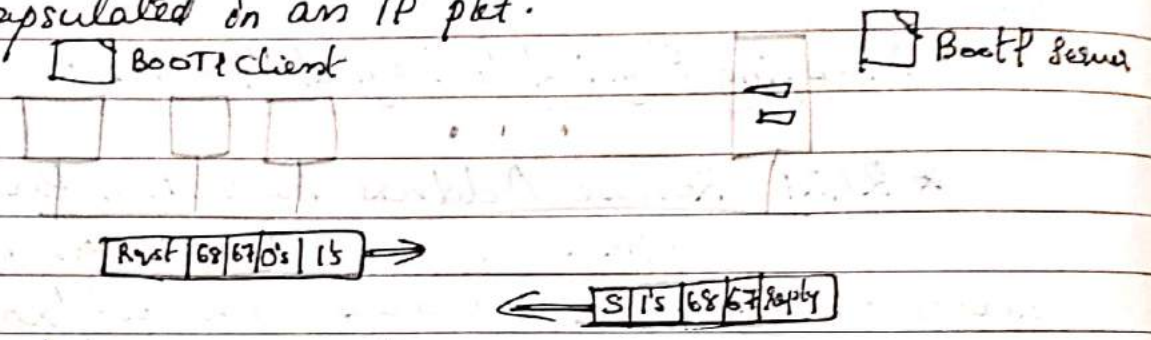
The ROM is not included the IP address b/c the IP addresses on a n/w are assigned by the n/w administrator. The m/c can get its phy. address (by reading its NIC), which is unique locally. It can then use the phy. addr. to get the logical address by using RARP protocol. A RARP rqst is created and broadcast on the local n/w. Another m/c on the local n/w. Another m/c on the local n/w that knows all the IP addresses will respond with RARP reply. The requesting m/c must be running a RARP client pgm; the responding m/c must be running a RARP server pgm.

Problem: ?

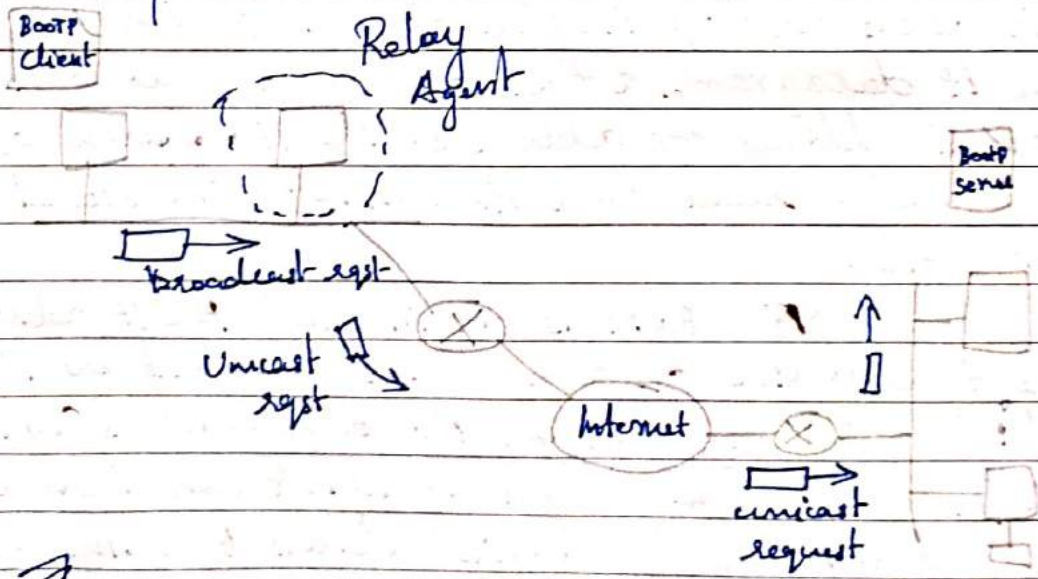
Bootstrap Protocol (BOOTP)

→ physical address to logical address mapping.

→ is an application layer protocol. The administrator may put the client and the server on the same n/w or on diff. n/ws. BOOTP msgs are encapsulated in a UDP pkt and the UDP pkt itself is encapsulated in an IP pkt.



Client & Server on the same N/w.



Client & Server on diff. n/ws.

Adv: over BOOTP over RARP is that, the client & server are application layer processes. As in other appln layer processes, a client

Internet Multicasting

IP supports multicasting using class D addresses. Each class D address identifies a group of hosts. 28 bits are available for identifying groups, so over 250 million groups can exist at the same time. When a process sends pkt to a class D ~~age~~ address, a best-efforts attempt is made to deliver it to all the members of the group addressed, but no guarantees are given. Some members may not get the pkt.

Two kinds of group addresses are supported: permanent addresses and temporary ones. A permanent group is always there & doesn't have to be set up. Each permanent group has a permanent group address.

Eg: 224.0.0.1 All s/ms on a LAN.
224.0.0.2 All routers on a LAN.

Temporary groups must be created before they can be used. A process can ask its host to join a specific group. It can also ask its host to leave the group. When the last process on a host leaves a group, that group is no longer present on the host.

Multicasting is implemented by special multicast routers, ~~which may or may~~ Each host sends back responses for all the class D addresses it is interested in. These query & response pkts use a protocol called IGMP.

Internet Group Management Protocol (IGMP).

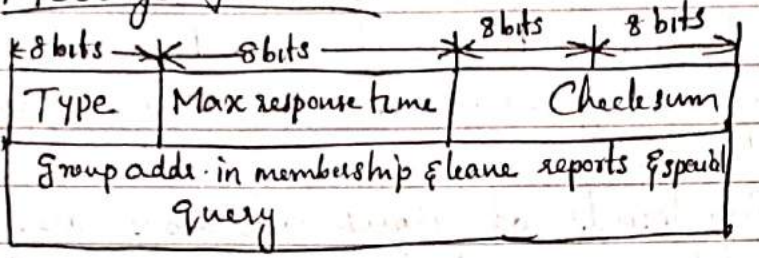
It is a protocol that manages group membership. There are one or more multicast routers that distribute multicast pkts to hosts & other routers. The IGMP protocol gives the multicast routers info about the membership status of hosts connected to the n/w.

IGMP Messages:

- General Query ✓
- Special Query ✓
- Membership report ✓
- Leave report ✓

two versions: One → IGMPv2.

Message format:



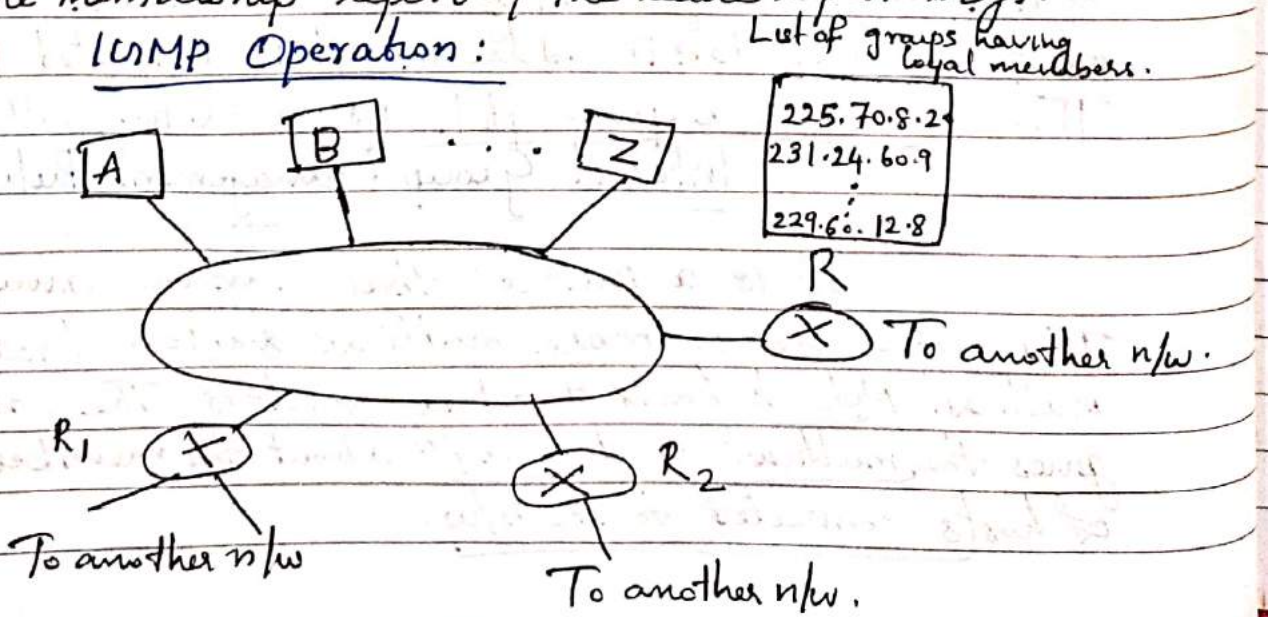
Type:

Type	Value
General/special query	0x11 or 00010001
Membership report	0x16 or 00010110
Leave report	0x17 or 00010111

Max. Response Time: This 8 bit field defines the amount of time in which a query must be answered. The value is in 10^{ths} of a second.

Checksum: This is a 16 bit field set 0 for a general query msg. The value defines the groupid in the special query the membership report & the leave report msgs.

IGMP Operation:



A multicast router connected to a n/w has a list of multicast addresses of the groups with atleast one loyal member in that n/w. For each group, there is one router that has the duty of distributing the multicast pkts destined for that group. Eg: Only Router R distributes pkts with the multicast address of 225.70.8.20.

Fig: router R is the distributing router. There 2 other multicast routers (R_1 & R_2) that, depending on the group list maintained by the router R, could be the recipients of router R in this n/w. Routers R_1 & R_2 may be distributors for some of these groups in other n/ws but not on this n/w.

Joining a Group: A host/router can join a group. A host maintains a list of processes that have membership in a group. When a process wants to join a new group, it sends its rqst to the host. The host adds the name of the process & the name of the requested group to its list. If this is the 1st entry for this particular group, the host sends a membership report msg.

Leaving a Group: When a host sees that no process is interested in a specific group, it sends a leave report. When a router sees that none of the n/ws connected to its I/fs is interested in a specific group, it sends a leave report about that group. To make sure after receiving the leave report, the router sends a special query msg & inserts the groupid or multicast address related to the group. The router allows a specified time for any host or router to respond.

Monitoring Membership: The router periodically sends a general query msg.

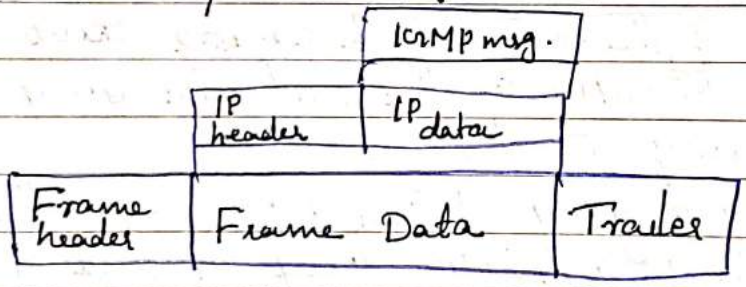
classmate
Date
Page

Delayed Response: When a host/router receives a query msg, it doesn't respond immediately; it delays the response. Each host or router uses a random no. to create a timer, which expires btw 1 & 10s. The expiration time can be in steps of 1s or less. A timer is set for each group in the list. For eg: the timer for the 1st group may expire in 2s, the timer for third in 5s.

Query Router: Query msgs may create a lot of responses. To prevent unnecessary traffic, ICMP designates one router as the query router for each n/w. Only this designated router sends the query msg, & the other routers are passive.

Encapsulation:

ICMP msg is encapsulated in an IP datagram which is itself encapsulated in frame.



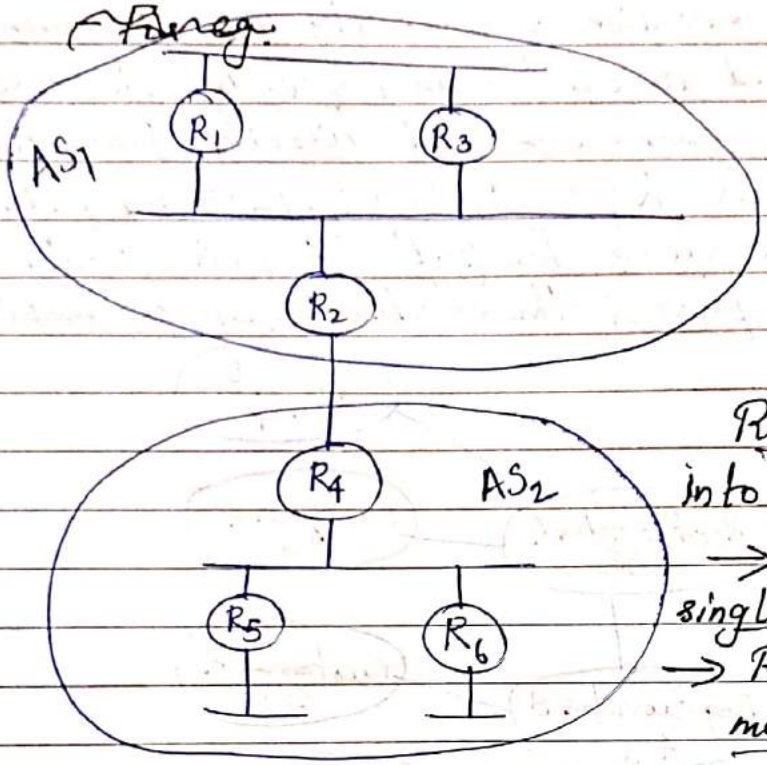
Encapsulation at N/w Layer: The value of the protocol field is 2 for the ICMP protocol. Every IP pkt carrying this value in its protocol field has data delivered to the ICMP protocol. When the msg is encapsulated in the IP datagram the value of TTL must be 1.

Encapsulation at Data Link Layer: Because the IP pkt has a multicast IP address, the ARP protocol cannot find the corres. phy. address to forward the pkt at the data link layer.

The Exterior Gateway Routing Protocol – BGP.

– Exterior Gateway protocol routers

Eg:



AS_1 Autonomous s/m

Routing pblms is devided into two parts:

→ Routing within a single autonomous s/m.

→ Routing b/w autonomous s/m.

ie; Interdomain routing & Intradomain routing.

→ Each A.S has one or more border routers through which pkts enter & leave the A.S. In fig: R2 & R4 would be border routers known as Gateways.

Each A.S that participates in BGP must also have atleast one BGP speaker, a router that 'speaks' BGP to other BGP speakers in other autonomous s/ms. It is common to find that border routers are also BGP speakers, but that doesn't have to be the case.

BGP advertises complete paths to reach a particular n/w. It is called path vector protocol.

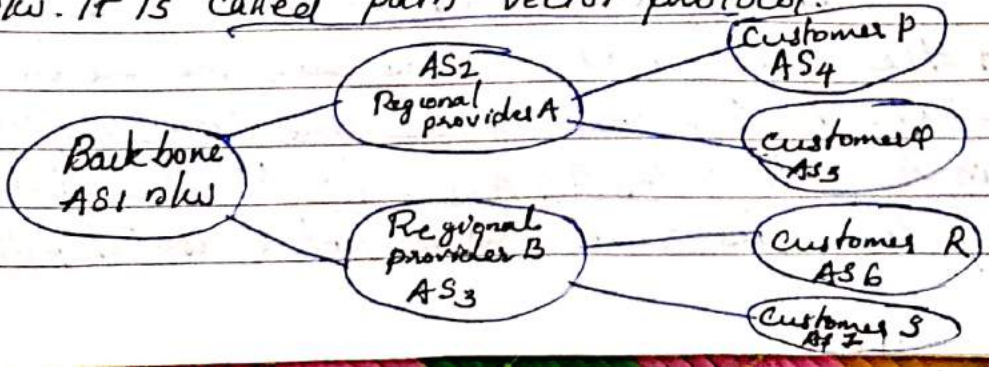
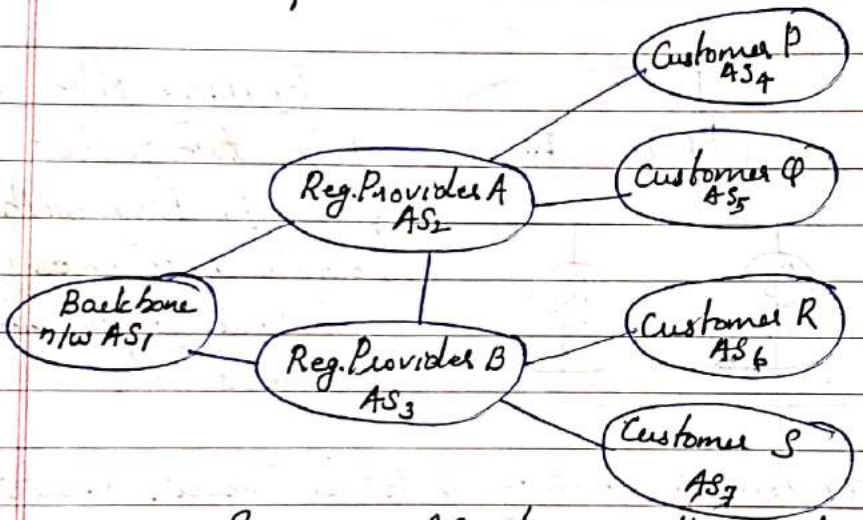


Fig: the providers are transit n/ws, while the customer n/w are stubs.

A BGP speaker for the AS of provider A (AS_2) would be able to advertise reachability inf^n for each of the n/w no.s assigned to customers P & Q. ie; The customer P & Customer Q can be reached directly from AS_2.

Ily The n/ws R & S (192.12.69, 192.4.54 & 192.4.23) can be reached along the path $\langle AS_1, AS_3 \rangle$. An imp. job of BGP is to prevent the establishment of looping paths.

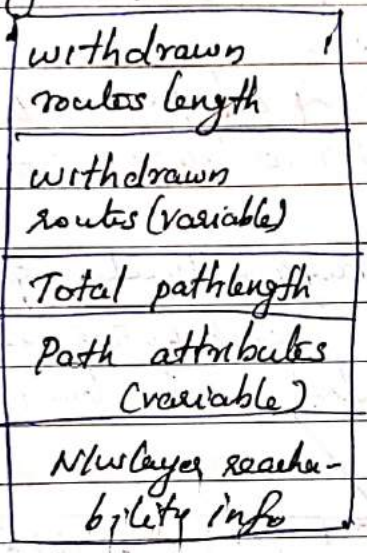


Suppose AS_1 learns that it can reach n/w AS_4 through AS_2, so it advertises this fact to AS_3 who in turn advertises it back to AS_2.

In the absence of any loop prevention mechanism, AS_2 could now decide that AS_3 was the preferred route for pkts destined for AS_4. If AS_2 starts sending pkts addressed to AS_4 to AS_3, AS_3 would send them to AS_1. AS_1 would send them back to AS_2 & they loop for ever.

This is prevented by carrying the complete AS path in the routing msgs. In this case, the advertisement for a path to AS_4 received by AS_2 from AS_3 would contain AS path $\langle AS_3\ AS_1\ AS_2\ AS_4 \rangle$. AS_2 sees itself in this path & concludes that this is not a useful path for it to use.

If a BGP speaker has a choice of several diff. routes to a dest^n, it will choose best one acc. to its own local policies & then that will be the route it advertises. Given that links fail & policies change, BGP speakers need to be able to cancel previously advertised paths. This is done with the form of negative advertisement as a withdrawn route. Both true & negative reachability inf^n are carried in a BGP update msg:



BGP update packet format.

IPv6 – Internetworking Protocol version 6.

Advantages over IPv4:

* Larger Address Space: 128 bits long (32 bits of IPv4)
* Better header format: options are separated & inserted when needed btw the base header & the upper layer data. This simplifies & speeds up the routing process b/c most of the options do not need to be checked by routers.
* New Options: to allow additional functionalities.
* Allowance for extension: if required by new technologies or applications.
* Support for Resource Allocation: support traffic for real time audio & video.
* Support for more security: Encryption & authentication options.

classmate
Date
Page

Packet Format:

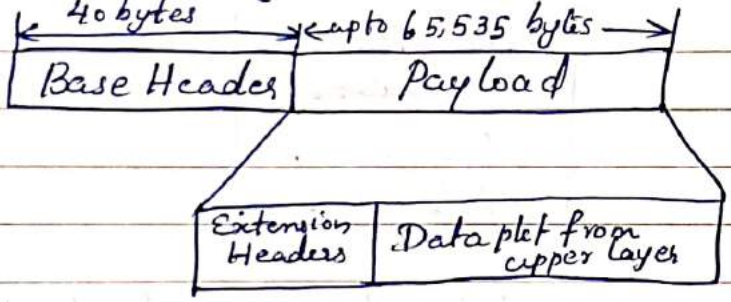
– composed of mandatory base header followed by the payload. The payload consists of 2 parts: optional extension headers & data from an upper layer.

Base Header: – 8 fields:

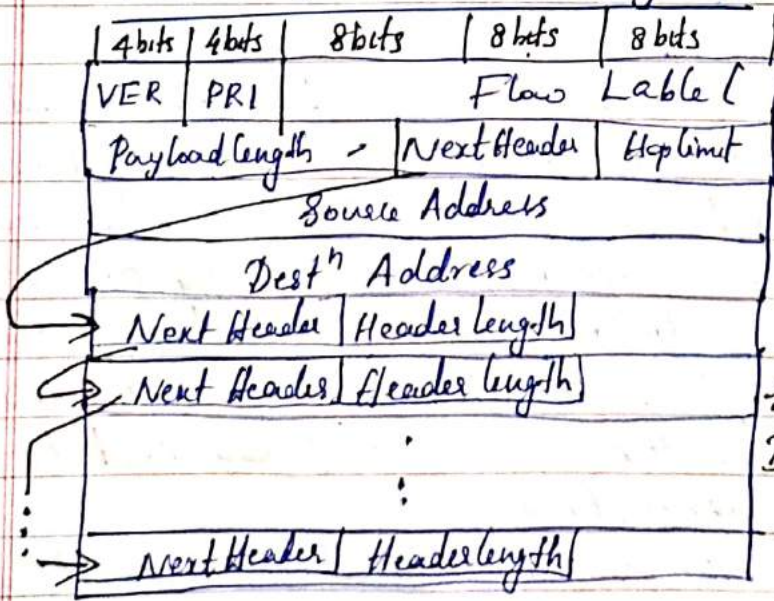
* Version - 4 bit field defines version no. of IP. For IPv6, value is 6.

* Priority: 4 bit priority field defines the priority of the pkt w.r.to traffic congestion.

IPv6 datagram Header & payload



Format of an IPv6 datagram:



Flow label: 3 byte field to handle flow of data.
Payload length: 2 byte
Next Header: 8 bit field.
Hop limit: 8 bit hop limit
Source addr: 16 byte
Dest^n addr: 16 byte.

Priority: priority of each packet w.r.to other pkts from the same source.
IPv6 divides traffic into two categories: congestion ctalled & non congestion ctalled.
Congestion Ctalled: Traffic: If a source adapts itself to traffic slow down when there is congestion, the traffic is called congestion ctalled traffic.
Priorities for congestion ctalled traffic:
0-No specific traffic, 1- Background data 2- unattended data 3-Reserved 4-attended bulk traffic. 5-reserved 6-Interactive traffic 7- conted traffic.
No specific traffic: -no priority.
Background data:- (priority 1) defines data that are usually delivered in the background.
Unattended data traffic: priority 2. Eg: E-mail.
Attended bulk data traffic: (priority 4) Eg: FTP & HTTP.
Interactive traffic: Eg: TELNET (priority 6)
Conted traffic: priority 7
Non congestion Ctalled: Priority nos from 8 to 15.

Priority	Meaning
8	Data with redundancy
...	...
15	Data with least redundancy

Flow Label: A sequence of pkts, sent from a particular dest^n, that needs special handling by routers is called a flow of pkts. The comb^n of source address & the value of the flow label uniquely defines a flow of pkts.
Flow label can be used to speed up the processing of a pkt by a router. When a router recieves a pkt instead of consulting the routing table & going through a routing

algm to define the address of the next hop, it can easily look in a flow label table for the next hop.

Comparison B/w IPv4 and IPv6 Headers

1. The Header length field is eliminated b/c it is fixed in IPv6.
2. The service type field is eliminated in IPv6. The priority & flow label fields together take over the fn of the service type field.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag & offset fields are eliminated from the base header in IPv6.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated b/c the checksum is provided by upper layer protocols.
8. The option fields in IPv4 are implemented as extension headers in IPv6.

Extension Headers:

The length of the base header is fixed at 40 bytes. To give greater fnality to the IP datagram, the base header can be followed by up to six extension headers. They are 6 types:

① Hop by hop option: is used when the source needs to pass inf^n to all routers visited by the datagram. Only 3 options have been defined: Pad1, PadN & Jumbo payload.

② The source routing extension header combines the concepts of the strict source route & the loose source route options of IPv4.

③ Fragmentation: In IPv6, only the original source can fragment. A source must use a path MTU discovery technique to find the smallest MTU supported by any n/w on the path.

③ Authentication: It validates the msg sender & ensures the integrity of data.

④ Encrypted Security Payload: provides confidentiality & guards against eavesdropping.

⑤ Destination Options: is used when the source needs to pass info to the destn only. Immediate routers are not permitted access to this info.

Comparison b/w IPv4 Options & IPv6 Extension Headers:

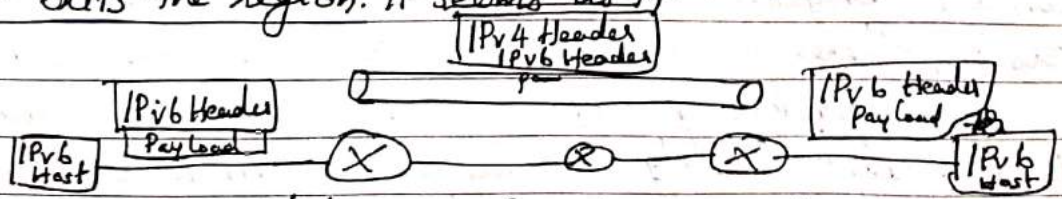
see: Forouzan

Transition from IPv4 to IPv6.

Three strategies: → Dual stack ✓
→ Tunneling ✓
→ Header translation. ✓

Dual Stack: All hosts, before migrating completely to version 6, have a dual stack of protocols. A station must run IPv4 & IPv6 simultaneously until all the internet uses IPv6.

Tunneling: When 2 computers using IPv6 want to communicate with each other & the pkt must pass through a region that uses IPv4. To pass through this region, the pkt must have an IPv4 address. So the IPv6 pkt is encapsulated in an IPv4 pkt when it enters the region, & it leave the capsule when it exits the region. It ~~seems as if~~



Header Translation: When the majority of the internet has moved to IPv6 but some s/ms still use IPv4. The sender wants to use IPv6, but the receiver doesn't understand IPv6. Tunneling doesn't work in this situation b/c the pkt must be in the IPv4 format to be understood by the receiver. Header format must be totally changed through header translation. The ~~IPv~~ header of the IPv6 pkt is converted to an IPv4 header

ICMPv6 (Internetworking Control Message Prot

Comparison of n/w layers in version 4 & version 6.

N/w layer in version 4 N/w layer in version 6

The ARP & IGMP protocols in version 4 are combined in ICMPv6. The RARP protocol is dropped from the suite b/c it was rarely used & BOOTP has the same finality.

ICMP msgs into 2 categories: Each category has more types of msgs than before.

* Error Reporting:

ICMPv6 forms an error packet, which is then encapsulated in an IP datagram. This is delivered to the original source of the failed datagram. The source quench msg is eliminated in version 6 b/c the priority & the flow label fields allow the router to control congestion & discard the least imp. msgs. In this version, there is no need to inform the sender to slow down.

The packet too big msg is added b/c fragmentation is the responsibility of the sender in IPv6. If the sender doesn't make the right pkt size decision, the router has no choice & but to drop the pkt & send an error msg to the sender.

* Query Messages:

4 diff. groups of msgs have been defined: echo-rqst & reply, router solicitation & advertisement, neighbor solicitation & advt. & group membership.

Neighbor solicitation & Advertisement: In version 4 an independant protocol called ARP. In version 6, this protocol is eliminated, & its duties are included in ICMPv6.

Group Membership: The nlw layer in version 4 contains an independant protocol called IGMP. In version 6, this protocol is eliminated, & its duties are included in ICMPv6.

20/11/18

classmate
Date
Page

MODULE - VI

→ Transport Layer
  * TCP
  * UDP
→ Application Layer
  * FTP
  * DNS
  * Electronic Mail
  * MIME, SNMP
  * Introduction to WWW.

1. Name the common 3 components of a browser.
2. How is HTTP is similar to SMTP.?
3. What is the diff b/w an active document & a dynamic doc.?
4. What are the 3 types of Web Documents?
5. Describe the relationship b/w Java & an active document?
6. What is a URL & what are its components?
7. What does CGI stand for & what is its functions?
8. Show a request that retrieves the document /usr/users/doc/doc1. Use at least 2 general headers, 2 rqst headers & one entity header.?
9. What is SNMP? Explain.
10. How does caching increase the effiiency of name resolution?
11. How does recursive resolution differ from iterative resolution?
12. What is the advantage of hierarchical name space over a flat name space for a s/m the size of the Internet?.
13. What is the diff. b/w primary server & a secondary server?
14. What are the 2 categories of DNS msgs?
15. Why do we need a DNS when we can directly use an IP address?
16. What are the 3 FTP transmission modes?
17. Describe the fns of 2 FTP connections?

18. What is anonymous FTP?
19. In E-mail, what is MIME?
20. In E-mail, what are the tasks of a user agent?
21. How does a storing a file differ from retrieving a file?
22. What kinds of file types can FTP transfer?
23. A sender sends a JPEG msg. Show the MIME header.
24. Explain why FTP doesn't have a msg format.
25. Why is a connⁿ establishment for mail transfer needed if TCP has already established a connection?
26. Compare TCP header & the UDP header.
27. Compare TCP & UDP.
28. What are the phases in TCP.?

April 2018

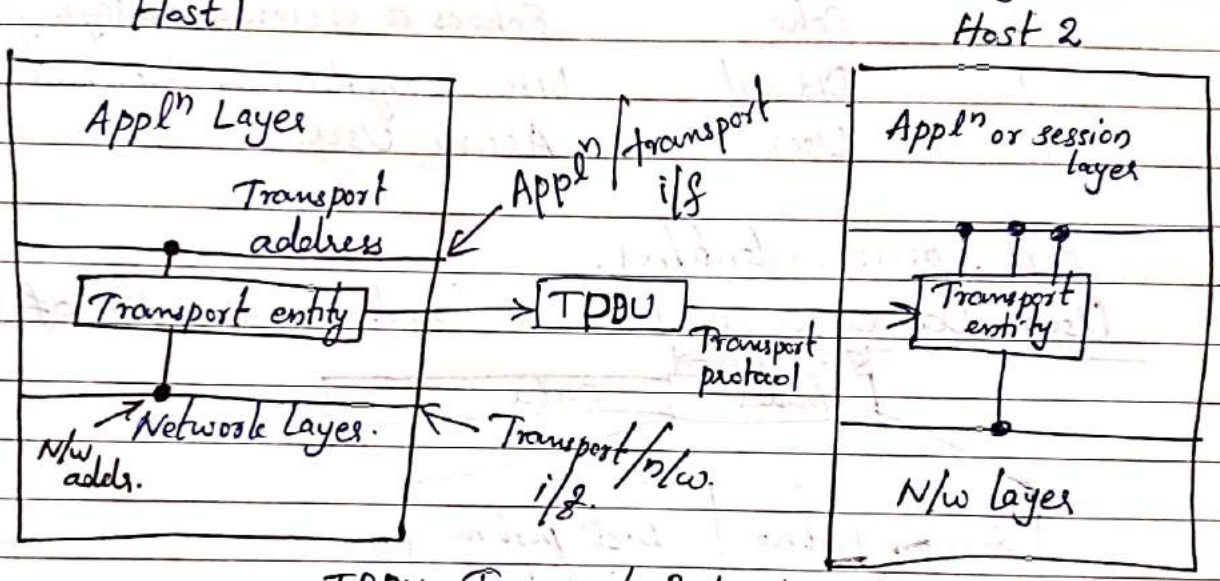
1. Describe ~~Ad~~ Name Address resolution techniques ~~used~~ used in DNS.
2. Write notes on MIME
3. Describe the Opⁿ & packet format of UDP.
4. partially qualified & fully qualified domain names.
5. Explain the 3 diff. phases in a TCP transmit with the help of diagram.
6. Explain the FTP & its features.
7.

Transport Layer:

→ to provide reliable, cost effective data transport from the source m/c to the dest^{n} m/c, independantly of the phy. n/w or n/ws currently in use.

* Services provided to the Upper Layers:

The transport layer makes use of the services provided by the n/w layer. The h/w or s/w within the transport layer that does the work is called the transport entity.

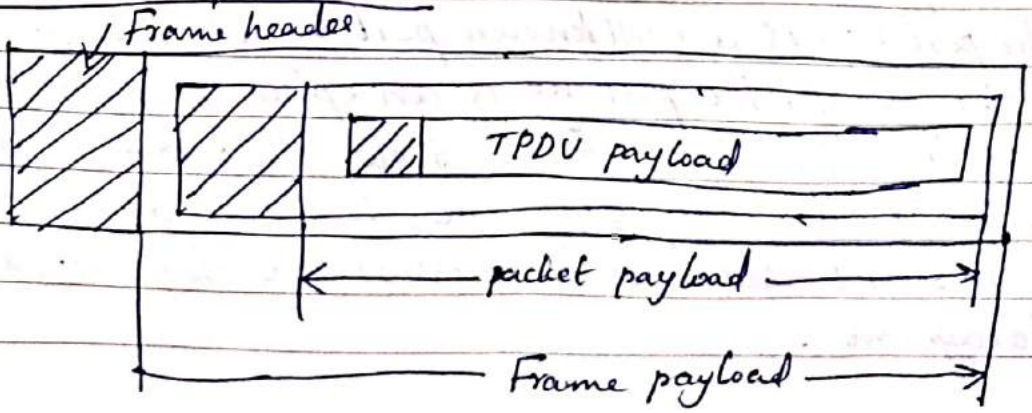


TPDU – Transport Protocol Dat Unit

* Transport Service Primitives

- LISTEN – Block until some process tries to connect.
- CONNECT – Actively attempt to establish a connection.
- SEND – Send Information.
- RECIEVE – Block until a DATA packet arrives.
- DISCONNECT – This side wants to release the Connⁿ.

TPDU, Packet & Frames



User Datagram Protocol (UDP)

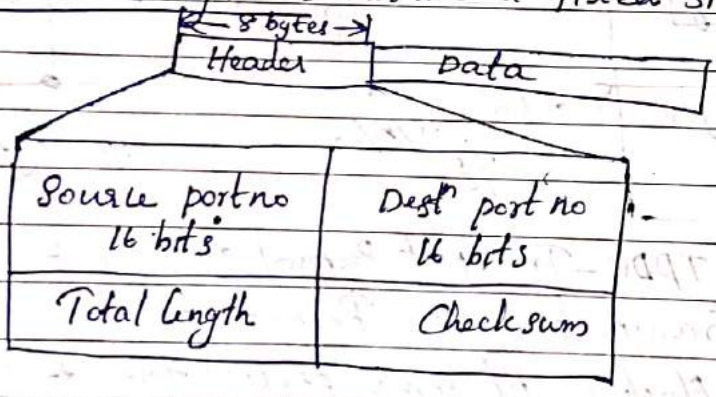
→ Connectionless, unreliable transport protocol. If a process wants to send a small msg & doesn't care much about reliability, it can use UDP.

Well-Known Ports for UDP: Examples.

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received.
11	Users	Active Users.

Port: process identifier.

User Datagram: have a fixed size header of 8 bytes.



Source port number: This is the port no used by the process running on the source host. It is 16 bits long, which means that the port no can range from 0 to 65,535.

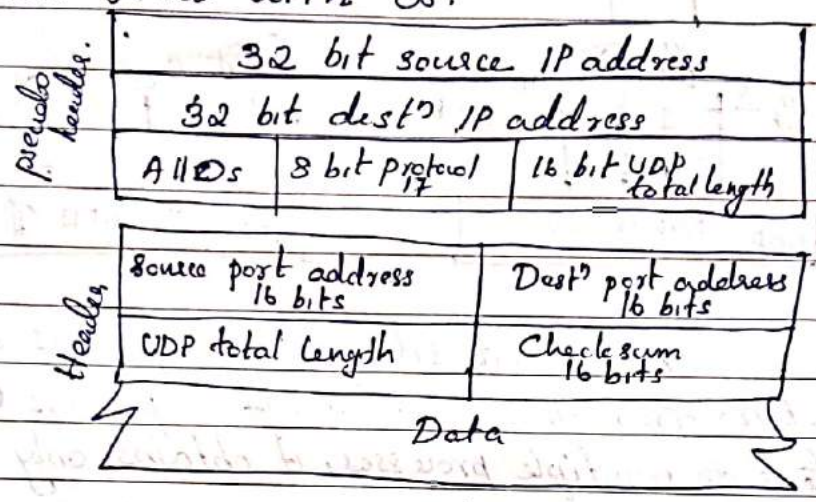
Destination port number: This is the port no. used by the process running on the destn host. If the destn host is the server, the port no, is a well-known port no. If the destn is host is the client, the port no is an ephemeral port number.

Length: This is a 16 bit field that defines the total length of the user datagram, header + data.

Checksum: used to detect errors over the entire user datagram.

The UDP checksum calculation is different from the one for IP and ICMP. Here the checksum includes 3 sections: a pseudoheader, the UDP header & the data coming from the application layer.

Pseudoheader: is the part of the header of the IP pkt in which the user datagram is to be encapsulated with some fields filled with 0s.



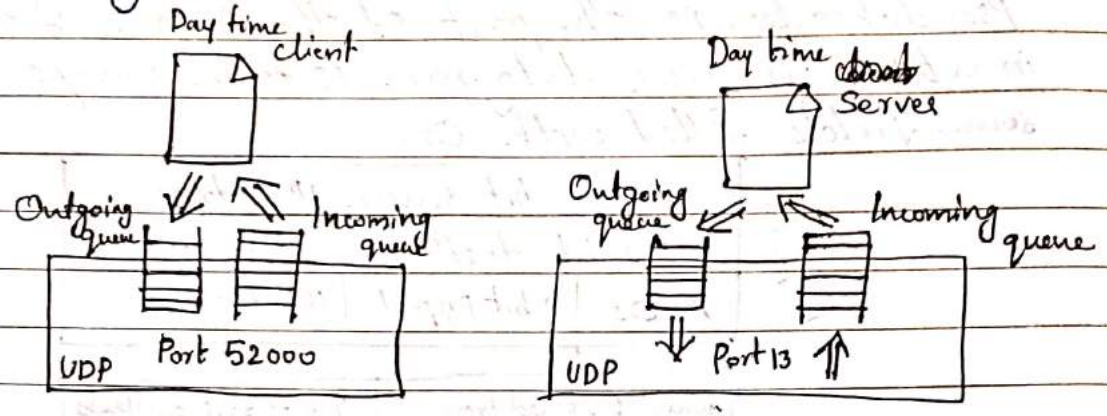
UDP provides a way for appl^ns to send encapsulated IP datagrams & send them without having to establish a connection. UDP transmits segments of an 8 byte header followed by the payload. The 2 ports serve to identify the end points within the source & dest^n m/cs. When a UDP pkt arrives, its payload is handed to the process attached to the dest^n port. This attachment occurs when BIND primitive or something similar is used.

Connectionless Services: Each user datagram sent by UDP is an independant datagram. There is no relationship b/w the diff. user datagrams even if they are coming from the same source process & going to the same dest^n pgm. There is no conn^n establishment & conn^n termination.

Flow & Error Control: Very simple, unreliable transport protocol. There is no flow control. The receiver may overflow with incoming msgs. There is no error control in UDP except for the checksum.

Encapsulation & Decapsulation: To send a msg from one process to another, the UDP protocol encapsulates & decapsulates msgs in an IP datagram.

Queuing: Queues are associated with ports.



At client site, when a process starts, it rqsts a port no from the O.S. Even if a process wants to communicate with multiple processes, it obtains only one port no & eventually one outgoing & one incoming queue. The queues ~~are~~ function as long as the process is running. When the process terminates.

The client process can send msgs to the outgoing queue by using the source port no specified in the rqst. UDP removes the msgs one by one and, after adding the UDP header, delivers them to IP.

At the server site, a server asks for incoming & outgoing queues, using its well known port, when it starts running. When a msg arrives for a server, UDP checks to see if an incoming queue has been created for the port no. specified in the dest^{n} port no. field of the user datagram. If there is such a queue, UDP sends the recieved user datagram to the end of the queue. If there is no such queue, UDP discards the user datagram ~~& asks the ICMP protocol~~

When a server wants to respond to

a client, it sends msgs to the outgoing queue, using the source port no specified in the rqst. UDP removes the msgs one by one and after adding the UDP header, delivers them to IP.

Uses of UDP

- suitable for a process that requires simple rqst-response comm^n. with little concern for flow & error ctrl.
- suitable for a process with internal flow & error ctrl mechanisms. For eg: the Trivial File Transfer Protocol (TFTP) process includes flow & error ctrl.
- suitable for multicasting.
- suitable for mgmt processes such as SNMP
- suitable for route updating protocols such as RIP.

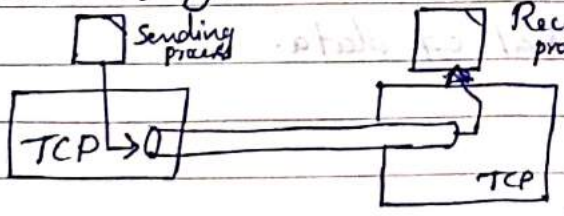
Transmission Control Protocol (TCP)

- process to process protocol.
- uses flow & error ctrl mechanisms.
- connection oriented.

TCP Services

* Process to process Communication: using port numbers. Well known ports eg: 7 - Echo, 9 - discard, 11, Users etc!

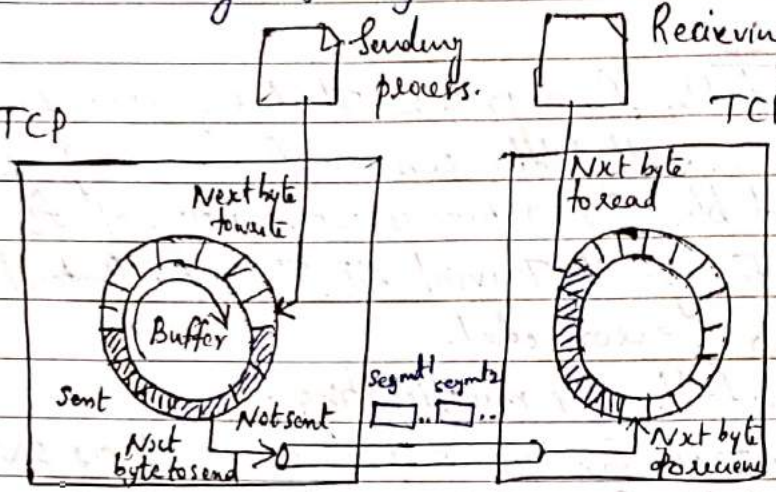
* Stream Delivery Servile: a stream oriented protocol. TCP allows the sending process to deliver data as a stream of bytes & allows the recieving process to obtain data as a stream of bytes.



TCP creates an envt. in which the 2 processes seem to be connected by an imaginary "tube" that carries their data across the Internet. The sending process produces (writes to) the stream of bytes, & the receiving process consumes (reads from) them.

*Sending & Recieving Buffers:

One way to implement a buffer is to use a circular array of 1-byte locations.



* Segments: At the transport layer, TCP groups a no. of bytes together into a pkt called a segment. TCP adds a header to each segment & delivers the segment to the IP layer for transmission.
* Full Duplex Communication: data flow in both directions at the same time.
* Connection-Oriented Service: When a process at site A wants to send & recieve data from another process at site B, the follo. occurs:
  1. The 2 TCPs establish a connection blw them.
  2. Data are exchanged in both directions.
  3. The connⁿ is terminated.
* Reliable Service: It uses an ack mechanism to check the safe & sound arrival of data.

TCP Features:

* Numbering System: There are 2 fields called seq. no & the ack no. These 2 fields refer to the byte no. & not the segment no.

Byte Number: TCP numbers all data bytes that are transmitted in a connection. When TCP recienes bytes of data from a process, it stores them in the sending buffer & numbers them.

Sequence Number: After the bytes have been numbered, TCP assigns a seq. no to each segment that is being sent. The seq. no for each segment is the no. of the first byte carried in that segment.

1. Suppose a TCP connection is transferring a file of 5000 bytes. The first byte is numbered 10,001. What are the sequence numbers for each segment if data are sent in 5 segments, each carrying 1000 bytes?.

Segment 1 ⟹ SeqNo: 10,001 (10,001 – 11000).
Segment 2 ⟹ SeqNo: 11,001 (11,001 – 12000)
" 3 ⟹ " : 12001 (12,001 – 13000)
" 4 ⟹ " : 13001 (13,001 – 14000)
" 5 ⟹ " : 14,001 (14,001 – 15000).

The value in the seq. no. field of a segment defines the no. of the first data byte contained in that segment.

Acknowledge Number: When a conn" is established, both parties can send & recieve data at the same time. Each party also uses an ack no to confirm the bytes it has recieved. The ack no defines the no. of the next byte that the party expects to recieve.

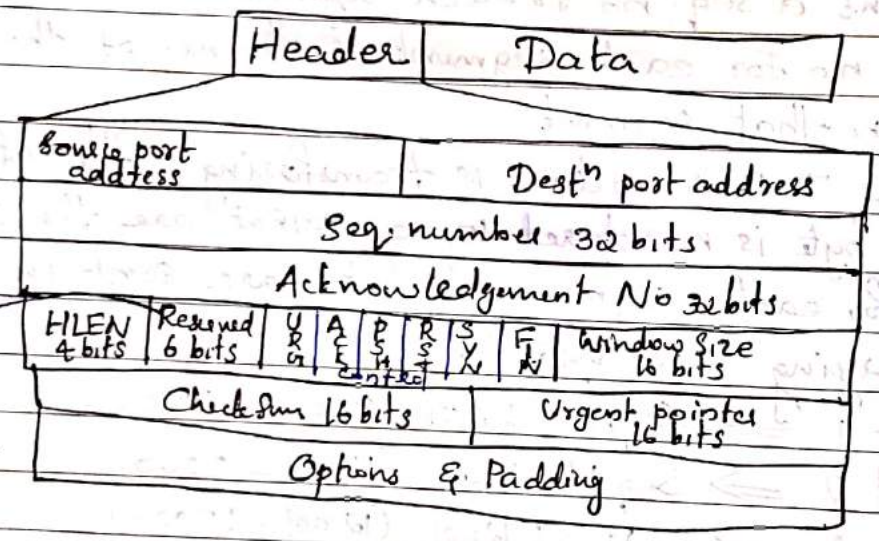
* Flow Control: The reciever of the data controls the amount of data that are to be sent by the sender. This is done to prevent the reciever from being overwhelmed with data.

* Error Control: To provide reliable service, TCP implements an error control mechanism. Error control is byte oriented.

* Congestion Control: The amount of data sent by a sender is not only ctalled by the receives (flow ctrl) but is also determined by the level of congestion in the n/w.

* Segment: A pkt in TCP is called a segment.

Format:



Control field: URG, ACK, PSH, RST, SYN, FIN

Flag	Description
URG	The value of the urgent ptr field is valid
ACK	The value of the ack field is valid
PSH	Push the data
RST	Reset the conn^n
SYN	Synch. seq. No during conn^n
FIN	Terminate the Conn^n.

Window Size: defines size of the window in bytes, that the other party must maintain. 16 bits → max. size of the window is 65,535 bytes.

Urgent Ptr: valid only if the urgent flag is set, i.e. the segment contains urgent data.

TCP Connection

– establishes virtual path b/w the source & destn. All the segments belonging to a msg are then sent over this virtual path.

Three phases:
- → Connn establishment
- → Data transfer
- → Connn termination.

Connection Establishment

TCP transmits data in full duplex mode.

Three way handshaking:

Eg: An applⁿ pgm, called ~~server~~ client, wants to make a connn with another applⁿ pgm, called the server, using TCP transport layer protocol.

The server pgm tells its TCP that is ready to accept a connection. This is called a rqst for a passive open. The client pgm issues a rqst for an active open. A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server.

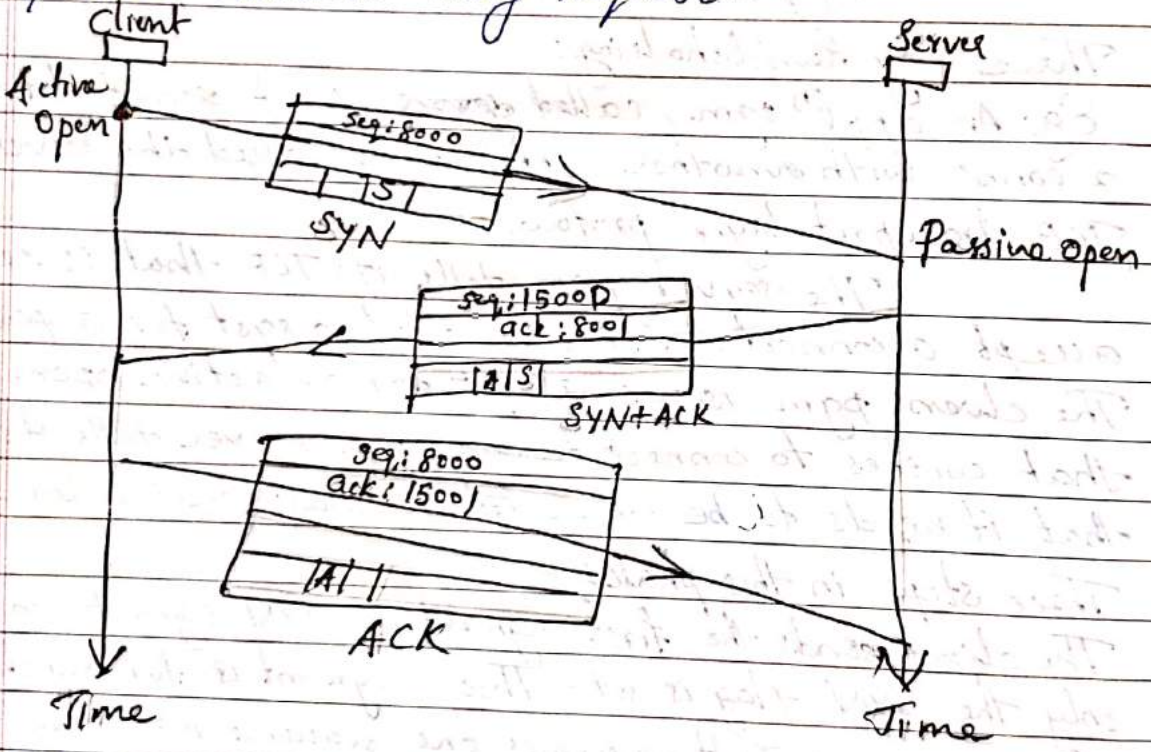
Three steps in this phase:

1. The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence no.s. It consumes one sequence no. When the data transfer starts, the seq. no is incremented by 1. SYN segment carries no real data.
2. The server sends the second segment, a SYN + ACK segment, with 2 flag bits set SYN & ACK. It is a SYN segment for commn in the other direction & serves as the ack for the SYN segment. It consumes one segment no.
3. The client sends the 3rd segment. This is just an ACK segment. It acknowledges the receipt of the 2nd segment with the ACK flag & ack no field. It doesn't consume seq. no.

Simultaneous Open: may occur when both processes issue an active open. Both TCPs transmit a SYN + ACK segment to each other.

SYN flooding Attack: Malicious attacker sends a large no. of SYN segments to a server pretending that each of them is coming from a diff. client.

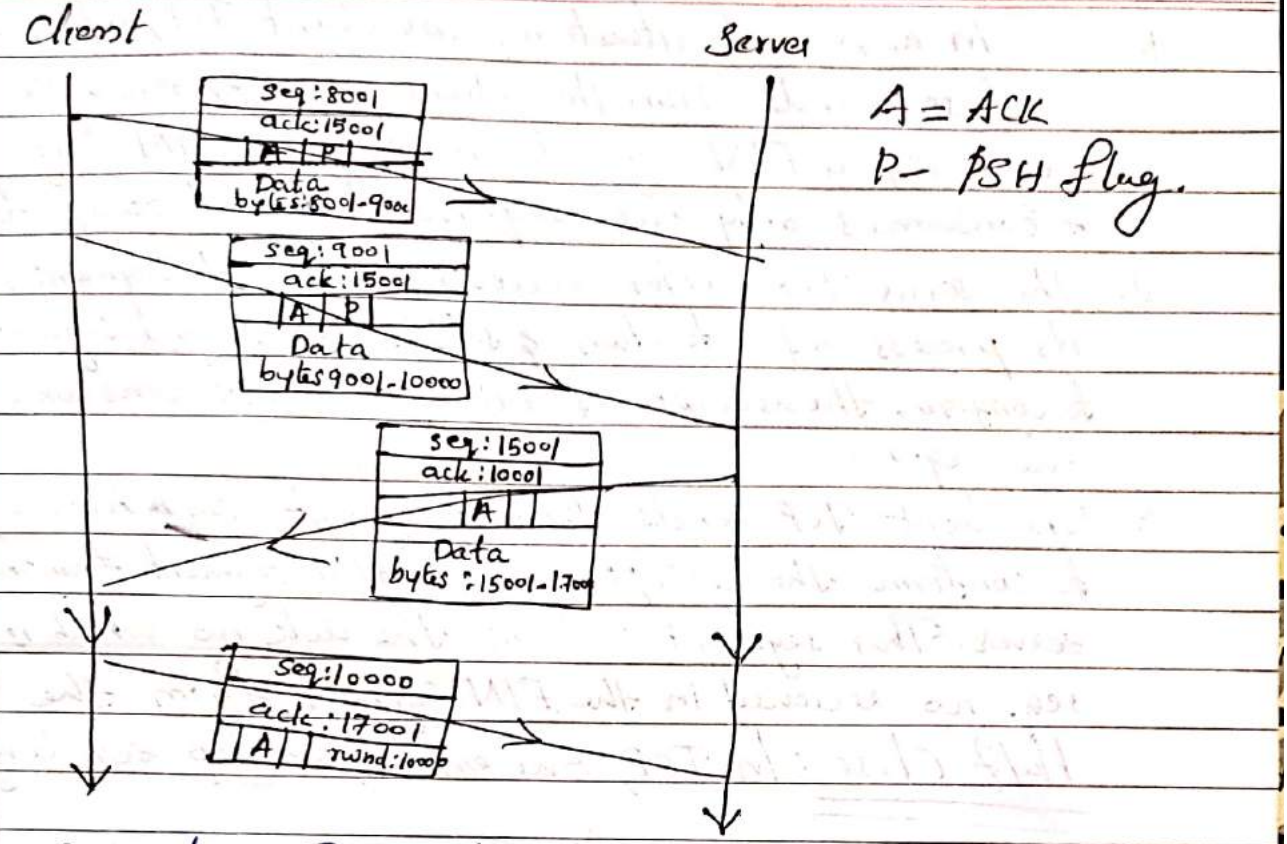
Denial of Service Attack: An attacker monopolizes a s/m with so many service reqsts. that the s/m collapses & denies service to every request.



Data Transfer:

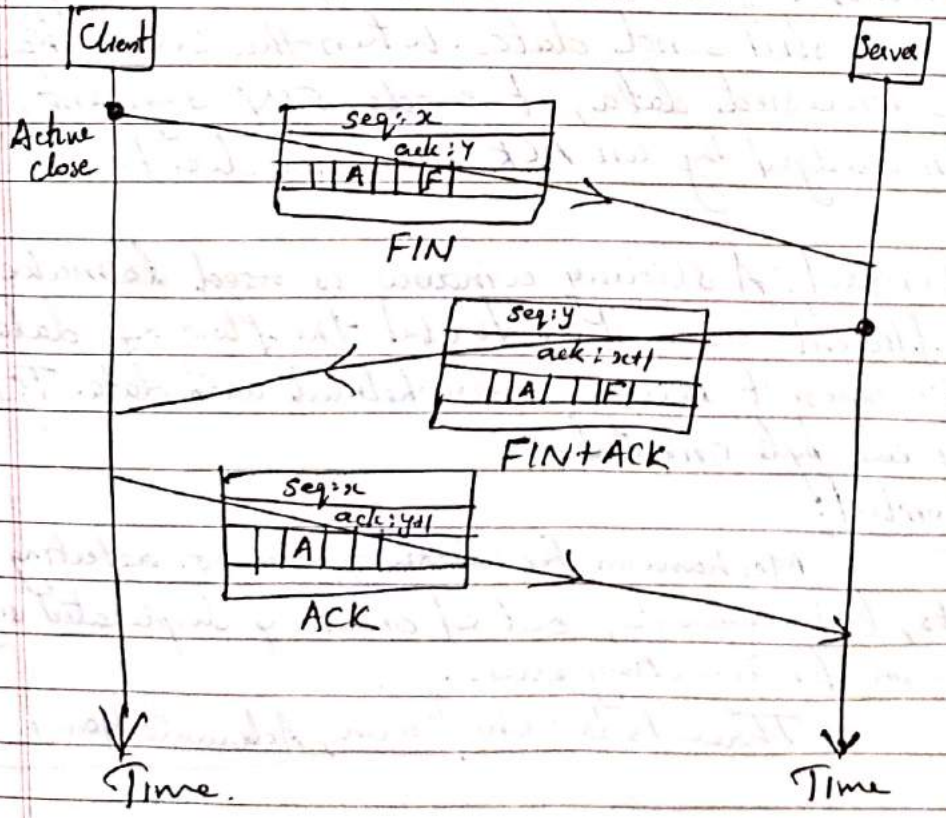
→ bidirectional; The client & server can both send data & acks.

Pushing Data: The sending TCP uses a buffer to store the stream of data coming from the sending appl^n pgm. The sending TCP can select segment size. The receiving TCP also buffers the data when they arrive & delivers them to the appl^n pgm.



Connection Termination:

Two options: → Three way handshaking
→ Four way handshaking.



1. In a normal situation, the client TCP, after receiving a close cmd from the client process, sends the first segment, a FIN segment in which the FIN flag is set. It consumes only one seq. no. It doesn't carry data.
2. The server TCP, after receiving the FIN segment, informs its process of situation & sends the second segment FIN+ACK to confirm the reciept of FIN segment. It consumes only one seq. no.
3. The client TCP sends the last segment, an ACK segment, to confirm the reciept of the FIN segment from the TCP server. This segment contains the ack no which is 1+ the seq. no received in the FIN segment from the server.

Half Close: In TCP, one end can stop sending data while still receiving data. ~~The server accepts~~ The client half closes the connection by sending FIN segment. The server accepts the half-close by sending the ACK segment. The data transfer from the client to the server stops. The server can still send data. When the server has sent all the processed data, it sends FIN segment, which is acknowledged by an ACK from the client.

Flow Control: A sliding window is used to make transmission more efficient as well as to ctrl the flow of data so that the destn doesn't become overwhelmed with data. TCP sliding windows are byte oriented.

Error Control:

Mechanism for ~~correcting errors~~. detecting corrupted segments, lost segments, out of order & duplicated segments. Mechanism for correcting errors.

∴ Three tools: Checksum, Acknowledgment & timeout

Checksum: to check for a corrupted segment; discarded by the destn.

Acknowledgement: to confirm the receipt of data segments.

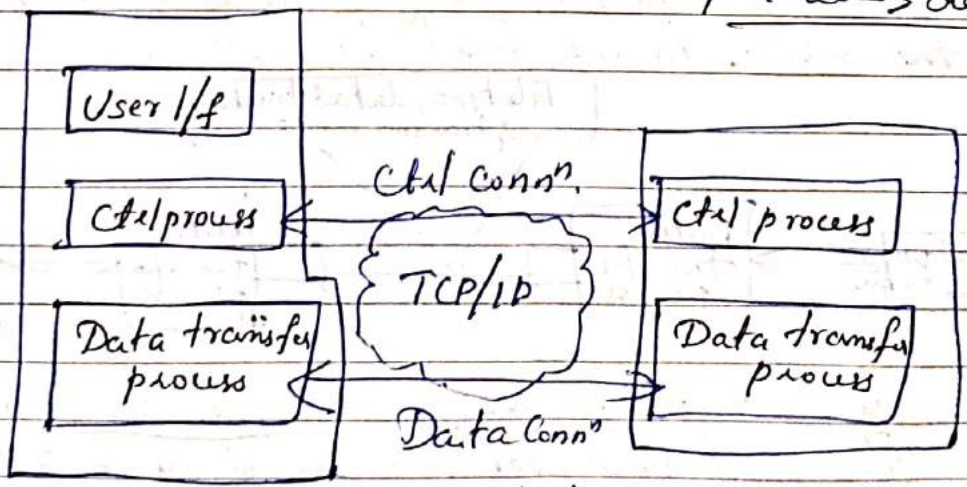
Retransmission: occurs if the retransmn times expires or 3 duplicate ACK segments have arrived.

Out of Order Segments: When a segment is delayed, lost or discarded, the segments follo. that segment arrive out of order. It results in retransmission of missing segment & the follo. segments.

File Transfer Protocol (FTP)

→ provided by TCP/IP for copying a file from one host to another. Two s/ms may be diff. in file name conventions, Data rep^n's, & directory structures. FTP establishes 2 connections blw the hosts. One conn^n is used for data transfer, the other for ctrl inf^n. The ctrl connn uses very simple rules of commn.

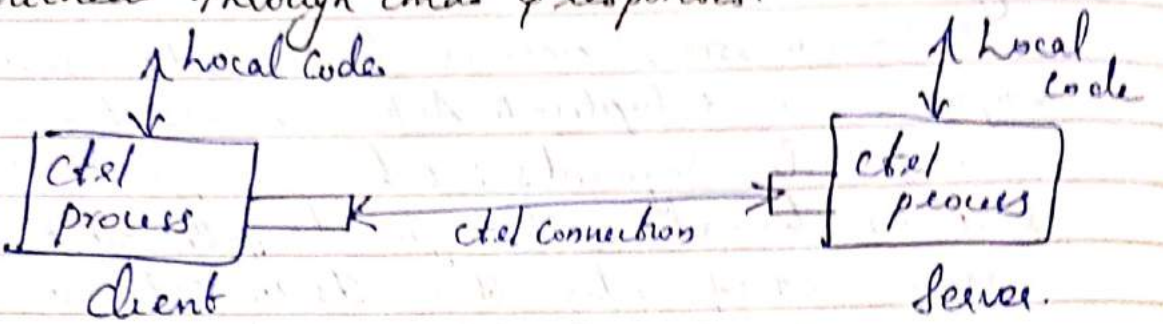
FTP uses 2 well known ports: port 21 → control connn
port 20 → data connn.



The control connn remains connected during the entire interactive FTP session. The data connn is opened & then closed for each file transferred.

Communication over Control Connection.

It uses 7 bit ASCII character set. Comm^n is achieved through cmds & responses.



- send one command at a time. Each cmd or response is only one short line. Each line is terminated with a 2 char. end-of-line token.

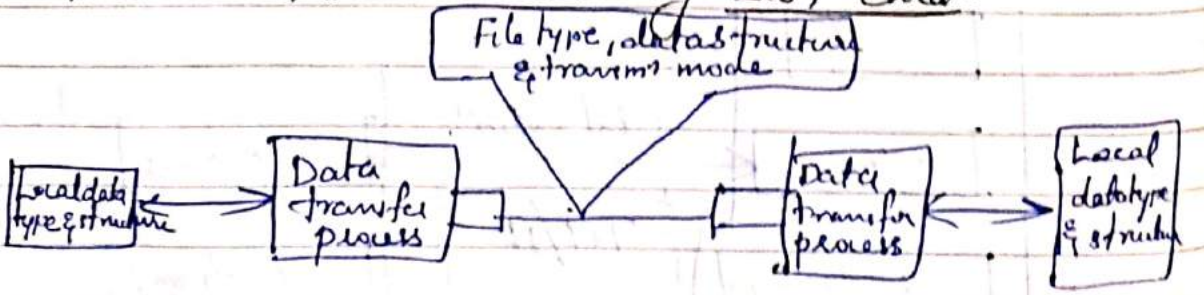
Communication over Data Connection.

⇒ transfer files through the data connection.

① A file is to be copied from the server to the client. This is called retrieving a file. It is under the supervision of RETR cmd.

② ⇒ A file is to be copied from client to the server. This is called storing a file. by STOR cmd.

③ A list of directory or file names is to be sent from the server to the client by LIST cmd.



File Type: an ASCII file, EBCDIC file or image file.

ASCII file: Each character is encoded using 7 bit ASCII.

EBCDIC file encoding using EDCDIC encoding.

Image file: continuous streams of bits.

Data Structure: file structure, record structure & page structure
↓ cont'l stream of bytes ↓ records
↓ pages.

Transmission Mode:

Stream mode: continuous stream of bytes.

Block mode: delivered in blocks. each block is preceded by a 3 byte header.

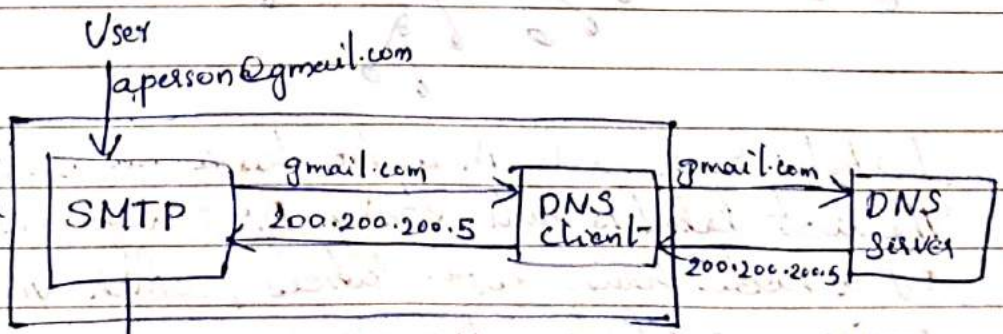
Compressed Mode: If the file is big, the data can be compressed.

Anonymous FTP

To use FTP, a user needs an account & password on the remote server. Some sites have a set of files available for public access, to enable anonymous FTP. To access these files, a user doesn't need to have an account or password. The user can use anonymous as username & guest as password.

Domain Name System

— is a supporting pgm that is used by other pgms such as e-mail.



→ to find email addr. of the recipient.

Transport layer.

The DNS client pgm sends a rqst to a DNS server to map the email addr. → to the corres. IP address.

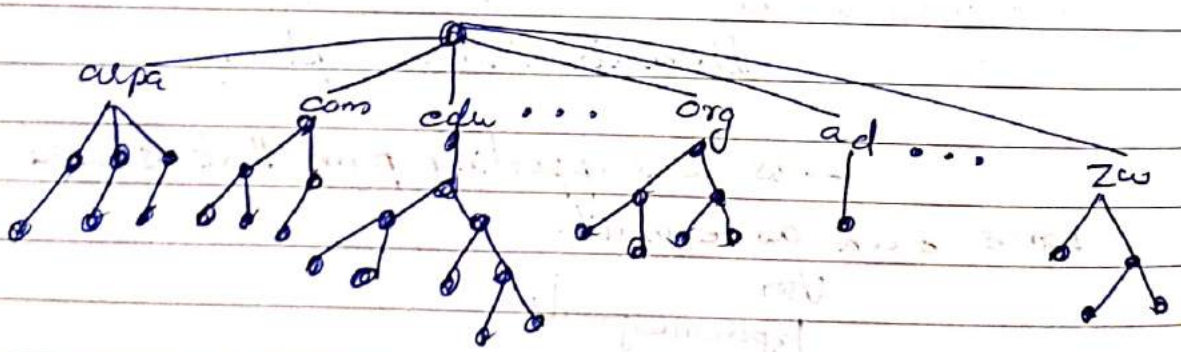
Name Space: The names assigned to m/cs must be selected from a name space with complete ctrl over the binding b/w the names & IP addresses.

Two ways → Flat Name Space
→ Hierarchical Name Space.

Flat Name Space: a name is assigned to an address. A name in this space is a seq. of characters without structure. The names may or may not have common sections. Disadv: It cannot be used in a large s/m such as Internet.

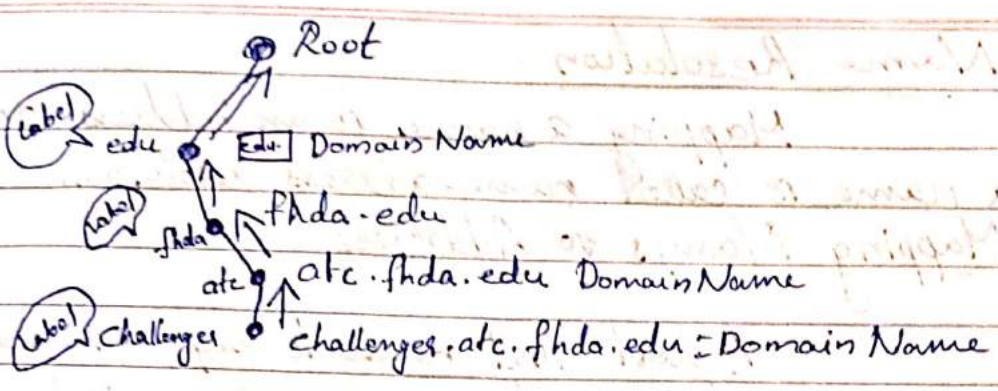
Hierarchical Name Space: Each name is made of several parts. The 1st part - nature of the orgn
IInd part - name of an orgn.
IIIrd part - depts in the orgn.
Eg: challenger.berkeley.edu.

Domain Name Space: Inverted tree structure.



Label: Each node in a tree has a label, string of 63 chars. The root label is null string. DNS requires that children of a node have diff. labels, which guarantees the uniqueness of the domain names.

Domain Name: is a sequence of labels separated by dots(.). The domain names are read from the node upto the root. The last label is the label of the root (null).



Fully Qualified Domain Name: If a label is terminated by a null string, it is called FQDN. It contains full name of a host.

Partially Qualified Domain Name: not terminated by null string. (PQDN)

~~For eg~~ Domain: is a subtree of the domain namespace.

Name Servers: — ~~Ro~~ to distribute information among many computers. called DNS Servers.

- Root Server
- Primary & Secondary Servers.

Root Server is a server whose zone consists of the whole tree. A root server doesn't store any inf^n about domains but delegates its authority to other servers.

Primary Servers: is a server that stores a file about the zone for which it is an authority. It is responsible for creating maintaining & updating zone file.

Secondary Servers: that transfers the complete inf^n about a zone from another server & stores the file on its local disk

A primary server loads all inf^n from the disk file; the secondary server loads all inf^n from the primary server. When the 2° downloads inf^n from primary, it is called zone transfer.

Name Resolution

Mapping a name to an address or address to a name is called name-address resolution.

Mapping Names to Addresses

A host that needs to map an addr. to a name or a name to an address calls a DNS client called a resolver.

Resolver gives a domain name to the server & asks for the corres. addr. In this case, the server checks the generic domain or the country domains to find the mapping.

Eg: chal.atc.fhda.edu (generic domain)

This query is sent by the resolver to the local DNS server for resolution. If the local server cannot resolve the query, it either refers the resolver to other servers or asks other servers directly.

Mapping Addresses to Names:

A client can send an IP address to a server to be mapped to a domain name. This is called inverse or ptr query. To answer these queries, DNS uses the inverse domain. For eg: If the resolver receives the IP address 132.34.45.121, the resolver first inverts the address & then adds the 2 labels before sending. The domain name sent is "121.45.34.132.in-addr.arpa"

Types of Records

Two types:
- Question records
- Resource records.

Question Records: is used by the client to get inf^n from a server. This contains the domain name.

Resource Records: Each domain name is associated with a record called the resource record. Resource records are also what is returned by the server to the client.

ELECTRONIC MAIL

The first component of an electronic mail s/m is the user agent (UA). It provides service to the user to make the process of sending & receiving a msg easier.

Services provided by a User Agent:

- User Agent
  - → Composing msgs
  - → Reading msgs
  - → Replying to msgs
  - → Forwarding msgs
  - → Handling msgs — Inbox & outbox.

User Agent Types:
- → Command-driven
- → CUI based.

Command-driven user agent accepts a one character cmd from the keyboard to perform its task. For eg:, a user can type the character r, at the cmd prompt, to reply to the sender.

Examples: mail, pine, & elm.

CUI based: Allow users to interact with the s/w by using both the keyboard & the mouse. They have graphical components such as icons, menu bars. Eg: M.S Outlook, Netscape etc

* Message: header & body
* Receiving mail:
* Addresses: local part & domain name separated by an @ sign

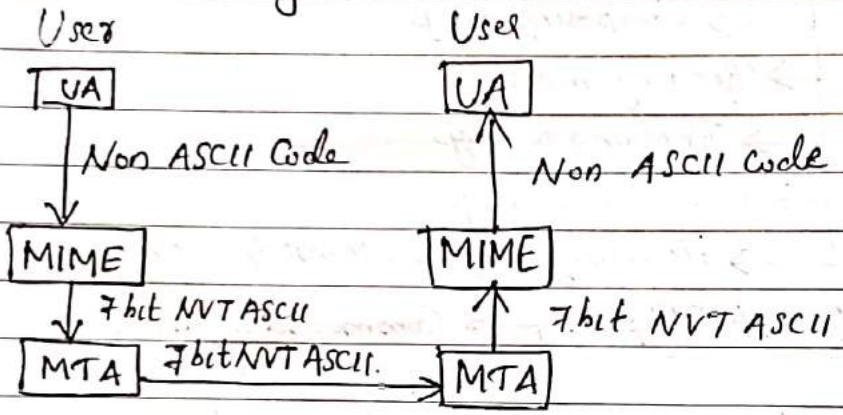
Local part defines the name of a special file called user Mailbox.

Domain Name:

* Mailing List:

Multipurpose Internet Mail Extensions (MIME)

MIME is a supplementary protocol that allows non-ASCII data to be sent through e-mail. MIME transforms non-ASCII data at the sender site to NVT ASCII data & delivers them to the client MTA to be sent through the Internet. The msg at the receiving side is transformed back to the original data.



Transformation Parameters:

1. MIME Version 2. Content-Type 3. Content Transfer Encoding 4. Content-Id 5. Content_Description.

Email Header
MIME-Version: 1.1
Content-Type: type/subtype
Content: Transfer Encoding
ContentId: Msg Id
Content: Description: textual explanation

MIME Version: version of MIME used..

Content Type: the type of data used in the body of the msg. The content type & content subtype are separated by a slash. (Table 26.5 Forouzan)

Content-Transfer Encoding: This header defines the method used to encode the msgs into 0s & 1s for transport.

Content-Transfer-Encoding: <type>
(See Table 26.6 for values)

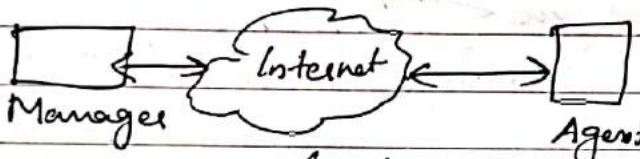
Content Id: uniquely identifies the whole msg in a multiple msg envt.

Content-Id: id = <content-id>

Content Description: whether body is image, audio or video.

Simple Network Management Protocol (SNMP)

is framework for managing devices in an internet using the TCP/IP protocol suite. It uses the concept of mngr & agent.

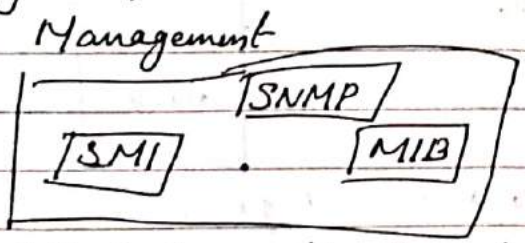


- is an application level protocol in which a few mngr stations ctrl a set of agents.

Manager - A mgmt station is called manager, is a host that runs the SNMP client programs. A managed station is called an agent, is a router that runs the SNMP server programs.

Management Components:

SNMP uses 2 protocols: Structure of Mgmt Information & Mgmt Information Base.



SNMP defines the format of the pkt to be sent from a mngr to an agent vice versa.

SMI - defines rules for naming objts, objt types & showing how to encode objects & values.

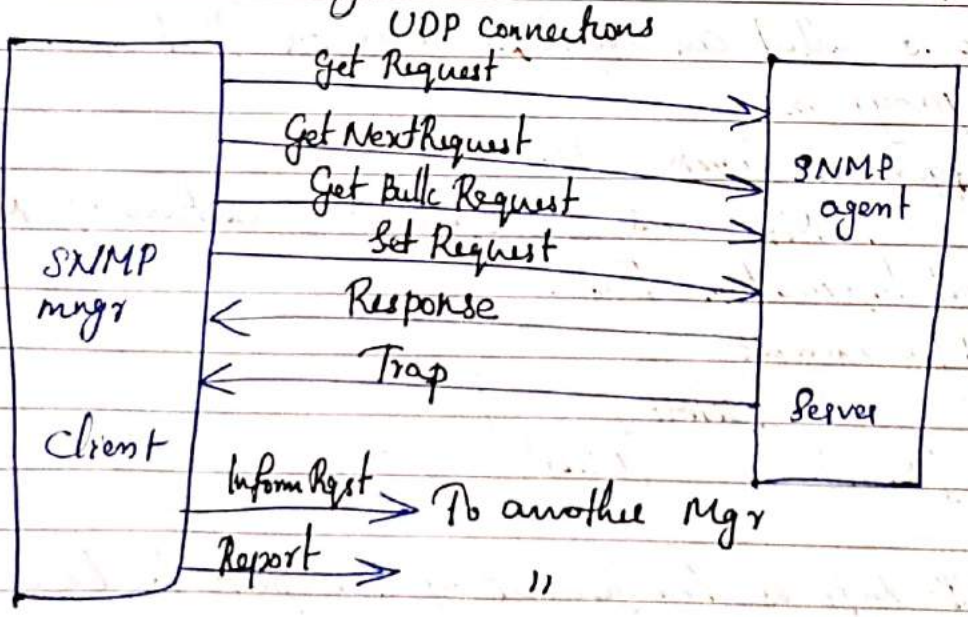
MIB: creates a collection of named objects, their types & their relationships to each other in an entity to be mnged.
Structure of Mgmt Information.

→ Name objects
→ define the type of data that can be stored in an object.
→ How to encode data for transmn over the n/w.

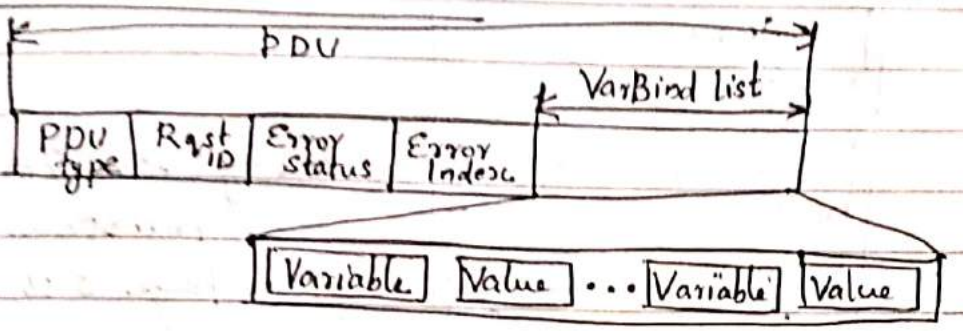
Object Attributes
→ Name – Identifies
→ Type < simple / structured < sequence / sequence of datatypes.
→ Encoding Method – Basic Encoding Rules.

SNMP uses both SMI & MIB in Internet n/w mgmt.

PDUs – 8 types



SNMP PDU format:



Differences: Error status & error index values are zeroes for all rqst msgs except GetBulkRequest.

Error status field is replaced by nonrepeaters field & error index field is replaced by max-repetitions field in GetBulkRequest.

* Request ID: It Sequence No used by the mngr in a rqst PDU & repeated by the agent in a response.

* Error Status: This is an integer to show types of errors reported by the agent.

* Nonrepeaters: This field is used only in GetBulkRequest & replaces the error status field.

* Max-repetition: This field is also used only in GetBulkRqst & replaces the error index field.

* Error index: The error index is an offset that tells the mngr which variable caused the error.

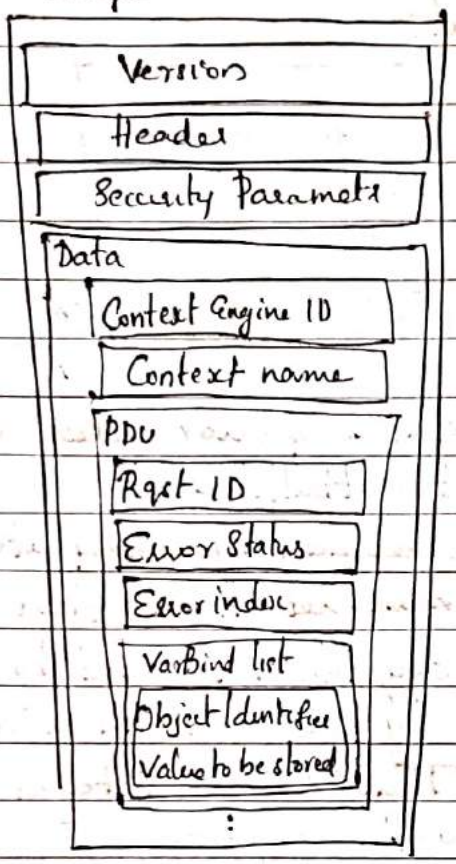
* VarBind list: This is a set of variables with corresponding values the mngr wants to retrieve or set.

* The values are null in GetRequest and GetNextRqst.

SNMP Message.

SNMP doesn't send only a PDU, it embeds the PDU in a msg. A msg in SNMPv3 is made of 4 elmts: version, header, security parameters & data. The version defines the current version (3). The header contains values for msg identification, max msg size, msg flag & a security msg model. The msg security parameter is used to create a msg digest.

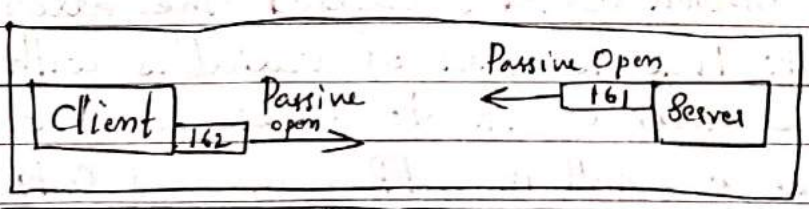
Message:



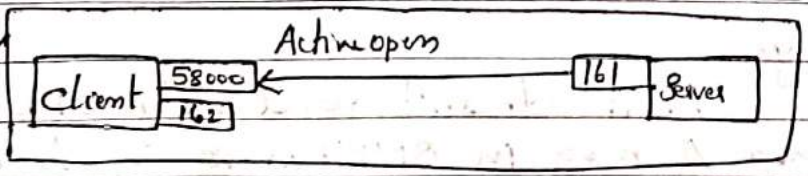
For eg: see 28.23 Forouzan Page 895.

UDP Ports

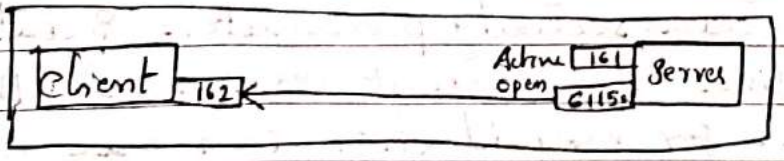
SNMP uses the services of UDP on two well known ports, 161 & 162. The well known port 161 is used by the server (agent), and the well known port 162 is used by the client (manager).



Passive open by both client & server



Exchange of rqst & response msgs

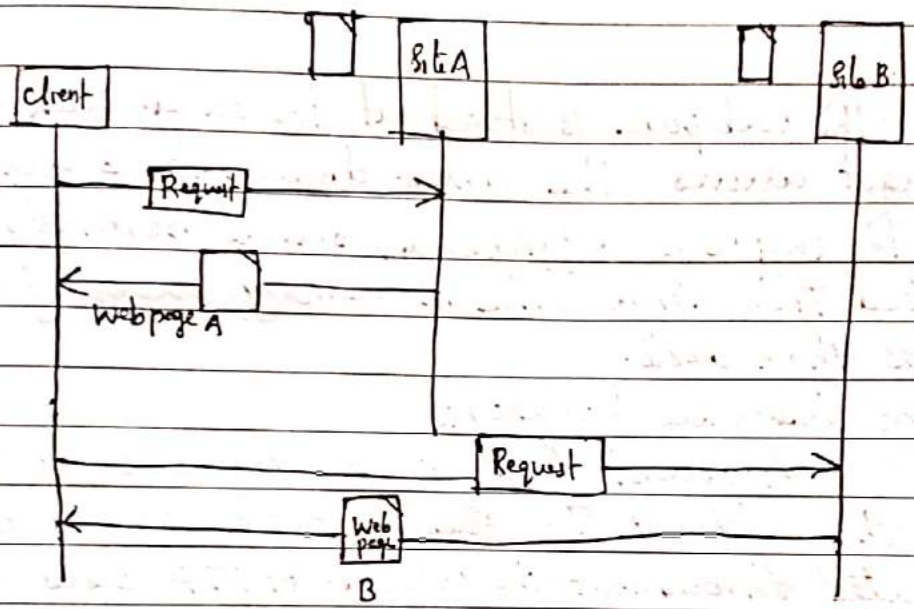


Server sends trap msg.

Introduction to WWW (World wide web)

WWW is a repository of information linked together from points all over the world.

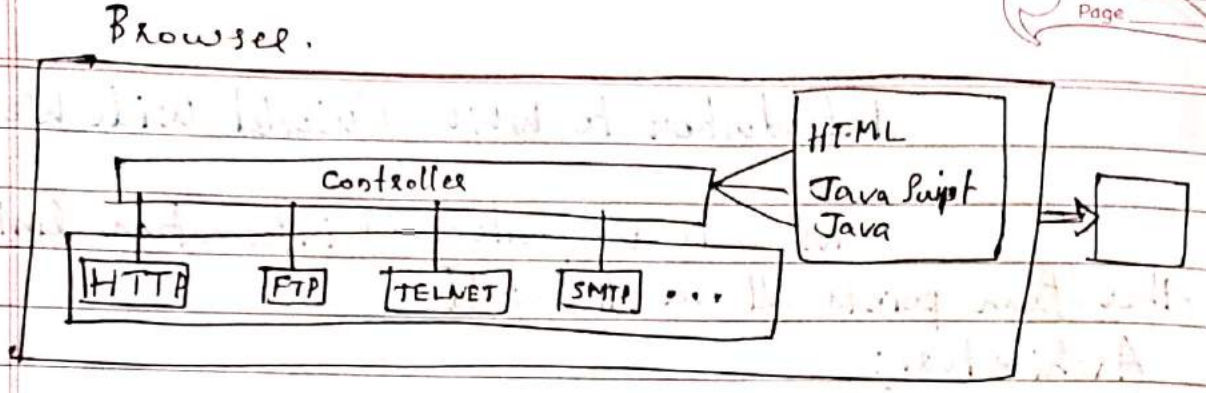
Architecture:



Each site holds one or more documents, referred to as web pages. Each web page can contain a link to other pages in the same site or at other sites. The pages can be retrieved & viewed by using browsers.

Client:

A variety of vendors offer commercial browsers that interpret & display a web document & all use nearly the same architecture. Each browser usually consists of 3 parts: a controller, client protocol, & interpreter. The controller recieves i/p from the keyboard or the mouse, and uses client pgms to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of the protocols such as FTP or HTTP. The interpreter can be HTML, Java, or JavaScript depending on the document type.



Server:

The web page is stored at the server. Each time a client rqst arrives, the corres. document is sent to the client. To improve efficiency, servers normally store requested files in a cache in memory; memory is faster to access than disk.

Uniform Resource Locator:

A client that wants to access a Web page needs the address. To facilitate the access of docums distributed throughout the world. HTTP uses locators. The URL is a standard for specifying any kind of inf^n on the Internet.

Protocol://Host:port:/Path.

The protocol is the client/server pgm used to retrieve the document. Many deff. protocols can retrieve a document.

Eg: HTTP.

The host is the computer on which the inf^n is located, although the name of the computer can be an alias.

Port: optional.

Path is the path name of the file where the inf^n is located.

Cookies:

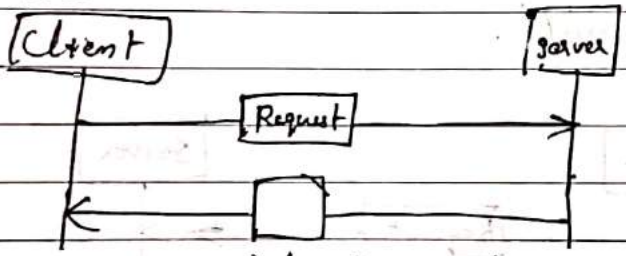
. When a server receives a rqst from a client, it stores inf^n about the client in a file or a string. The inf^n may include the domain name of the

client, the conts. of the cookie, a timestamp & other inf^n depending on the implementation.
The server includes the cookie in the response that it sends to the client.
When the client receives the response, the browser stores the cookie in the cookie directory, which is sorted by the domain server name.

Web Documents

—grouped into 3 categories
- Static
- Dynamic
- Active.

Static Documents: are fixed-cont. documents that are created & stored in a server. The client can get only a copy of the document.



Static HTML document.

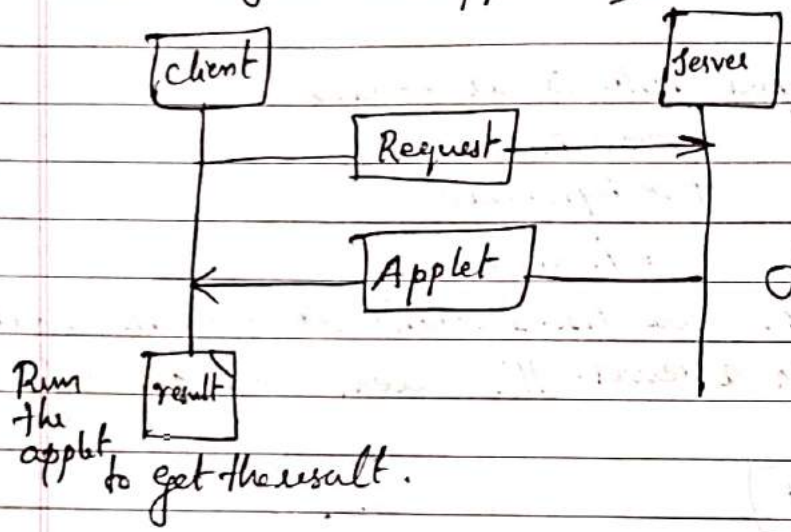
HTML: Hypertext Markup Language: is a lang. for creating Web pages. — Tags.

Dynamic Documents: created by a Web server whenever a browser requests the document. When a rqst arrives, the Web server runs an appl^n pgm or a script that creates the dynamic document. The server returns the output of the pgm or script as a response to the browser that rqsted the document.

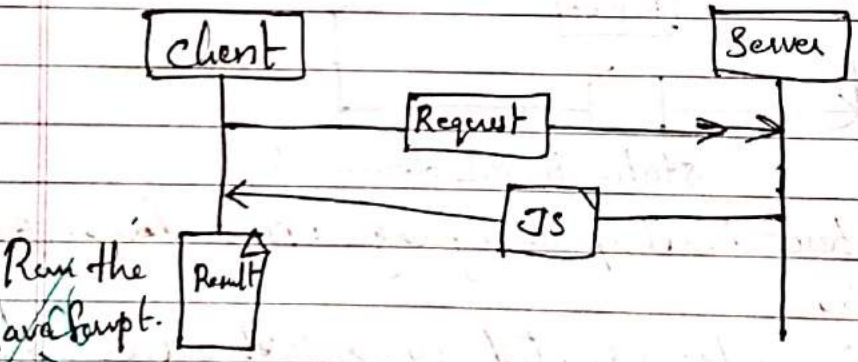
Common Gateway Interface (CGI): creates & handles dynamic documents. CGI is a set of standards that defines how a dynamic document is written, how data are i/p to the pgm & how the o/p result is used.

Technologies involved in creating dynamic documents using scripts: PHP (Hypertext Preprocessor), Java Server Pages (JSP), Active Server Pages (ASP).

Active Documents: A pgm or a script to be run at the client site. These are called Active documents.
Eg: Java applets., JavaScript.



Active document using Java applet.



16/11

"ALL THE BEST"

CONTENT BEYOND SYLLSBUS

Cellular networks

A **cellular network** or **mobile network** is a communication network where the last link is wireless. The network is distributed over land areas called "**cells**", each served by at least one fixed-location transceiver, but more normally, three cell sites or base transceiver stations. These base stations provide the cell with the network coverage which can be used for transmission of voice, data, and other types of content. A cell typically uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed service quality within each cell.

When joined together, these cells provide radio coverage over a wide geographic area. This enables numerous portable transceivers (e.g., mobile phones, tablets and laptops equipped with mobile broadband modems, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

Cellular networks offer a number of desirable features:

- More capacity than a single large transmitter, since the same frequency can be used for multiple links as long as they are in different cells
- Mobile devices use less power than with a single transmitter or satellite since the cell towers are close
- Larger coverage area than a single terrestrial transmitter, since additional cell towers can be added indefinitely and are not limited by the horizon

Major telecommunications providers have deployed voice and data cellular networks over most of the inhabited land area of Earth. This allows mobile phones and mobile computing devices to be connected to the public switched telephone network and public Internet. Private cellular networks can be used for research[3] or for large organizations and fleets, such as dispatch for local public safety agencies or a taxicab company.

Structure of the mobile phone cellular network

A simple view of the cellular mobile-radio network consists of the following:

- A network of radio base stations forming the base station subsystem.

- The core circuit switched network for handling voice calls and text
- A packet switched network for handling mobile data
- The public switched telephone network to connect subscribers to the wider telephony network

This network is the foundation of the GSM system network. There are many functions that are performed by this network in order to make sure customers get the desired service including mobility management, registration, call set-up, and handover.

Any phone connects to the network via an RBS (Radio Base Station) at a corner of the corresponding cell which in turn connects to the Mobile switching center (MSC). The MSC provides a connection to the public switched telephone network (PSTN). The link from a phone to the RBS is called an *uplink* while the other way is termed *downlink*.

Radio channels effectively use the transmission medium through the use of the following multiplexing and access schemes: frequency division multiple access (FDMA), time division multiple access (TDMA), code division multiple access (CDMA), and space division multiple access (SDMA).

Cellular frequency choice in mobile phone networks

The effect of frequency on cell coverage means that different frequencies serve better for different uses. Low frequencies, such as 450 MHz NMT, serve very well for countryside coverage. GSM 900 (900 MHz) is a suitable solution for light urban coverage. GSM 1800 (1.8 GHz) starts to be limited by structural walls. UMTS, at 2.1 GHz is quite similar in coverage to GSM 1800.

Higher frequencies are a disadvantage when it comes to coverage, but it is a decided advantage when it comes to capacity. Picocells, covering e.g. one floor of a building, become possible, and the same frequency can be used for cells which are practically neighbors.

Cell service area may also vary due to interference from transmitting systems, both within and around that cell. This is true especially in CDMA based systems. The receiver requires a certain signal-to-noise ratio, and the transmitter should not send with too high transmission power in view to not cause interference with other transmitters. As the receiver moves away

from the transmitter, the power received decreases, so the power control algorithm of the transmitter increases the power it transmits to restore the level of received power. As the interference (noise) rises above the received power from the transmitter, and the power of the transmitter cannot be increased anymore, the signal becomes corrupted and eventually unusable. In CDMA-based systems, the effect of interference from other mobile transmitters in the same cell on coverage area is very marked and has a special name, *cell breathing*.

One can see examples of cell coverage by studying some of the coverage maps provided by real operators on their web sites or by looking at independently crowdsourced maps such as OpenSignal or CellMapper. In certain cases they may mark the site of the transmitter, in others, it can be calculated by working out the point of strongest coverage.

A cellular repeater is used to extend cell coverage into larger areas. They range from wideband repeaters for consumer use in homes and offices to smart or digital repeaters for industrial needs.

Multimedia Networking

Multimedia is a form of communication that combines different content forms such as text, audio, images, animations, or video into a single presentation, in contrast to traditional mass media, such as printed material or audio recordings. Popular examples of multimedia include video podcasts, audio slideshows and Animated videos.

Multimedia can be recorded for playback on computers, laptops, smartphones, and other electronic devices, either on demand or in real time (streaming). In the early years of multimedia, the term "rich media" was synonymous with interactive multimedia. Over time, hypermedia extensions brought multimedia to the World Wide Web.

Multimedia presentations may be viewed by person on stage, projected, transmitted, or played locally with a media player. A broadcast may be a live or recorded multimedia presentation. Broadcasts and recordings can be either analog or digital electronic media technology. Digital online multimedia may be downloaded or streamed. Streaming multimedia may be live or on-demand.

Multimedia games and simulations may be used in a physical environment with special effects, with multiple users in an online network, or locally with an offline computer, game system, or simulator.

The various formats of technological or digital multimedia may be intended to enhance the users' experience, for example to make it easier and faster to convey information. Or in entertainment or art, to transcend everyday experience.

A lasershow is a live multimedia performance.

Enhanced levels of interactivity are made possible by combining multiple forms of media content. Online multimedia is increasingly becoming object-oriented and data-driven, enabling

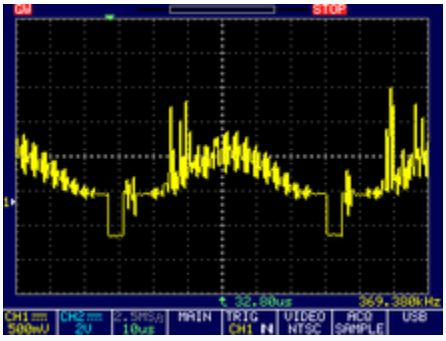
applications with collaborative end-user innovation and personalization on multiple forms of content over time. Examples of these range from multiple forms of content on Web sites like photo galleries with both images (pictures) and title (text) user-updated, to simulations whose co-efficients, events, illustrations, animations or videos are modifiable, allowing the multimedia "experience" to be altered without reprogramming. In addition to seeing and hearing, haptic technology enables virtual objects to be felt. Emerging technology involving illusions of taste and smell may also enhance the multimedia experience.

Video standards, quality and adaptations

Video is an electronic medium for the recording, copying, playback, broadcasting, and display of moving visual media.[1] Video was first developed for mechanical television systems, which were quickly replaced by cathode ray tube (CRT) systems which were later replaced by flat panel displays of several types.

Video systems vary in display resolution, aspect ratio, refresh rate, color capabilities and other qualities. Analog and digital variants exist and can be carried on a variety of media, including radio broadcast, magnetic tape, optical discs, computer files, and network streaming.

Analog video



Analog video signal from a Sony PlayStation

Video technology was first developed for mechanical television systems, which were quickly replaced by cathode ray tube (CRT) television systems, but several new technologies for

video display devices have since been invented. Video was originally exclusively a live technology. Charles Ginsburg led an Ampex research team developing one of the first practical video tape recorder (VTR). In 1951 the first VTR captured live images from television cameras by writing the camera's electrical signal onto magnetic videotape.

Video recorders were sold for US$50,000 in 1956, and videotapes cost US$300 per one-hour reel.[2] However, prices gradually dropped over the years; in 1971, Sony began selling videocassette recorder (VCR) decks and tapes into the consumer market.[3]

Digital video

The use of digital techniques in video created digital video. It could not initially compete with analog video, due to early digital uncompressed video requiring impractically high bitrates. Practical digital video was made possible with discrete cosine transform (DCT) coding,[4] a lossy compression process developed in the early 1970s.[5][6][7] DCT coding was adapted into motion-compensated DCT video compression in the late 1980s, starting with H.261,[4] the first practical digital video coding standard.[8]

Digital video was later capable of higher quality and, eventually, much lower cost than earlier analog technology. After the invention of the DVD in 1997, and later the Blu-ray Disc in 2006, sales of videotape and recording equipment plummeted. Advances in computer technology allows even inexpensive personal computers and smartphones to capture, store, edit and transmit digital video, further reducing the cost of video production, allowing program-makers and broadcasters to move to tapeless production. The advent of digital broadcasting and the subsequent digital television transition is in the process of relegating analog video to the status of a legacy technology in most parts of the world. As of 2015, with the increasing use of high-resolution video cameras with improved dynamic range and color gamuts, and high-dynamic-range digital intermediate data formats with improved color depth, modern digital video technology is converging with digital film technology.