"Heaven's Light is Our Guide"

RAJSHAHI UNIVERSITY OF ENGINEERING & TECHNOLOGY

RUET

Name : Md. Ismail AMH sir

Subject : CSE-3205 (Computer Networks) Year : ○1st ○2nd ✓3rd ○4th

Roll No : 1503094 Semester ○1st ○2nd ○3rd ○4th ○5th ○6th ○7th ○8th

Department CE EEE ME CSE ✓ ETE IPE URP GCE MTU ARCH

* IP Address
* Introduction
* Network layers
* Switching
* IP Address

CamScanner

IP address

IP addressing:

~~An IP address is unique~~ Unique global address for a network interface. which is 32 bit ~~log~~ long identifier.

Every host and every router on the Internet has an IP address that can be used in the source address and destination address field of IP packets.

Notation:

2 notations are used
→ dotted decimal notation
→ hexadecimal notation

written in the dotted decimal notation

CS CamScanner

Properties of IP address:

→ 32 bit long → broken up into 4 groups, called octet (Set of 8 bits)

→ encodes a network number

→ " a host number

→ written in dotted decimal notation (IPV4)

→ network portion has the same value for all hosts on the single network, such as an Ethernet LAN.

Prefix:

The network portion has the same value for all hosts on a single network, such as an Ethernet.

So network correspond to a contiguous block of IP address space.

This block is called a prefix.

→ identifies a network.

→ indicated by a netmask.

Ocet

- **Host number**: identifies the specific host (actually interface on the network)

network prefix	host number

Example:

- ellington.cs.virginia.edu has

★★ IP

128.143.	137.144

∴ Network Id: 128.143

host number: 137.144

network mask: 255.255.0.0

or ffff0000

* prefix notation: 128.143.137.144/16

Classifull IP Addressing:

32 bit IP address is divided into five sub classes. These are.

→ Class A

→ Class B

→ Class C

→ Class D } reserved for multicast

→ Class E } and " for experimental purposes respectively.

NB: The order of bits in the first octet determine the IP class.

IPV4 divided into 2 parts

→ Network ID

→ Host ID

CamScanner

Something interesting

Class name	Application field	Network ID length	Host ID length	High order bit
A	→ reserved for government → large organization	8	24	0
B	medium companies	16	16	10
C	small companies	24	8	110
D	created to enable multicasting	–	–	1110
E	reserved for experimental purpose	—	—	1111

~~Start and End IP of~~ (11)

Start, End IP and Subnet Mask of each class

Class	high order bits	Start	End	Subnet mask
A	0	0.0.0.0	127.255.255.255	255.0.0.0
B	10	128.0.0.0	191.255.255.255	255.255.0.0
C	110	192.0.0.0	223.255.255.255	255.255.255.0
D	1110	224.0.0.0	239.255.255.255	
E	1111	240.0.0.0	255.255.255.255	

Determination:

Class-A

Start IP:

00000000.00000000.00000000.00000000

= 0.0.0.0

End IP:

01111111.11111111.11111111.11111111

= 127.255.255.255

Class B: Start IP:

10000000.00000000.00000000.00000000

= 128.0.0.0

End IP:

10111111.11111111.11111111.11111111

= 191.255.255.255

Classe:

Start IP:

11000000.00000000.00000000.00000000

= 192.0.0.0

End IP:

11011111.11111111.11111111.11111111

= 223.255.255.255

ClassD

Start IP:

11100000.00000000.00000000.00000000

= 224.0.0.0

End IP:

11101111.11111111.11111111.11111111

= 239.255.255.255

Class-E Start IP:

11110000.00000000.00000000.00000000

= 240.0.0.0

CamScanner

End IP:

11111111.11111111.11111111.11111111

= 255. 255. 255. 255

High Order Bit:

Leftmost 8 bits of IP address.

Number of Networks and Hosts per Network for each class

Address class	first octet range	Number of network	number of hosts/network
A	0 to 127	$128 = 2^7$	$16777214 = 2^{24} - 2$
B	128 to 191	$2^{14} = 16384$	$2^{16} - 2 = 65534$
C	192 to 223	$2^{21} = 2097152$	$2^8 - 2 = 254$
D	224 to 239	NA (multicast)	
E	240 to 255	NA (experimental)	

NB: Net

→ No of network address

$= 2^{(\text{Network length} - \text{length of fixed bit})}$

→ No of host per network

$= 2^{\text{host Id length}} - 2$

→ network address

→ broadcast

Network address:

when all bits of host portion is zero (0)

→ 0

Broadcast address:

when all bits of host portion is one (1)

→ 1

Determination of IP address's class:

→ 227.12.14.87 ⇒ 1st byte is between (224-23 ∴ class D

→ 193.14.56.22 → 1st byte is between (192 223), so class

→ 14.23.120.8 → 1st byte is between (0 to 127), so class A

→ 252.5.15.111 → 1st byte is between (240 to 255) So class E

→ 10.10.5.109 ⇒ class A

→ 197.105.0.25 ⇒ class C

→ 255.255.255.255 ⇒ class E

→ 172.0.0.1 ⇒ class B

CamScanner

ICANN:

Network number is managed by a nonprofit corporation called ICANN to avoid conflict

→ Internet corporation for Assigned Names and Numbers.

Mask:

It is a binary number that gives the network address in the address block when AND operation is bitwise applied on the mask and any IP address of the block.

The default mask in different classes are:

- Class A: 255.0.0.0
- class B: 255.255.0.0
- class C: 255.255.255.0

CamScanner

Determine the network address of 132.6.17.85

Soln:

First byte is in between 128 to 191

So it is an IP address of Class B.

So Network address of given IP is

132.6.0.0

**

Subnetting:

Dividing the large block of address into several sub-blocks/parts for internal use as multiple networks, while still acting like a single network to the ~~outsi~~ outside world. This is called subnetting and networks that result from dividing up a larger network are called subnets.

→ dividing network into seperate networks

→ borrowing bits from the Host portion.

CamScanner

Find the network address of 201.24.67.32. ~~of~~

Solⁿ:

First byte is in range
192 - 223

∴ It is ~~the~~ an IP of class C.

Destination address → 201.24.67.32
Default mask → 255.255.255.0
∴ Network address → 201.24.67.0

Properties of subnetting:

→ ~~IP~~ IP use a 3 layer hierarchy
- → network
- → subnet
- → Host

→ Improves efficiency of IP address ~~as~~ by ~~not consuming an entire~~

→ Reduces router complexity

→ don't consume entire address space for each physical network. So improves efficiency

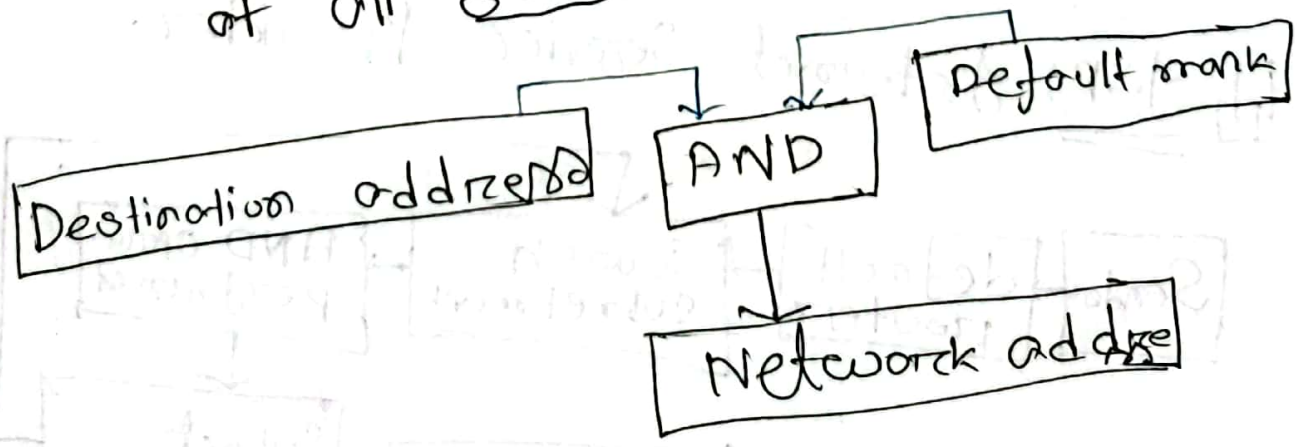
→ External router don't know about subnetting, complexity ~~of~~ of routing tables at external routers is reduces.

Subnet mask:

Routers and hosts use an ~~external~~ extended network prefix to identify the start of the host numbers.

length of the subnet mask need ~~to be~~ not be identical at all subnetworks.

NB



Steps of sending data from Sender to receiver by using subnetmask:

→ packet send from sender

→ packet arrive at default router

→ ~~Search~~

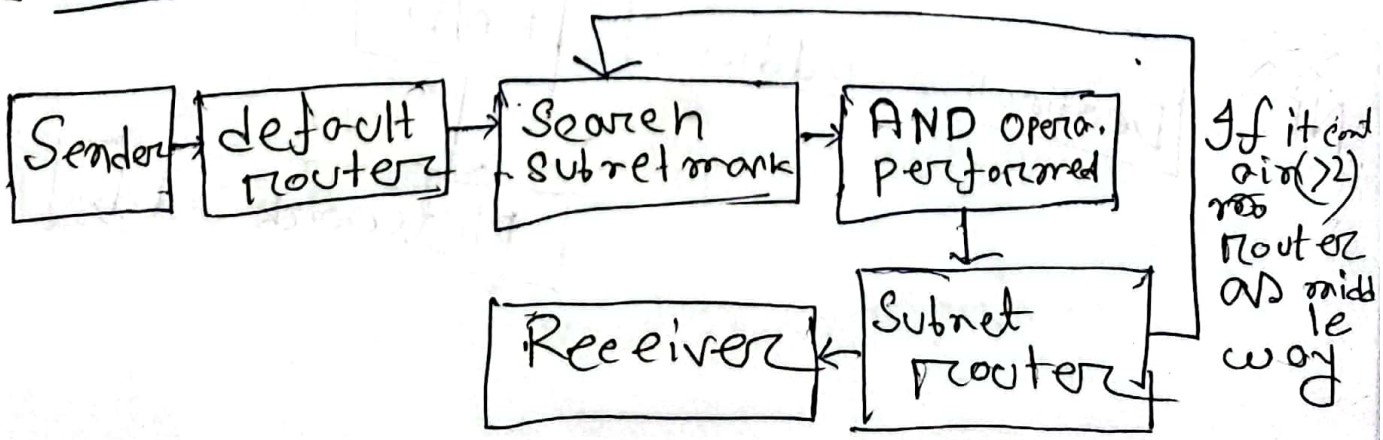
→ router looks at the destination address of packet

→ Check which subnet is belong to.

→ by AND operation router send the packet to the proper subnet network.

→ packet received by receiver.

ISP: Internet Service Provider.



Some important formula/ Calculation in Subnetting :

1. Number of subnets:

Given bit for mask − No of bits in default mask

2

2. Subnet address: AND result of subnet mask and given IP address

or Network address

নেট ঠিকানা

3. Broadcast address: By putting the host bits as 1 and retaining the network bits as in the IP address

Host এর সব bit 1 এবং Network এর bit যেমন ছিল তেমনি

4. Number of hosts per ~~number~~ subnet:

no of host bit $2^{(32-\text{Given bits for mask})}-2$

or, 2^n-2

5. First host ID: Subnet address + 1

6. Last host ID: Subnet address + Number of Hosts.

CamScanner

Classfull IP addressing:

Before 1993 IP addresses were divided into the five categories. This allocation has come to be called classfull addressing

CamScanner

You have 192.168.1.0/24 and want

- 6 subnets.
- Determine Network Address, First address Last address, Broadcast address

Sol^n: we need extra $\left\lceil \frac{\log 6}{\log 2} \right\rceil = 3$ bits

∴ total ~~ne~~ length of subnet $= (24+3) = 27$ bit

Subnet No	Net. Add.	Range	Broadcast Address
0	11000000. 10101000. 00000001. 00000000/27	192.168.1.1 – 192.168.1.30	192.168.1.31
1	11000000. 10101000. 00000001. 00100000/27	192.168.1.33 – 192.168.1.62	192.168.1.63
2	192.168.1. 64/27	192.168.1.65 – 192.164.1.94	192.168.1.95
3	192.168.1 96/27	192.168.1.97 – 192.168.1.125	192.168.1.127

CamScanner

Subnet No	Net. Add	Range	Broad-Add
4	192.168.1.128/27	192.168.1.129-192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161-192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193-192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225-192.168.1.254	192.168.1.255

For A company has 201.70.69.0/24 as site address, needs 6 subnets. Design subnets.

Sol^n total no of bit in network

$= 24 + \lceil \log 6 / \log 2 \rceil = 24 + 3$
$= 27$

$\therefore$ no of host per subnet

$= 2^{(32-27)} - 2$
$= 2^5 - 2$
$= 32 - 2$
$= 30$

subnet [illegible] Network [illegible] — [illegible] 2 [illegible]

Subnet No	Net. Add	Range	Broad. Add
0	201.70.64.0/27	201.70.64.1 – 201.70.64.30	201.70.64.31
1	201.70.64.32/27	201.70.64.33 – 201.70.64.62	201.70.64.63
2	201.70.64.64/27	201.70.64.65 – 201.70.64.94	201.70.64.95
3	201.70.64.96/27	201.70.964.97 – 201.70.64.128	201.70.64.127
4	201.70.64.128/27	201.70.64.129 – 201.70.64.158	201.70.64.159
5	201.70.64.160/27	201.70.64.161 – 201.70.64.190	201.70.64.191
6	201.70.64.192/27	201.70.64.193 – 201.70.64.222	201.70.64.223
7	201.70.64.224/27	201.70.64.225 – 201.70.64.254	201.70.64.255

defined [illegible] bit. Subnet [illegible] 3 bit. So, Extra 3 bit [illegible] Combination [illegible] Network [illegible]

[illegible] host [illegible]

A company is granted the site address 181.56.0.0 (class B), needs 1000 subnets.

Design subnet.

Soln:

∴ No of bits in network

$= 16 + \lceil \log 1000 / \log 2 \rceil$

$= 16 + 10$

$= 26$

∴ Hosts per subnet $= \log_2^{32-26} - 2$

$= \log_2^{6} - 2$

$= 62$

∴ Subnet Mask is 11111111.11111111.11111111.11000000

$= 255.255.255.192$

181.56.0.0 ← Apply subnet mask — 181.56.0.63

1st subnet

181.56.255.128 ← Apply subnet mask — 181.56.255.191

1023th subnet

Subtract 1

181.56.255.192 ← Apply subnet mask — 181.56.255.255

1024th subnet

Q. We have 170.170.0.0 as an IP address and need 512 subnets. Find all information about 100th subnet.

Soln:

As first octet is 128-191

So it is a class B IP address.

We need extra $\left\lceil \frac{\log 512}{\log 2} \right\rceil$ bits

$= 9$ bit

∴ Information of 100th subnet,

Network address

(100 - 1) = 99 এর binary value 25 No. এর পরের Left to right এর অংশের সব address এর হবে

~~170.170.99.00000000~~ /25

170.170.01100001.10000000/25 = 170.170.99.128/25

First address

~~170.170.99.1/25~~

= 170.170.99.129/25

Last address

~~170.170.99.126/25~~

= 170.170.99.254/25

Broadcast address

~~170.170.99.127/25~~

170.170.99.255/25

64/2 = 32
32/2 = 16
16/2 = 8
8/2 = 4
4/2 = 2
2/2 = 1
2^6/2 = 10

32 16 8 4 2 1
1 1 1 1 1 1 1 0 1

010019

2^7 128

0 127

32 16 8 4 2 1
0 1 1 1 0 1
0 1 0 0 1 1

☆☆☆

170.160.0.0 is an IP address.

Create subnet in such a way that each subnet can connect maximum 1022 PCs.

Find out the followings.

1. How many subnet can you create?
2. Subnet mask = ?
3. 20th subnetwork address?
4. 20th broadcast address = ?
5. 30th subnetwork 15th PC address?
6. 60th subnet range = ?

Sol^n: Number of bit in host portion

$$= \left\lceil \frac{\log 1022}{\log 2} \right\rceil$$

$$= 10$$

∴ Number of bit in network portion $= 32 - 10$

$= 22$

CamScanner

∴ Number of bit for subneting $= 22 - 16$
$= 6$

1. Number of subnet $= 2^6$
$= 64$ Ans

2. Subnet mask,

11111111.11111111.11111100.00000000

$= 255.255.252.0/22$

3.

32 16 8 4 2 1
0 1 0 0 1 1

20th subnetnetwork address,

$= 170.160.76.0/22$

4. 20th broadcast address.

$= 10101010.10100000.01001111.11111111$

$= 170.160.79.255/25$

5. 30th subnetnetwork address.

10101010.10100000.01110100.00000000

$= 170.160.116.0/22$

∴ 30th subnetnetwork 15th PC address

$= 170.160.160.15/22$

~~Network~~

Introduction

Computer network:

If a large number of computer devices and other computing hardware devices that are linked together through communication channel to facilitate communication and resource-sharing among wide range of users is called computer network.

A Network or computer network is a set of devices capable of communication.

A device is called hopt (core and sys ...)

& A " " connecting device

- router (Network ↔ Network)
- switch (device ↔ devices)
- modem changes the form of data (modulator – demodulator)

- computer,
- desktop
- laptop
- workstation
- cellular phone
- security system

Network criteria:

Must be able to meet.

most important is 3

1. Performance:

2. reliability:

3. Security:

Performance:

→ measured by in many ways including transit time and response time

→ evaluated by two networking metrics
- → throughput
- → delay

reliability:

→ measured by the frequency of failure.

CamScanner

→ time it takes to recover from a failure.

→ the network's robustness

Security: include → protecting data from unauthorized access

→ protecting data from damage and development

→ implementing policies and procedures

Link: A connections pathway that transfers data from one device to another.

2 types

1. point-to-point
2. multipoint.

CamScanner

- **Point-to point:** provides a dedicated link between two devices

Example:

When we change tv channels by infrared remote control, we are establishing a point-to point connection between the remote control and the tv control system.

- **Multipoint/multidrop:** One in which more than two specific devices share a single link.

* The capacity of the channel is shared, either spatially or temporally.

CS CamScanner

Introduction

Physical topology:

→ geometric representation of the relationship

refers to the way in which a network is laid out physically.

Classification

A basic topology

→ mesh

→ star

→ bus

→ ring

→ hybrid } complex

→ tree

CamScanner

Mesh topology:

every device has a dedicated point-to-point link to every other device.

The term dedicated means that the link carries traffic only between the two devices it connects.

For n device we need $n(n-1)/2$ duplex mode link.

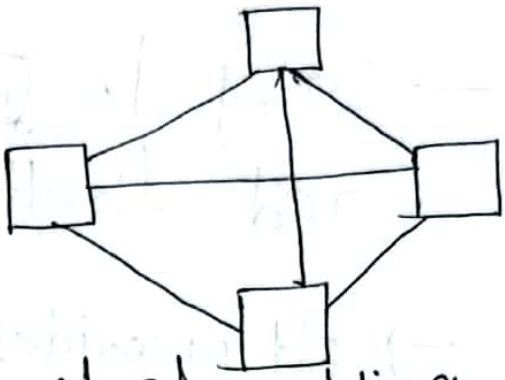
Advantages:

→ A mesh topology is robust. If only one link become unusable, it does not incapacitate / affect the entire system

→ has advantages of privacy and security.

CamScanner

→ It taken few time to send data from one station to another.



Disadvantages:

→ large amount of cabling

→ large number of I/O ports

Use telephone regional office.

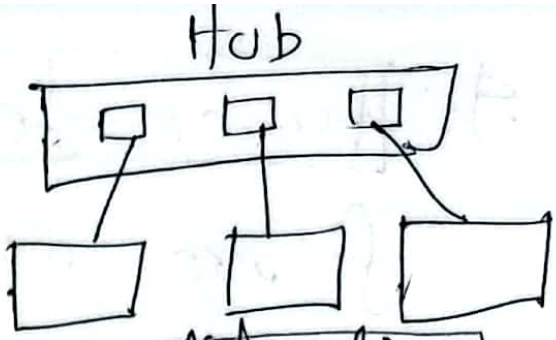
Star topology:

Each device has a dedicated point-to-point link only to a central controller, usually called hub.

→ Number of cable/links = n

→ device are not directly connected to each other.

CamScanner



Advantages:

→ Easy to fault identification and fault isolation

→ It provides robustness. If one link fails only that link is affected

→ less cable than a mesh

Disadvantages:

→ dependency of the whole topology on one single point, the hub. If hub goes down the whole system is dead.

Use: Used in Local Area Network (LAN)

CamScanner

Bus topology:

A bus topology is one, which is multipoint.

One long cable act as a backbone to link all devices in a network.

→ Number of cable is n+1

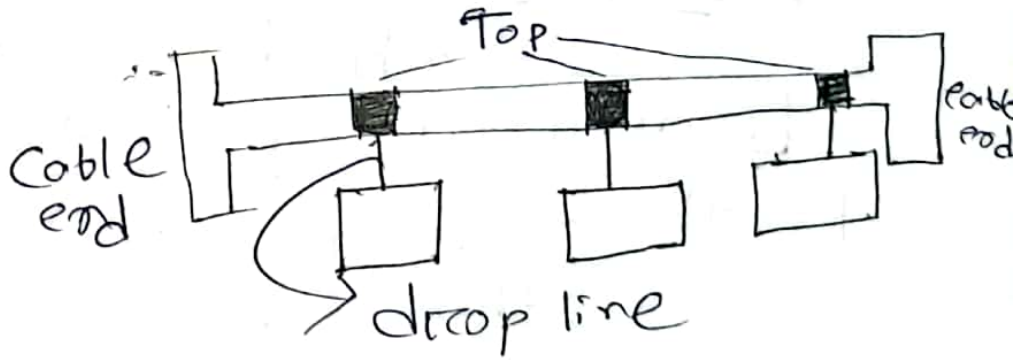
→ Nodes are connected to the bus cable by drop lines and taps.

~~Advantages~~:

Advantages:

→ ease of installation

→ use less cable than star or mesh topology. So cost is very few.



Disadvantages:

→ A fault or break in the bus cable stops all transmission

→ include ~~defoult~~ difficult reconnection and fault in isolation

→ difficult to add new devices.

Use: early local area network, traditional ~~et~~ Ethernet LANs

~~Ring topog~~

Ring topology:

Each devices has a dedicated point-to-point connection with only the two devices on either side of it.

CamScanner

→ Signal is passed along the ring in one direction.

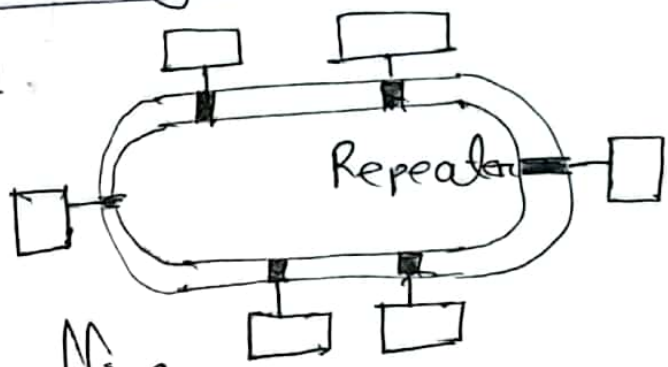
→ each devices in the ring incorporates a repeater (পরিবর্তন করা)

→ number of cable n-1

Advantages:

→ ease to install and reconfigure

→ to add or delete a device requires changing only two connections.



Disadvantages:

→ Unidirectional traffic

→ A break in the ring can disable the entire network.

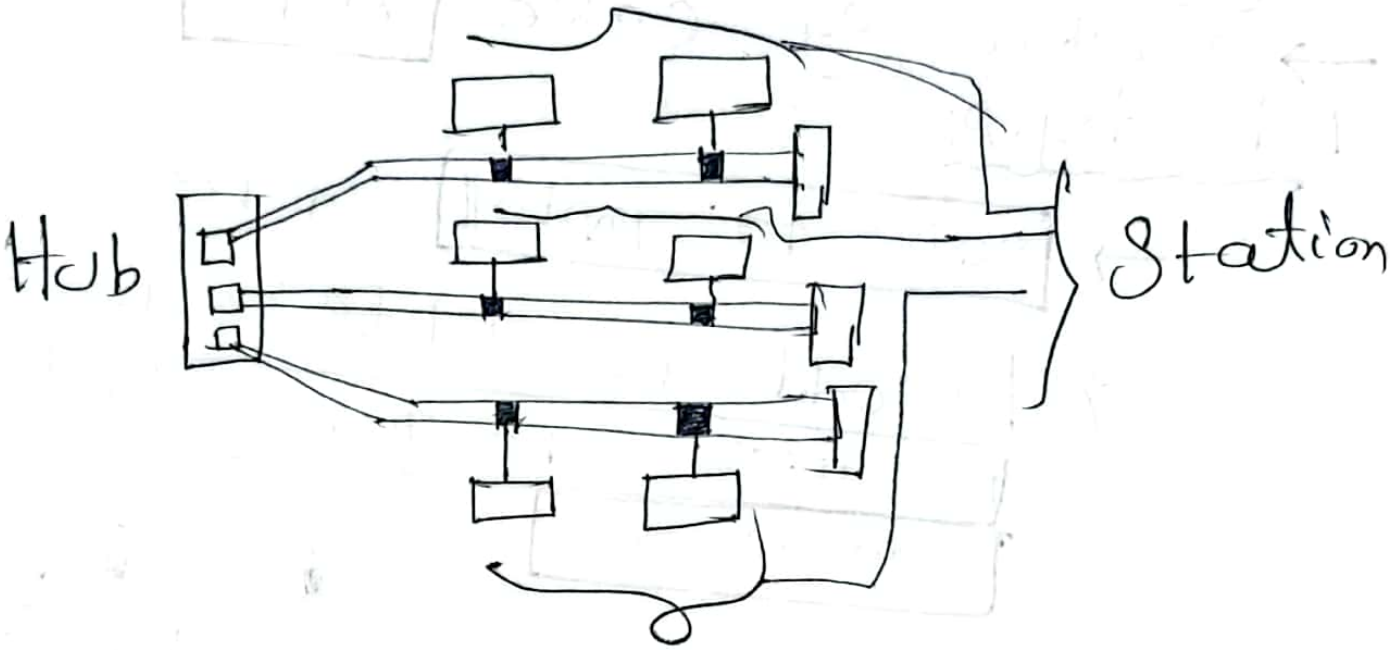
Use: Token ring network.

CamScanner

~~Class~~

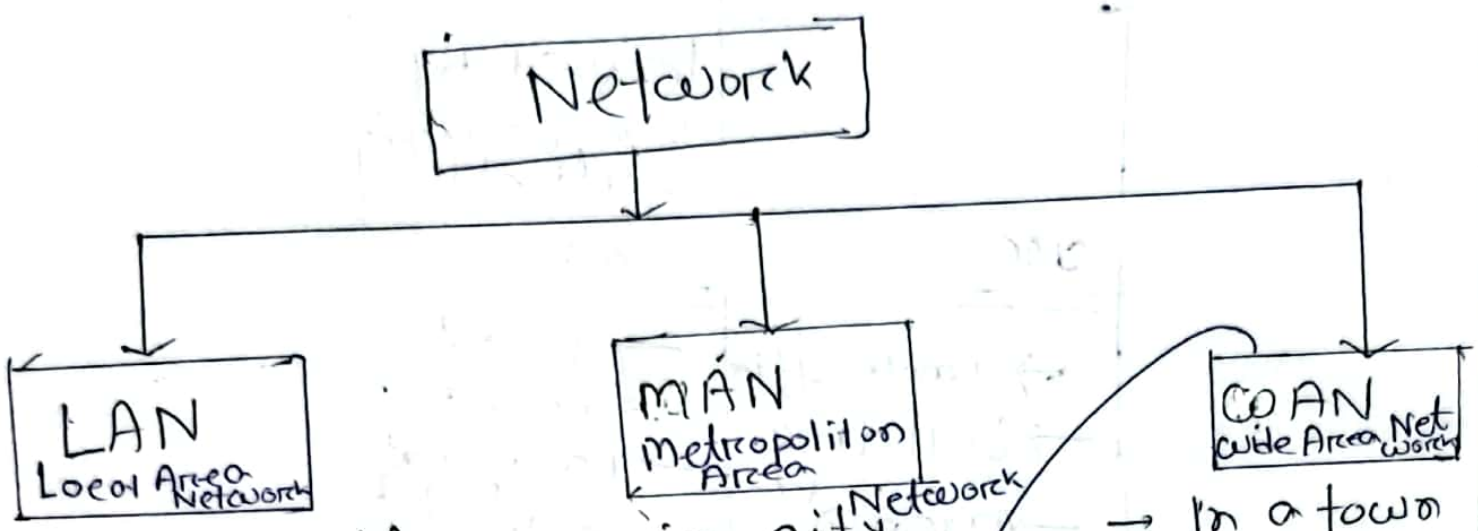
Hybrid network:

A star backbone with bus network



CamScanner

Classification of network:



use: → Single office
→ building
→ campus

→ in city
→ in campus

→ in a town
→ in a state
→ in a country
→ in the world

2 types → Point-to-point → network that connects 2 communicating devices through a transmission media

→ Switched → network with more than two ends

LAN VS WAN

LAN	WAN
→ LAN interconnects hosts	→ WAN interconnects connecting devices → Switch, → Router, → modem
→ Privately owned by the organization	→ Run by communication company and

LAN	WAN
	leased by an organization
use	use:
→ Simple office → building → campus	→ in a town → in a state → in a country → in the world

★ PAN: Personal Area Network.

☐ Internetwork:

When two or more networks are connected, they make an internetwork or internet.

☐ Switching:

An internet is a switched network in which a switch connects at least two links together

CamScanner

Classification

2 types

→ circuit-switched network

→ packet-switched network

→ a dedicated connection, called a circuit is always available between two end systems.

→ communication between the two end is done in blocks of data called packet.

A router in a packet switched network has a queue that can store and forward the packet

Internet: The most notable internet is called the Internet, and is [illegible] of thousands of

interconnected network.

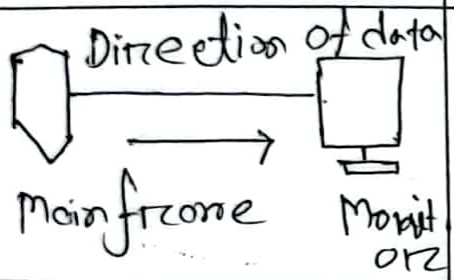
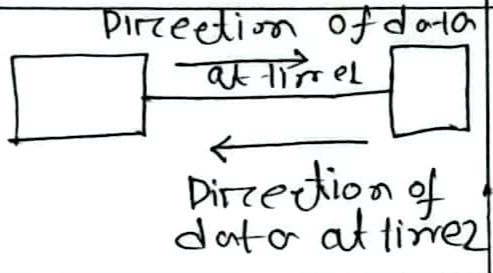
Data flow:

Communication between 2 devices can be

→ Simplex 3 types
→ half-Duplex
→ Duplex

Simplex	half-duplex	duplex
→ Communication is unidirectional, as on a one way Street.	→ Communication is bidirectional, not at a time	→ communication is bidirectional at a time
→ Only 1 of the 2 devices on a link can transmit, the other can only receive	→ each station can both transmit and receive, but not at the same time	→ both station can transmit and receive simultaneously

CamScanner

Simplex	half duplex	duplex
Example: keyboards, traditional monitors.	Ex: → walki-talkies → CB (citizens band)	Ex: telephone network
		
→ can use the entire capacity of the channel	→ used when, no need of communication in both directions at the same time	→ used when communication of the both in directions is required

CamScanner

** Connecting Devices / Networking devices

Connecting device:

Devices that used to connect host together to make a network or to connect networks together to make an internet.

→ can operate in different layers of internet model.

Types of connecting device:

	Operates in
→ Hub	physical layer
→ Switch	physical layer / data link layer
→ Router	physical / data link / Network
→ Bridge	data link layer
→ Gateway	

→ Repeater physical layer

→ managed → processes through pg
→ unmanaged → can be managed po from remote

Hub :

Hub sends data to all outgoing except one who send it.

★ frame is broadcast.

Repeater:

Received a signal and before it become too weak or corrupted regenerate and restores the original bit pattern.

★ They do not amplify the the signal.

~~Types of~~

Characteristics of Hub/Repeater

→ have no filtering capability

→ hub /repeater is a physical layer device

→ don't have link layer address

→ don't check link layer address

frame arrive at a switch

→ examine the destination address

→ forward the frame ~~to~~ out the necessary connection

Switch: link layer switch:

→ operates ~~on~~ in both physical layer and data link layer.

→ as a physical layer device it regenerates the signal it received

→ as a link layer device, it ~~can~~ can check the MAC address

→ Source and destination

Filtering:

→ it has filtering capability.

→ It has a table store port no and address from whom receives data packet.

→ doesn't change the link layer (MAC) addresses in a frame.

Transparent Switch:

~~Sto~~ Switch, in which the stations are completely unaware of the switch's existance

A system equipped with transparent switches must meet three criteria:

→ frames must be forwarded from one station to another

CamScanner

→ Forwarding table is automatically made by learning frame movements in the network.

→ Loop in the system must be prevented.

Router:

It is a three-layer device

it operates in physical layer, data link layer, network layer

as a physical layer

it regenerate the signal it receive

as a data link layer

it check the physical addresses (source & destination)

as a network layer

check the network layer addresses.

CamScanner

Router vs repeator/ Switch

Router	repeater/Switch
→ has physical & logical (IP) address for each of its interfaces	→ repeater doesn't have physical or logical or any address → but switch has MAC
→ router changes the link layer address	→ Switch doesn't change the link layer address
→ act only on those packets, in which link layer destination address matches the address of the interface.	

Gateway :

→ also called protocol converter

→ can operate at any network layer

→ It is a passage to connect two networks together that may work upon different networking models.

→ work as the messenger against

→ take data from a system, interpret it and transfer it to another

→ not produce any data, rather they transfer data between ending device.

CS CamScanner

Bridge:

→ to connect two closely similar LAN
→ to connect two similar LAN
→ CSMA/CD LAN.
→ token ring LAN

→ It is ~~also~~ used for interconnecting two LANS working on the same protocol

→ has single input port &
" output "

→ it is a 2 port device

→ It is a repeater with add on functionality of filtering content by reading the MAC addresses of source & destination.

Types of bridge:

2 types

→ Transparent bridges

→ Source Routing bridges.

NB
→ bridge examines the destination address of a frame → forward frame onto the next lont
→ " " source " → places address in a routing table

Chapter-5
Network layer:

Characteristics of Network layer:

→ lowest layer, deals with end-to-end transmission

→ connected with getting packets from the source all the way to the destination.

→ must know about the topology of the network.

→ choose appropriate path through it.

→ take care to avoid overloading
→ some of the communication lines
→ routers

CamScanner

Network layer

Design issue: (involves → service provided to the transport layer; internal design of the network.)

→ Store and forward packet switching

→ service provided to the transport layer

→ Implementation of connectionless service

→ Implementation of connection oriented "

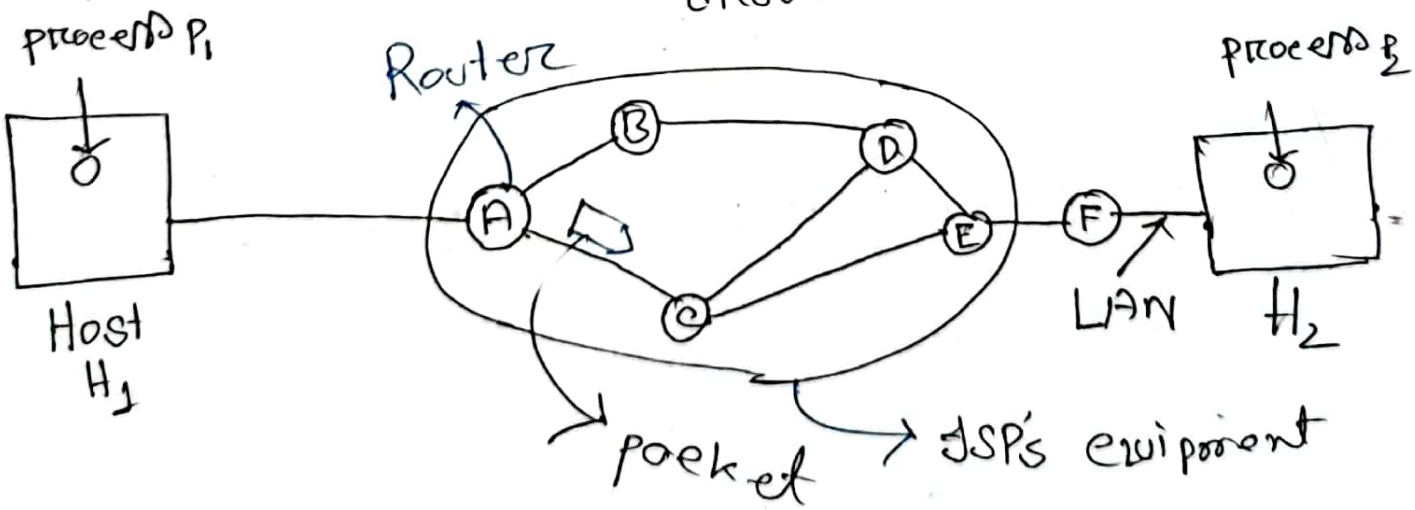
→ Comparison of virtual-circuit and datagram networks.

Store and forward packet switching

or, How network layer protocol operate?

Ans:

The environment of the network layer protocols is ~~given~~ drawn below.



Major components of the network.

→ ISP's equipment → Routers connected by transmission line
Inside the oval

→ customer equipment
(Outside the oval)

→ H_1 is directly connected to ISP's router

→ H_2 is on a LAN. → might be an office ethernet.
↳ operated by customer.

Process:

→ Host send a packet to the nearest router.

→ packet is stored there until it has fully arrived.

→ By verifying the checksum, link has finished its processing

→ ~~fro~~ forwarded to the next router along the path, until it reaches the destination host.

CamScanner

Service provided to the transport layer:

The services need to be carefully designed with the following goals in mind.

1. Services should be independent of router technology

2. Transport layer should be shielded/protect from

   → number
   → type
   → ~~technology~~
   → topology

   } of the routers present

3. network addresses make available to the transport layer,
   should use uniform numbering plan

Classification of services:

2 types

→ connection-less service → data network ~~Sehan, X.25~~, ~~ATM~~, ARPANET

→ connection-oriented "

Example:

→ MPLS (~~multiple~~ multiprotocol Label Switching)

VLAN

IP protocol

data network such as X.25

Implementation of connectionless service:

→ packets are injected into network individually

→ packets are routed independently

→ setup phase is not needed

Datagram: packets are called datagram which is basic transfer unit.

Datagram network: Network is called datagram network.

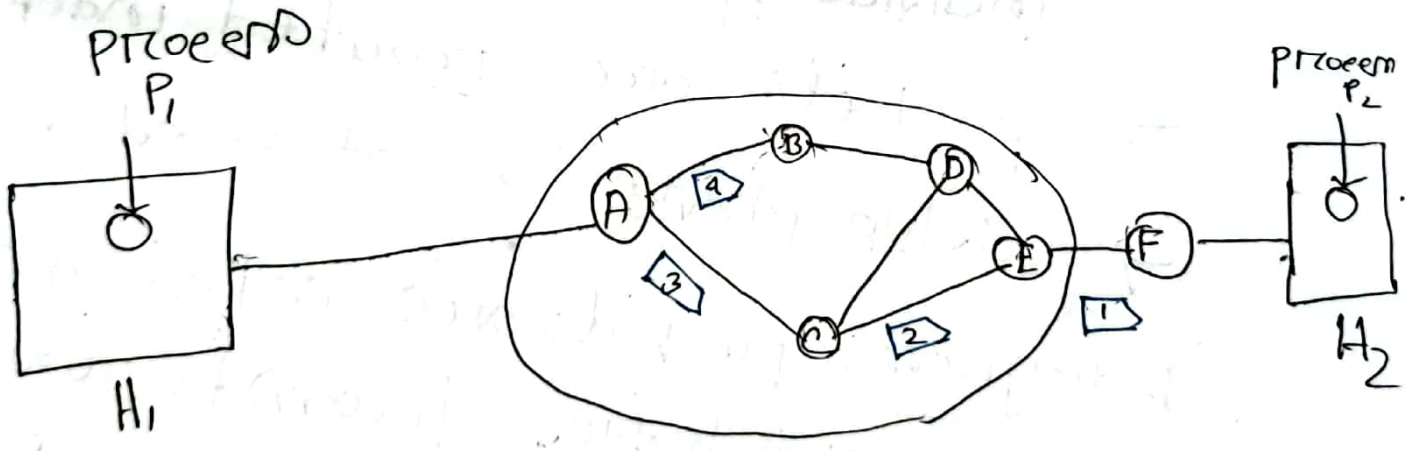
CamScanner

Virtual circuit:

If connection-oriented service is used, a path from the source router all the way to the destination router must be established.

This connection is called virtual circuit and the network is called a virtual circuit network.

Example of connectionless service:



Example:
- → Internet protocol
- → each packet carries a destination address
- → IPV4 packet address is 32 bit
- → IPV6 " " " 128 "

→ Message is four times longer than the maximum size.

→ So message is break into 4 packets (1, 2, 3, 4)

→ Routing table :

Every router has an internal table.
It tells where to send packets for each of the possible destination.

2 entry.
- → destination
- → outgoing line to use

→ packets 1, 2, 3 are ~~sent~~ stored at A and checksum is checked.

→ forward to the E and then F.

→ ~~AD at path~~

→ ~~AD at~~

→ Path ACE has a traffic jam

→ So A send 4 packet 4 via a different route than first 3.

A's table (initially)

Dest	Line
A	–
B	B
C	C
D	B
E	C
F	C

A's table (later)

A	–
B	B
C	C
D	B
E	B
F	B

C's table

A	A
B	A
C	–
D	E
E	E
F	E

E's table

A	C
B	D
C	C
D	D
E	–
F	F

Implementation of connection-oriented service:

→ also called label switching network.

→ use a virtual-circuit network.

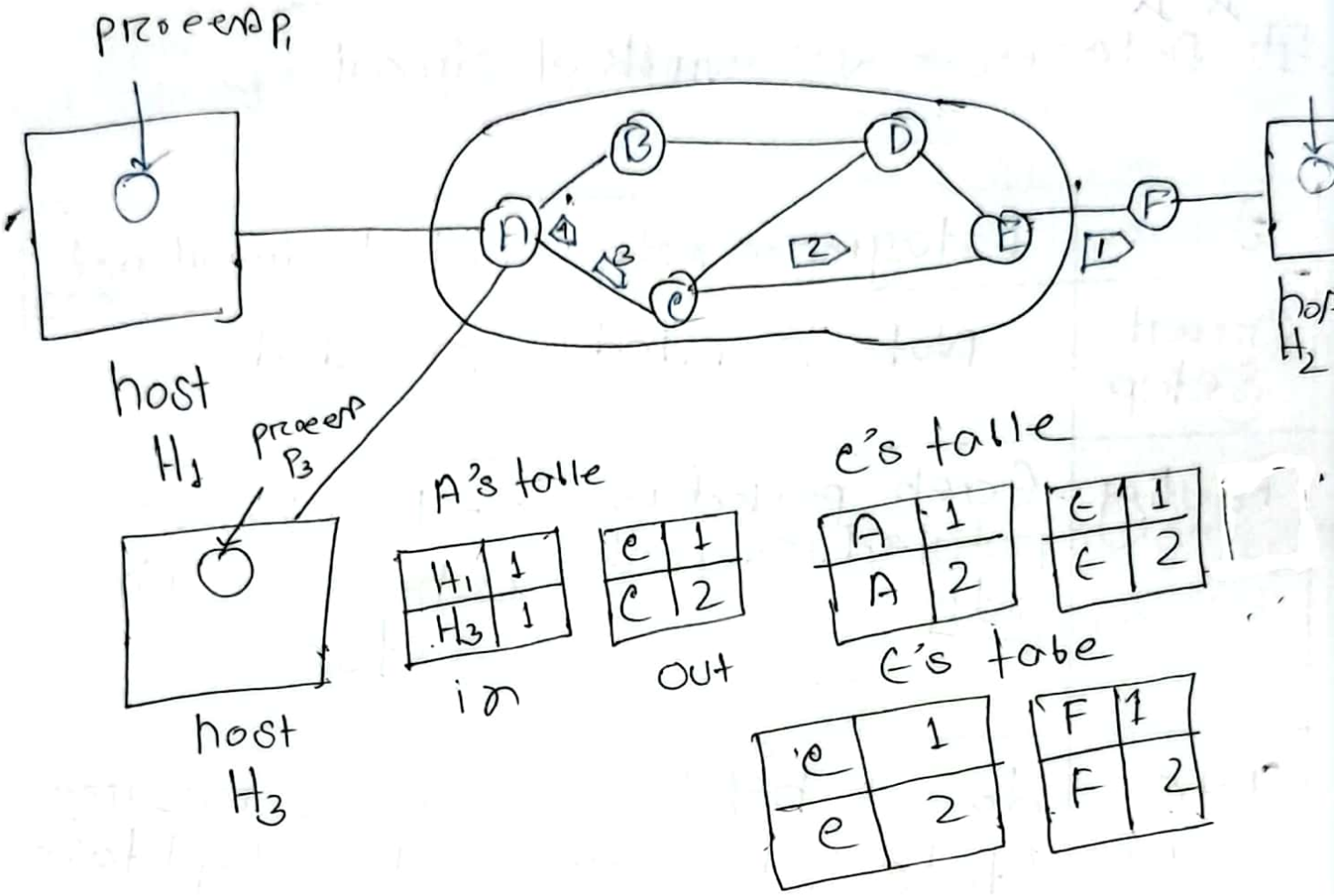
→ avoid having to choose a new route for every packet sent.

→ has a setup phase

→ route is stored in tables inside the routers.

→ one route is used for all traffic over the connection.

→ each packet carries an identifier tells which VC it belongs to.



NB: A assigns a different connection identifier to the outgoing traffic for the second connection.
It helps to avoid conflict.

Example: → MPLS (Multiprotocol Level Switching)

→ used within ISP network.
→ has 20 bit connection identifier
→ often hidden from customers.
→ ISP long term connections for

Datagram vs virtual circuit:

Issue	Datagram network	Virtual-circuit network
Circuit Setup	Not needed	needed
Routing	Each packet is routed independently	Route chosen when VC is setup
State information	do n't hold State information about connection	Each VC require router ~~tapt~~ table space per connection.
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
পাশাপাশি Congestion control and Quality of service.	Difficult	Easy if enough resources can be allocated in advanced for each VC
Effect of router failure	None	All ~~pac~~ VC's that passed through the failed router are ~~failed~~ terminated

trade off between

Virtual circuit & datagram

→ setup time versus address parsing time.

→ destination address used in datagram networks are longer than circuit numbers used in virtual circuit number.

→ Amount of table space required in router memory.

datagram → an entry for each possible destin

vc → an " for " virtual circuit

→ Virtual circuit → guaranteeing quality of service

quality → avoiding congestion

→ as resources can be reserved in advance.

→ virtual circuits have vulnerability problem

Routing Algorithm:

Routing algorithm:

Algorithm that manages the routing table and make the routing decision is called routing algorithm.

→ part of the network layer

→ responsible for deciding which output lines an incoming packet should be transmitted on.

Session routing:

If the network uses virtual circuit internally, routing decision is made only when a new virtual circuit is being setup.

CamScanner

Routing Algorithm:

Routing algorithm:

Algorithm that manages the routing table and make the routing decision is called routing algorithm.

→ part of the network layer
→ responsible for deciding which output lines an incoming packet should be transmitted on.

Session routing:

If the network uses virtual circuit internally, routing decision is made only when a new virtual circuit is being setup.

CamScanner

* If the network uses datagrams, the routing decision must be made anew for every arriving data pockets,

→ as the best route may have changed.

Classification of Routing algorithm:

2 major classes:

1. nonadaptive algorithm
2. adaptive "

Adaptive algorithm:

→ algorithm change their routing decision to reflect changes in the topology

→ sometimes changes in the traffic as well.

→ it's dynamic routing

~~Optimization matrix~~

→ for optimization matrix is used

→ topology changes every 4T seconds. when they routes changes

Matrix:

→ distance

→ number of hops

→ estimated transmit time

Non-adaptive algorithm:

→ Do not change/base their routing decisions. on any measurements or estimates of the current topology & traffic.

→ Choise of route to use to get from I to J is computed in advance.

→ it is static routing procedure

→ as it does not respond to failures.

CamScanner

~~Static~~

* useful for stations in which routing choice is clear.

Property of Routing algorithm:

Correctness & simplicity:

→ packet should be delivered to correct destination.

→ algorithm should be simple.

Robustness:

Ability of the network to deliver packets via some route even in face of failure

* Algorithm should be able to cope with → changes in the topology
  → traffic without requiring in all jobs

Stability: A stable algorithm reaches equilibrium and stays there.

CamScanner

Fairness and optimality

may should contradicts but conflicting

Efficiency:

Minimum overhead.

Routing

3 types

→ Static routing

→ Default routing

→ Dynamic routing

Static routing:

Process in which we have to manually add routers in routing table.

Advantages:

→ it adds security as only administrator can allow routing to particular network

→ No bandwidth usage between routers.

CamScanner

Disadvantages:

→ For large network, it is a hectic task for administrator to add router manually.

→ Administrator should have good knowledge about routing

Dynamic routing:

Make automatic adjustment of the routes according to the current state of the route in the routing table.

→ uses protocol to ~~reach~~ discover network distinations.

CamScanner

Advantages:

→ Easy to configure

→ more effective at selecting the best route to a destination remote network.

Disadvantages:

→ less secure than static routing

→ consumes more bandwidth for communicating with other neighbour.

CS CamScanner

Static Routing Vs Dynamic Routing:

Static Routing	Dynamic Routing
1. Manual configuration	~~1. Dynamic~~ 1. Automatic
2. If a new router add or delete, need to configure again	2. Need not to configure newly
3. Doesn't employ complex routing algorithm	3. Uses complex routing algorithm
4. Routes are user defined	4. Routes are updated according to the change in topology
5. Implemented in small networks	5. Implemented in large networks
6. It provides high security	6. Less secure than static routing
7. No routing protocols are involved	7. Routing protocol, such as RIP, OSPF are involved.

CamScanner

Routing algorithm:

1. The optimality principle
2. Shortest path algorithm → static
3. Flooding
4. distance vector Routing
5. Link state routing.

dynamic

Optimality principle:

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

part of the route from J to $J \Rightarrow r_1$
" " " " " J to $k \Rightarrow r_2$

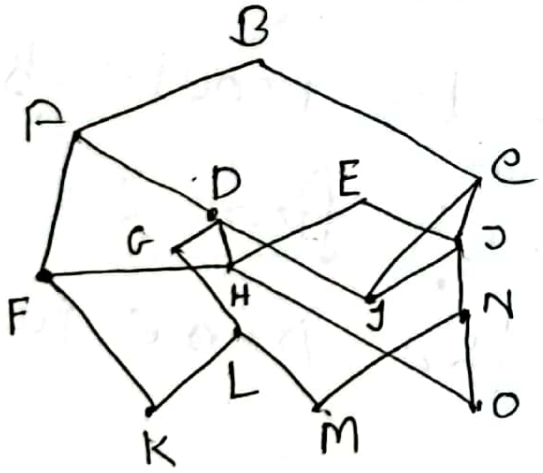
If a route better than r_2 from J to k will find, it can be connected with r_1 to improve the route from J to k.

Sink tree:

Set of all optimal routes from source to a given destination form a tree rooted at the destination. Such a tree is called sink tree.

→ it does not contain any loops

Example:



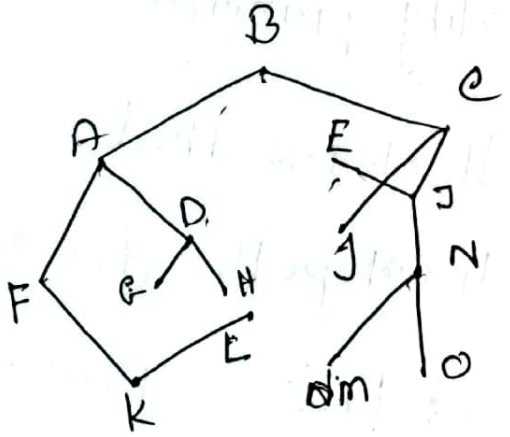


Fig: Sink tree for router B

distance matrix is number of hops

goal: discover and use the sink tree for all routers.

Shortest path Algorithm:

→ goal / idea is to build a graph

→ each node representing a router

→ each edge " a connection line or link

→ algorithm just finds the shortest path between routers of the graph.

→ labels of the edge could be computed as a function of

- distance
- bandwidth
- average traffic
- communication cost
- measured delay.

★ → distance must be non-negative.

Steps: represent the shortest path from source to that node.

→ initially no paths are known,

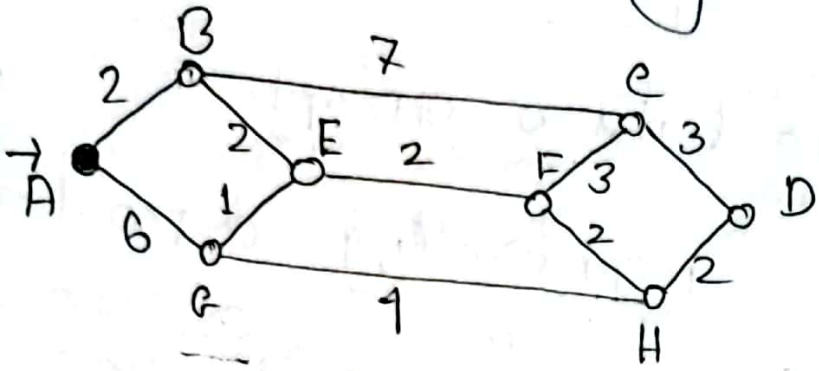
→ nodes are labeled infinity.

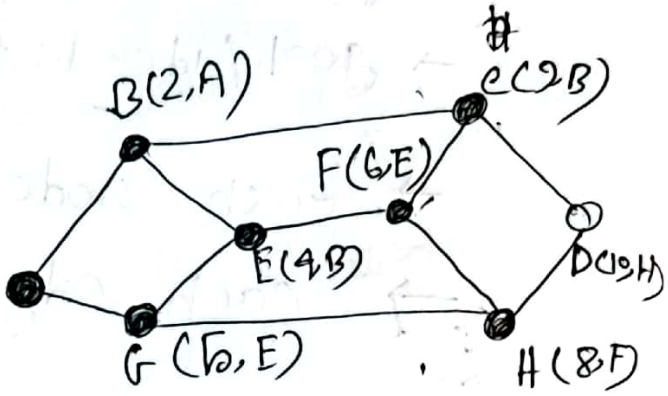
→ algorithm proceed and label changes

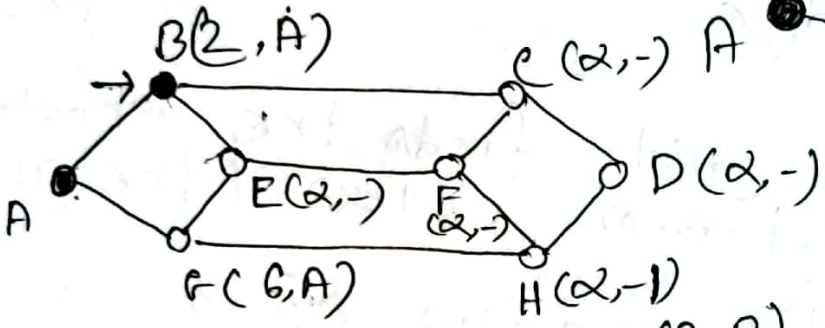
→ label may be tentative / permanent.

CS CamScanner

Steps of computing shortest path from A to D

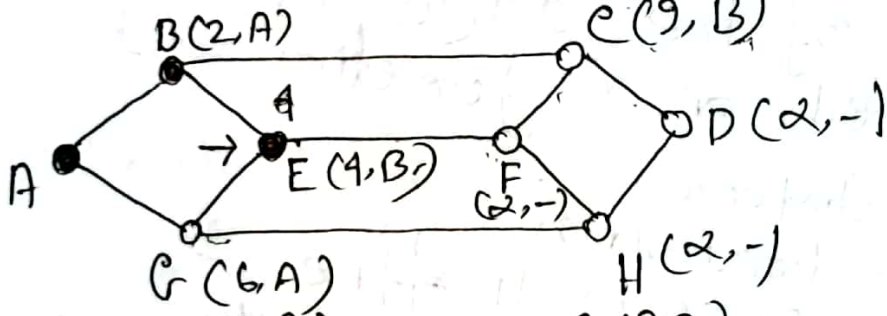


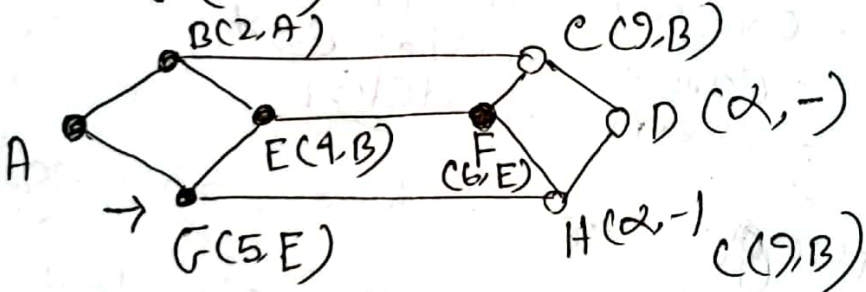


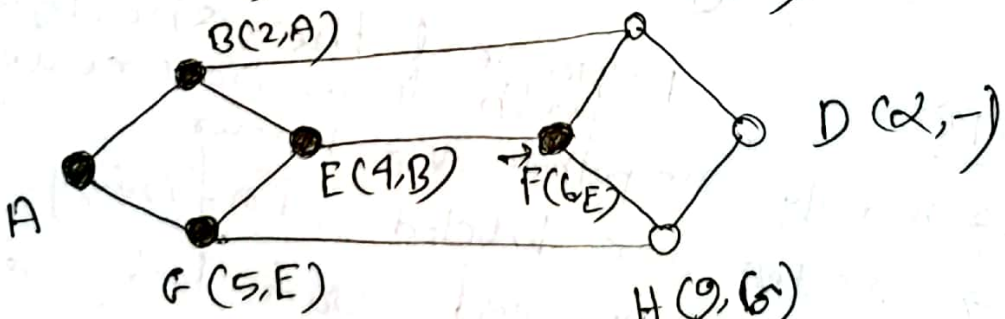


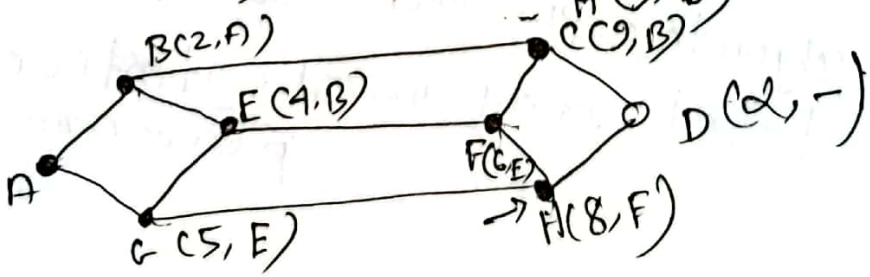
∴ Shortest path

A – B – E – F – H – D









Flooding:

→ every incoming packet is sent out every outgoing line except the one it ~~to~~ arrived on.

→ generate vast numbers of duplicate packets.

→ hope counter is initialized to length of the path from source to destination

→ All possible routes are tried.

→ So there will be atleast one route which is the shortest

→ All nodes directly or indirectly connected are visited.

Limitations:

→ generate vast number of duplicate packet

→ suitable damping mechanism must be used.

Solution:

→ Hope counter contained in the packet header which is decremented at each hope.

CamScanner

→ Sender initializes the hope counter. If no estimate is known (initially) it is set to the full diameter of the subnet.

→ A sequence number is used to keep track of the packets to prevent flooding.

Advantages/use:

→ always chooses the shortest path

→ broadcast messages to all the nodes

→ highly ~~Re~~ Robust ~~emerge~~

→ emergency messages can be sent

CamScanner

Distance vector Routing:

→ dynamic routing algorithm.
→ also called distributed Bellman-Ford routing algorithm.

Step-1:

Each router maintain a routing table (vector)
→ best known distance to each destination.
→ which link to use to get there.

Each router knows about-
- ☆ All the router present in the network.
- ☆ Distance to it's ~~one~~ neighbouring router.

Step-2:

→ Each router exchange its distance vector with its neighboring routers

→ Each router prepares a new routing table using the distance vector obtained from its neighbour

→ this step is repeated for (n-2) times. where n = number of routers

Routing table entry:

2 entry.

~~→ pr~~

→ outgoing line to use for destination

→ estimate of the distance to that destination.

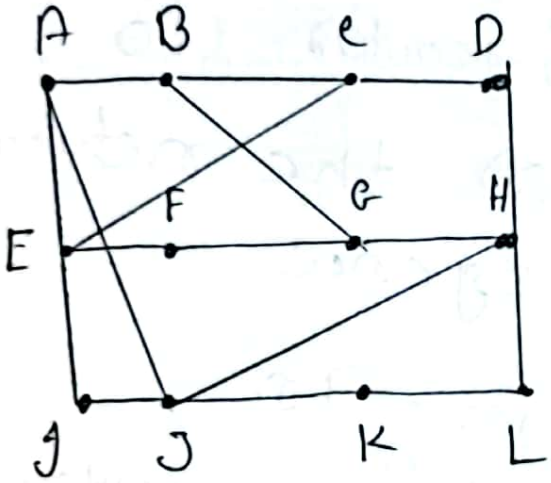
→ measured as the number of hops

→ " " propogation delay

measure it directly

with special ECHO packets that the receiver just timestamps and sends back as first as it can.

Example:



To	A	I	H	K
A	0	24	20	21
B	12	36	31	28
C	25	18	19	36
D	40	27	8	24
E	14	7	30	22
F	23	20	19	40
G	18	31	6	31
H	17	20	0	19
I	21	0	14	22
J	9	11	7	10
K	24	22	22	0
L	29	33	9	9
	JA delay 8	JI delay 10	JH delay 12	JK delay 6

Vector's received from J's four neighbors.

New estimated delay from J

↓	Line
8	A
20	A
28	I
20	H
17	I
30	I
18	H
12	H
10	I
0	–
6	K
15	K

New routing table for J

Count-to-infinity problem

Convergence: the setting of routers to best paths across the network is called convergence

→ One of the important issue in DVR is count-to-infinity problem

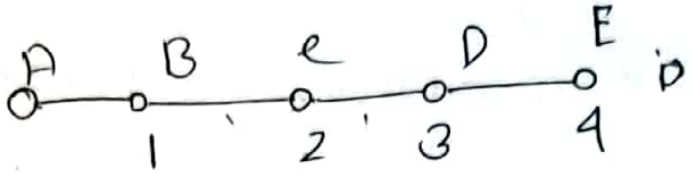
→ it is another name of routing loop.

→ Occurs when an interface goes down

→ also occur when two routers send update to each other at the same time.

CamScanner

Example:



1	2	3	4	initially
3	2	3	4	1st exchange
3	4	3	4	2nd "
5	4	5	4	3rd "
5	6	5	6	4th "

Routers ~~B, D, D~~ B, C, D & E have distance to A of 1, 2, 3 & 4 hops respectively

Now consider A goes down or link AB is cut.

→ At the first packet exchange B does not hear anything from A

→ C, says I have a path to A of length 2.

→ B suspect that C's path runs through B itself.

→ B think it can reach A via C with a path length 3.

CamScanner

→ On the second exchange
C notices that each of its neighbours claims to have

→ On the second exchange.
C picks one of it's neighbour whose path cost to A is 3.

→ So it makes new distance to A is 4.

lution:

Can be solved by 2 ways

Split horizon

→ preventing routers from advertising their best ~~path~~ path back to the neighbours from which they heard them.

Chapter-8
Switching

Objective: creating a point-to-point connection.

Switching:

A switched network consists of a series of interlinked nodes called switches

→ device that capable of creating temporary connection between 2 or more devices

#Classification

3 types

1. Circuit switching
2. Packet switching → Virtual circuit switching / Datagram switching.
3. Message "

CamScanner

Switching at TCP/IP layers:

Physical layer: Circuit switching

data link layer: packet switching
→ packet means frames (virtual circuit switching)
or cells

Network layer: packet switching
→ internet uses (virtual circuit and datagram approach datagram)

application layer: message switching

→ communication occurs by exchanging messages
→ e-mail is a kind of message switched communication.

Circuit Switched Network:

→ set of switches connected by physical links.

→ connection between 2 station is two dedicated path.

→ each connection uses only one dedicated channel or one link.

Steps/procedure:

→ takes place at physical layer

→ before starting communication station must make a reservation of resources. → { channel in FDM, time slot in TDM, switch buffers, processing time

→ transfer between two stations are not packetized.

→ continuous data flow

→ no addressing is involved during data transfer

3 step
→ connection setup
→ data transfer
→ termination

Classification of Structure of circuit switching

2 types

→ space division switching
→ used for both
→ path in the circuit are separated from each other
→ designed for analog network

→ time " "
→ use time division multiplexing (TDM)
→ most popular technology is called time slot interchange

Crossbar switch:

→ connect n inputs to m outputs
→ in a grid using electronic micro switches at each cross point

→ limiting factor:
→ number of cross point required
→ to connect n inputs to m outputs
required cross point = n×m
→ crossbar switch with this number of cross point is impractical

~~→ in~~

→ in practice fewer than 25% of crosspoint are in use.

Solution of crossbar switch

→ multistage switch is the solution

→ it combines crossbar switch with several stages.

→ normally three stage.

Design a three stage switch:

1) N/n crossbar of size n×k (first stage)

2) k " of size (N/n × N/n) (at middle stage) (crossbar at middle stage)

3) N/n " of size (K×n) (at last stage)

∴ total number of crosspoints

$= N/n(n \times k) + K(N/n \times N/n) + N/n(k \times n)$

$= 2KN + K\left(\frac{N}{n}\right)^2$

CamScanner

□ 15×15 Single Stage crossbar

Ans: Number of crosspoints

$= 15 \times 15$

$= 225$

□ Number of crossbar for 15×15 multistage crossbar

3 Stage

$\therefore 15/3 = 5$

$\therefore N = 15$

$n = 3$

$N/n = 3$

$k = 2$

$k \leq 2n-1$

$\Rightarrow$

$\frac{d}{dn}(2kN) + \frac{(N)^2}{k^2} = 0$

$2 \times 2 \times 15 + (5)^2(2)$

$= 60 + 50$

$2kN + k(N/n)^2$

$= 2 \times 2 \times 15 + 2(3)^2$

$= 60 + 18$

$= 78$

Ans

Let $n = 5$

$k = 2$

$\therefore N/n = 15/5 = 3$

$= 72k \frac{N}{n}$

$(-1)(n-1-1) = 0$

$=$

$\Rightarrow$

∴ total crosspoint.

$$2KN + K\left(\frac{N}{n}\right)^2$$

$$= (2 \times 2 \times 15) + 2\left(\frac{15}{5}\right)^2$$

$$= 60 + (2 \times 9)$$

$$= 60 + 18$$

$$= 78$$

Ans

Given that,

$N = 200$

$n = 20$

$k = 4$

$\therefore N/n = \frac{200}{20} = 10$

∴ total number of crosspoints

$$= 2KN + k\left(\frac{N}{n}\right)^2$$

$$= (2 \times 4 \times 200) + (4 \times 10^2)$$

$$= 1600 + 400$$

$$= 2000$$ Ans

CamScanner

Disadvantage

→ Multistage switching has blocking during periods of heavy traffic.

→ Main idea:

Share the crosspoints in the multi edge crossbars.

It cause a lack of availability

→ resources are limited

→ all users want a connection at a time

Blocking:

Time when one input cannot be connected to an output because there is no path available between them.

CS CamScanner

Clos criteria:

→ used to remove blocking problem

Statement:

number of middle stage switches must be at least $2n-1$

i.e $\boxed{k \geq 2n-1}$

According to clos criteria,

$\boxed{n = (N/2)^2 \text{ and } k \geq 2n-1}$

∴ Total no of crosspoint, $\geq 4N\left[(2N)^2 - 1\right]$

$2kN + k\left(\frac{N}{n}\right)^2$

$2(2n-1)N + (2n-1)N^2 \left(\frac{2}{N}\right)^2$

$2(2n-1)N + 4(2n-1)\frac{1}{N^2}$

$= 4(2n-1)$

$4N$

Time division switching:

→ it uses time division multiplexing

it consists ~~on~~ of

→ a TDM multiplexer
→ a TDM demultiplexer
→ random access memory
→ TSI

→ RAM has several memory location.

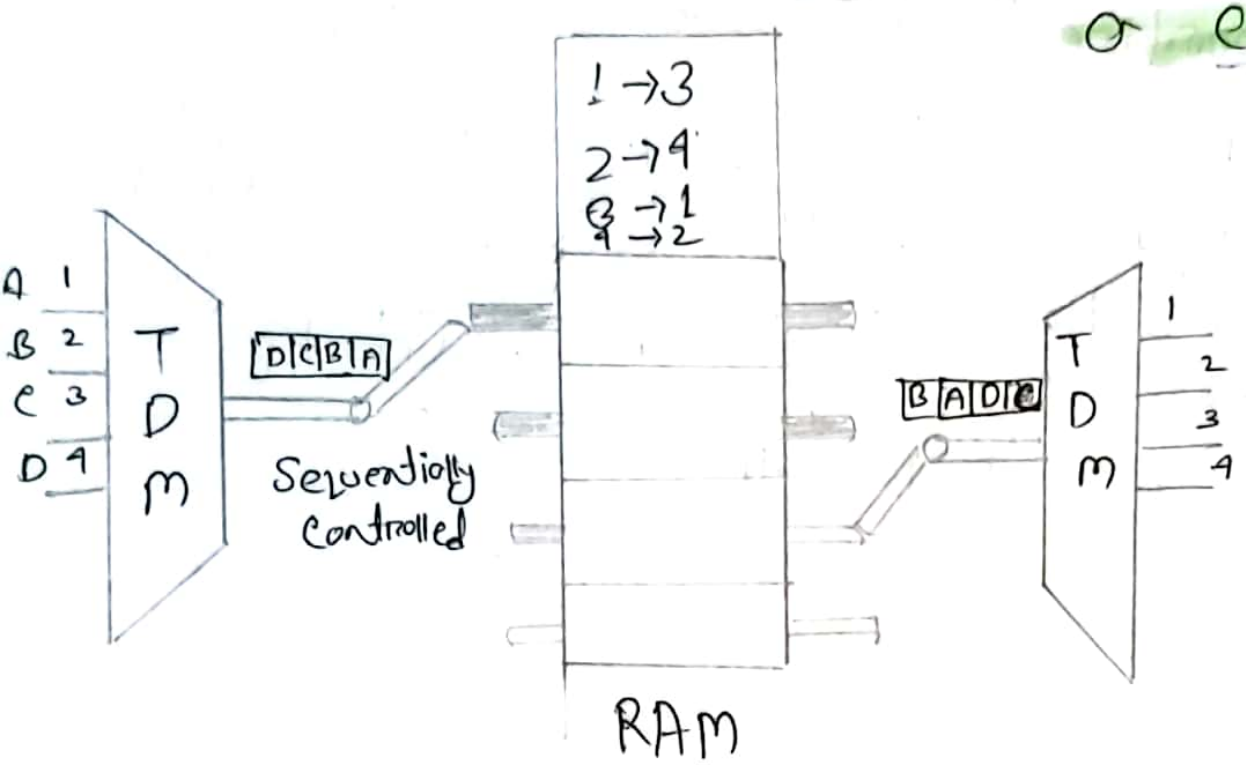
→ Size of each location is size of a single time slot

→ number of location ~~size of a single time slot.~~ number of inputs.

Procedure:

→ RAM fills up with incoming data from time slots in order received.

→ Slots are sent out ~~order~~ order based on the decions of a control unit



~~Time divis~~

Space division switching

Ad → it is instantaneous (তাৎক্ষণিক)

D.Ad → it's require crosspoints, that make blocking

Time division switching

Ad. → it does not need no crosspoints

D.Ad → processing each connection creates delays.

CamScanner

Time space time switching

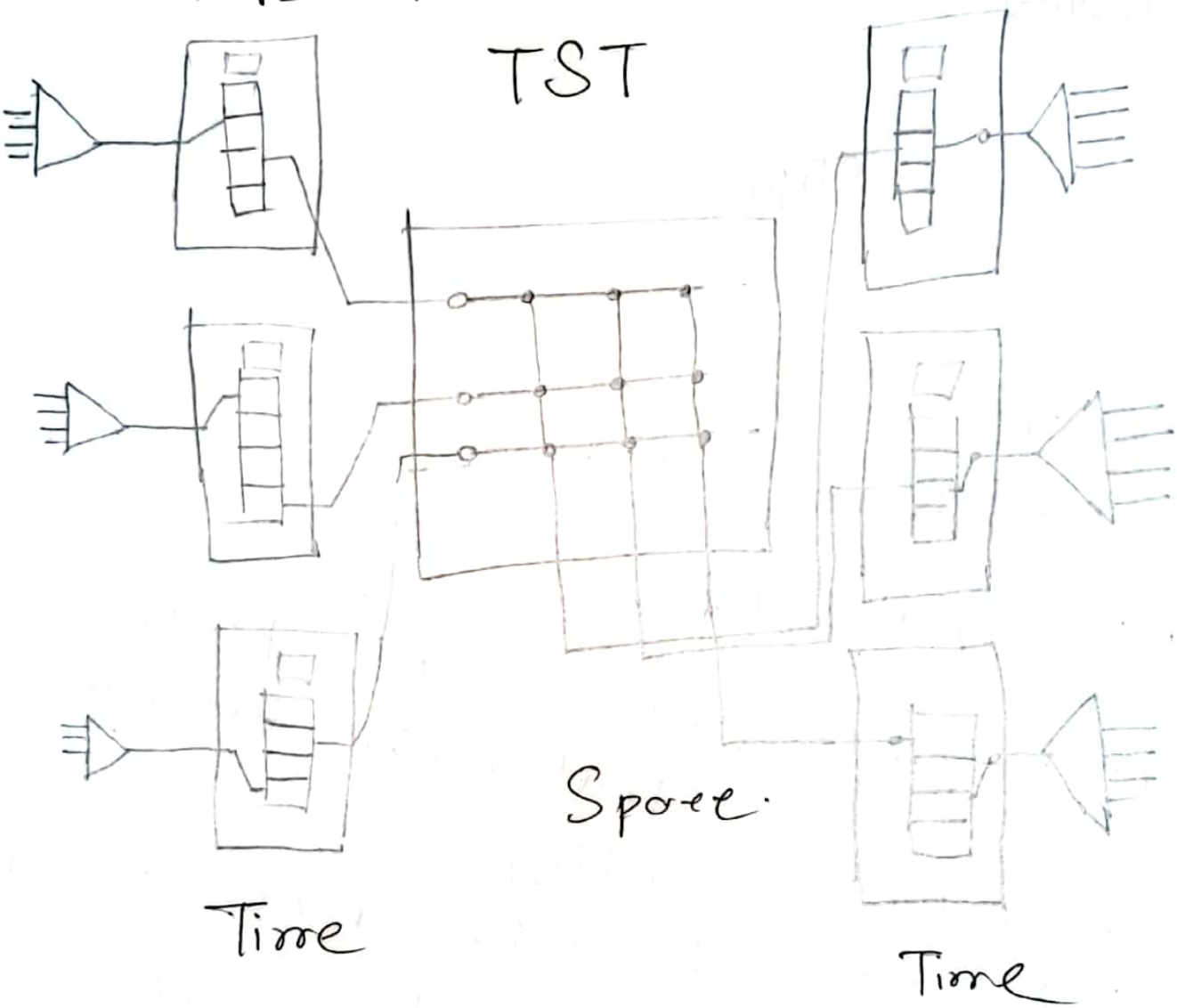
→ combine both space & time division switching

→ comoptimize both — physically (crosspoints), temporally (delay)

→ two time stage

→ one space "

→ 12 input & 12 output



Packet Switching

fixed size
variable "

→ message are devided into packets

→ Size of the packet determined by
→ the network
→ the governing protocol

→ no resource allocation.
→ no reserved bandwidth
→ no scheduled processing time

~~allocation is done~~
first come first served basis
→ resource are allocated on demand
→ packet are received
→ ~~when a switch re~~
→ packet must wait if there are other packet being processed

NB : See data communication (2)

CamScanner

IPV4 vs IPV6

IPV4	IPV6
1. It can generate 4.29×10^9 (2^{32}) address space	1. It can produce 3.40×10^{38} (2^{128}) address space
2. It has 32-bit address length	2. 128-bit address length
3. Support manual and DHCP configuration	3. Support auto and renumbering configuration.
4. Address representation of IPV4 in decimal. Support VLSM	4. Address representation of IPV6 in hexadecimal Doesn't support VLSM
5. In IPV4 Checksum field is available	5. Checksum field is not available
6. Encryption and Authentication facility not provided	6. In IPV6 Encryption and Authentication are provided
7. It has five classes	7. It doesn't have any different classes

Security: how secret the datagram is
Secret source routing: gives the complete path to be followed
Loose source routing: " list of router not to be visited

IPV4 header:

Version	IHL	Differentiated Service	total length		
Identification			P F	m F	fragment offset
Time to live		protocol	Header checksum		
Source address					
Destination address					
Option (0 or more words)					

Security
Strict source routing
loose source routing
Record route
timestamp

IP address of source & destination

Version: keeps track of which version of the protocol the datagram belongs to

IHL: provided to tell how long the header is in 32 bit words

minimum value is 5
maximum " is 15 → 4 bit field

Differentiated Service: It's called type of service field.

It is intended to distinguish between different class of service

It provide 3 bits to → signal priority
3 bits to → signal whether a host cared more about delay, throughput

Record route: makes each router append it IP add rem

total length:
includes everything in the datagram- both header and data.

Identification:
to allow the destination host to determine which packet is newly arrived fragment belong to.

1 unused bit

DF: Stands for Don't fragment.
order to the router not to fragment the packet.

MF: Stands for more fragment.

Time to live: counter used to limit packet lifetimes.

protocol: tells which transport proceeds ~~packet~~ to give the packet to.
→ TCP
→ UDP

header checksum: It rates its own check sum for protection.

timestamp: makes each router append its address

VLSM

Given the no of hosts as 100, 50, 20 & 6. Find IP address & subnet masks using Class C (192.168.1.0)

Ans: Given,
Network address, 192.168.1.0

For 100,
Number of host bit $= \lceil \log_2 100 \rceil$
$= 7$

$\therefore$ Network & subnet bit $= 24 + (8-7)$
$= 24+1$
$= 25$

$\therefore$ Subnet masks,
255.255.255.1000000/25
$= 255.255.255.128/25$

Range 192.168.1.00000000/25
— 192.168.1.01111111/25
$= 192.168.1.0/25$ –
192.168.1.127/25

Ans

For 50 hosts,

Number of host bit $= \lceil \log_2 50 \rceil$
$= 6$

$\therefore$ Network & subnet bit $= 24 + (8-6)$
$= 24+2$
$= 26$

$\therefore$ Subnet mask $= 255.255.255.11000$

$= 255.255.255.192$

Range,
$192.168.1.10000000/26$
$- 192.168.1.10111111/26$
$= 192.168.1.128/26 -$
$192.168.1.191/26$ Ans

For 20 hosts,
Number of host bit $= \lceil \log_2 20 \rceil$
$= 5$

$\therefore$ Network & subnet bit $= 24 + (8-5)$
$= 24+3$
$= 27$

$\therefore$ Subnet mask $= 255.255.255.11100000/27$
$= 255.255.255.224$

CamScanner

Range,

192.168.1.11000000/27 –

192.168.1.11011111/27

= 192.168.1.192/27 –

192.168.1.223/27 Ans

For 6 hosts

number of host bit = $\lceil \log_2 6 \rceil$

= 3

∴ Subnet & network bit

= 24+(8-3)

= 24+5 = 29

∴ Subnet mask = 255.255.255.

11111000

= 255.255.255.24

Range = 192.168.1.11100000/29 –

192.168.1.11100111/29

= 192.168.1.224/29 –

192.168.1.231/29 Ans

CS CamScanner

Benefit of subneting:

→ Improve network performance & speed

→ Reduce network congestion

→ Control network growth

→ Boost network security

→ Ease administration.

CamScanner

Given that,

network address = 170.170.0.0

each subnet has = 1024 hosts

i. Number of host bit

$= \left\lceil \frac{\log 1024}{\log 2} \right\rceil$

$= 10$

∴ Network bit is = $32 - 10 = 22$

∴ Subnet mask = 11111111.11111111.11111100.00000000

= 255.255.252.0/22

ii. Subnet bit = $32 - (10+16) = 6$

∴ Number of subnet = $2^6 = 64$

IP address of last subnet, 63

170.170.11111100.00000000/22

= 170.170.252.0/22

∴ Network address = 170.170.252.0/22

Broadcast " = 170.170.255.255/22

170.170.252.1/22

IP range 170.170.255.254/22

Ans

iii Number of subnet $= 2^{(32-16-10)}$

$= 2^{32-26}$

$= 2^{6}$

$= 64$ Ans

iv 2nd subnet address

170.170.00000100.00000000/22

= 170.170.4.0/22

∴ 2nd subnet's broadcast address

= 170.170.7.255/22

Ans

2013 - 2(a)

Given that,

Network address = 160.160.0.0

Need 1024 hosts

a

∴ we need extra $\left\lceil \frac{\log 1024}{\log 2} \right\rceil$

= 10 bits for host

∴ ~~total bits in network portion~~

~~= 16+10~~

~~= 26~~

∴ Subnet bit = 32 − (16 + 10)

= 6

∴ Number of subnet = 2^6

= 64

b Subnet mask = 11111111.11111111.11111100.00000000

= 255.255.252.0

c 64th subnet = Last subnet = 63

∴ Last subnet network address

160.160.111111 00.00000000/22

32/16/8/4/2/1

1 1 1 1 1 1

$= 160.160.252.0/22$

$\therefore$ ~~Range~~ Last address:

$160.160.11111111.11111110/22$

$= 160.160.255.254/22$

First address

$= 160.160.252.1/22$

$\therefore$ Range $160.160.252.1/22$ –

$160.160.255.254/22$

d

2nd subnet = 01

$\therefore$ Network address

$160.160.00000100.0/22$

$= 160.160.4.0/22$

Ans

$\therefore$ Broad cast address,

$160.160.00000111.11111111/22$

$= 160.160.7.255/22$

Ans

What is the maximum number of subnets in class C networks using the following masks?

i) 255.255.255.224

ii) 255.255.255.240

Answer:

C class network address

i: Subnet mask = 255.255.255.224

= 11111111.11111111.11111111.11100000

∴ 3 bits for subnet.

∴ ~~maxim~~ maximum number of subnets

~~= 2^4 = 1~~

$= 2^3 = 8$ Ans

ii Subnet masks = 255.255.255.240

= 11111111.11111111.11111111.11110000

∴ 4 bits for subnet.

∴ maximum number of subnets = $2^4 = 16$ Ans

CamScanner

A network on the internet has a subnet mask of 255.255.240.0 what is the maximum number of hosts it can handle?

Answer:

Subnet mask = 255.255.240.0

= 11111111.11111111.11110000.0

∴ number of host bits = 32 − 20

= 12

∴ maximum number of hosts

$= 2^{12}$

= 4096

What are the maximum number of subnets in class C networks using the following masks?

i) 255.255.255.192

ii) 255.255.255.240.

Answer: i Subnet bit = 2 ∴ number of subnet = 2^2

ii Subnet bit = 4 " of " = 2^4

An organization has network 160.56.0.0/16. The administrator wants to create 1024 subnets

a) Find the subnet mask.
b) " " number of IP address in each subnet
c) " " network and broadcast address of ~~Se~~ subnet 100
d) " " first and last address of subnet 700
e) " " both pe IP address of the 600th subnet.

Ans:

a) IP address 160.56.0.0/16

Subnet mask 11111111.11111111.00000000.00000000
= 255.255.0.0/16

b) ~~Num~~ Number of bit's in network portion

$= 16 + \left\lceil \frac{\log 1024}{\log 2} \right\rceil$

$= 16 + 10$

$= 26$

∴ Number of bit's in host portion

$= 32 - 26$

$= 6$

∴ Number of IP address in each subnet $= 2^6$

$= 64.$

CamScanner

c

100th subnet address.

Rough

100th : 99

128/64/32/16/8/4/2/1

0 1 1 0 0 0 1

∴ 10100000.00111000.

00011000.11000000

= 160.56.24.192/26

∴ Network address = 160.56.24.192/26

Broadcast " = 160.56.24.255/26

d 700th subnet address.

Rough

700th − 699

512/256/128/64/32/16/8/4/2/1

1 0 0 1 0 1 1 0 1 1 1

10100000.00111000.

10101110.11000000/26

= 160.56.174.192/26

∴ ~~First addr.~~

∴ 700th subnet network address

= 160.56.174.192/26

∴ 700th subnet's first address.

= 760.56.174.193/26

700th subnet's last address =

760.56.174.254/26

(by adding 62)

e) 60th subnet network address

∴ 10100000.00111000.10010101.11000000/26

= 160.56.149.192/26

Rough 600=59

512/256/128/64/32
1 0 0 1 0
16/8/4/2/1
1 0 1 1 1

as it is half
0 is return

30th = 30

64/32/16/8/4/2
0 1 1 1 1 0

∴ 30th pc's address.

∴ 10100000.00111000.10010101.11011110/26

= 160.56.149.222/26

Ans

2017-5(a)

Given IP address = 172.160.0.0

each subnet required = 510 pc

i) As first octet range from 128-191

So given IP address is a B class IP

For 510 pc we need = $\frac{\lceil \log 510 \rceil}{\log 2}$ bits

= 8.994 bits

≃ 9 bits

∴ For host's number of bits = 9 And
∴ For Subnet work " " " = 32 − (9 + 16)
= 7 bits Ans

∴ total number of network bit = (16 + 7)
= 23

ii ∴ Subnet mask = 11111111.11111111.11111110.
00000000/23
= 255.255.254.0/23
Ans

iii 50th subnet,
∴ ~~49~~

Rough
50 mean
49
64/32/16/8/4/2
0 1 1 0 0 1

∴ 50th subnet address,
172.160.01100110.00000000/23
= ~~172.160.49~~
= 172.160.98.0/23

∴ First address,
= 172.160.98.1/23

last address,
= 172.160.01100011.11111110/23
= 172.160.99.254/23 Ans

IV 80th subnetwork address,

~~= 170~~

= 172.160.10011110.00000000/23

= 172.160.158.0/23

all host bit 0

Ans

Rough
80 = 79
64/32/16/8/4
1 0 0 1 1

Broadcast address,

= 172.160.10011111.11111111/23

= 172.160.159.255/23

all host bi
1

V 20th subnetwork address,

= 172.160.00100110.00000000/23

= 172.160.38.0/23

Rough
20, 19
64/32/16/8/4
0 0 1 0 0 1

∴ 250th pc's of address of 20th subnetwork

= 172.160.00100110.11111010/23

= 172.160.38.250/23

Ans

Rough.
250/250
256/128/64
0 1 1
32/16/8/4/2
1 1 1 0 1

Network address = 192.168.10.0

Subnet mask = 255.255.255.240

Number of subnet?

Number of hosts/Subnet?

Ans:

Network address = 192.168.10.0

∴ It is a class C address

Subnet mask

255.255.255.240

= 11111111.11111111.11111111.11110000/28

∴ Number of subnet = 2^{28-24}

= $2^4 = 16$ Ans

Number of hosts per subnet,

$(2^{32-28}-2) = (2^4-2) = 16-2$

$= 14$ Ans

~~Cable for~~

Connecting cable → to connect same device.

→ Cross over → used to connect unlike/different device

→ Straight through

→ Roll over

Cross over exception

Router - PC → as Router is performed/considered as PC.

Switch - hub

Cross-over

Switch - switch

Hub - hub

Router - router

PC - PC

Straight through

Switch - router

Switch - PC/server

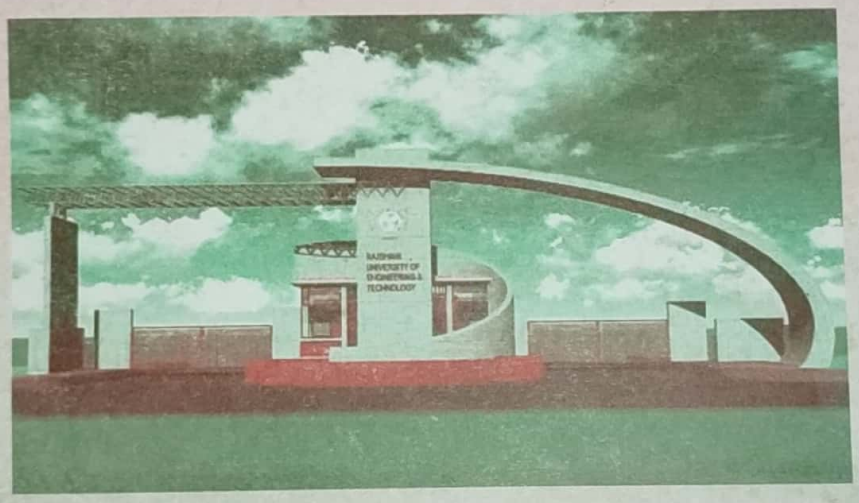
Hub - server

CamScanner

"Heaven's Light is Our Guide"

RAJSHAHI UNIVERSITY OF ENGINEERING & TECHNOLOGY

RUET



Name : Md. Ismail (MSS sir)

Subject : CSE-3205 (Computer Networks) Year : ○1st ○2nd ✓3rd ○4th

Roll No : 1503094 Semester ○1st ○2nd ○3rd ○4th ○5th ✓6th ○7th ○8th

Department CE EEE ME CSE ETE IPE URP GCE MTU ARCH

CamScanner

Data Link Layer

Node to node delivery

Function of data link layer / Design issues of data link layer

1. providing a well defined service interface to the network layer.

2. Dealing with transmission errors.

3. Regulate the flow of data so that slow receivers are not swamped by fast senders. (waited)

⇒ error control
2 ways
- → correct error
- → detect error

Every layer provides service to its previous layer through interface.

communication point of layers.

Services provided by data link layer:

3 types

→ Unacknowledged connectionless service

→ Acknowledged connectionless service

→ Acknowledged connection oriented service.

→ most sophisticated service

Unacknowledged connectionless

Service:

Source machine send independent frames to destination machine without having the destination machine acknowledge them

Example: Ethernet

Characteristics:

→ if a frame is lost due to noise on the line, no attempt is made to detect the loss

→ recover from it in data link layer.

→ appropriate when error rate is low

→ " for real time traffic (voice)

Aeknowledged connectionless service:

~~There~~ When this service is offered, there is no logical connection used but each frame sent is individually aeknowledged.

Example: 802.11 wifi

→ Sender knows whether a frame has arrived correctly or been lost.

guarantees that each frame sent is indeed receiv
" " frame is received exactly on
" " " are received in the right order

Aeknowledged connectionoriented service:

~~Sour~~ In this service, the source and destination machines establish a connection before any data are transferred

Phases of connectionoriented service:

~~It is in~~

Transfer go through three distinct phases:

1. Connection is established

→ both side initialize variable
→ counter needed to keep track of which frame has been received

2. One or more frames are actually ~~transfer~~ ~~transf~~ transmitted

3. Connection is released, freeing up the variables, buffers and other resources used to maintain the connection.

appropriate over
- → long unreliable links
- → satellite channel
- → long distance telephone circuit

Framing Method:

It has four methods

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

CamScanner

Byte count:

→ uses a field header

→ header specify the number of bytes in the frame including itself.

disadvantage

→ count can be garbled (বিকৃত হওয়া) by a transmission error

→ due to a single bit flip the destination will get out of synchronization

→ so it is unable to locate the correct start of the next frame

Example:

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

Flame 1 5 byte | Frame 2 5 byte | Frame 3 8 byte

Flag byte with byte stuffing:

~~→ gets~~

→ each frame has a start and end with special byte

→ both bytes are same called flag byte

→ two consecutive flag byte indicates the end of one frame and the start of another "

→ flag byte may occurs in the data

→ So, sender inserts a escape byte (ESC) to escape flag byte in data

~~→ receiver~~

→ receiver, remove the escape byte before giving the data to the network layer

→ escape byte may occurs in the data

→ So, escape byte is stuffed with another escape byte.

→ this schema is used in PPP (point-to-point protocol)

Example:

Original byte:

A	Flag	B

After stuffing:

A	ESC	Flag	B

Original byte:

A	ESC	B

After stuffing:

A	ESC	ESC	B

Original byte:

A	ESC	FLAG	B

After stuffing:

A	ESC	ESC	ESC	FLAG	B

CamScanner

Flag bit with bit stuffing:

→ frame can contain an arbitary number of bits

→ each frame begins and end with a special bit pattern (01111110 / 0x7E)

→ whenever sender encounter five consecutive ones in the data it automatically stuffs a 0 bit into the outgoing bit stream.

→ whenever receiver encounter five consecutive ones followed by a zero it destuff the zero (0)

Advantages → ensure minimum density of transitions

→ helps the physical layer minimum synchronization

use

→ USB (Universal Serial Bus) uses it

→ developed for HDLC (High Level data Link Control)

Example:

original data

00111111 00001111 11110000

after bit staffing:

01111110 00111110 00001111 01110000 01111110

flag flag

Disadvantages:

Character oriented framing:

data to be carried are 8 bit characters ~~frame~~ form a codding system such as ASCII. Example: flag byte with byte stuffing.

Bit oriented framing:

data section of a frame is a sequence of bits to be interpreted by the upper layer as text, video, etc. Example: flag bit with bit stuffing

A: 01000011

B: 11100011

FLAG: 01111110

ESC: 11100000

determine the bit sequence for the four characters frame [A][B][ESC][FLAG] by using i) byte count

ii) flag byte with byte stuffing

iii) flag bit with bit stuffing

Soln:

i) byte count A B ESC FLAG

00000101 01000011 11100011 11100000 01111110

ii) flag byte with byte stuffing:

A B ESC FLAG

01111110 01000011 11100011 11100000 11100000

11100000 01111110 01111110

iii) flag bit with bit stuffing A B ESC FLAG

01111110 01000011 11100011 11110000 00000

01111010 01111110

middle of the data fragment,

A B ESC C ESC FLAG FLAG D

determine the output by using byte stuffing algorithm.

Soln:

FLAG A B ESC ESC C ESC ESC ESC FLAG ESC FLAG D FLAG

A bit string 01111011111011111110 needs to be transmitted at the data link layer. determine the bits string output of bit stuffing method!

Soln:

01111011111001111010

Maximum overhead in byte stuffing:

Maximum overhead occurs ~~here~~ when the payload consists of only ESC and FLAG bytes.

In this case overhead will be 100%

B: for bit stuffing overhead will be 12.5%

*But my decision is 11.11%

* for 2 Byte data → 16 bit data
due to bit stuffing 2 extra bit will be required for 2 Byte data
increase → $\frac{2}{16} * 100 = 12.5\%$

CamScanner

Types of error:

2 types

→ Single bit error

→ burst error

Single bit error:

Only one bit of the given data unit ~~ess~~ is changed from 0 to 1 or 1 to 0.

~~burst~~

Example:

Sent: 0 0 0 0 0 0 1 0

received: 0 0 0 0 1 0 1 0

burst error:

2 or more bits in the data unit have changed from 0 to 1 or 1 to 0

CamScanner

Redundancy:

→ the central concept in detecting or correcting error ~~is~~ is redundancy

→ Redundancy means adding some extra bit

→ added by sender and removed by receiver.

★★ Error detection Vs error correction

Error detection	error correction
→ we are only looking to see if any error have occurred	→ we ~~wont~~ try to detect error and correct them
→ not interested in number of corrupted bits	→ interested in number exact corrupted bits,
→ not interested in corrupted bit location	→ interested in corrupted bit location
→ easier than correction	→ more ~~or~~ difficult than detection.

Coding schema:

2 types

→ block coding

→ convolution coding

datawords:

In block coding message is devided into blocks of k bits, called datawords

Codeword:

To detect / correct error we add r extra bits with datawords to make the length of $n = k + r$. The resulting n bit is called codeword.

CamScanner

- data word size = k

  code word " = $\boxed{n = k + r}$

  number of data word = 2^k

  number of codeword = 2^n

  " of unused " = $\boxed{2^n - 2^k}$

☆ block coding process is $\boxed{\text{one to one}}$

the same dataword is always encoded as the same codeword.

Error detection technique: 4 method

→ Simple Parity check

or, one dimensional parity check (VRC)

→ two dimensional parity check (LRC)

→ Checksum

→ CRC (cyclic redundancy check)

VRC: vertical redundancy check

LRC: longitudinal " "

CamScanner

Linear block code:

Code in which ~~ex~~ the exclusive ~~OR (⊕)~~ OR (addition modulo-2) of two valid codewords create another valid codeword.

One dimensional parity check (VRC)

adv.
- → most common method
- → least expensive

→ a redundant bit (parity bit) is added to every data unit so that the number of 1s in the unit become even.

→ k bit dataword changed to a n bit codeword where $n = k+1$

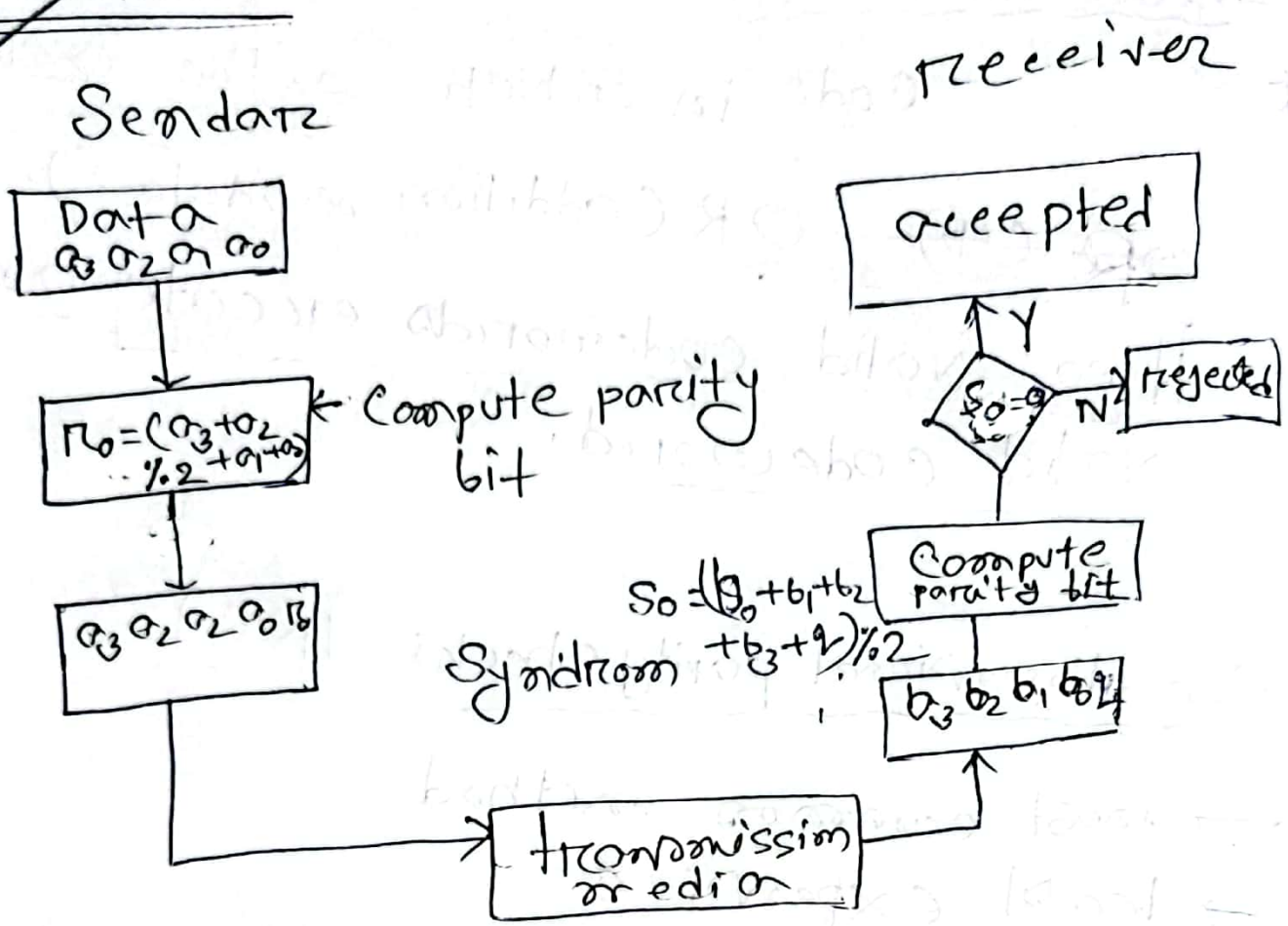
→ Calculation is done by modular-2 arithmatic

→ $r_0 = (a_3 + a_2 + a_1 + a_0)$ modulo 2

→ data may be corrupted during transmission

→ receiver check the each unit. if even parity accepted

Flowchart:



Example

$m = 00100110 \; 0001 \; 0011$

$w = 00101100 \; 00011 \; 00110$

Two dimensional parity check: (LRC)

→ Organize the block of bits in a form of rectangular matrix

→ parity bit are check for each row

→ " " " also " " " column

→ this is equivalent to 1 dimensional parity check.

Example:

Original data:

m = 10110011 : 10101011 : 01011010 : 11010101

$$\left.\begin{array}{r} 10110011\ \underline{1} \\ 10101011\ \underline{1} \\ 01011010\ \underline{0} \\ 11010101\ \underline{1} \end{array}\right\} \text{row parity}$$

$$\underbrace{10010111}_{} \rightarrow \text{column parity}$$

codeword:

w = 10110011 : 10101011 : 01011010 : 11010101 : 10010111

Performance of 1 dimensional parity check:

To move from one codeword to another codeword, at least two data bits should be changed. So these set of code words are said to have a minimum hamming distance of 2.

It can detect all single bit errors in each code word.

Performance of 2 dimensional parity check:

→ can diteet a burst error of n bits.

→ A burst error more than n bits is also detected

Checksum:

→ error detecting technique, can be applied to a message of any length

→ message is first devide into m-bit units

→ generator then creates an extra m-bit unit called the checksum.

→ at sender's end segment are added using 1's complement arithmatic to get the sum.
The sum is complemented to get the checksum.

→ at the receiver end same way find a checksum

→ If the result is zero, the the received data is accepted. ~~otw~~ otherwise rejected.

CamScanner

Example:

$m = 0010\ 0110\ 1001\ 0011$

Sender

```
  0010
  0110
 ------
  1000
  1001
 ------
  0001
     1
 ------
  0010
  0011
 ------
  0101
 -> 1010 ← checksum
```

$\therefore\ w = 0010\ 0110\ 1001\ 0011\ 1010$

Receiver

```
  0010
  0110
 ------
  1000
  1001
 ------
  0001
     1
 ------
  0010
  0011
 ------
  0101
```

```
  0101
  1010
 ------
  1111
  0000 ← checksum
```

As at receiver end checksum result is zero the received data is accepted.

CRC (Cyclic Redundancy Check)

→ used in networks such as (LANs and WANs)

→ also known as polynomial code

Polynomial:

A pattern of 0s and 1s can be represented as a polynomial with coefficients of 0 and 1.

Polynomial can be ~~shortth~~ shortened by removing all terms with zero coefficient and replacing x^1 by x and x^0 by 1.

→ k bit datacword

→ ~~datacword~~

→ codeword is n bit

→ datacword is augmented by adding (n-k) or number of bit same as degree of polynomial.

→ generator uses a devisor of size $n-k+1$

CamScanner

→ generator divides the augmented dataword by the divisor (modulo-2 divison)

→ ~~quo~~ quotient of the division is discarded.

→ reminder is appended to the dataword to create codeword.

→ In the receiver end some reminder is produced by similarly, called syndrom

→ If syndrom bit is zero data is accepted

divison operation:

→ addition and subtraction in this case are the same

→ we use the XOR operation to do both

→ If in divison operation if the leftmost bit of the dividend is 0 the step can't use the regular divisor.

Degree of polynomial:

the highest power in the polynomial.

Multiplying of dividing term:

multiplying: just add the powers

dividing: subtract the powers

Shifting:

leftshift: shifting to the left means adding extra 0s as rightmost

rightshift: deleting some rightmost bit.

CamScanner

Example:

$m = 1001$

$G(x) = x^3 + x + 1$

$\therefore$ divisor $= 1011$

degree of polynomial $= 3$

Now add 3 zero at the last of m

$\therefore m' = 1001000$

```
1011 ) 1001000 ( 1010
       1011
       ----
        0100
        0000
        ----
         1000
         1011
         ----
          0110
          0000
          ----
           110
```

$\therefore$ reminder $= 110$

~~codeword~~

$\therefore$ codeword $w = 1001110$

$\therefore CRC = 110$

at receiver end,

divisor = 1011

~~remain~~

w = 1001110

Now,

```
1011) 1001110 (1010
      1011
      ----
       0101
       0000
       ----
        1011
        1011
        ----
         0000
         0000
         ----
          000
```

So reminder is 000

As reminder is 000,
data is accepted

Performance of CRC:

→ can detect all single bit error

→ " " " double " "

→ " " any odd number of errors (X+1)

→ " " all burst errors of less than the degree of polynomial

→ CRC detect most of the larger burst errors with a high probability

→ CRC-12 detects 99.97% of errors with a length of 12 or more.

CamScanner

Error correcting technique:

→ forward error correction
→ receiver can use an error-correcting code
→ automatically corrects certain errors

→ backward
→ discovered an error
→ sender retransmit the entire data unit

four different error correction technique

1. Hamming codes
2. Binary convolutional codes
3. Reed-Solomon codes
4. Low density parity check codes

→ developed by R.W. Hamming

Hamming codes:

A set of error correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver.

→ can be applied data unit of any length

→ used to correct single bit error.
detect and

Redundant bit:

Extra bit binary bit that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer.

→ number of redundant bit = r

→ ~~data bin~~ =

→ " of data " = m

Formula to calculate redundant bit

$$\boxed{2^r \geq m + r + 1}$$

→ $\boxed{\text{Check bit is } 2^n}$ (power of two)

→ ~~hamming code is a~~ can be

→ Check bit is also called $\boxed{\text{parity bit}}$

bit that append to the data to ensure the total numbers of 1's in the data is even or odd.

☆☆ → Check bit can also use module-2 technique.

→ all the other bits marked as data bit.

→ Each data bit included in a unique set of parity bit

Check 1 Skip 1 → parity bit 1 : 1 in the least significant

" 2 : 1 " " 2nd position

Check 2 Skip 2 → " " 3rd "

" 4 : 1 " " 4th "

Check 4, Skip 4 → " " 8 : 1 " "

Check 8, Skip 8 → " " " " "

→ parity bit = 1 if total no of 1 is odd
otherwise 0

At receiver:

→ receiver check all parity bit pattern

→ parity bit = 1, if total no of 1 is odd
otherwise 0

→ Sequence of parity bit ~~make~~ determine the error location

→ if all parity bit is zero data is accepted.

otherwise there is an error and invert

→ Check result is also called error syndrom.

Hamming distance:

Hamming distance between two words is the number of differences between corresponding bits.

→ can easily found by applying XOR operation (⊕) and counting the number of one's.

→ denoted as $d(x, y)$

two words

Minimum hamming distance:

Minimum Hamming distance is the

> Smallest Hamming distance between all possible pairs of codeword.

Bit sequence = 1010011110

divisor = 1011 = $x^3 + x + 1$

Find out the CRC!
and check the answer!

Soln.

Given that,

divisor = 1011

Bit sequence = 1010011110

Finding CRC

```
                 10010001 1
1011 ) 1010011110 0000
       1011
       ----
        0010
        0000
        ----
         0101
         0000
         ----
          1011
          1011
          ----
           0001
           0000
           ----
            0011
            0000
            ----
             0110
             0000
             ----
              1100
              1011
              ----
               1110
               1011
               ----
                1010
                1011
                ----
                 001
```

∴ Codeword, $\omega = 101001111 0001$

Checking

```
              1001000111
1011) 101001111 0001 (
      1011
      ----
       0010
       0000
       ----
        0101
        0000
        ----
         1011
         1011
         ----
          0001
          0000
          ----
           0011
           0000
           ----
            0110
            0000
            ----
             1100
             1011
             ----
              1110
              1011
              ----
               1011
               1011
               ----
                000 ← reminder
```

As reminder is zero, so there is no error and message is accepted

~~b) m polynomial of one~~

b) Given that,

polynomial of message $= x^7 + x^5 + 1$

generator polynomial $= x^3 + 1$

$$
\begin{array}{l}
x^3+1 \,\big)\, x^7 + x^5 + 1 \;\big(\, x^4 + x^2 + x \\
\quad\; x^7 + x^4 \\
\hline
\quad\; x^5 + x^4 + 1 \\
\quad\; x^5 + x^2 \\
\hline
\quad\; x^4 + x^2 + 1 \\
\quad\; x^4 + x \\
\hline
\quad\; x^2 + x + 1 \text{ (remainder)}
\end{array}
$$

So the CRC is $x^2 + x + 1$

Ans

Given that,

b message stream, $m = 100\ 1110\ 1$

generator polynomial $G(x) = x^3 + 1$

$\therefore$ divisor $= 1001$

augmented bit stream, $m' = 1001110\ 1000$

P.t.o

```
1001) 10011101000 (10001100
      1001
      ----
       0001
       0000
       ----
        0011
        0000
        ----
         0110
         0000
         ----
          1101
          1001
          ----
           1000
           1001
           ----
            0010
            0000
            ----
             0100
             0000
             ----
              100
```

∴ actual bit string transmitted is = 10011101100

After inverting 3rd bit from left

to ∴ w = 10111101100

Now, devide w by 1001.

```
          10101000
1001) 10111101100
      0001
      ----
       0101
       0000
       ----
        1011
        1001
        ----
         0100
         0000
         ----
          1001
          1001
          ----
           0001
           0000
           ----
            0010
            0000
            ----
             0100
             0000
             ----
              100
```

As reminder is 100. which is not zero.
So error is detected.

Given that,

$m = \underline{1001}\,\underline{1100}\,\underline{1010}\,\underline{0011}$

4 bit word

Finding value of checksum,

```
  1001
  1100
 ------
  0101
     1
 ------
  0110
  1010
 ------
  0000
     1
 ------
  0001
  0011
 ------
  0100 (complement)
  1011 ← checksum
```

Given that,

received, hamming code, = 0xE4F

= 111001001111

As total length of message = 12

and, $12+1 \leq 2^4$

$16 + 6 + 1 < 2^5$

So there are 4 redundant bit.

~~For,~~

~~For r_1 = 1, 3, 5, 7, 9, 11 =~~

~~For r_1 = 1, 3, 5, 7, 9, 11 → r_1 =~~

Now,

r_1	r_2		r_4	r_8			r_6				
1	1	1	0	0	1	0	0	1	1	1	1
~~12~~ 1	~~11~~ 2	~~10~~ 3	~~9~~ 4	~~8~~ 5	~~7~~ 6	~~6~~ 7	~~5~~ 8	~~4~~ 9	~~3~~ 10	~~2~~ 11	~~1~~ 12

r_1 : 1, 3, 5, 7, 9, 11 → r_1 = 0

r_2 : 2, 3, 6, 7, 10, 11 → r_2 = 1

r_4 : 4, 5, 6, 7, 12 → r_4 = 0

r_8 : 8, 9, 10, 11, 12 → r_8 = 0

$r_8\, r_4\, r_2\, r_1$ = 0010 = 2

∴ from left no 2 bit should be inverted

So original bit string =

1010010011111

= A4F

∴ in hexadecimal original data value was 0 ← A4F (with hamming code)

Original data value

= 10101111

= AF

Find out the checksum for

1001 1100 1010 0011

4 bit word.

Ans:

Given,

dataword, m = 1001 1100 1010 0011

```
 1001
 1100
 ----
 0101
   1
 ----
 0110
 1010
 ----
 0000
   1
 ----
 0001
 0011
 ----
 0100

 1011
```

```
 0011
 1010
 ----
 1101
 1100
 ----
 1001
   1
 ----
 1010
 1001
 ----
 0011
   1
 ----
 0100
 1011
```

Hamming code for

1011110

Ans

$m = 7$

$m + r + 1 \leq 2^r$

$\Rightarrow 7 + r + 1 \leq 2^r$

$\Rightarrow 8 + r \leq 2^r$

$\Rightarrow 2^r \geq 8 + r$

$r = 4$

r_1	r_2	1	r_4	0	1	1	r_8	1	1	0
1	2	3	4	5	6	7	8	9	10	11

$r_1 = f(1, 3, 5, 7, 9, 11)$

$= 1$

$r_2 = f(2, 3, 6, 7, 10, 11)$

$= 0$

$r_4 = f(4, 5, 6, 7)$

$= 0$

$r_8 = f(8, 9, 10, 11)$

∴ ~~original~~
∴ Hamming code,

1 0 1 0 0 1 1 0 1 1 0

16 bit message.

$\therefore m = 16$

∴ Check bit r =?

$m + r + 1 \leq 2^r$

$\Rightarrow 2^r \geq 16 + 1 + r$

$\Rightarrow 2^r \geq 17 + r$

$\therefore r = 5$

∴ 5 bit check bit needed at position. 1, 2, 4, 8, 16

Ans

message = 1101 0011 0011 0101

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
r_1	r_2	1	r_4	1	0	1	r_8	0	0	1	1	0	0	1	r_{16}	1	0

19	20	21
1	0	1

$r_1 = f(1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21)$
$= 0$

$r_2 = f(2, 3, 6, 7, 10, 11, 14, 15, 18, 19)$
$= 1$

$r_4 = f(4, 5, 6, 7, 12, 13, 14, 15, 20, 21)$
$= 1$

$r_8 = f(8, 9, 10, 11, 12, 13, 14, 15)$
$= 1$

$r_{16} = f(16, 17, 18, 19, 20, 21)$
$= 1$

$\therefore$ The bit pattern transmitted

$= 0111011\,0011001\,1\,0101$

21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4
~~1~~	~~1~~	~~0~~	~~1~~	~~0~~	~~r_{16}~~	~~0~~	~~1~~	~~1~~	~~0~~	~~0~~	~~1~~	~~1~~	~~r_8~~	~~0~~	~~1~~	~~0~~	~~r_4~~

3	2	1
~~1~~	~~1~~	~~r_2~~	~~r_1~~

data word m = 10100 1111

devisor 10111

∴ augmented data word m' = 10100 1111 0000

At sender side

```
10111 ) 10100 1111 0000 ( 10011 0111
        10111
        -----
         00111
         00000
         -----
          01111
          00000
          -----
           11111
           10111
           -----
            10001
            10111
            -----
             01100
             00000
             -----
              11000
              10111
              -----
               11110
               10111
               -----
                10010
                10111
                -----
                 01001
```

∴ Codeword = 10100 1110101

At receiver side,

```
10111) 10100111101 (10011011
       10111
       -----
        00111
        00000
        -----
         01111
         00000
         -----
          11111
          10111
          -----
           10001
           10111
           -----
            01100
            00000
            -----
             11001
             10111
             -----
              11100
              10111
              -----
               10111
               10111
               -----
                0000
```

As reminder is zero

∴ So data ~~add~~ accepted.

Flow control:

Process of data flow between computers or devices or between nodes so that data can be handeled in a effieient way.

→ both nodes needs to be in aggrement of data rates and buffer size.

→ used to controls the folow of data

→ ensures the rate at which a sender is transmitting is propoto proportion with receiver's receiving capabilites.

Classification of flow control

→ Utopia

→ Stop & wait protoeol

→ Sliding window protoeol.
  - → Go back-N
  - → Selective repeat

Characteristics of UTOPIA:

→ data transmission is one direction
→ no sequence number or acknowledgement are used
→ does not worry about the possibility of anything going wrong
→ transmitting and receiving network layers are always ready
→ processing time is ignored
→ infinite buffer space

disad → unrealistic, as it doesn't handle either flow or error

→ Channel is error free.

Steps: At sender:
→ data link layer gets a packet from network layer
→ make a frame
→ Send frame

At receiver:
→ data link layer receives a frame
→ extract the packet
→ deliver the packet to the network layer.

★ processing is ~~close to~~ that of an ~~unacknowledged~~ connectionless service

★ It ~~doesn't provide~~ error detection

★ Connectionless service ~~provide error dete~~

Stop and wait:

★★
- → Sender will send a packet
- → then stop and wait
- → receiver send an acknowledgement to the sender.

~~types of~~ Stop and wait:

- → Error free Stop & wait
- → Noisy Stop and wait
  - → Data can be lost
  - → Acknowledgement can be lost
  - → Delayed acknowledgement
  - → Delayed data
  - → Damaged frame.

→ receiver hardware will detect when when it compute checksum.

Characteristic:

→ Used in connection oriented communication

→ offers ~~error~~ error & flow control

→ data traffic is simplex

→ Used in Data link & transport layer

Error free Stop & wait / Simple Stop & wait

At Sender:

→ Sender send one data frame at a time

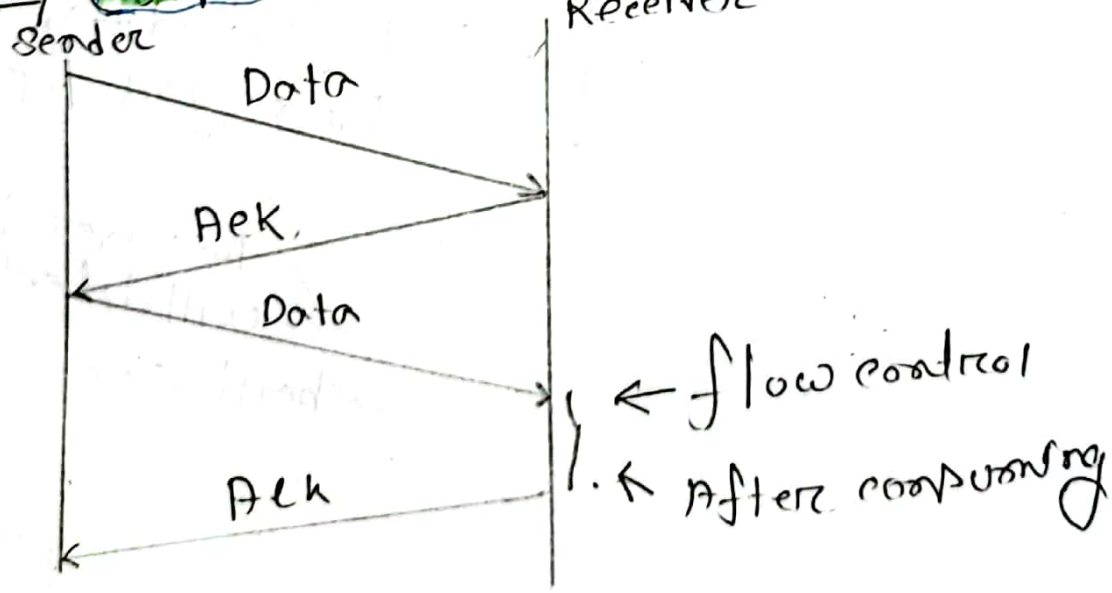
→ " " next packet after receiving acknowledgement

At receiver:

→ receive the ~~da~~ frame

→ Send an acknowledgement.

→ consume the data



~~For A~~ Noisy S

Noisy Stop & wait:

→ frame can be damaged / lost

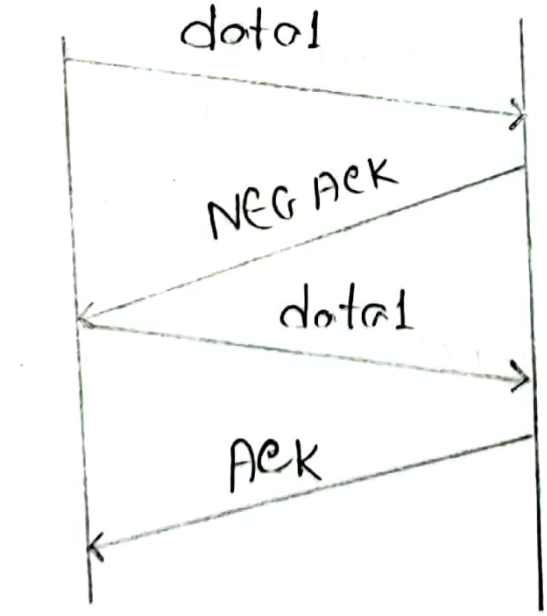
→ when damaged occur, receiver hardware detect by computing checksum.

→ discard the data

→ Send a negative acknowledgement

→ sender would time out

→ Sender send the data ~~gai~~ or frame again.



Data can be lost:

→ Receiver doesn't send an acknowledgement

→ Sender assume, data is lost or damaged

→ Sender, add a sequence number to the header of

→ Sender add a timer

→

Data can be lost:

→ ~~Recei~~ Data is lost

→ Receiver doesn't send ackn.

→ Sender add a timer

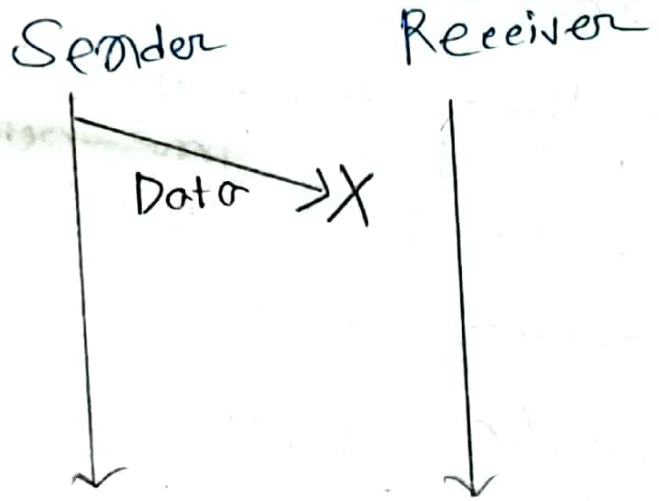
→ if timer is out, assume that data is lost or damaged

→ Send the

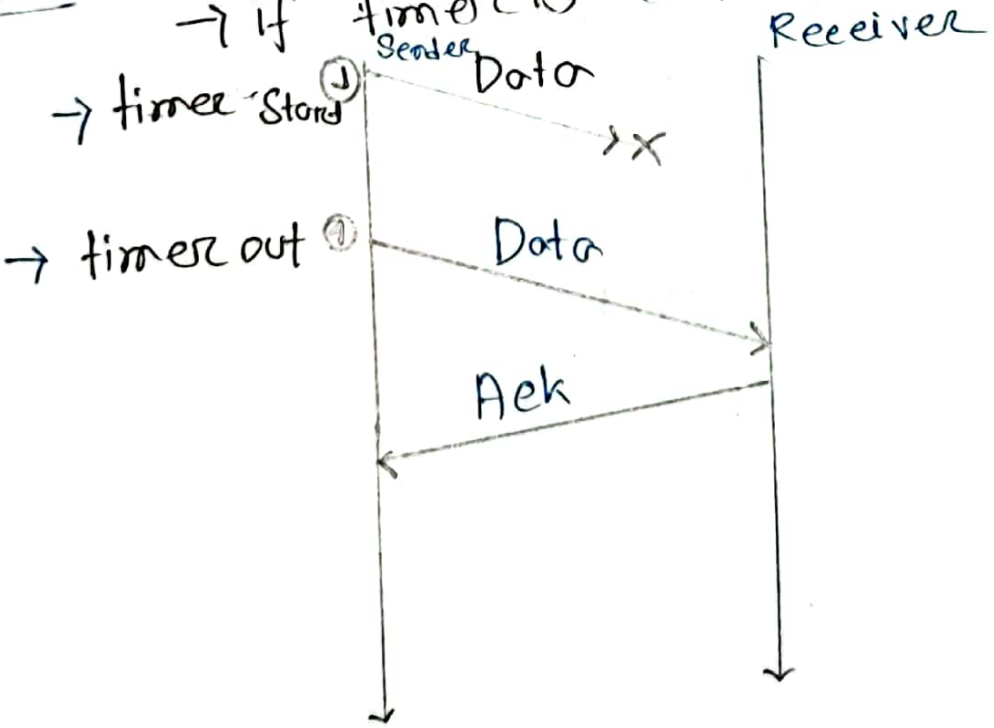
Data is lost

→ Sender send a data
→ Dat is lost
→ Sender wait for acknowledgement
→ Receiver " " data

Deadlock



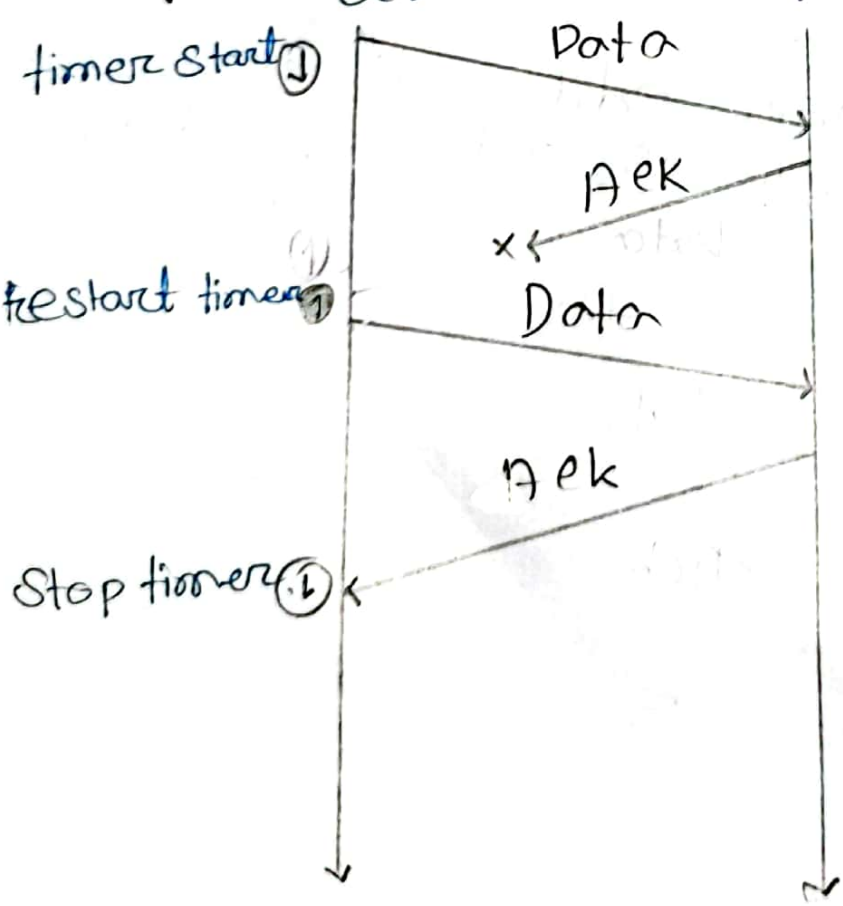
Solution: → Sender add a timer
→ if timer is out resend the data



~~Aeknowledgement can be lost~~

Aeknowledgement can be lost:

- → Sender add a timer
- → Sender send a frame
- → receiver receive it
- → " send an aeknowledgement
- → Aeknowledgement is lost.
- → ~~Sen~~ timer is out
- → Restat the time out timer
- → Sender retransmit the data
- → receiver receive it data
- → create problem of duplicate



Solution

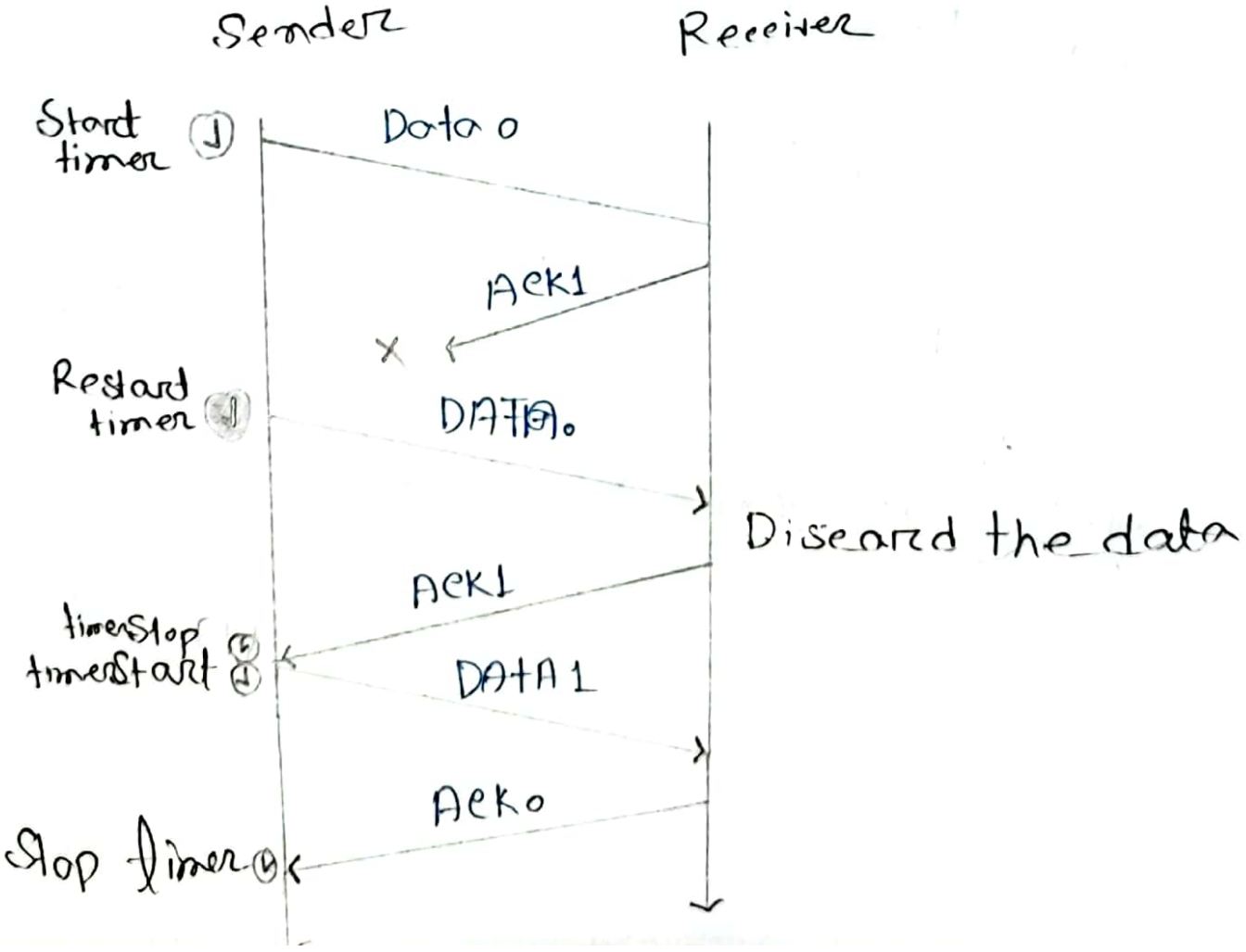
→ Add a sequence number at the header of data frame

→ Add an acknowledgement number of the Ack frame

NB: An acknowledgement number always define sequence number of next frame to receive

→ sequence numbers are 0, 1, 0, 1, ..

→ Ack " " 1, 0, 1, 0.



Note: When receiver find DATA frame with same sequence number as previous DATA frame, it discard the data, and send previous ACK no.

Thus duplicate is avoided.

ARQ / PAR:

Protocol in which the sender waits for positive acknowledgement before advancing to the next data item are often called

ARQ or PAR

ARQ → Automatic Repeat request.

PAR → positive acknowledgement with Retransmission

How to prevent duplicate & damaged frame are not passed to the network layer)

Ans

After transmitting a frame & starting the timer, sender waits for something to happen.

3 possibilities exist

→ an acknowledged frame arrives undamaged

→ a damaged acknowledgement frame

→ timer expires

neither buffer nor the sequence number is changed.

sender fetches the next packet ~~from its network layer~~ & put it in the buffer

advances the sequence number.

when a valied frame arrive,

→ its sewence number is checked

→ take decision if it duplicate or not

→ if not duplicate passed it to the network layer

→ an acknowledgement is generated

Timer

→ if timer ~~is~~ was already running it will be reset to allow full timer interval

→ Interval should be chosen to allow enough time

→ for the frame to get to the receiver

→ for the receiver to process it in the worst case

→ for the ack frame to propogate back to the sender

Sliding window protocol:

→ data traffic is duplex

→ each outbound frame contains a sequence number, ranging from,

$0 - (2^n - 1)$ → Sender window size

→ sender has a sending window

→ receiver has a receiving "

→ sender and receiver window need not be same size

→ " and receiver window ~~nee~~ need not have same lower & upper limits.

→ Sender maintains a set of sequence numbers corresponding to frame it is permitted to send.

buffer size:

→ frames currently within the sender's window may lost or damaged in transmit.

→ So sender must keep all of these frames in its memory

for possible retransmission.

→ So if window size is n,
buffer size is n.

Piggybacking:

Technique of temporarily delaying outgoing acknowledgement so that, they can be hooked onto the next outgoing data frame is known as ~~piggyp~~ piggybacking.

Advantages:

→ better use of available channel bandwidth.

CamScanner

Types of Sliding window:

→ Go-back-N

→ Selective Repeat.

NB: Sliding window with window size = 1 is a Stop & wait protocol.

→ Sender transmits a frame

→ waits for its acknowledgement before sending the next one.

pick

Go back-N:

→ Sender window size = N

→ Receiver " " = 1

→ Sender can sent N consecutive frame without acknowledgement

→ keep a copy of these frames until the ACK ~~are~~ arrive.

→ ~~there~~ this technique of keeping multiple frames in flight is an example of pipelining.

CamScanner

What happen if a frame in the middle of a long stream is damaged in go-back-n?

Ans:

→ Receiver simply discard the damaged frame

→ receiver discard all subsequent frames

→ sending no acknowledgements for the discarded frames.

→ After time out sender re transmit all unacknowledged frames in order

→ Starting with the damaged or lost one.

Disadvantages:

→ Wast a lot of bandwidth if error rate is high.

Cumulative acknowledgement:

When an acknowledgement comes in for frame n, frames n-1, ~~fr~~ n-2 and so on are also acknowledge. This type of acknowledgement is called cumulative acknowledgement.

Selective Repeat

→ Sender and receiver maintain a window of outstanding

→ Sender window size : $10(2^n-1)$

→ receiver " " is fixed.

→ " has a buffer for each sequence number

→ whenever a frame arrive

→ sender receive it

→ check it by computing checksum

→ if good and ~~not received~~ accept duplicate before

→ Send an acknowledgement.

What happen if the frame is lost at the middle of the long stream is damaged)

Solⁿ:

→ bad frame is received is discarded

→ any good frame that after it is accepted and buffered.

→ ~~Sender~~ receiver send a negative acknowledgement

→ after time out sender retransmit the only oldest unacknowledged ~~fre~~ frame.

CamScanner

Formula related to selective Repeat:

→ window size = (maximum sequence + 1)/2

→ number of buffer = window size

→ number of timer = number of timer.

CamScanner

Go-Back-N vs Selective Repeat

Go-Back-N	Selective Repeat
1. Retransmit all the frames that sent after the frame which suspect to be damaged	1. Retransmit only those frames that are suspects to be damaged
2. It waste a lot ~~of~~ bandwidth	2. Comparatively less bandwidth is wasted in retransmitting
3. Less complicated	3. More complex as it require to apply extra logic Storing & Sorting at sender & receiver side
4. Window size N−1	4. Window size <= (N+1)/2
5. Storing is not required at receiv side	5. Receiver stores the frame received after the damaged frame in the buffer

6. Sorting is not required	6. Receiver must be able to sort as it maintain the sequence number
7. Searching is not required	7. Sender must be able to search and select only the requested frame
8. More often used	8. Less used for it's complexity
9. NAK refered to the next expected frame	9. NAK number refered to the frame lost

CS CamScanner

Computer Security
Chapter 1

Computer Security:

The protection afford to an automated information system in order to attain the applicable objective of preserving

- → the integrity
- → availability
- → confidentiality

} of information system resources

Security components:

- → Confidentiality → Data confidentiality, privacy
- → Integrity → Data integrity, System ,,
- → Availability

Confidentiality:

2 types

Data confidentiality:

Assure that,

~~→ coninformation in~~

→ information is not made available to unauthorized individual

→ information is not disclosed to unauthorized individual

not available/ disclosed

disclose = অনাবৃত

Privacy:

→ it is a reason for confidentiality.

→ ~~determine~~ degree to which entity is willing to share infon.

→ right of an entity ~~own~~ acting in its own behalf.

→ to determine the degree to which it will interact with environment.

→ Assures ~~to~~ individuals control or influence

→ what information related to them

Integrity:

2 types

Data integrity:

information and programs are changed in a specified and authorized manner.

~~Availa~~

System integrity

System perform its intended information in an unimpaired manner.

→ free from deliberate ~~or~~ unauthorized manipulation of the system.

Availability:

Assured that system work promptly and service is not denied to authorized users.

NB:
These three concept is often referred to as the CIA triad.

Example:
Turning off a computer
→ provides confidentiality
→ " Integrity
→ hurts availability

CamScanner

Characteristics of security elements

Confidentiality:

→ preserving unauthorized restrictions on information access & disclosure

→ protecting personal privacy and property information.

→ A loss of confidentiality is the unauthorized disclosure of information.

Integrity:

→ guarding against improper information modification, distruction

→ insuring information authenticity

→ A loss of integrity is unauthorized modification of information destruction " "

Example:

Confidentiality:

- Students grade information in USA is regulated by ~~Form~~ FERPA.

Result is available to

Students
their parents &
employees

While covered by FERPA this information is seen by more people.

~~The~~ This information is typically freely available to the public and published on a school's website.

CamScanner

Integrity:

→ Hospital patients allergy information stored in a database.

Doctor should be able to trust that information is correct and current.

Now suppose that an employee who is authorized to view and update this information

→ Anonymous online poll.

Many web sites such as a news organizations, offer these polls to their user with a very safeguards.

CamScanner

Availability:

→ having moderate availability requirement is a public web site for a university.

→ An online telephone directory lookup application would be classified as a low availability requirement.

Vulnerability:

→ error or weakness in the design, imple ~~imple~~ ~~mentati~~ on

→ error in the implementation

→ " in the operation of a system.

Threat:

→ potential for violation of security

→ exists when there is a circumstance, capability, action or event that could breach (ভাঙা) security and cause harm.

→ a threat is a possible danger that might exploit vulnerability.

Attack:

→ An assault (আকস্মিক আঘাত) on system security that derives (উৎপন্ন) from an intelligent threat.

→ An intelligent act, that is a deliberate (ইচ্ছাকৃত, intentional) attempt (প্রচেষ্টা) to evade (avoid) security services and violate the security policy of a system.

NB :

→ technical failing in a system is vulnerability

→ different enemies have different abilities

→ One can't design a security system → unless ~~you k~~ he/she know who the enemy is.

OSI Security architecture:

(Open System Interconnection)

· Provides a systematic frame-work for defining

→ security attacks

→ mechanisms

→ security service

Security attack:

Action that compromises the security of information owned by an organization

Security mechanism:

A Process that is designed to ~~detect~~

- → detect
- → prevent
- → or recover from a security attack

Security service:

A processing or communication service that ~~enhances the~~ enhance the security of the

- → enhance the data processing system
- → information transfer of an organization.

CamScanner

Attack:

Types of attack:

2 types

* Active attack → affect their operation → attempt to alter system resources

* passive attack
  → attempt to learn or make use of information from the system
  → doesnt affect system resources.

Passive attack:

goal: Oponent goal is to obtain information that is being transmitted.

Classification:

2 types

* The release of message content
* traffic analysis

CamScanner

Release of message content:

- A telephone conversation,
- or electronic mail message
- and a transferred file may contain sensetive /confidential information.

We would like to prevent opponent from learning the contents of these transmission.

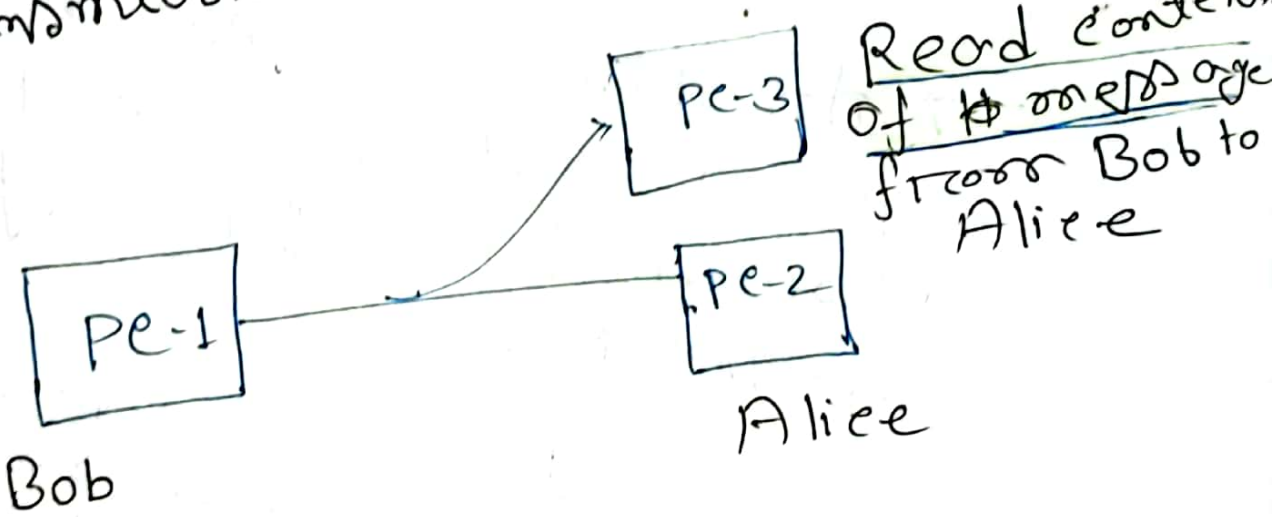


Fig: Release of message contents.

Traffic analysis:

~~Suppose that we have had a way of masking the way~~

→ had a way of masking the contents of message / other info.

→ common technique for masking is encryption

→ In this case case an oponent might be able to observe the pattern of there message.

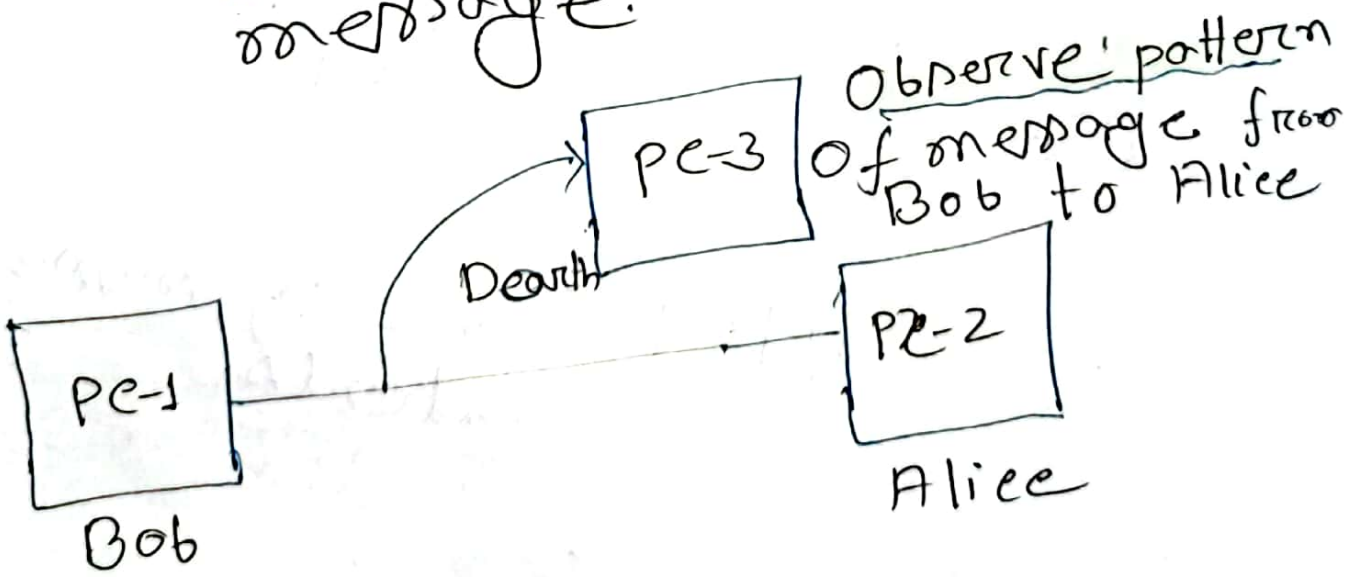


Fig: Traffic analysis.

NB:

→ passive attacks ~~is~~ are difficult to detect as they don't involve any alteration of data.

Active attack:

involves → modification of the data stream
→ creation of false stream.

4 types

→ masquerade
ছদ্মবেশ ধারণ করা

→ replay

→ modification of message

→ denial of service.

CamScanner

Masquerade:

→ Takes place when one entity pretends to be a different entity.

Example:

→ authentication sequence can be captured

→ replayed after a valid authentication sequence has taken place.

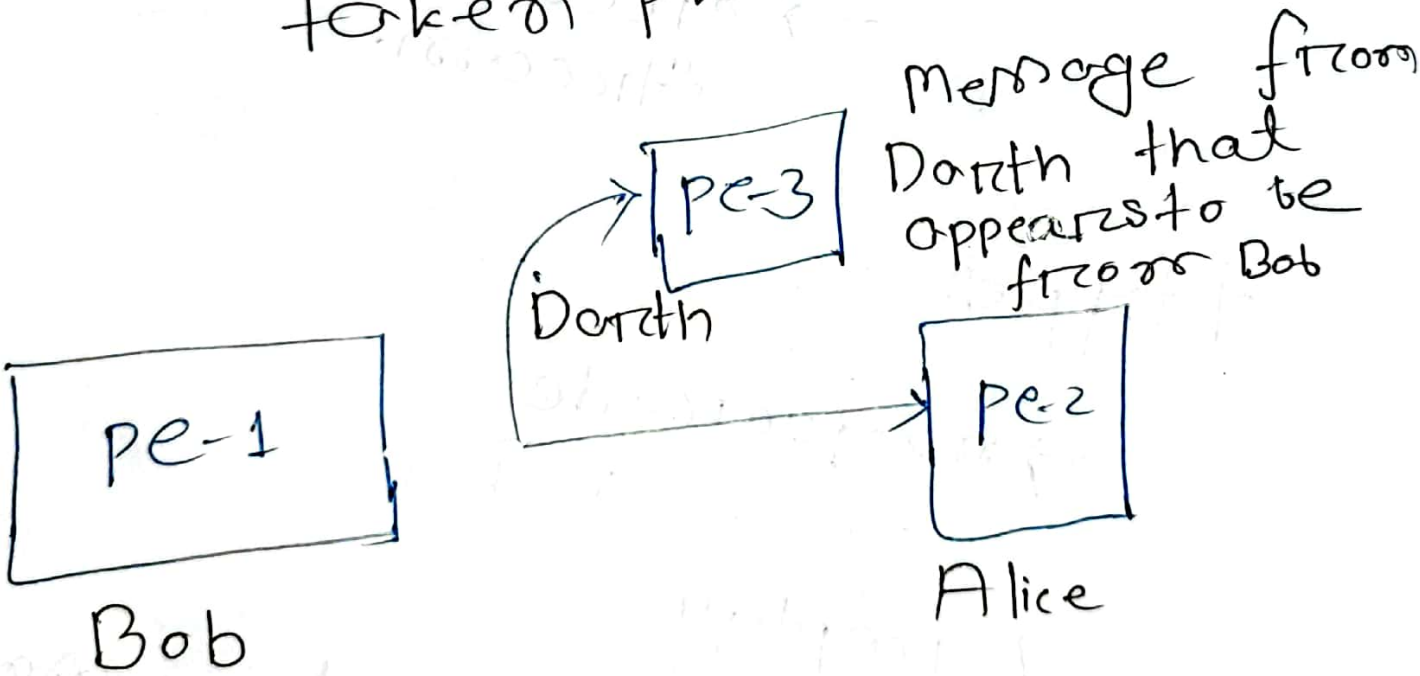


Fig: Masquerade.

~~Re~~

Reply:

→ passive capture of data unit opponent

→ its subsequent transmission to produce an unauthorized effect.

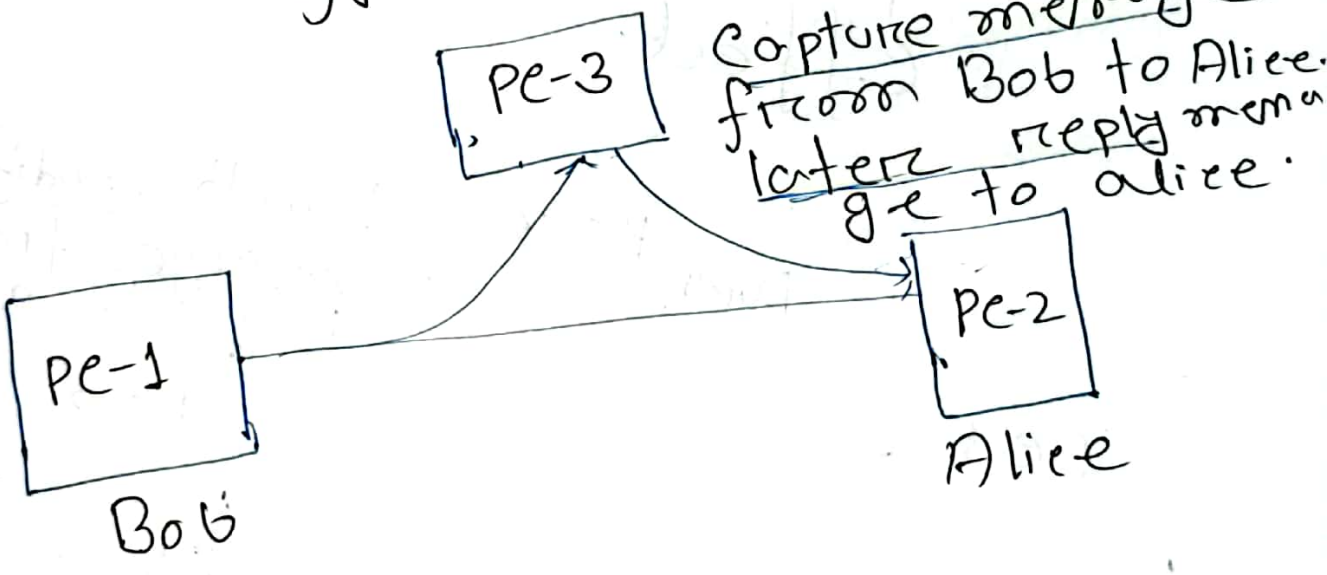


Fig: Replay

Modification of message:

→ Some portion of message is altered

→ messages are delayed or reordered

→ produce an unauthorized effect.

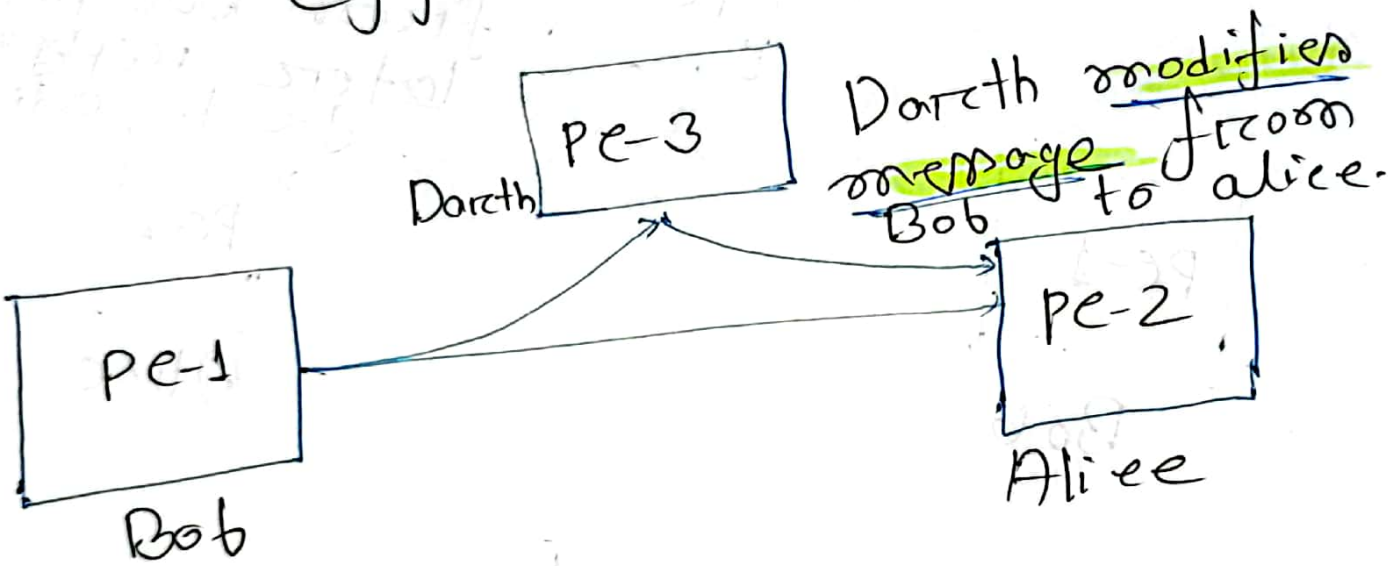


Fig: Modification of message.

CamScanner

denial of service:

→ prevent the normal use of communication facilitin.

→ attack may have a specific target.

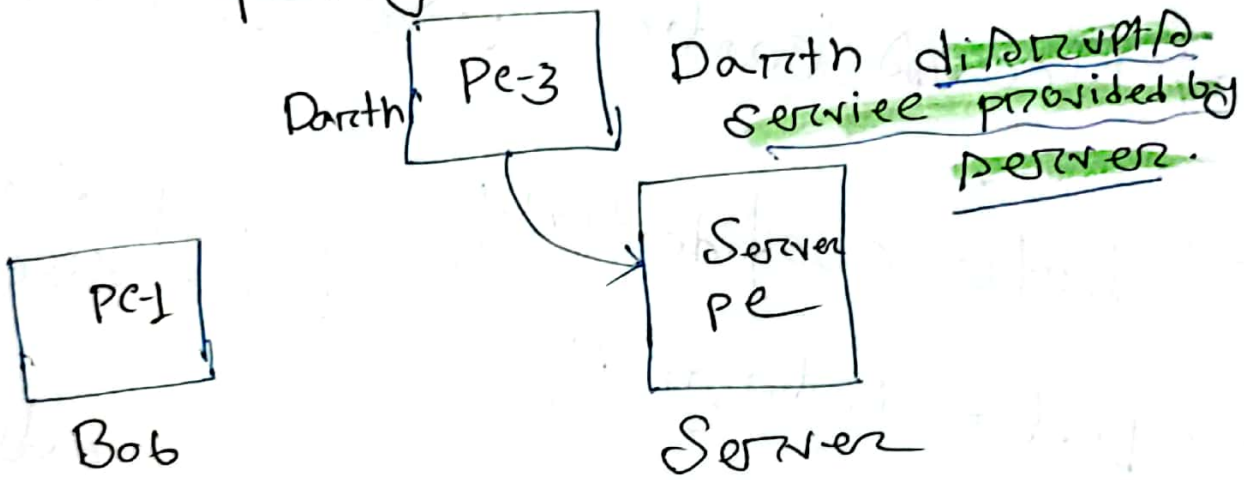


Fig: denial of service

NB: It is quite difficult to prevent active attacks absolutely because of wide variety of potential physical S/W and network vulnerabilities.

CamScanner

Security service:

X800 devides these service into 5 categories

→ Authentication

→ Access control → prevention of unauthorized use of resource

→ Data confidentiality → protection of data disclosure

→ Data integrity → prevention of unauthorized modification.

→ Non repudiation

★ Availability service → protect a system to ensure availability

Authentication:

Assurance that communicating entity is the one claimed.

CamScanner

Ex:

Consider a person using online banking service.

Both the user and the bank should be assured in identities of each other.

Access control:

Example:

In online banking a user may be allowed to see his balance. But not allowed to make any transaction for some of his accounts.

CamScanner

→ connection → Selective-field
→ connection Less
→ traffic-flow

Data confidentiality:

protection of data disclosure.

Example:

In online banking a user may be allowed to see his balance, but not allowed to see other's resource balance.

Data integrity:

Assurance that data received are exactly as sent by an authorized entity

i.e contain

- → no modification
- → no insertation
- → no deletion
- → no replay

~~Non-redul~~ → নিজের বলে অস্বীকার করা

Non-repudiation:

Provide protection against denial by one of the entities involved in communication.

Example:

An online banking who has made a transaction, but later denied that. How the bank can protect itself in such a situation?

CamScanner

Security Mechanism:

used to implement security services.

They include (X.800):

- Encipherment
- Digital signature
- Access control mechanism
- Data integrity "
- Authentication Exchange
- Routing control

CamScanner

Classical Encryption Technique
Chapter-2

Symmetric encryption:

→ encryption and decryption are performed using same key.

→ Also known as conventional encryption.

Example: DES, AES

→ also known as single key encryption

Pla

Asymmetric algorithm

→ also known as public key encryption

→ use different keys for encryption & decryption.

CamScanner

Some basic terminology:

Plaintext:

An original message is known as plaintext

Ciphertext:

Coded message is called ciphertext

Encipher / encryption

The process for converting from plaintext to ciphertext.

Decipher / decryption:

The process for restoring the plain text from ciphertext is deciphering or decryption.

CamScanner

Cryptography:

Study of encryption principles/ methods.

Cryptanalysis:

Study of principles / methods of deciphering ciphertext without knowing key.

Cryptology:

The areas of cryptography and cryptanalysis together are called cryptology.

Key:

Info or value used in cipher, known by sender and receiver and independent of the plaintext and algorithm.

CamScanner

Cipher:

Algorithm for transforming plaintext to ciphertext.

Cryptosystem:

A pair of algorithms that

→ take a key ~~and~~

→ convert plaintext to ciphertext and back

Symmetric Cipher Model:

~~As~~ Symmetric encryption model has five ingredient
उपादान

1. Plaintext
2. Encryption algorithm → perform various substations
3. Secret key → perform various transformation ~~of~~ on the plaintext
4. Ciphertext
   → depends on plaintext & secret key
   → also input to the encryption algorithm
5. Decryption algorithm → a value independent of plaintext and algorithm
   → encryption algorithm run in reverse
   → takes ciphertext and secret key

CamScanner

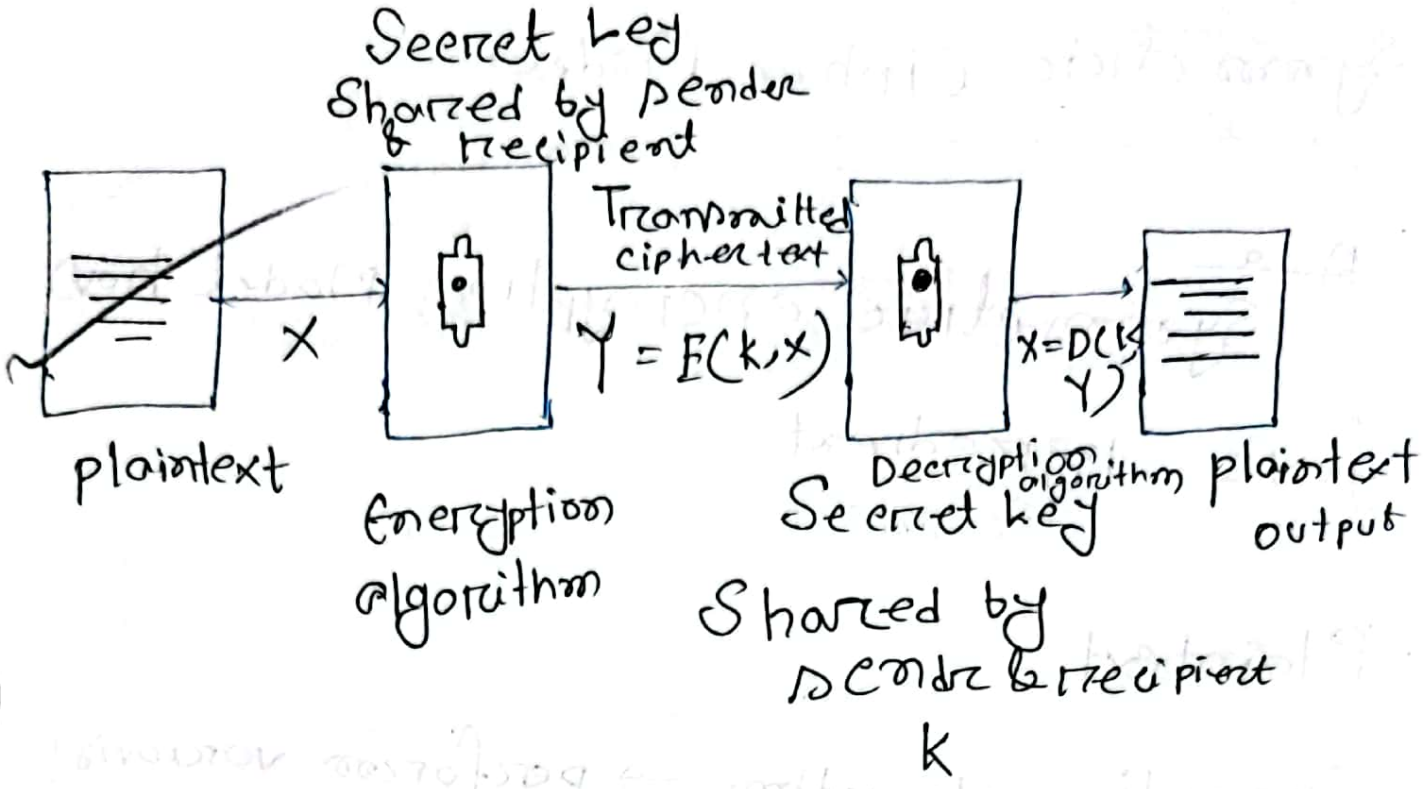


Fig: Simplified Model of symmetric encryption

~~Encryption~~

Requirement of encryption:

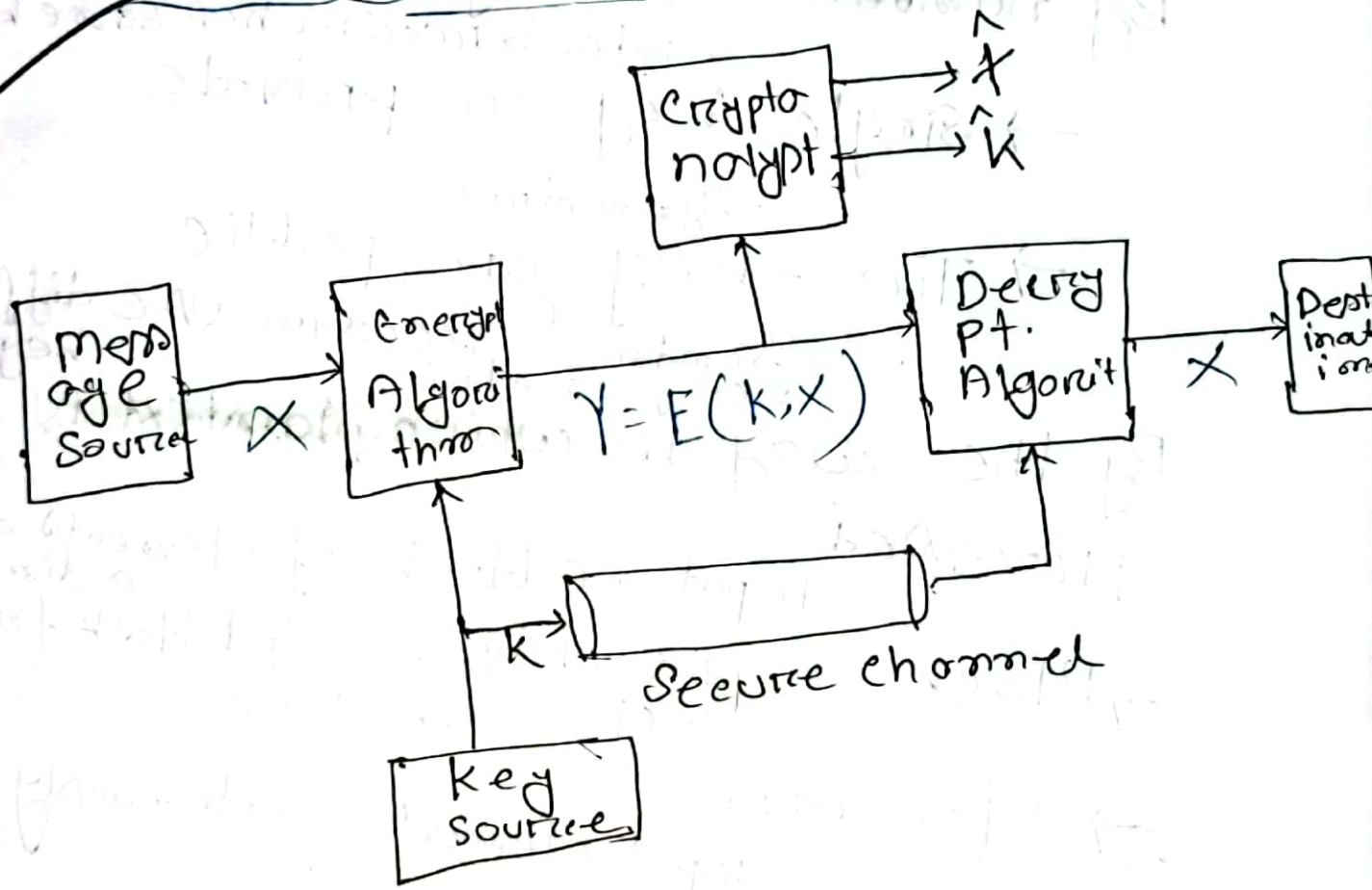
1. Need a Strong encryption algorithm.

Algorithm would like that, opponent, would be unable to decipher the ciphertext

→ figure out the key.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

Model of symmetric cryptosystem:



Cryptosystem Classification:

→ characterized by three independent dimensions

By type of encryption operations used for

→ each element in the plaintext is mapped into another element

→ Substitution

→ Transposition

→ element in the plaintext are rearranged

By number of keys used

→ Single-key or private

→ Sender & receiver has same key

→ Symmetric

→ Two-key or public

→ Sender & receiver use diff. keys

→ asymmetric

By the way in which plaintext is processed

→ input one block of elements at a time

→ Block

→ producing an output block for each input block

→ Stream

→ input elements continuously

→ producing an output block one element at a time.

Cryptanalysis:

The process of attempting (try) to discover plaintext (x) or key (K) or both is known as cryptanalysis

~~Appr~~ Objective

To recover key not just message.

Approaches:

- → exploit the characteristic of the algorithm
- → relay on nature of the algorithm
- → some knowledge of charact. of plaintext & ciphertext pair

→ Cryptanalytic attack
→ try to deduce a specific plaintext/key being used

→ Brute-force attack
→ attacker tries every possible key or a piece of cipher text until ~~an it intel~~ a translation into plaintext is obtained

2 more defination

→ unconditionally secure encryption scheme can be → ~~chi~~ ciphertext generated by the scheme doesn't contain enough info. to determine the plain text

→ computationally secure

Criteria for computationally secure

Algorithm:

1. Cost of breaking the cipher exceeds the value of the encrypted information

2. The time required to break the cipher exceeds the useful lifetime of the information.

effort < benefit ⇒ not secure
effort > benefit ⇒ secure

CamScanner

unconditionally secure:

- if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext.

Substitution technique: technique in which letter or plaintext are replaced by other letters or by number/symbol

- → ~~Cas~~
- → Caesar Cipher
- → monoalphabetic cipher
- → playfair cipher
- → Hill cipher
- → polyalphabetic cipher
- → One-Time pad.

CamScanner

Caesar Cipher:

→ invented by Julius caesar

→ replacing each latter of the alphabet with the 3rd letter.

→ alphabet is wrapped around so that letter following Z is A

Plain: a b c d e f g h i j k l m n o p q

Cipher: D E F G H I J K L M N O P Q R S T

plain: r s t u v w x y z

cipher: U V W X Y Z A B C

→ assign a numerical equivalent to each letter

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z	—	—	—
13	14	15	16	17	18	19	20	21	22	23	24	25	—	—	—

→ For each plaintext letter p.
substitute the ciphertext letter c

$$c = E(3, p) = (p+3) \bmod 26$$

Generally

$$\boxed{c = E(k, p) = (k+p) \bmod 26}$$

☆ k is in range 1 to 25

For decrypt.

$$\boxed{p = D(k, c) = (c-k) \bmod 26}$$

NB : Brute force cryptoanalysis is easily performed.

CS CamScanner

Characteristic: ~~of this~~

→ encryption & decryption algorithm is known

→ there are only 25 key

→ language of plaintext is known and easily recognizable.

★ triple DES algorithm

→ use 168 bit key

→ give 2^{168} key space

Monoalphabetic cipher:

→ shuffle the letters and map each plaintext letter to a different random ciphertext letter

→ secure against brute-force attack

→ not " " cryptanalytic attack

→ key space is 26!

CamScanner

cryptanalytic attack:

→ in english E is the most common letter followed by T, R, N, I, O, A, S

→ Other letters like Z, J, K, Q, X are fairly rare

→ relative frequency of the letters can be determined

→ compared to a standard frequency distribution

→ for long message this technique is sufficient.

→ A powerful tool is to look at the frequency of two letter combinations known as diagram.

developed by Charles Wheatstone
→ named after his friend Baron Playfair
1854

Playfair

→ multiple letter encryption

→ it is based on use of a 5×5 matrix

→ filling the keyword
from left to right
from top to bottom

→ remainder of the matrix
with the remaining letters
in alphabetic order.

→ letter I and J count as
one letter.

→ plaintext is encrypted 2 letters at a
time.

→ একই Row তে পড়লে clock wise ঘুরে যাবে

→ একই ~~এক~~ column এ " replaced by the
letter beneath with the top ele
ment

→ If form a rectangle replaced by
letter lies in the own row
and column in the other

* J/I থাকলে যেকোন একটা নিলেই হবে
* বিজোড় " X দ্বারা প্রতিস্থাপিত করব.

Key = MONARCHY

matrix:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Key = JLJKEZOO

J/I	L	K	E	Z
O	A	B	C	D
F	G	H	M	N
P	Q	R	S	T
U	V	W	X	Y

Original letter: COMPUTERS

∴ = COMPUTERSX

= ~~DAFSPY~~

Cipher text = DAFSYPOKSXE

CamScanner

Characteristics:

→ advanced over simple monoalphabetic

→ there are 26×26=676 diagram

→ identification of each individual diagram is difficult.

→ considered long time unbreakable.

→ by British Army in World WAR I

→ by U.S Army and other Allied force during World WAR II

Hill Cipher:

→ developed by mathematician Hill in 1929

→ multiple letter cipher.

→ take m successive plaintext letters

→ substitutes for m ciphertext column.

~~For m~~ For m=3

$$\begin{pmatrix} c_1 & c_2 & c_3 \end{pmatrix} = \begin{pmatrix} P_1 & P_2 & P_3 \end{pmatrix} \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \bmod 26$$

$$C = PK \bmod 26$$

CamScanner

~~P=CK~~ $\boxed{C = PK \bmod 26}$

$\boxed{P = CK^{-1} \bmod 26}$

→ it hides single letter frequencies

→ large matrix also hide more frequency

→ 3×3 hides single-letter, two- " } frequency

Polyalphabetic Cipher:

→ set of related ~~mel~~ monoalphabetic substitution rules is used

→ A key determines which particular rule is chosen for given transformation.

One time pad:

→ used in secure place.

→ random key as long as message is used.

→ unbreakable → since ciphertext bears no statistical relationship

→ any ciphertext and any plaintext → exist a key mapping one to other

Transposition technique:

Technique in which mapping is achieved by performing some sort of permutation on the plaintext letters.

→ transposition.

→ hide the message by rearranging the letter order.

→ ~~without~~ or
→ doesn't alter the actual letter

Classification:

→ rail fence
→ row transposition ciphers.
→ product cipher.

~~Rem~~

CamScanner

Rail fence:

→ plaintext is written down as a sequence of diagonals.

→ read off as a ~~rece~~ sequence of rows.

Example: rail fence of depth=2

plaintext: "meet me after the toga party"

m e m a t r h t g p r y
e t e f e t e o a a t

ciphertext: mematrhtgpryetefeteoaat

Row transposition technique:

→ write the message in a rectangle row

→ read the message column by column.

→ permute the order of the column.

CamScanner

Example:

Key: 4 3 1 2 5 6 7

Plaintext: a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z

Cipher text: T T N A A P T M T S U O A O d W
C O J X K N L Y P E T Z

→ easily recognized ~~as it has~~
as it has same letter frequency as ~~as~~ the original plaintext.

→ make more secure by performing more than one stage of transposition

→ (transpopition + substitution)
→ cover cipher

Product Cipher:

→ two substitutions make a more complex subst

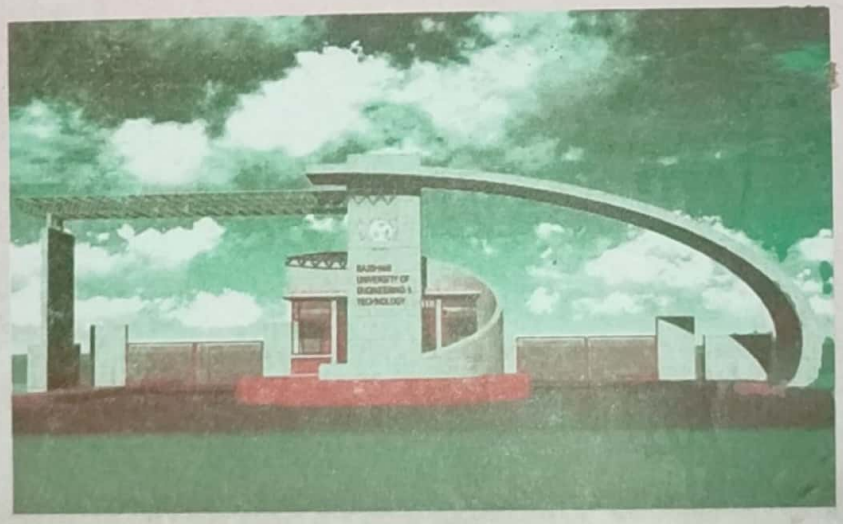
a bridge from original to

→ two transpopition " | a " compl.

"Heaven's Light is Our Guide"

RAJSHAHI UNIVERSITY OF ENGINEERING & TECHNOLOGY

RUET



Name : MD Ismail

Subject : CSE-3205 (Computer Network) Year : ○1st ○2nd ○3rd ○4th

Roll No : 1503094 Semester ○1st ○2nd ○3rd ○4th ○5th ○6th ○7th ○8th

MSS Sir

Department CE EEE ME CSE ETE IPE URP GCE MTU ARCH

120 PAGE

CamScanner

Chapter-2

Stegaro graphy:

Concealing message or information within others.

CamScanner

Chapter-3

Block Cipher & The Data Encryption Standard:

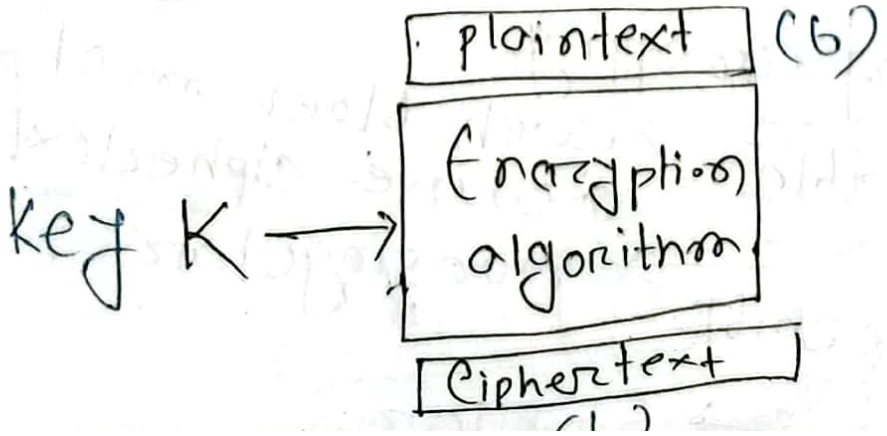
Stream cipher:

encrypt a digital data stream, one bit or one byte at a time

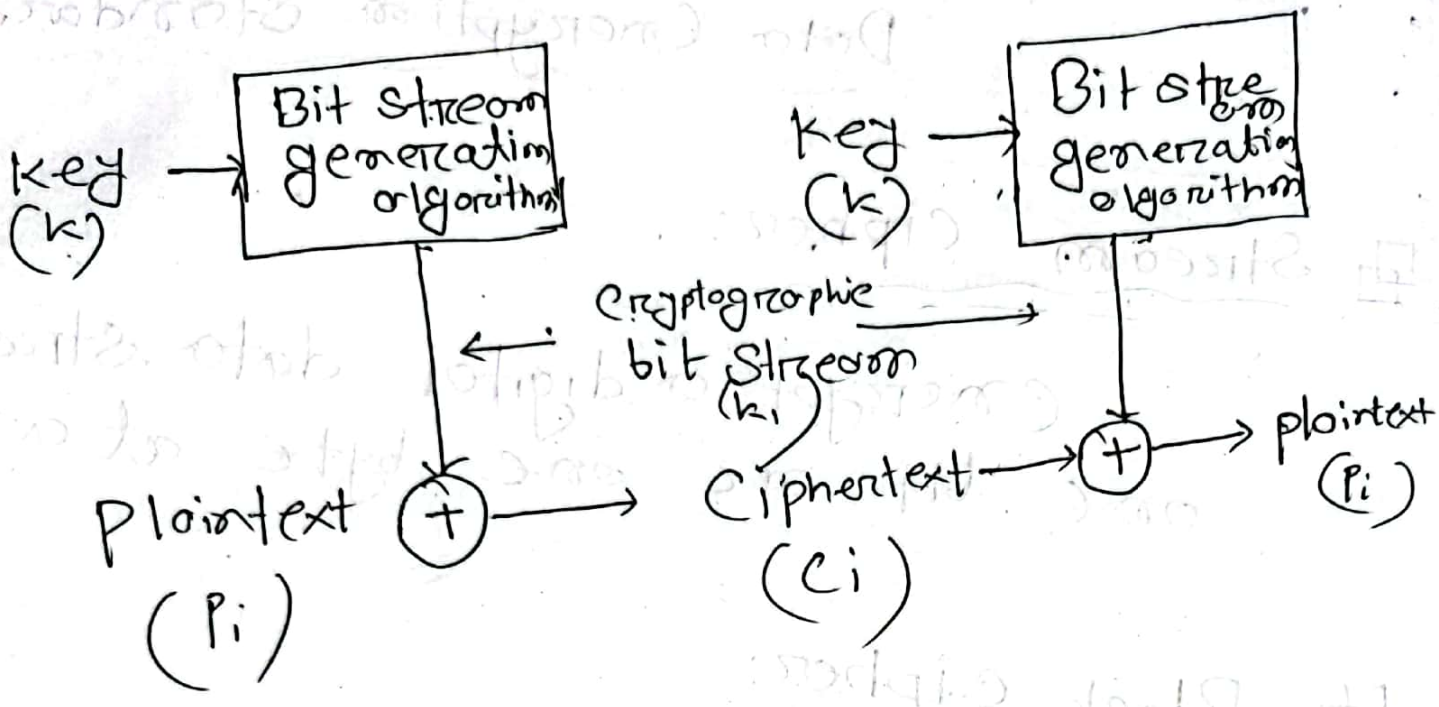
Block cipher:

A block of plaintext treated as a whole and used to produce a ciphertext block of equal length.

Block diagram of block cipher:



Block diagram of Stream cipher.



Feistel Cipher Structure

→ plain text block n bit

→ cipher " " n bit

→ 2^n possible different plaintext block

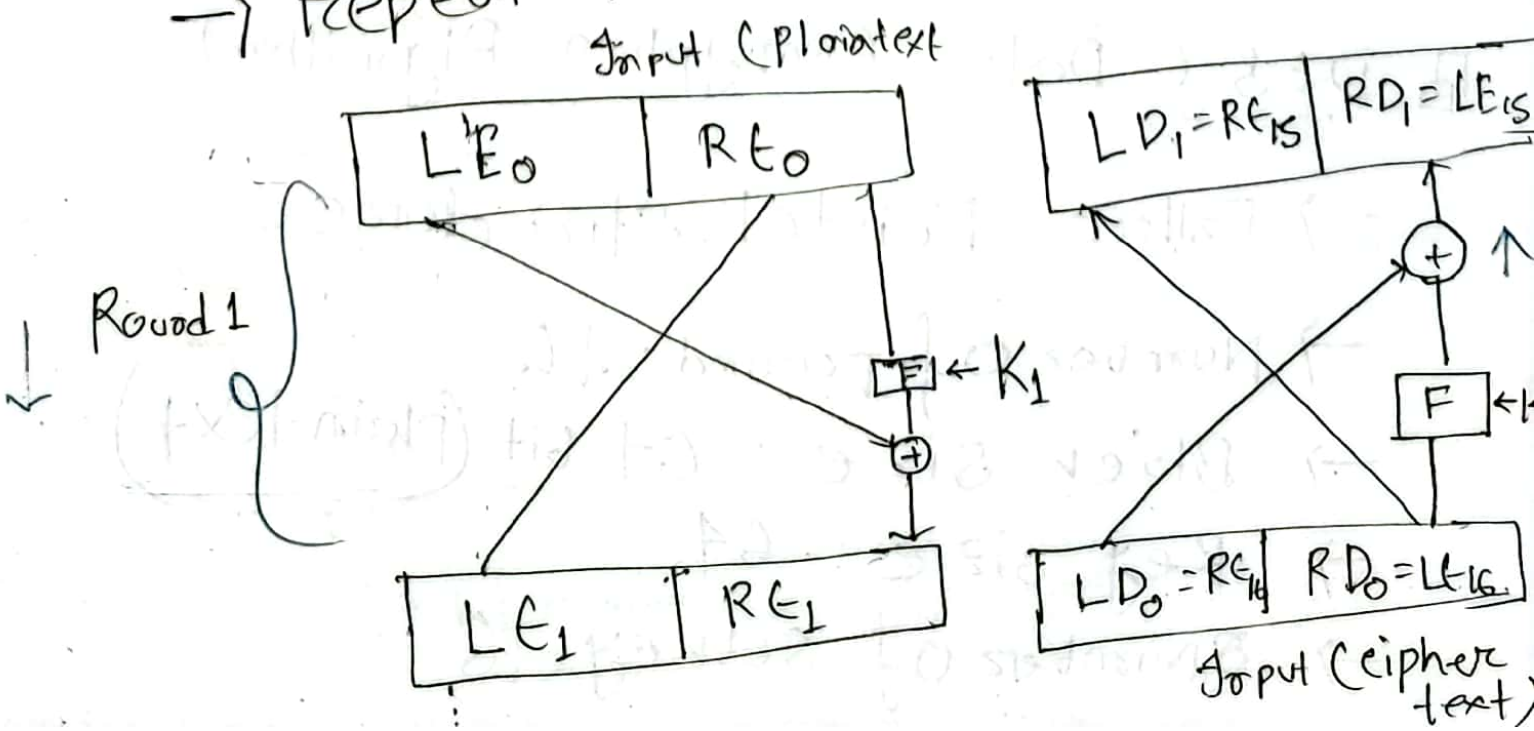
2 types of mapping

→ reversible → each block must produce a unique ciphertext block → nonsingular.

→ Irreversible → Singular

Feistor Cipher Structure:

- → plaintext is devided into 2 halves
- → perform a substitution on left data
  - → based on a function on right half
  - → subkey
- → permutation by swapping halves
- → repeat this round of "S-P"



Block Cipher design principles:

Block Ciphers are or variations of Feistel Cipher with diff.

- → Block size
- → key size
- → Number of rounds
- → Subkey generation algorithm
- → Round function
- → Fast sw encryption/ decryption
- → Ease of analysis.

DES (Data Encryption Algorithm)

- → Follow Feistel structure
- → Number of round : 16
- → Block size : 64 bit (plain text)
- → Key size : 64
- → Number of subkey = 16.

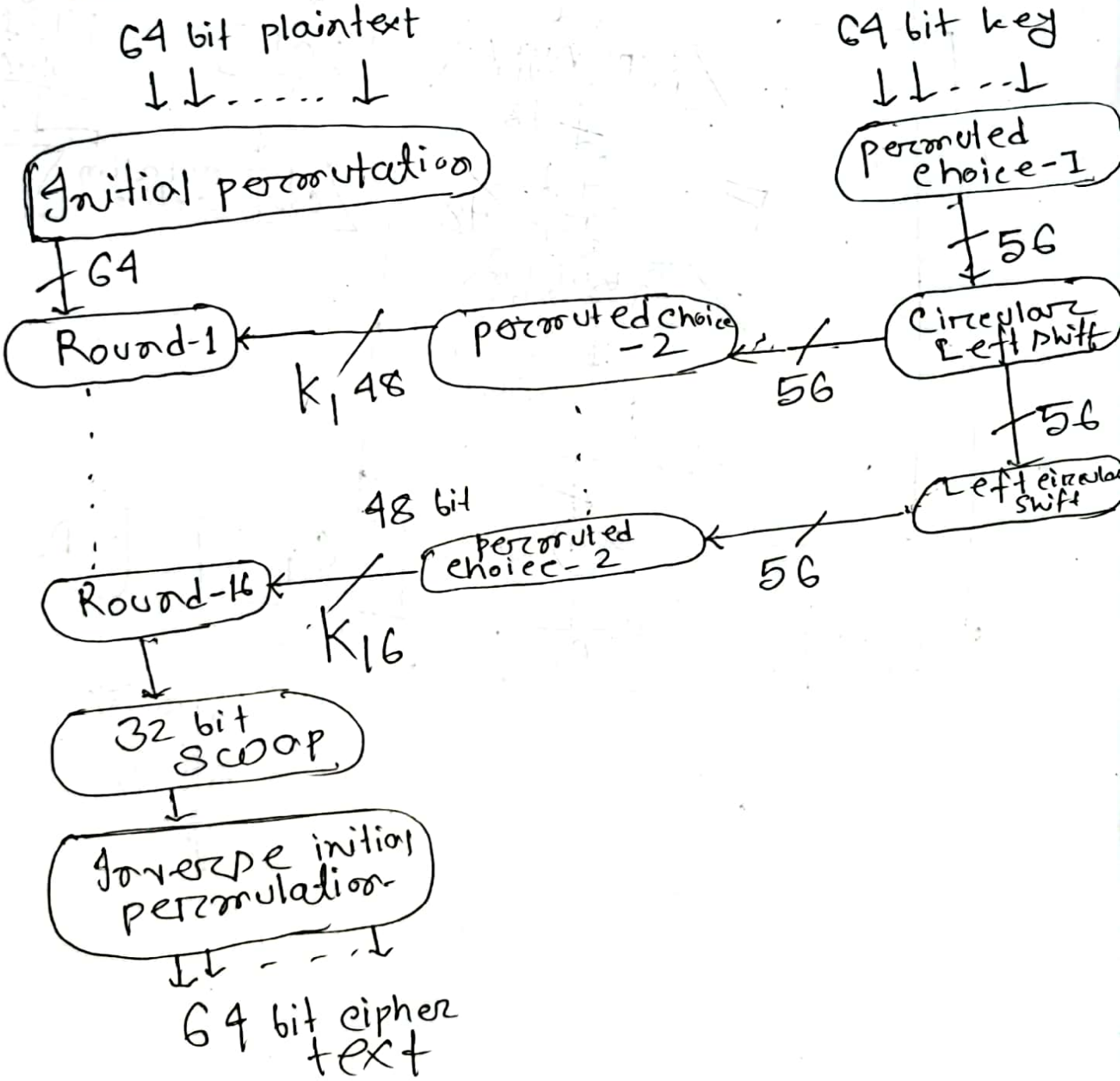
CamScanner

→ Subkey size: 48

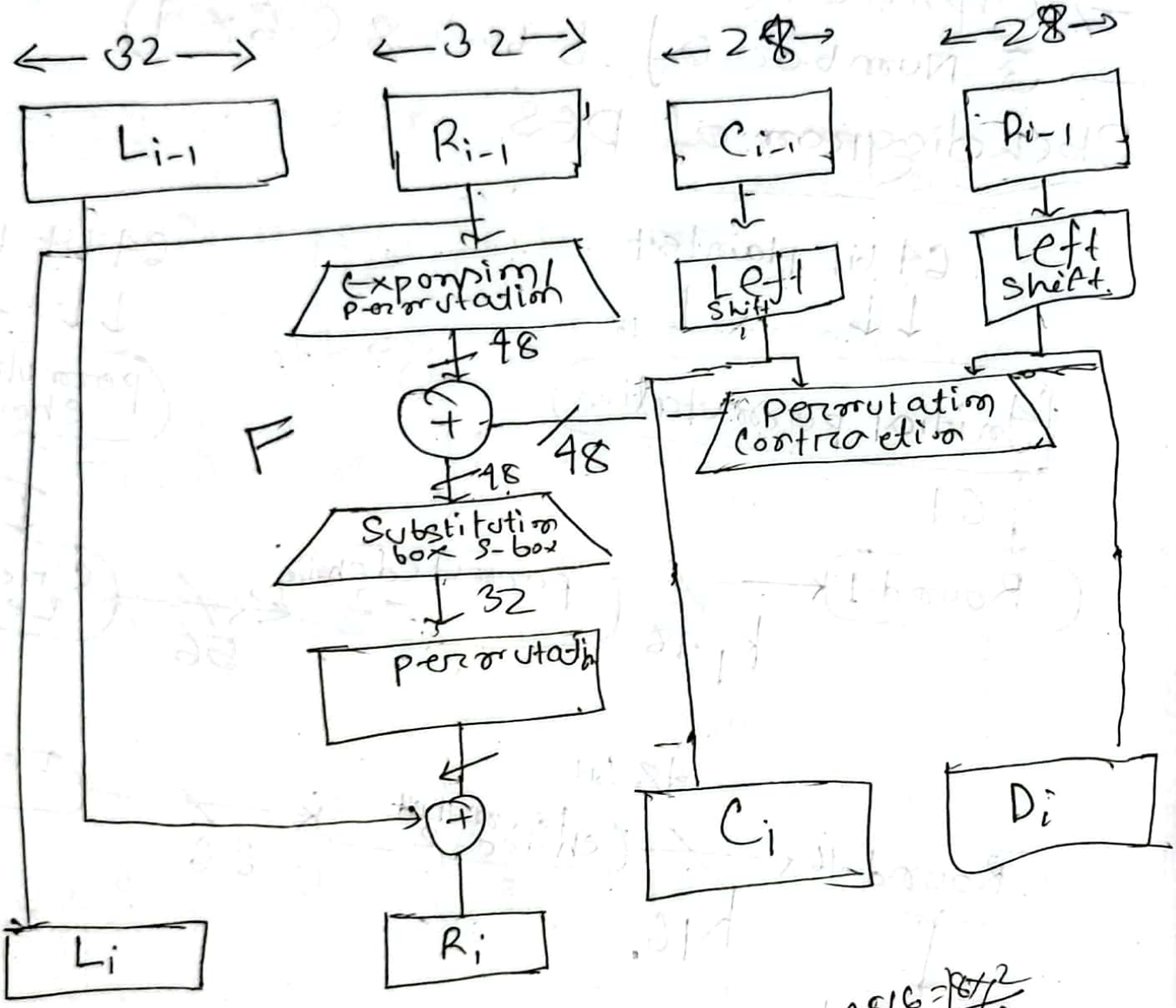
→ ciphertext: 64 bit

→ ~~S~~-Number of S-box: 8 (6×4)

Blockdiagram of DES



Block diagram of Round function



$48/6 = 8$

2^2

$48/6$

2^2

4P-

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	
59	51	43	35	27	19	11	
61	53	45	37	29	21	13	
63	55	47	39	31	23	15	

4P-1

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

DES subkey generation:

→ permutation PC1 devides 56 bit into two 28-bit halves

→ rotate each half separately depending on key routine schedule

→ ~~Permutation~~

→ Select 24 bit from each half

Input key 64 bit

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

CamScanner

Pe-1 (C4-56)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36

→ half

63	55	47	39	23	15	7
62	54	46	38	30	22	14
6	61	53	45	37	29	21
13	5	60	52			

63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

→ half

Substitution box (16 × 4) box

→ 6 - bit input

4 - bit output

→ take Random value (1 to 16)

→ but both side have same value

→ last & first bit indicates row

→ middle 4 bit " column

Column → / Row ↓	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
00	10	9	2	11	4	8	9	12	2	9	11	12	2	1	11	12
01	7	11	12	5	16	7	11	4	3	16	7	9	15	7	9	13
10	13	15	1	15	6	10	15	14	2	3	6	10	8	13	12	2
11	12	16	7	2	3	1	16	7	4	5	4	3	6	15	10	1

NOW 100 0 11

Row no = 11 = 3

Column no = 0001 = 1

output value is = 12 = 1100

Avalanee effect:

A change in one bit in plain text
or one " " the key
should produce a change in many
bits in ~~chip~~ ciphertext.

This is referred to as a avalanee effect.

Shannon S-P network

2 primitive cryptographic operation:

Substitution (S-box)
Replace n bit by another n bit

Diffusion:
One bit change in plain text
changes many bits in ciphertext

CS CamScanner

permutation (P-box)

→ bits are rearranged

Confusion:

make relationship between ciphertext and key as complex as possible

☆ Combination S-P = Product cipher.

CamScanner

Characteristic of AES

→ AES: Advanced Encryption Standard

→ block size : 128

→ key size: 128, 192 or 256

→ does not use Feistel structure

→ Each round consists of 4 functions

- → Substitution
- → permutation
- → arithmatic operation over a finite key
- → XOR with a key

CamScanner

AES vs DES

AES	DES
→ block size 128 bit	→ block size 64 bit
→ key size 128, 192 or 256	→ key size 56 bits
→ invented at 2000	→ invented at 1977
Cipher type Symmetric Block Cipher	symmetric Block cipher
→ Security is considered highly secured	→ it proven inadequate

★ Both are symmetric algorithm

Hashing

Hash function:

Function which maps a variable length message into a fixed length hash value or message digest.

★ Value returned by a hash function is called
- → hash value
- → hash codes
- → hash sums
- → message digest
- → hashes..

→ one way function

→ it helps to check data integrity

CamScanner

Characteristic

- → it check integrity of data
- → one way function
- → hash value of two message is not same
- → one message has exactly one hash value.

Good hash function / requirement

- → produce outputs that are evenly distributes
- → apparently random.

Cryptographic hash function

Hash function needed for Security application is referred too as a cryptographic hash function.

CamScanner

Block diagram of cryptographic hash function.

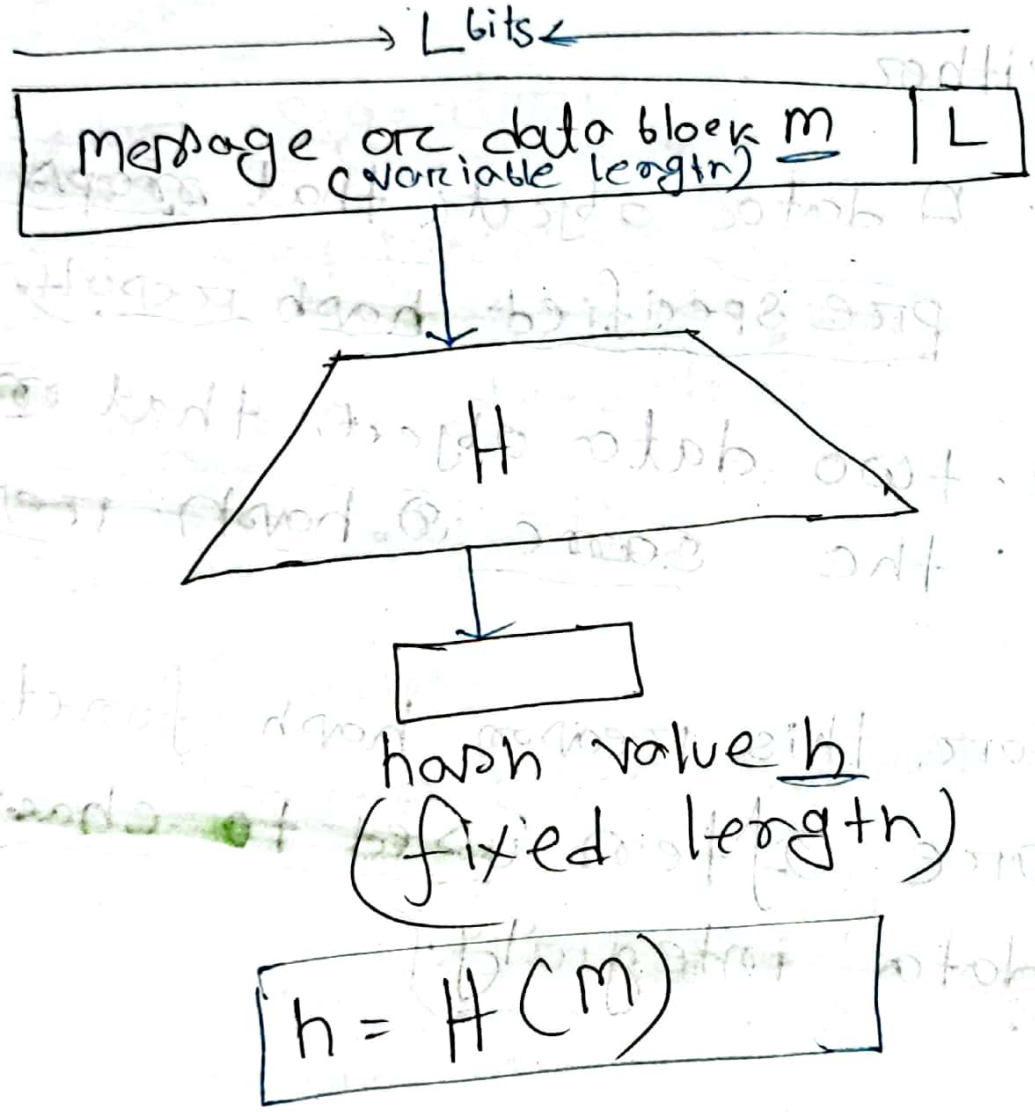


Fig: Block diagram of cryptographic Hash function.

computationally infeasible to find either

1. A data object that maps to a pre specified hash result
2. two data object that maps to the same hash result.

For this reason hash functions are often used to check data integrity.

CamScanner

Application of cryptographic hash function

→ Message authentication

→ Digital signature

→ one way password file

→ Intrusion detection
অবাঞ্ছিত

→ Virus detection.

Some hash function:

SHA-1 (Secure Hash Algorithm)

SHA-3

MD5

MAC (Message authentication code) → Keyed hash function.

→ used to authentic a message

NB When a hash function is used to provide message authentication, hash function value often called message digest.

CamScanner

Simplified hash function:

→ Simplest hash function is the bit-by-bit exclusive-OR (XOR) of every block.

$$\boxed{c_i = b_{i1} \oplus b_{i2} \oplus \cdots \oplus b_{im}}$$

c_i = ith bit of the hash code

b_{ij} = ith bit in jth block

$\oplus$ = XOR operation.

m = number of n bit block in the input.

Chapter - 12
Media Access Control

Multipoint / broadcast link:

When nodes or stations are connected and use a common link.

Multiple access protocol:

protocol that needs to coordinate access to the link

→ All protocols are belong to a sublayer in the data link layer.

→ Sublayer is called media access control (MAC)

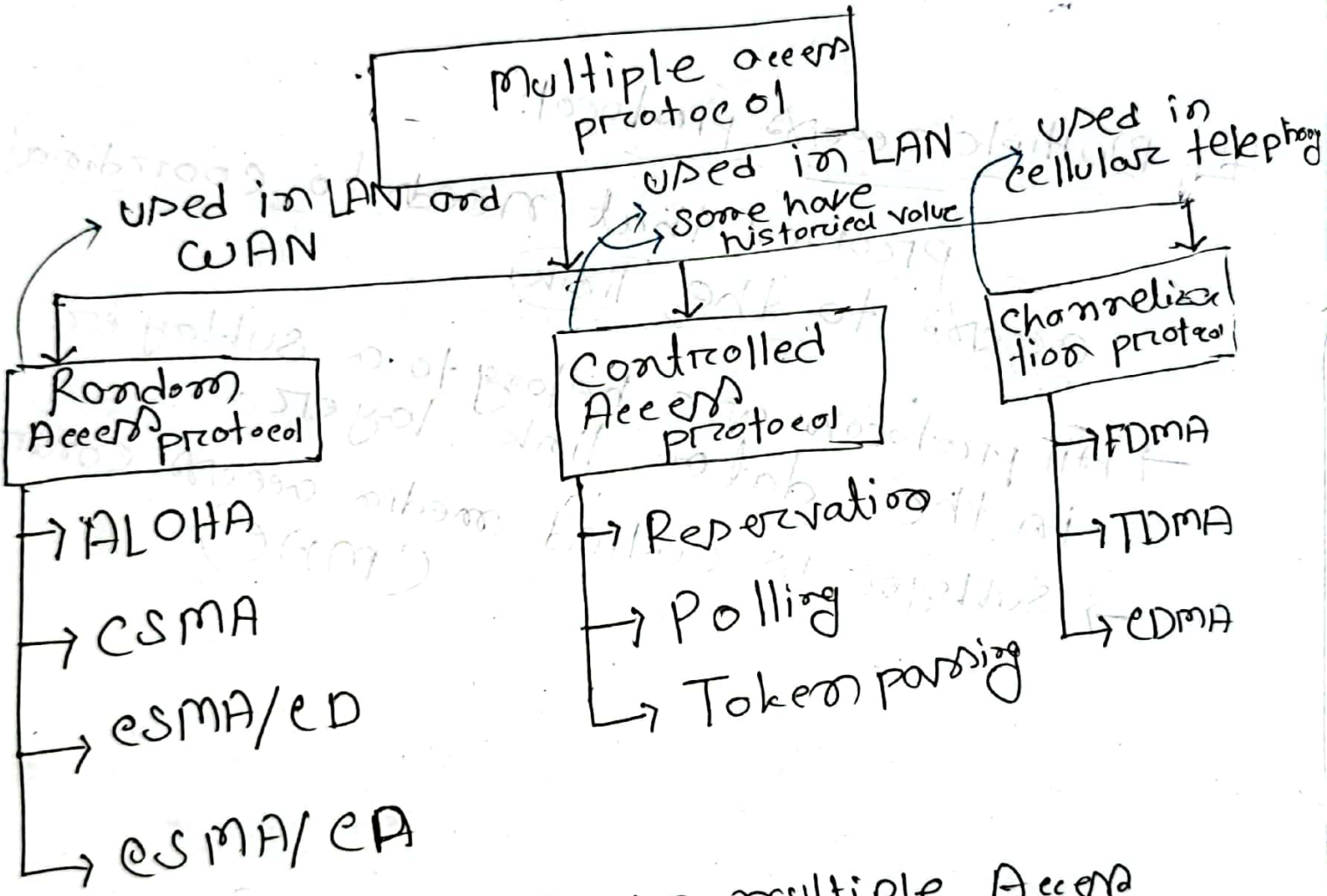
CamScanner

Sublayer of data link layer

→ data link control

→ multiple-access resolution

Classification of MAC:



CSMA: Carrier Sense multiple Access

CSMA/CD = CSMA with collision detection

CSMA/CA = CSMA with " avoided.

Random Access

→ no Station is superior to another Station

→ none is assigned control over another.

→ No station permit another station to send data

→ A Station that has data to send

→ send data in a procedure defined by protocol

Why they are called Random?

→ there is no scheduled time for Station to transmit

→ transmission is random.

→ no rules specify which station send next.

CS CamScanner

Why collision at Random access?

Ans :

→ each station has the right to the medium without being controlled by another.

☆ ~~when~~ → more than one station tries to send,

→ that causes an access conflict-collision

→ frame will be destroyed

Pure ALOHA

→ each station sends a frame whenever it has a frame to send.

Slotted ALOHA:

→ divide the time into slots of T_{fr}

→ force the station to send frame at the beginning of the time slot.

Vulnerable time:

Length of time at which there is a possibility of collision

G: Average number of frames generated by the system during one frame transmission time.

CamScanner

Pure ALOHA vs Slotted ALOHA

Pure ALOHA	Slotted ALOHA
1. send frame whenever it has a frame to send	1. at the beginning of the slot
2. Vulnerable time $= 2 \times T_{fr}$	2. Vulnerable time $= T_{fr}$
3. Throughput $S = G \times e^{-2G}$	3. Throughput $S = G \times e^{-G}$
4 Maximum through put $= (1/2e)$	4. maximum throughput $= 0.368$

Time out period:

Amount of time wait ~~before~~ after sending a frame to take ACK

For pure ALOHA it is $2 * T_p$

Backoff time:

Amount of time before re attempt to resend a frame.

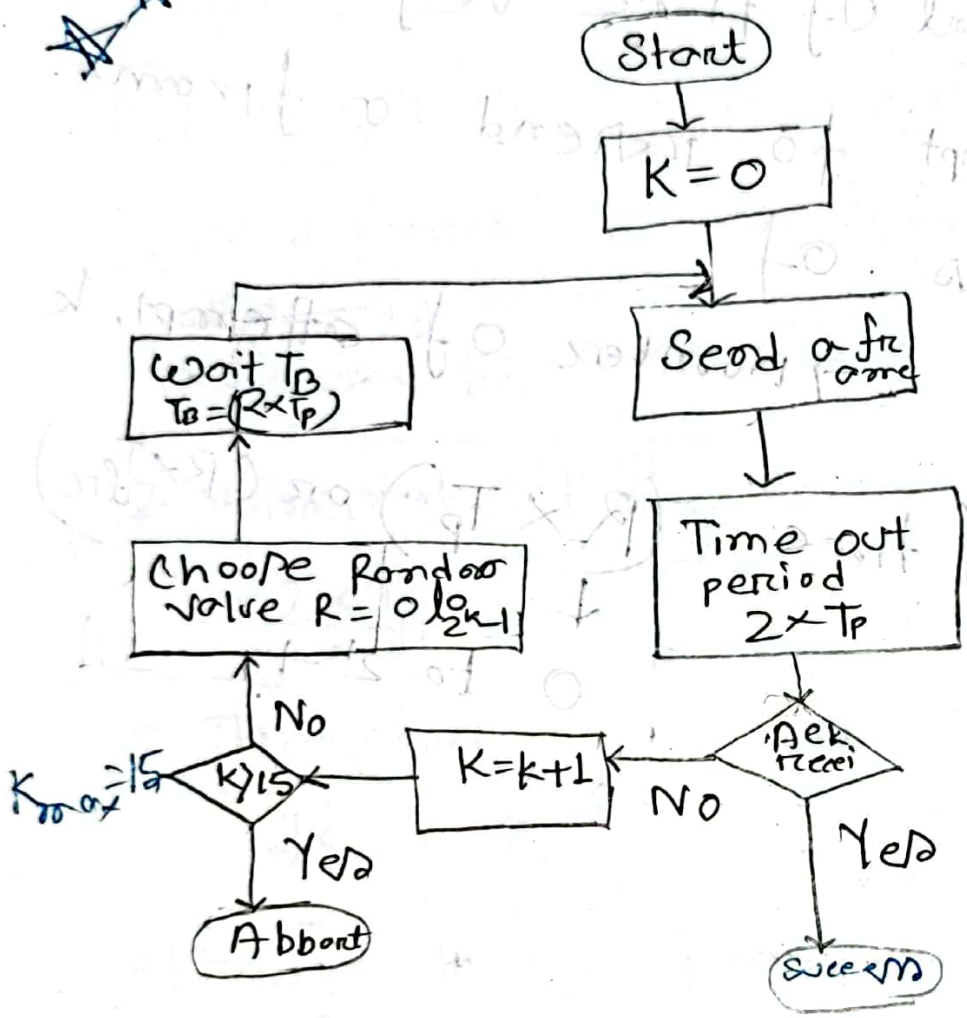
it depends of

→ Number of attempt, k

Backoff time = $(R \times T_p)$ or $(R \times T_{fr})$

R → 0 to $2^k - 1$

flow diagram of Pure ALOHA:



Carrier Sense multiple access (CSMA)

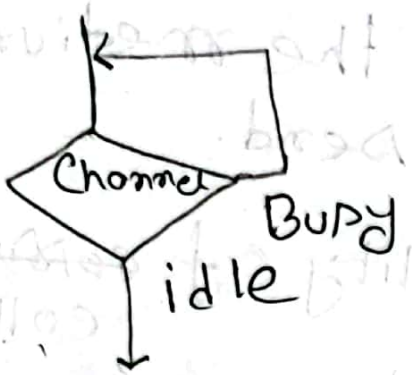
→ first listen to the medium.
→ if find idle then send.
→ reduce the possibility of ~~collis~~ collision.
→ not eliminate it.
→ Sense before transmit
→ Vulnerable time for CSMA = T_p

Method to avoid collision:

3 methods
1 - persistent → If find the ~~station~~ idle, sends frame
nonpersistent → used when Slot duration // T_{prop} max
p - persistent → with p station send a frame
" (1-P) " wait for the bg

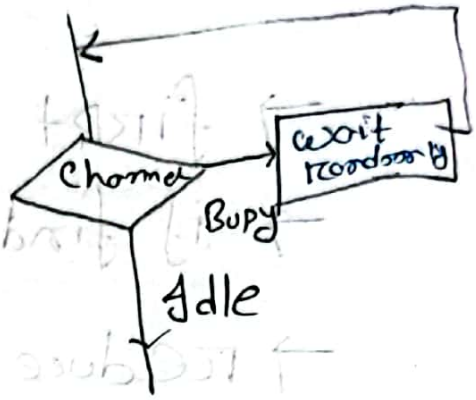
if line is idle send immediately
if " is not idle it waits a random amount of time
Sense the line again

flowdiagram



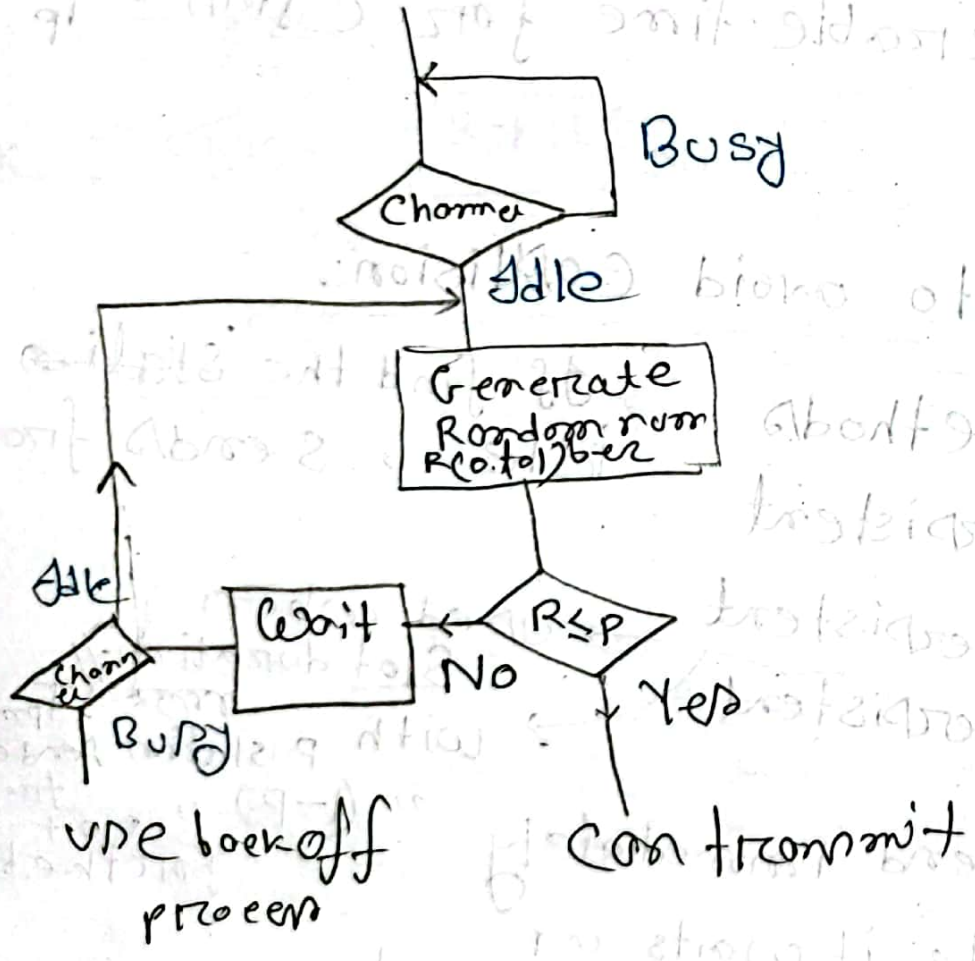
Station can transmit

1- perpistent



Station can transmit

nonperpistent



P- perpistent

CSMA/CD vs CSMA/CA

CSMA/CD	CSMA/CA
1. After send a frame it monitor the medium.	
2. Try to ~~avo~~ detect collision	2. Try to avoid collision
3. Use persistence method to detect collision.	3. Use IFS, CTS, RTS and contention window to avoid collision

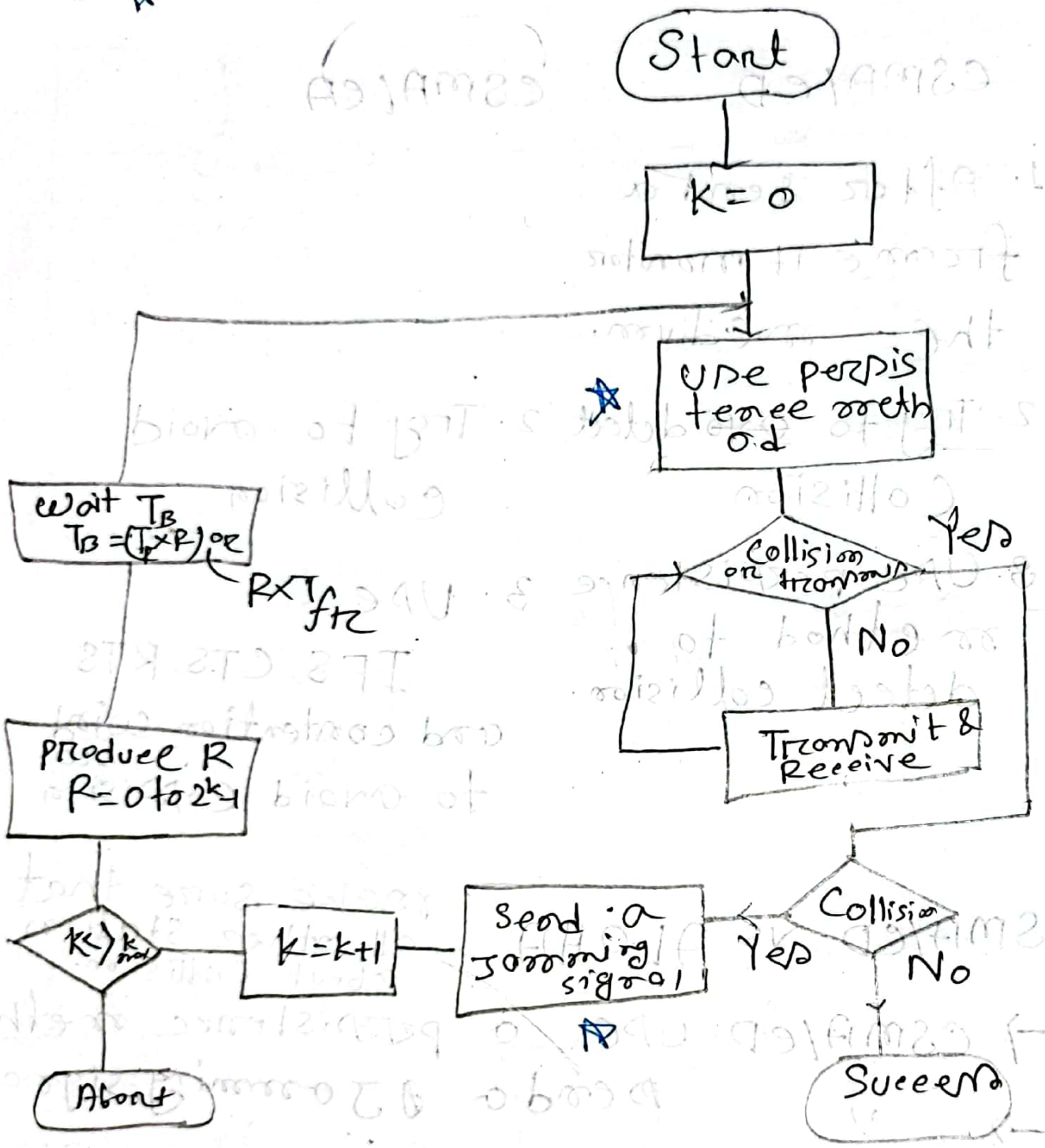
CSMA/CD vs ALOHA

→ CSMA/CD use a persistence method → make sure that all other station about collision.

→ " send a jamming signal

→ In " transmission and collision detection are continuous process

Flow diagram of CSMA/CD



Energy level 3 level

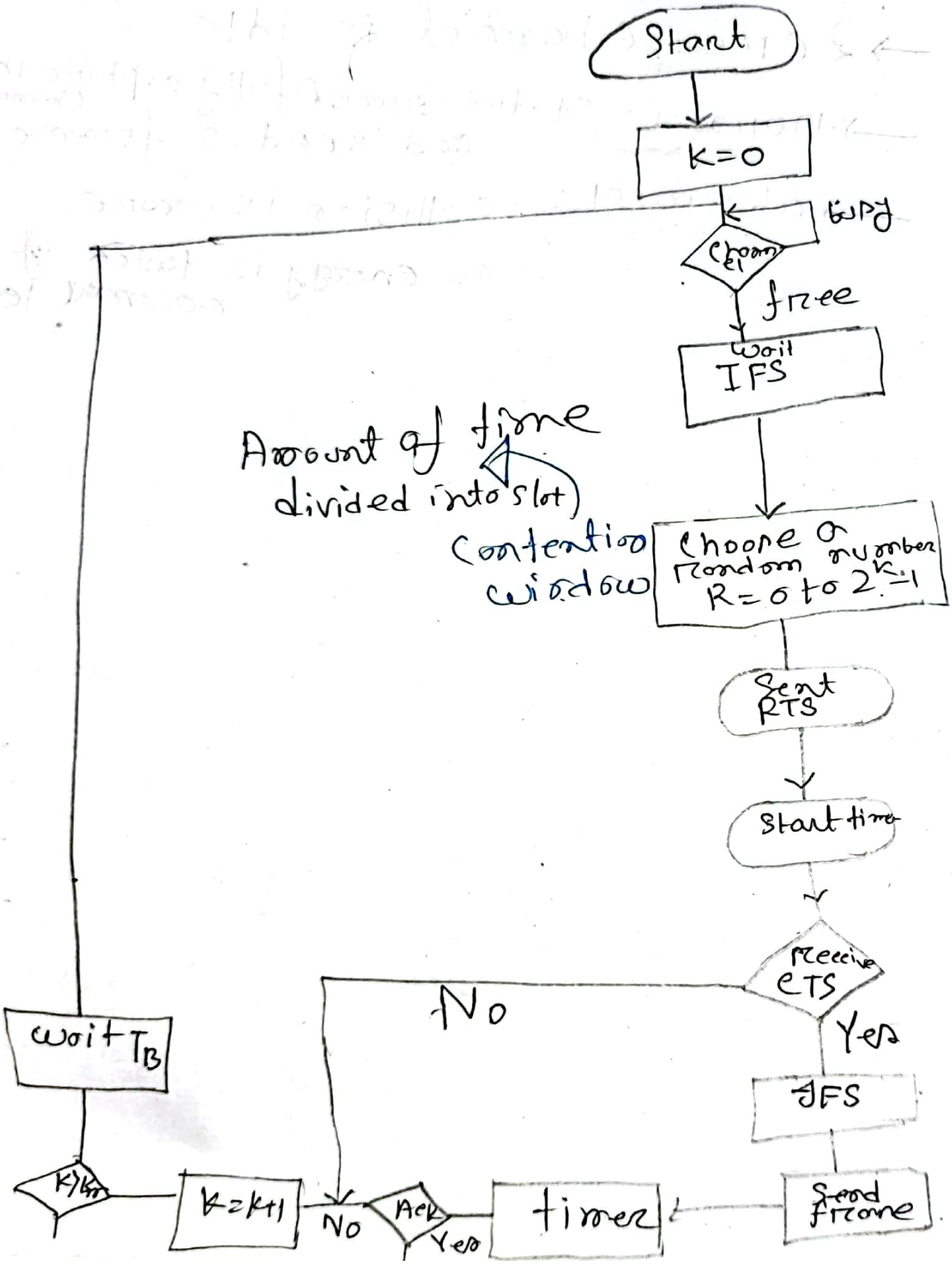
→ zero: channel is idle

→ normal: station successfully capture the channel and send a frame

→ abnormal: collision is occure
energy is twice of normal level.

CamScanner

flow diagram of CSMA/CA



Controlled Access:

→ Station consult one another
↳ to find which station has the right to send.

Classification:

→ Reservation

→ Pooling

→ token ring passing

Reservation:

→ Station make a reservation before sending data

→ time is divided into interval.

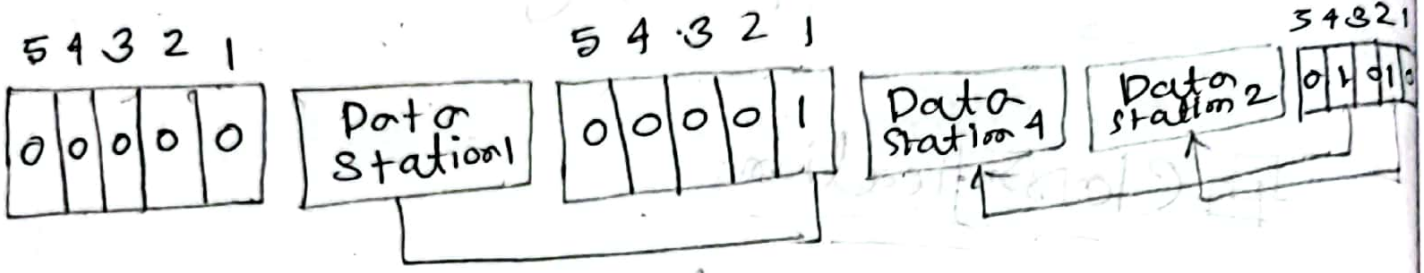
CamScanner

For N Station

Number of mini slot = N

→ each mini slot belong to a Station.

direction of packet →



Pooling:

→ works with topologies

2 device

→ primary device

→ secondary "

Method to Avoid collision:

2 function

→ SELECT → used if primary device have something to send

→ POLL → request transmission from secondary device

Token Passing:

→ Station in the network are organized in a logical ring

→ Token is a special packet passed through the ring.

→ token gives the station right to send.

4 different kinds of physical topologies

→ physical ring

→ dual " → it has logical path

→ Bus "

→ Star ring

Chapter-6

Transport layer:

TCP vs UDP:

TCP	UDP
1. Connection oriented protocol	1. UDP is connection less protocol
2. Transmission control protocol	2. User datagram protocol
3. ~~Exam~~ TCP header is 20 byte	3. UDP header is 8 byte
4. Reliable, as it guarantees delivery of data to the destination router	4. Delivery of data to the destination cannot be guaranteed in UDP
5. Comperatively Slower than UDP	5. UDP is faster
6. TCP is ~~uper~~ heavy weighted	6. UDP is light weighted

CamScanner

TCP	UDP
7. TCP is used by HTTP, HTTPs, FTP, SMTP, and	7. UDP is used by ~~DS~~ DNS, DHCP, TFTP, SNMP, RIP
8. Source port destination port Check Sum	8. Source Port Destination port

common in header

□ UDP header

← 32 bits →

Source port	Destination port
UDP length	UDP checksum

NB → UDP is a transport layer protocol
→ typically runs in the operating system
→

Two ports
Source port
Destination port

two port serve to identify the end point
within the source & destination machine.

UDP length:

8 byte header and the data
minimum length is 8 byte
maximum " is 65515 byte

Checksum:

used to provide extra reliability

If checksum the header
the data
a conceptual IP pseudo header

Pseudo header

← 32 →		
Source address		
Destination address		
00000000	protocol (17)	UDP length

Pseudo header for the case of TPK contains

- → Source address
- → destination "
- → protocol number for UDP (17)
- → byte count for the UDP

TCP Service Model

* ~~TCP~~
* Service is obtained by both sender and receiver creating points called Socket.

Socket

each socket has
→ socket number
→ 16 bit number local to the host

Port ~~number:~~

→ Port is the TCP ~~an~~ name for a TASP.

→ port number below 1024
→ reserved for standard service
→ called well known point.

CamScanner

→ port from 1024 - 49151
→ registered with IANA.

List of some assigned port

25 SMTP → email
20,21 FTP → file transfer
80 HTTP → world wide web
443 HTTP.S → Secure web (HTTP over SSL/TLS)

631 IPP → printer sharing
543 RTSP → media player control
110 POP-3
143 IMAP } → Remote email access
22 SSH → Remote login
Replacement for telnet