6a) 2-D Parity.

Following even-parity we arrange all the bits as 2D-matrix.

1	0	1	1	0	1	0	1	1
0	1	1	1	0	1	1	1	0
1	0	1	0	0	0	0	1	1
0	1	1	0	0	0	1	1	

This the codeword to be sent. Each row and column has parity-bits.

This method can correct 1-bit errors. If we reverse bit at second row second colum.

1	0	1	1	0	1	0	1	1
0	0x	1	1	0	1	1	1	0
1	0	1	0	0	0	0	1	1
0	1	1	0	0	0	1	1	

The parity is 0 with odd ones in a row so it can know some error has occured. And in second column parity bit is 1 but even number of ones are there so it corrects 0 to 1.

Limitations:

It can only detect odd-bit errors. It can't detect even-bit errors.

1	0	1	1	0	1	0	1	1
0	0	0	1	0	1	1	1	0
1	0	1	0	0	0	0	1	1
	0	1	1	0	0	0	1	1

If two bits in second row at second and third column are flipped to zero then while checking second row then will be even number of ones so 0 is the correct parity bit. And thus it can't handle even-bit errors. There might go unnoticed.

6b) Characteristics of broadcast channel of rate R bps.

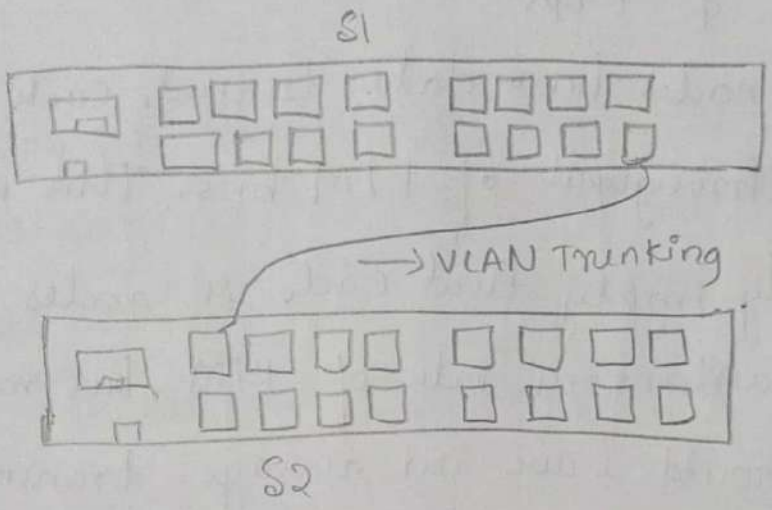
i) When only one node has data to send, that node has a throughput of R bps.

ii) When M nodes have data to send, each of these nodes has a throughput of R/M bps. This need not necessarily imply that each M nodes always has an instantaneous rate of R/M, but rather each node should have an average transmission rate of R/M over some suitably defined interval of time.

iii) The protocol is simple and inexpensive to implement

iv) The protocol should be decentralized; no master node that represents the single point of failure for the network.

6c) Connecting two or more switches to satisfy VLAN needs is called VLAN trunking. The last port of a switch is connected to the first port of the next one.



S1 - switch one

S2 - switch two

Consider 16 port switches. For efficient use to meet demands we connect last and first of two switches. So if N switches exists then the first port of first switch and last port of last switch. So two ports are left out. If K VLAN groups exists then efficiency depends on no. of hosts in each group. If numbers is very less than all groups can fit n-port switch if total hosts in all groups is lesser than number of ports $-\underline{\underline{2}}$ of a switch. This gets more efficient usage (VLAN Trunk) of switches with better traffic isolation.

Else we need to go for VLAN trunking and achieve this
It's more efficient to keep all hosts of a group to be on same switch as switching time reduces, lesser no. of switches are there. If not we have VLAN tags to identify them.

So considering the trunking protocol. The very first switch does not use the input port and the last switch does not use the output port all other switches all all ports. First switch uses outputport only. Last switch use input port only.

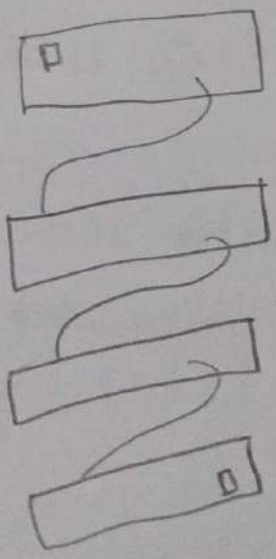
Therefore no. of ports all switches use is leaving first and last.

$2 \times (N-2)$ ports.

Including one ports used by first and last switch.

$$2 \times (N-2) + 2 = (2*N-2)$$

Therefore $2*N-2$ ports are required.



9a) Master Device

→ A master device is used in Bluetooth network.

→ A master device sets up the Bluetooth network and manages all communications in the network.

→ Any device can be Bluetooth master in bluetooth network.

→ A bluetooth master can be any node when it wishes. It can be temporary

Base Station.

* Base station is used in infrastructure network such as 802.11 network.

* A base station is responsible only sending and recieving data to and from a wireless host that is associated with the base station.

* Specially configured device like access points act as base station in 802.11 networks

* A access point in network is always working once turned on.

8b) ARP -or- Address Resolution Protocol.

→ It is a plug and play device protocol.

→ It is used to obtain MAC address from IP address.

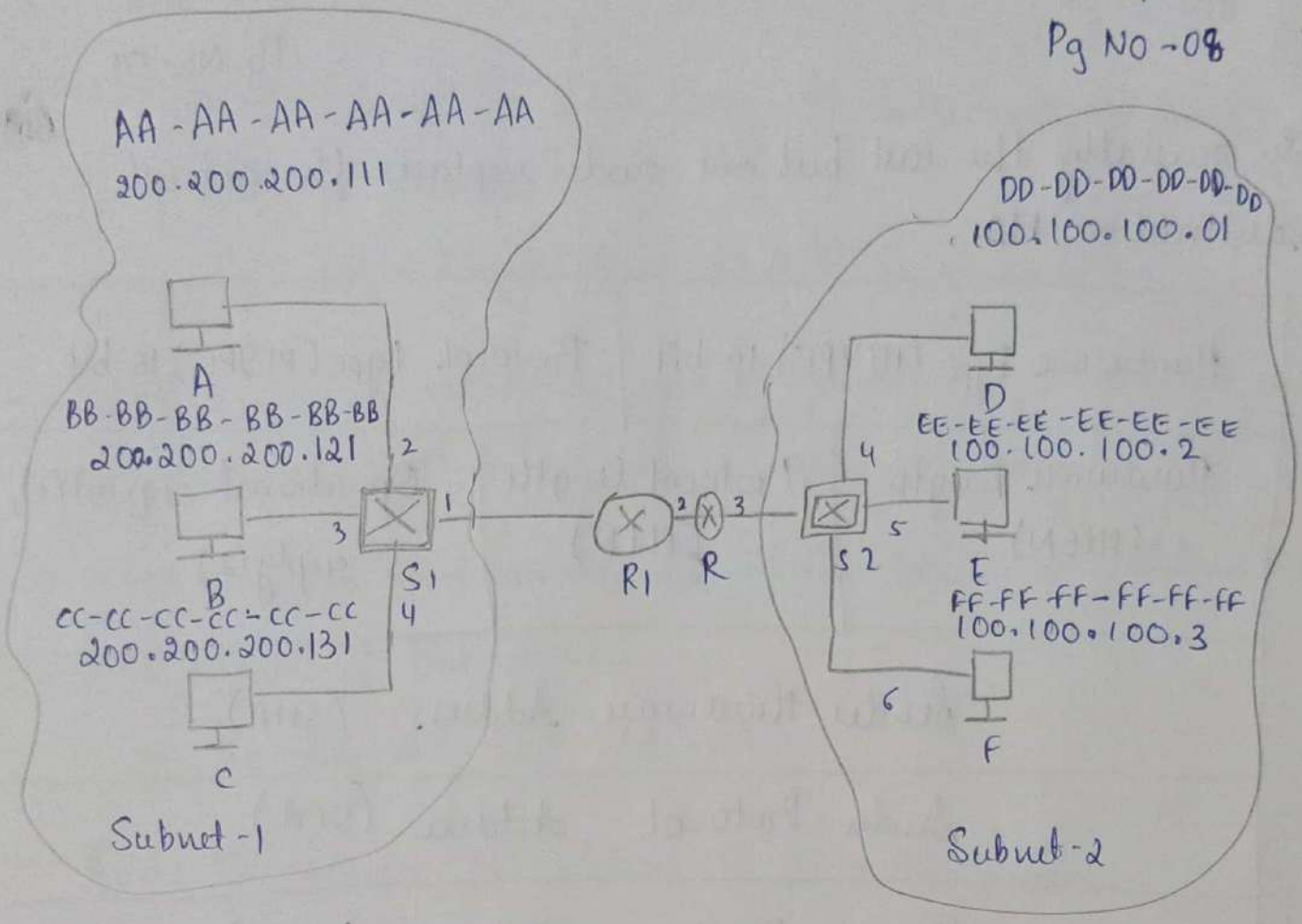
→ It has two types of messages:

i) Query message: When some host wants to know the MAC of another it uses a query message puts destination IP and tells its adapter it needs MAC of this IP. Then adapter adds broadcast MAC FF-FF-FF-FF address and forwards this broadcast packet to all nodes. The one with matching IP replies back with its MAC

ii) Response message: This is unicast message. As the distination knows the senders MAC. He will reply only to sender his MAC address.

→ It is helpful for MAC addressing. and to achieve forwarding with switches in LAN's such as our University.

→ Why? for obtaining MAC address of nodes that can in turn achieve forwarding without much of layer 3 overhead.



Suppose if host A wants to send data to host E in different subnet then it does not ~~at~~ put MAC of E insted puts MAC of R1 which is the connecting point so it inputs destination as MAC of routers interface 1. When packet reaches R1. It goes upto L3 of network layer to find on which of its interface should it forward the packet so it decides on interface 2 and inputs the dest MAC of R3 of that interface. Now when it reaches R3. R3 searches for the interface of its on which it has to forward and replaces the dest MAC address of E i.e EE-EE-EE-EE-EE. Thus forwarding to E

So, generally the last but one node replaces the actual destination MAC.

Hardware Type (HTYPE) 16-bit		Protocol-type (PTYPE) 16-bit
Hardware length (HLEN)	Protocol length (PLEN)	Operational request(1), reply(2)
Sender Hardware Address (SHA)		
Sender Protocol Addres (SPA)		
Target Hardware Address (THA)		
Target Protocol Addres (TPA)		

→ Hardware type - It is 16 bit field. defines the network type that the local network needs to transmit ARP message.

Ex: Ethernet - 1

→ Protocol type - Used to specify the protocol type.

Ex: IP.

→ HLEN (Hardware length) - 8 bit size. length of physical address in bytes.

Eg: 6 bytes in Ethernet

→PLEN (Protocol length) → 8 bit long. It determines the lugth of protocol's addess

Eg: IP – 4 bytes long as it is of 32-bits

→ OPER is 16 bit determines type of packet. If 1 request and broadcast packet. If 2 then unicast reply

→ SHA (Source hardware Address) → The hardware address or MAC address of the source

eg: AA-AA-AA-AA-AA-AA

→ SPA: the source IP address if IP is the protocol

eg: 100.100.1.1

→ THA: Hardware address of destination.

eg: BB-BB-BB-BB-BB-BB

→ TPA: Target protocol address. The ip addes of target / destination host.

eg: 200.200.1.1

8a) Because in the virtual circuit mechanism the links are permanent, the switch can send a message of failure to all its ports, the recieving switches will check their virtual circuits table, to check if they have a connection is set through the damaged switch. If so these switches will send to their incoming ports message of the failure of that switch.

8c). Data = Roll Number = 419 in binary.

419's binary equivalent is 110100011
8 7 6 5 4 3 2 1 0

Divisor = 1011

I) Data in polynomial.

Dataword should be right shifted by 3 times because the divisor is of 4 bits or 3+1 bits.

Therefore final dataword,

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

x^3 x^2 x 1

$x^{11} + x^{10} + x^8 + x^4 + x^3$ in polynomial.

Codeword is 1011
3 2 1 0

$x^3 + x + 1$

codeword = $D.2^r$ XOR G

$D.2^r$ → right shifts by r bits

G → appends r bits

II) Source side

x^3+x+1) $x^{11}+x^{10}+x^8+x^4+x^3$ ($x^8+x^7+x^6+x^5+x+x^2$

$x^{11}+x^9+x^8$

$x^{10}+x^9+x^4+x^3$

$x^{10}+x^8+x^7$

$x^9+x^8+x^4+x^3+x^7$

$x^9+x^7+x^6$

$x^8+x^4+x^3+x^6$

$x^8+x^6+x^5$

$x^4+x^3+x^5$

x^4+x^2+x

$x^5+x^3+x^2+x$

$x^5+x^3+x^2$

x

Redundant bits = is made of 3 bits as generator is of 4 bits. So redudant bits is 010. or x.

Codeword = $x^{11}+x^{10}+x^8+x^4+x^3+x$.

3) If error occurs in x^2 i.e is my case 0 should be flipped to 1. as 010 was redudant bits x^2 is 0 tuning it to 1 will change the codeword as

Codeword - $x^{11}+x^{10}+x^8+x^4+x^3+x^2+x$

↳ made 1

$$x^3+x+1 \;\overline{)\; x^{11}+x^{10}+x^8+x^4+x^3+x^2+x \;}\; x^8+x^7+x^6+x^5+x^2+x$$

$x^{11}+x^9+x^8$

$x^{10}+x^9+x^4+x^3+x^2+x$

$x^{10}+x^8+x^7$

$x^9+x^8+x^7+x^4+x^3+x^2+x$

$x^9+x^7+x^6$

$x^8+x^6+x^4+x^3+x^2+x$

$x^8+x^6+x^5$

$x^5+x^4+x^3+x^2+x$

$x^5+x^3+x^2$

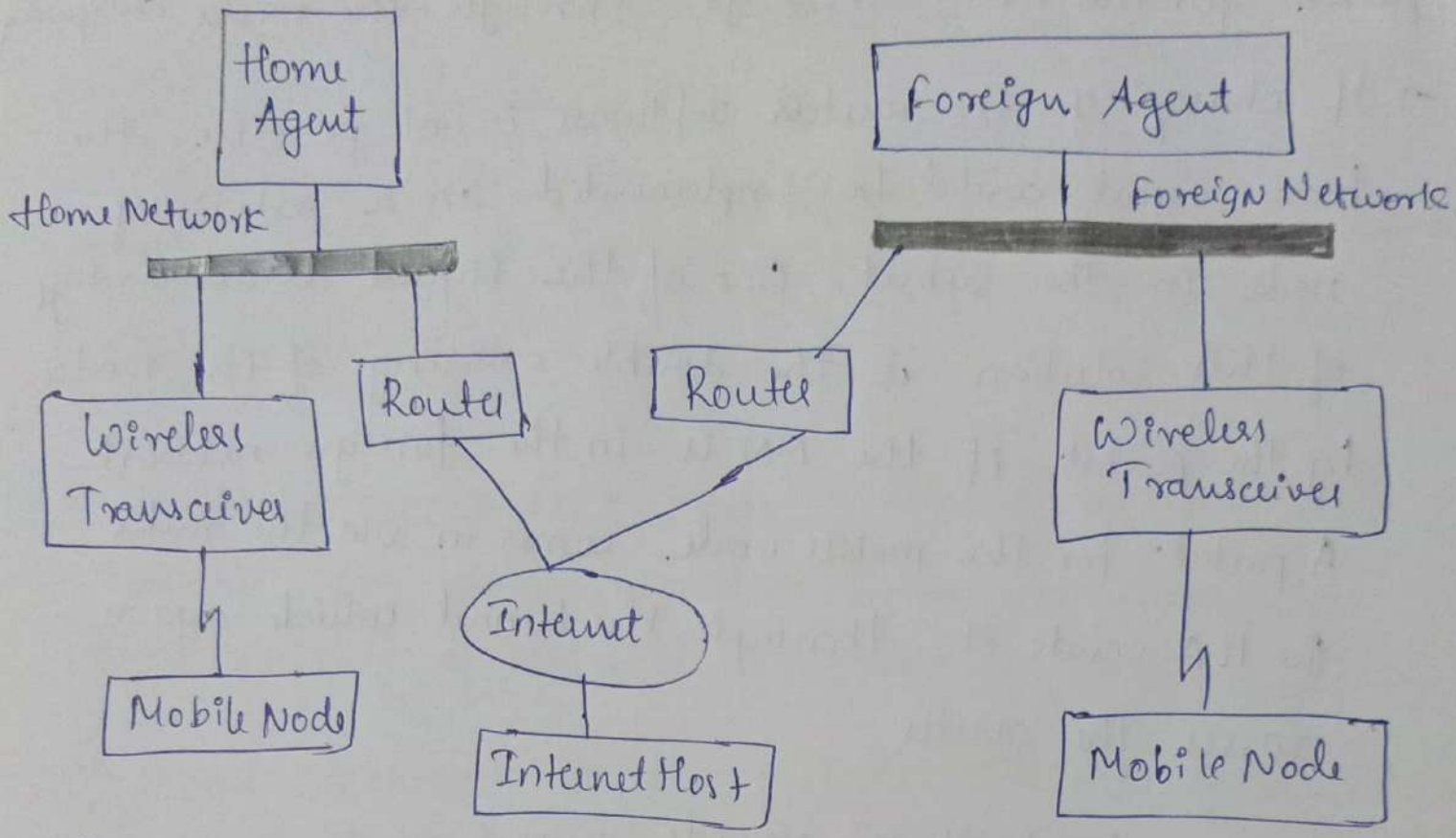
x^4+x

x^4+x^2+x

x^2

Source adds remainder of codeword by Generator to codeword if no error occured then codeword should be completely divisibly at ~~sendr~~ receiver side. But it is not the case as x^2 was flipped. Hence remainder is now zero and distination identifies the error has occured.

9b)



Component

i) Mobile Node (MN) - It is an end system or a device such as cell-phone, PDA (Personal Digital Assistant), or laptop whose software enable network roaming capabilities

ii) Home Agent (HA) → It provides several services for the mobile node and is located in home network. The tunnel for packets towards the mobile node starts at the home agent. The home agent maintains a location registry, ie. it is informed of the mobile node's location by the current (COA) care of address. Following alternatives for implementation of HA exists.

→ Home Agent can be implemented on a router that is responsible for the home network. This is obviously the best position, ∵ without optimization to mobile IP, all

packets for the MN have to go through the router anyway

→ If changing the router's software is not possible, the home agent could be implemented on a arbitrary node in the subset. One of the biggest disadvantage of this solution is the double crossing of the router by the packet if the MN is in the foreign network. A packet for the mobile node comes in via the router the HA sends it through the tunnel which again crosses the router

3) Foreign Agent: It can provide several services to the mobile node during its visit to the foreign network. The FA can have the COA (care of address) acting as a tunnel endpoint and forwarding packets to the MN. The foreign agent can be the default router for the MN.

FA can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.

FA is a router that may function as the point of attachment for the mobile node when it roams to foreign network delivers packets from the HA to MN

4) COA - defines the current location of the MN from an IP point of view. All IP packets sent to MN are delivered to the COA, not directly to the IP address of MN. Packet delivery toward MN is done using a tunnel

5) CN or Correspondent Node : Atleast one partner is needed for communication. The CN represents this partner of MN. It can fixed or mobile nod.

6) Home Network is the subset the MN belong to wrt to its IP address. No mobile IP support is needed within this network

7) Foreign Network is the current subset the MN visits and which is not in home network.

It consists three main pieces:

1) Agent discovery: Mobile IP defines the protocols used by home or foreign agent to advertise its services to MN, and protocols from MN to solicit the services of FA or HA

ii) Registration with HA: Mobile IP defines the protocols used by the MN and / or FA to register and deregister COAs with MN's HA.

iii) Indirect routing of datagrams: The standard also defines the manner in which datagrams are forwarded to MN's by HA, including rules for forwarding datagrams, rules for handling error conditions, and several forms of encapsulation.