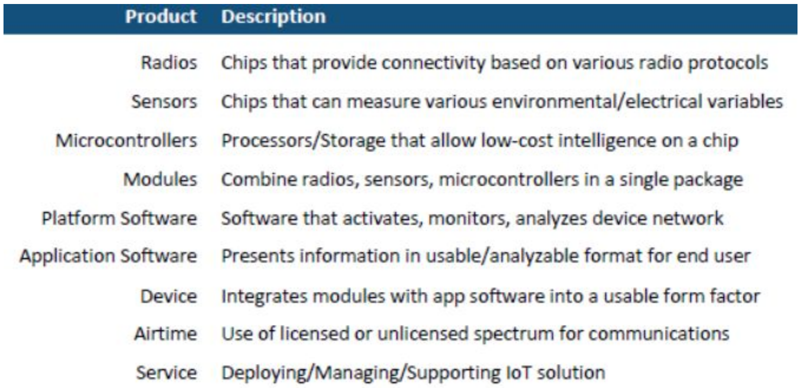
T3 : IOT and SDN

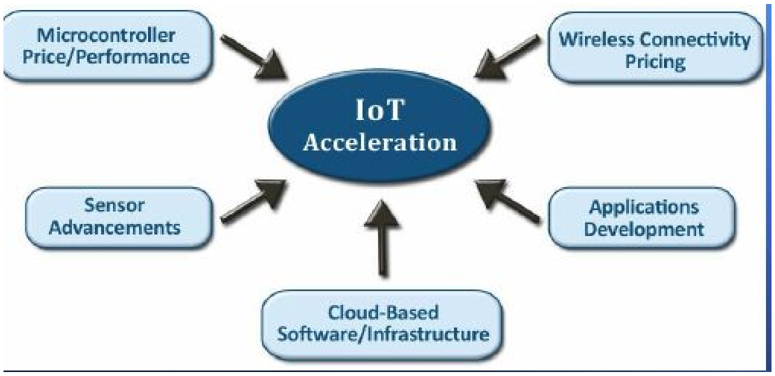
1. What is IOT ? (7X)
   a. When there are embedded short range mobile transceivers in gadgets which lead to the formation of wireless network between objects
   b. Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts”.
   c. IOT can consist of :



Product	Description
Radios	Chips that provide connectivity based on various radio protocols
Sensors	Chips that can measure various environmental/electrical variables
Microcontrollers	Processors/Storage that allow low-cost intelligence on a chip
Modules	Combine radios, sensors, microcontrollers in a single package
Platform Software	Software that activates, monitors, analyzes device network
Application Software	Presents information in usable/analyzable format for end user
Device	Integrates modules with app software into a usable form factor
Airtime	Use of licensed or unlicensed spectrum for communications
Service	Deploying/Managing/Supporting IoT solution

2. Factors driving IOT
   a. There is a demand for higher range and less power consumption technology
   b. Need for connectivity at any time, place and with anything
   c. Need for more data which would lead to more wisdom

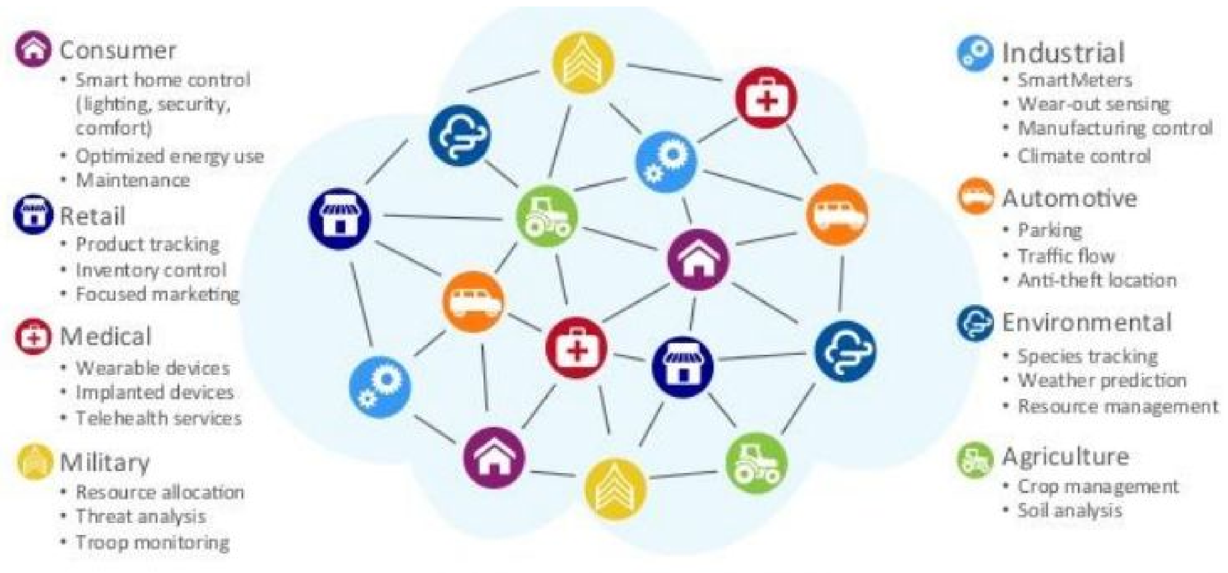
3. Why is IOT accelerating ?


Microcontroller Price/Performance
Wireless Connectivity Pricing
IoT Acceleration
Sensor Advancements
Applications Development
Cloud-Based Software/Infrastructure

4. Why do we need IOT ?
   a. Dynamic control over daily life (energy conservation → use a pi to shut off your laptop)
   b. Improve Resource utilization (use pi to switch off fan so energy saved)
   c. Better relation between human and nature
   d. Internetworking (diff kinds of devices are connected together)
   e. Integrate technologies (not just cellphone and comp networks anymore)

   f. Need for easy access anywhere

5. Application of IOT



- Home
    - Video survellaince
    - Door lock
    - Power meter
    - Smart irrigation
- Shopping
    - Goods tell u abt product
    - Identify tags on customer clothing
    - When moving out new goods reader tells staff to add product
- Medical
    - Equipment management
    - Health monitoring
    - If heart rate goes high , tells what to do
- Transport
    - Congestion detection
    - Pollution detection
    - Driver behavior

6. State of the Art in IOT ?
   a. RFID-->Sensor-->Smart tech-->Nano tech
   b. An idea travels from the research agencies to the market in the following ways :
      i. Organisations like DARPA, MIT labs, NFC, intel and other university labs will do R & D on ideas in different fields and send it out for production to places like Texas instruments , Tyco retail, sony and Hughes
      ii. Then from production it will move to market as a usable product
         1. Paypass at mcdonalds

2. RFID wristbands for patients
3. Item level tracking
4. Mobile payments via a FeliCO chip
5. Great Duck island habitat monitoring (satellite)

7. What is sensor technology ?

    a. The ability to detect changes in the physical status of things is essential for recording changes in the environment.

    b. Wireless sensor technology play a pivotal role in bridging the gap between the physical and virtual worlds, and enabling things to respond to changes in their physical environment. Sensors collect data from their environment, generating information and raising awareness about context.

    c. Sensor Market includes :

        i. Micro-electromechanical systems (MEMS) -based sensors, optical sensors, ambient light sensors, gesture sensors, proximity sensors, touch sensors, fingerprint sensors .

8. What are the challenges of IOT ?

    a. Its not tested in extreme conditions

    b. Interoperability ?

    c. Technological Standardization in most areas remain fragmented.

    d. managing and fostering rapid innovation is a challenge for governments; Vulnerability to internet attack

        i. Law

        ii. Cyberlaw

    e. Education : (most ppl dont believe it will work and that its secure) privacy and security → solution :

        i. Capacity building programs

        ii. Breadth and depth engines

        iii. Strategic communication Plan

        iv. Opportunities Vs Threats of the IoT

9. What is the future of IOT ?

    a. ELIMINATES the need for going online !

    b. There are three core sectors of the IoT :

        i. enterprise,

        ii. home,

        iii. Government,

    c. It will have to account for the huge size of the network

    d. Network will not be human centric → need for geo spatial standards

    e. What about privacy concerns

SDN (6)

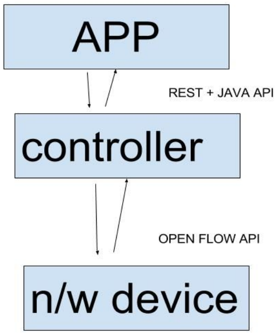
1. Issues in current network architecture :
    a. Changes easy only at edge , in the network theres problem like s/w+h/w is encapsulated into one entity, protocol sharing is slow, less scope for innovation cuz ppl who design it change it
    b. Networks are hard to manage, expensive , have buggy equipment
2. Every device comes packed with two planes :
    a. Control Plane : software → here you program how to forward traffic and all other algorithms, computations based on local routing table (brain)
    b. Data plane : hardware → here there is the copy of the routing table, how to forward the packet
        i. Simple packet-handling rules
            1. Pattern: match packet header bits
            2. Actions: drop, forward, modify, send to controller
            3. Priority: disambiguate overlapping patterns
            4. Counters: #bytes and #packets
            5.
3. SDN can be implemented in three ways :
    a. Open SDN → Open flow
    b. SDN + API
    c. SDN +overlaw

4. Basic principle of SDN (use the diagram)
    a. Software-Defined Networking (SDN) is an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today's applications.
    b. App → For any OS → on some hardware (HP laptop) (there is abstraction here, but in networks this is not there !)
    c. Centralized access point in controller controlling all the access points (brain is in controller), easy to update the flow tables in switches through this one point by controller.
    d. Features of SDN:
        - **Directly programmable**: Network control is directly programmable because it is decoupled from forwarding functions.
        - **Agile: A**bstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.
        - **Centrally managed**: Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch.
        - **Programmatically configured**: SDN lets network managers configure, manage, secure, and optimize network resources very quickly via

dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.

- **Open standards-based and vendor-neutral:** When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.

5. **OpenFlow :**
    a. IDEA : Create abstraction layer for rapid app development
    b. Network device → openflow → controller

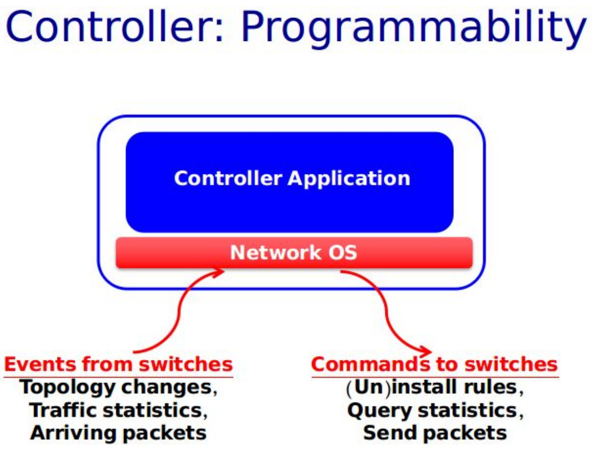


6. Advantage of SDN over conventional network

Conventional network	**SDN**
So for every device in the network you need to create that many data and control planes. (cuz each switch has its own brain)	One brain : controller
All the boxes will run their own os and they might be from diff companies(eg Cisco switch, Juniper etc so diff proprietary rules) If i need to add a new routing algo, ill need to adjust and make sure my algo works in all these cases → lack of interface [interoperability]	Abstraction established through one brain in controller and open flow api
Different action needed for diff box	Unites all the three different boxes (router, nat, firewall and switch)

Hard to innovate	Easy to innovate
Costly software	Cheap and minimal software

7. Controller



Controller: Programmability

Controller Application

Network OS

Events from switches
Topology changes,
Traffic statistics,
Arriving packets

Commands to switches
(Un)install rules,
Query statistics,
Send packets

8. Example Open Flow applications :
    a. Dynamic access control
        i. Inspect first packet of a connection
        ii. Consult the access control policy
        iii. Install rules to block or route traffic

    b. Seamless mobility/migration
        i. See host send traffic at new location
        ii. Modify rules to reroute the traffic

    c. Server load balancing
        i. Pre-install load-balancing policy
        ii. Split traffic based on source IP

    d. Network virtualization
9. Challenges in SDN : // see slides here
    a. Heterogenous switches
    b. Controller delay and overhead
    c. Distributed controllers complexity
    d. Better programming abstraction

T3 : Wireless Networks (20)

1. Five factors deciding range achievable between wireless transmitter and receiver
    a. Transmitting power
    b. Receiver sensitivity
    c. Weather
    d. Modulation technique
    e. Interference

2. Role of Access point in WIFI

    Wireless access points (APs or WAPs) are special-purpose communication devices on wireless local area networks (WLANs). Access points act as a central transmitter and receiver of wireless radio signals.

    Mainstream wireless APs support Wi-Fi and are most commonly used to support public Internethotspots and other business networks where larger buildings and spaces need wireless coverage. The term *base station* is sometimes used to refer to wireless access points, particularly those used in cellular networking. Access points are small physical devices closely resembling home broadband routers. Wireless routers used for home networking have these access points built into the hardware, and can work together with standalone AP units.Wi-Fi hotspots commonly deploy one or more wireless APs to support their Wi-Fi coverage area. Business networks also typically install APs throughout their office areas. While most homes only require one wireless router (AP) to cover the physical space, businesses may use many of them. Determine the optimal locations for where to install a set of APs can be a challenging task even for network professionals due to the need to cover spaces with a reliable signal.
3. Difference between 3G n 2G
    Difference between 2G and 3G Technology

· Cost: The license fee to be paid for 3G network is much higher as compared to 2G networks. The network construction and maintenance of 3G is much costlier than 2G networks. Also from the customers point of view the expenditure for 3G network will be excessively high if they make use of the various applications of 3G.

· Data Transmission: The main difference between 2G and 3G networks is seen by the mobile users who download data and browse theInternet on the mobile phones. They find much faster download speeds, faster access to the data and applications in 3G networks as compared to 2G networks. 2G networks are less compatible with the functions of smart phone. The speed of data transmission in 2G network is less than 50,000 bits per sec while in 3G it can be more than 4 million bits per sec.

· Function: The main function of 2G technology is the transmission of information via voice signals while that of 3G technologies is data transfer via video conferencing, MMS etc.

· Features: The features like mobile TV, video transfers and GPS systems are the additional features of 3G technology that are not available with 2G technologies.

· Frequencies: 2G technology uses a broad range of frequencies in both upper and lower bands, under which the transmission depends on conditions such as weather. A drawback of 3G is that it is simply not available in certain regions.

· Implication: 3G technology offers a high level of security as compared to 2G technology because 3G networks permit validation measures when communicating with other devices.

· Making Calls: Calls can be made easily on both 2G and 3G networks with no real noticeable differences except that in 3G network video calls can also be made. The transmission of text messages and photos is available in both the networks but 2G networks have data limit and the speed of the data transmission is also very slow as compared to 3G.

· Speed: The downloading and uploading speeds available in 2G technologies are up to 236 Kbps. While in 3G technology the downloading and uploading speeds are up to 21 Mbps and 5.7 Mbps respectively.

4. Architecture of cellphone network with diagram

5. Hidden node problem in wireless (dg)

   In wireless networking, the **hidden node problem** or **hidden terminal problem** occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with that AP.[1] This leads to difficulties in media access controlsublayer.

6. Advantage of Wireless over Wired

   As I mentioned in the introduction, the main advantage of a wireless network over a wired one is that users can move around freely within the area of the network with their laptops, handheld devices etc and get an internet connection.

- Users are also able to share files and other resources with other devices that are connected to the network without having to be cabled to a port.

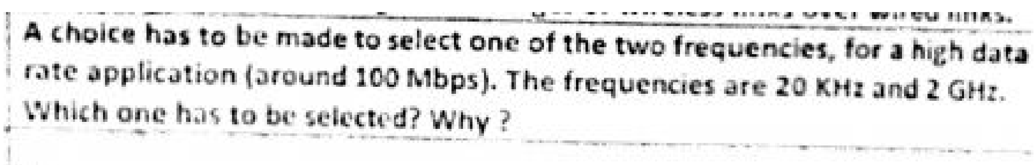
- Not having to lay lots of cables and put them through walls etc. can be a considerable advantage in terms of time and expense. It also makes it easier to add extra devices to the network, as no new cabling is needed.
- If you are a business such as a café, having a wireless network that is accessible to customers can bring you extra business. Customers generally love wireless networks because they are convenient.
- Wireless networks can sometimes handle a larger amount of users because they are not limited by a specific number of connection ports.
- Instant transfer of information to social media is made much easier. For instance, taking a photograph and uploading it to Facebook can generally be done much quicker with wireless technology

7. Disadvantage of Wireless over Wired

It can require extra costs and equipment to set up, although increasingly routers have built-in wireless capability, as do devices such as laptops, handheld devices, modern DVD players, and TVs.

- Setting up a wireless network can sometimes be difficult for people who are not experienced with computers. (Although there are issues with setting up a wired network too, off course!)
- File-sharing transfer speeds are normally slower with wireless networks than they are with cabled. The speeds can also vary considerably according to your location in relation to the network.
- The general speed of a wireless connection is also usually much slower than a wired one. The connection also gets worse the farther you are from the router, which can be a problem in a large building or space.
- Wireless connections can be obstructed by everyday household items and structures such as walls, ceilings, and furniture.
- Wireless networks are generally less secure. There can also be problems with neighbors stealing bandwidth, if the network hasn't been set up to be password protected. Information is also less secure too and can be easier to hack into.

8. Significance in providing mobile access :
    a. Home agent
    b. Foreign agent
    c. Tunnelling

9. 

of wireless links over wired links.

A choice has to be made to select one of the two frequencies, for a high data rate application (around 100 Mbps). The frequencies are 20 KHz and 2 GHz. Which one has to be selected? Why ?

2 GHz..higher the frequency, higher the bandwidth..

The key reason for the interest in higher operating frequencies is the increased data rate available. Put simply, the higher the carrier frequency, the higher the practical data rate and the link between carrier frequency and data rate is well understood. However the move up in frequency is slowed by the cost of equipment and the performance of available component parts.

10. Difference between ad hoc and infrastructure mode

Most Wi-Fi networks function in infrastructure mode. Devices on the network all communicate through a single access point, which is generally the wireless router. For example, let’s say you have two laptops sitting next to each other, each connected to the same wireless network. Even when sitting right next to each other, they’re not communicating directly. Instead, they’re communicating indirectly through the wireless access point. They send packets to the access point — probably a wireless router — and it sends the packets back to the other laptop. Infrastructure mode requires a central access point that all devices connect to.

Ad-hoc mode is also known as “peer-to-peer” mode. Ad-hoc networks don’t require a centralized access point. Instead, devices on the wireless network connect directly to each other. If you set up the two laptops in ad-hoc wireless mode, they’d connect directly to each other without the need for a centralized access point.

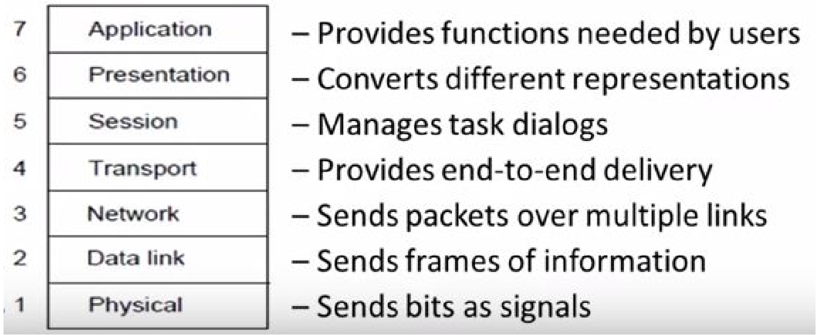
11. What is SNR ?
12. Hands Off
13. Main protocols:
    a. Foreign Agent-Mobile register-deregister
    b. Foreign Agent-Home Agent
    c. Home Agent-encap
    d. Foreign Agent-decap
14. Main Architecture:

    Phone=>Radio Net Controller=>MSC and SGSN=>MSC for phone; SGSN is for data

T1 : Chapter 4 (20)

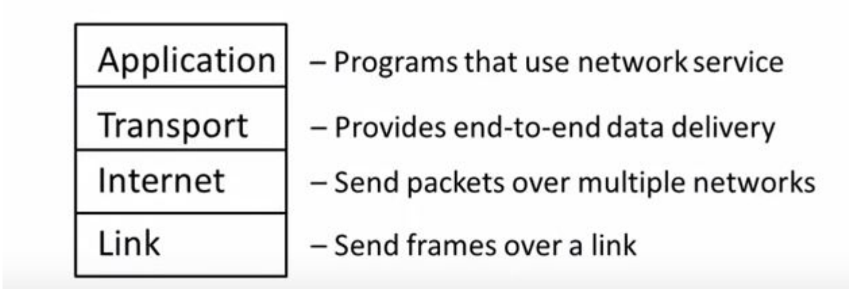
Reference Models Review

OSI (Open System Interconnection) : 7 layer model , not used in real life

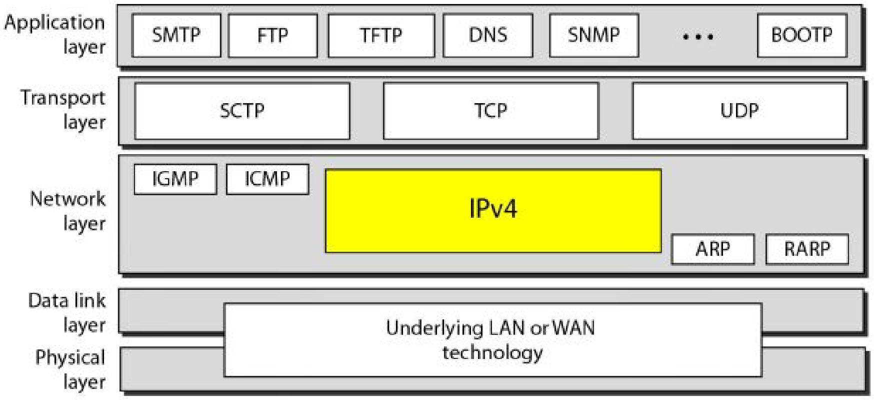


7	Application	– Provides functions needed by users
6	Presentation	– Converts different representations
5	Session	– Manages task dialogs
4	Transport	– Provides end-to-end delivery
3	Network	– Sends packets over multiple links
2	Data link	– Sends frames of information
1	Physical	– Sends bits as signals

Internet Reference Model



Application	– Programs that use network service
Transport	– Provides end-to-end data delivery
Internet	– Send packets over multiple networks
Link	– Send frames over a link



1. Why use Network Layer when u can transport frames through switches ?
    a. Switched network will not scale to large network , each routing table will bloat up because of the broadcast system which will expect the router to have all the possible addresses.
    b. No control on routing mechanisms (the spanning tree algo doesnt guarantee the best path)
    c. The switching will not work across different link layer technologies
2. Advantages of Network Layer method
    a. Scaling : hierarchy → network prefixing
    b. Bandwidth control → QOS/ Lower Cost Routing

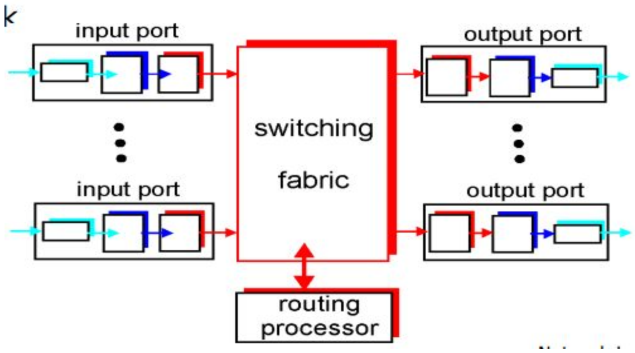
   c. Heterogeneity → IP

3. Network Layer Duties :
   a. Create Packet [Protocol Data Unit of Network Layer]
   b. Addressing – Take care of uniquely identifying host
   c. Routing-execute routing algorithm to determine paths across the network
   d. Forwarding – Send the packet arriving at the input port to right output port (transfer packet across a node)
   e. Congestion control to deal with traffic jam
   f. Connection setup, maintenance, and teardown
   g. Quality Of Service connection-based

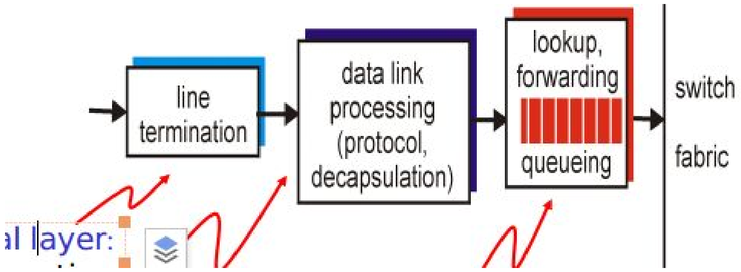
4. Routing vs Forwarding ?

Routing	Forwarding
Determines which way in network traffic will go to	Decides which port in router the traffic is sent to
Global, involves >1 router	Local , involves one router
slower	Has to be fast

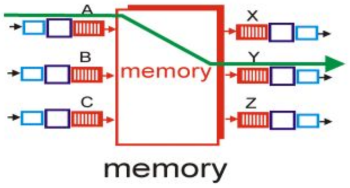
5. What kind of service does network Layer provide to the transport layer ? OR what are the network service models ?
   a. Datagram Service Model
   b. Virtual Service Model
6. What kind of features do we look for in a datagram service model when its about individual packets and when its about many packets together ?
   a. Individual packets :
      i. Speed of packet
      ii. Guaranteed delivery
   b. Many packets
      i. Order of delivery
      ii. Inter packet time
      iii. Guaranteed minimum bandwidth
7. What is a router ?
   a. Device that allows for:
      i. run routing algorithms/protocol (RIP, OSPF, BGP)
      ii. forwarding datagrams from incoming to outgoing link
8. Explain the router architecture ?



- Input Lines
  - After decapsulating the packet, we need to use the datagram dest to lookup the output port using the forwarding table in input port memory.
  - This processing should happen at line speed, if the datagrams come faster than the forwarding rate then there is queueing in the buffer.
  - Input buffering can be due to :
    - Above point
    - HOL Blocking

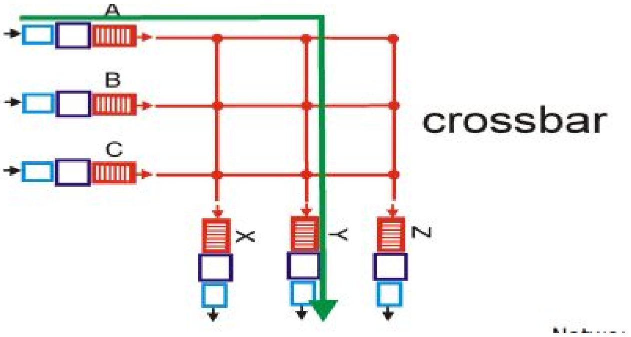


- Output Lines
  - Switching fabric is slower than output line
- Routing Processor
- Switching Fabric
  - There are three types :
    - Memory
      - packet copied to system's memory
      - speed limited by memory bandwidth (2 bus crossings per datagram)
      - Local Routers

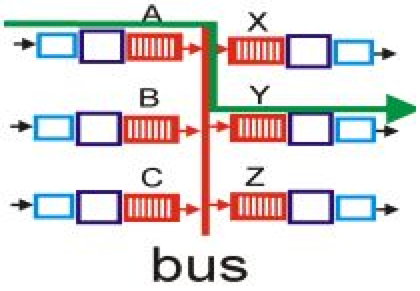


    - Crossbar

        - Banyan networks, other interconnection nets initially developed to connect processors in multiprocessor
        - Advanced design: fragmenting datagram into fixed length cells, switch cells through the fabric.
        - Interconnected Routers

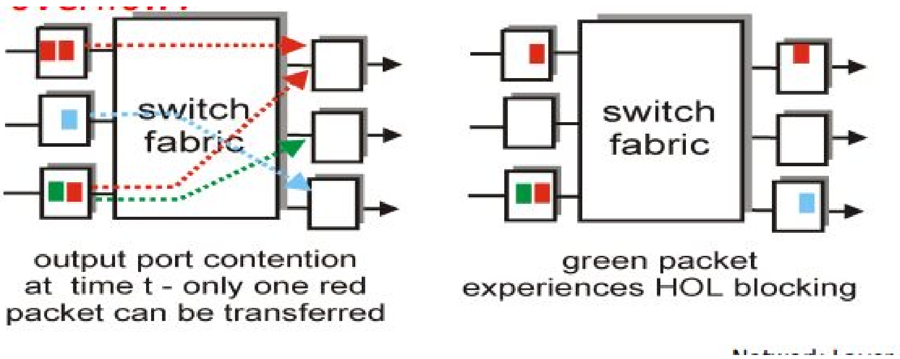


    - Bus
        - datagram from input port memory to output port memory via a shared bus
        - bus contention: switching speed limited by bus bandwidth
        - Enterprise and Access Routers



- Buffers
    - When there are competing packets for an output port say, there has to be multiplexing of the output link
    - Scheduling discipline : will be applied when you need to decide which of the queued packets you want to transmit

9. What is head of line blocking ?

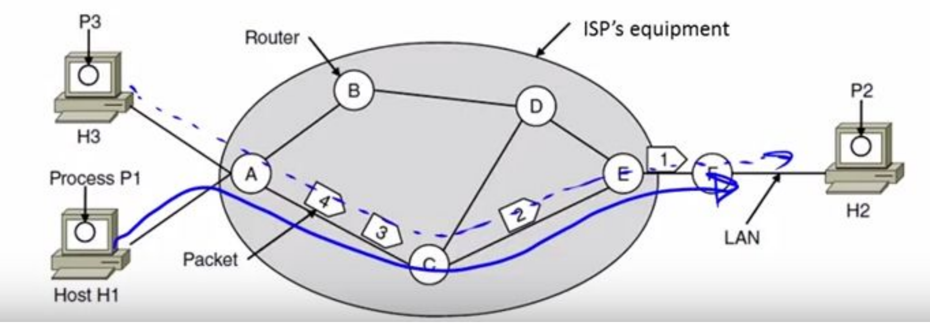

switch fabric
output port contention at time t - only one red packet can be transferred
switch fabric
green packet experiences HOL blocking

a.

10. Difference between Datagram and Virtual Circuit model ?

Datagram	**Virtual Circuit**
Connection less	Connection Oriented (setup + teardown)
No state maintained	VC routers maintain state of connection. Resources like buffer, link reserved fr that specific VC number
Need long destination address	Need only a short label to id circuit
Router needs to know destination address and next hop. This may cause delay if network changes during forwarding	Router needs to know vc number/identifier and interface and sends over to outgoing interface with new vc number
Used in IP	Used in ATM, Frame Relay
Smart end systems; simple to implement inside a network, complex in edge	Dumb end systems; Complex inside network only
Adv : not complex, systems dont need to be reserved and packets can come in any order , no state	Adv : Resource and bandwidth is allocated, inorder delivery

11. What if two hosts want to use similar route to transfer info in VC ?



Here host 1 and 3 are transmitting to router A in the path.
When the pkt comes out from A and goes to C , at C how do u distinguish which ckt it belongs to ?

Router A :
Input : h1 → rename vc from 1 -->2
Output : h3 → rename vc from 1-->5

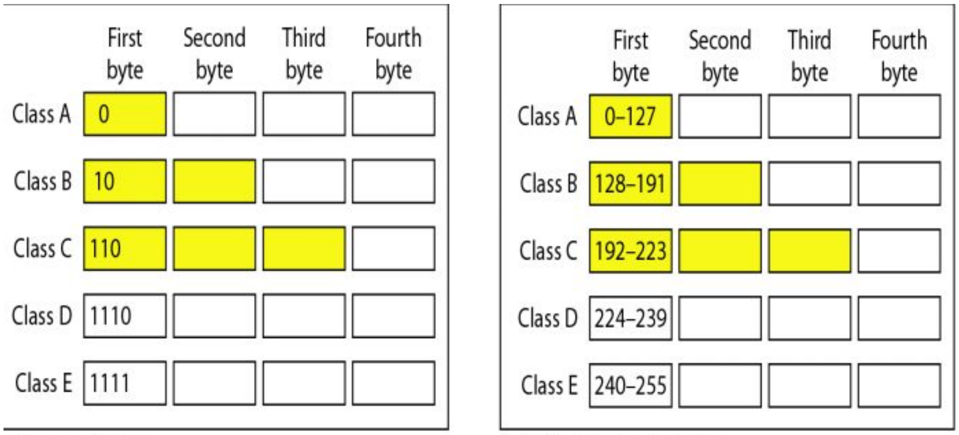
Router C :
Input : A (2)
Output : A (5)

If the renaming had not been done for the VC then at C it would have been A(1) and A(1) and there would be confusion. Hence both circuits are separated.

12. What is the solution to the address range division problem ?
    a. Longest prefix matching
        i. when looking for forwarding table entry for given destination address, use longest address prefix that matches destination address.
        ii. Helps in hierarchy, so that u need to know only less specific address
13. Public IP allocation :
    a. (hierarchical allocation) IANA → regional bodies → isps and companies → customer via DHCP
14. Any network is characterized by the following 4 parameters :
    a. Net ID or Subnet ID
    b. Total number of addresses in that network (Address space)
    c. First usable address
    d. Last usable address

15. IPV4 addressing :
    a. Rules :
        i. There must be no leading zero (045).
        ii. There can be no more than four numbers.
        iii. Each number needs to be less than or equal to 255.
        iv. A mixture of binary notation and dotted-decimal notation is not allowed.

16. Classful addressing :



	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10	▨		
Class C	110	▨	▨	
Class D	1110			
Class E	1111			

. Binary notation

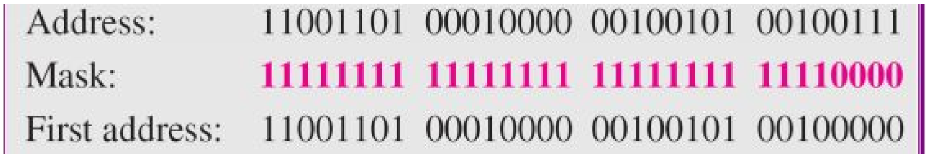
	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191	▨		
Class C	192–223	▨	▨	
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

    a. Fixed size blocks form classes
    b. Classes :
        i. Large A 0 /8 : network address 8 bits while rest is free
        ii. Medium B 10 /16
        iii. Small C 110 /32

17. Class less addressing :

a. First n bits : network/prefix , 32-n bits : host
b. Longest prefix matching
c. Lookup is more complex, but its hierarchical which allows scalability and its a compact system
d. A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first & last address in the block?
   i. The first address in the block can be found by setting the rightmost 32 − n bits to 0s. This is also found by **anding** the given address with the mask.

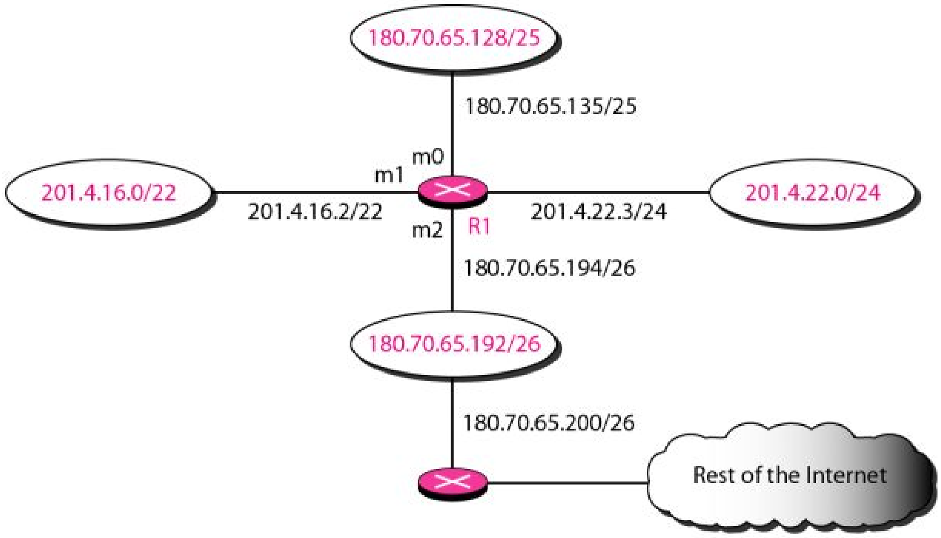


Address:	11001101	00010000	00100101	00100111
Mask:	**11111111**	**11111111**	**11111111**	**11110000**
First address:	11001101	00010000	00100101	00100000

   39 : 0010 0111 → set last 32-38=4 bits to 0 → 32, 205.16.37.32

   ii. The last address in the block can be found by setting the rightmost 32 − n bits to 1s.
   39 : 0010 0111 → set last 32-38=4 bits to 1 → 47, 205.16.37.47

   iii. The total number of addresses is found by : The number of addresses can be found by complementing the mask, interpreting it as a decimal number, and adding 1 to it. (OR , 2^(32-prefixbits))



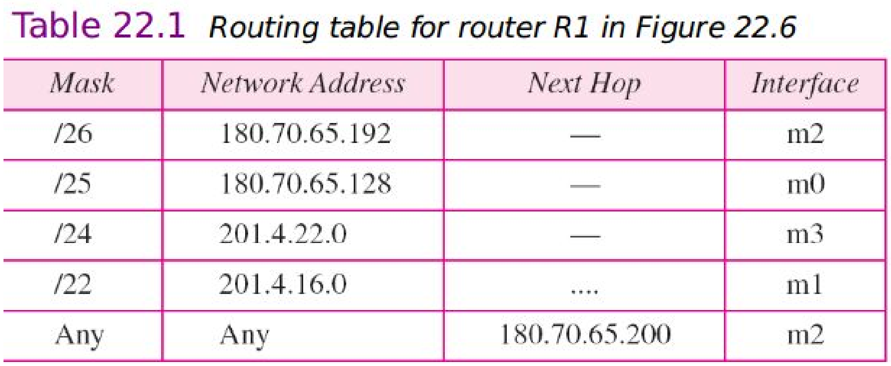


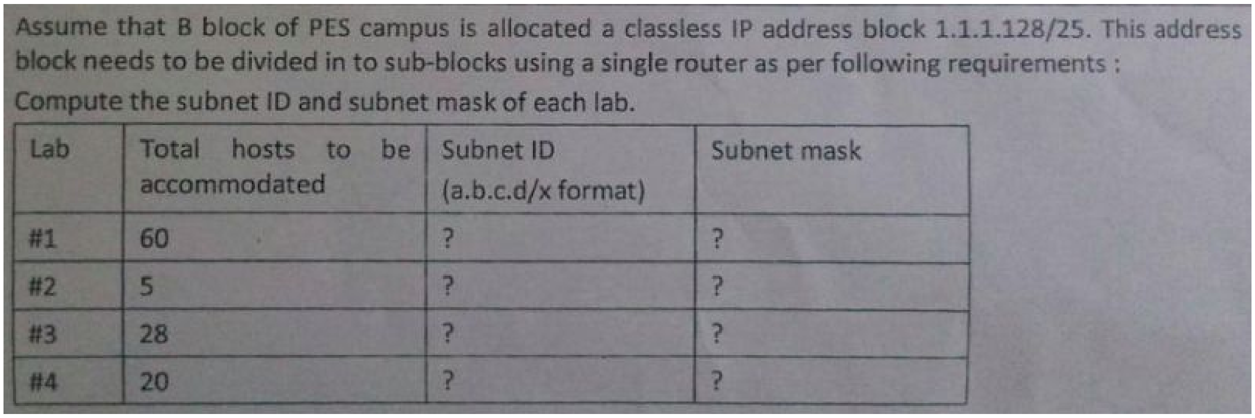
Table 22.1 *Routing table for router R1 in Figure 22.6*

Mask	*Network Address*	*Next Hop*	*Interface*
/26	180.70.65.192	—	m2
/25	180.70.65.128	—	m0
/24	201.4.22.0	—	m3
/22	201.4.16.0	....	m1
Any	Any	180.70.65.200	m2

Mask	Network address	Next hop	interface

e. Get the destination address, convert into bits and compare against subnet id for longest match

18. Subnetting :
    a. First address is subnet id
    b. Last address is broadcast id
    c. Total usable address : 2 ^ prefix bits -2



Assume that B block of PES campus is allocated a classless IP address block 1.1.1.128/25. This address block needs to be divided in to sub-blocks using a single router as per following requirements :
Compute the subnet ID and subnet mask of each lab.

Lab	Total hosts to be accommodated	Subnet ID (a.b.c.d/x format)	Subnet mask
#1	60	?	?
#2	5	?	?
#3	28	?	?
#4	20	?	?

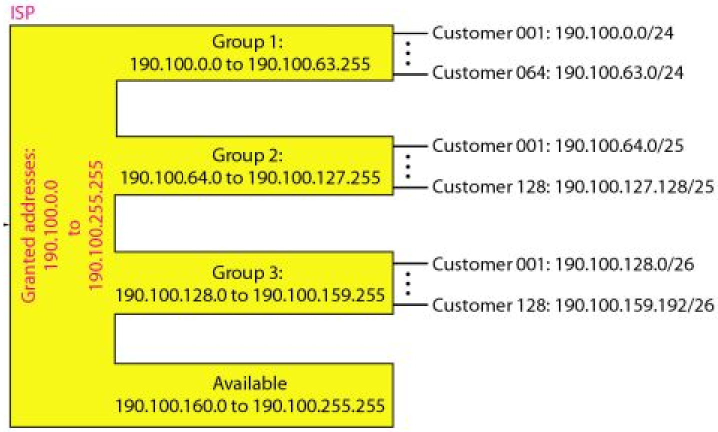
i. This means subnet id has 25 bits fixed while last 7 bits are free 00000001.00000001.00000001.10000000 is what we have.
Possible free addresses : 2^7

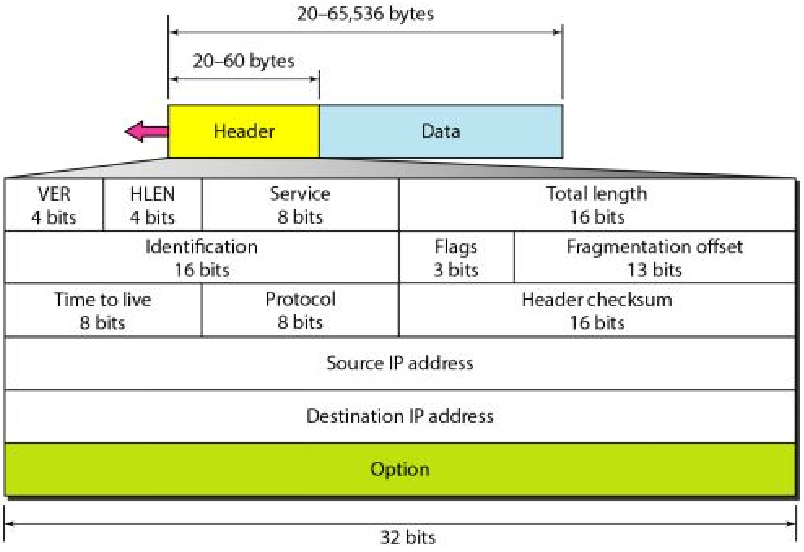
- First divide into subnets and obtain ids, change a bit move down by a power of 2.
- Lab 1 needs 60 computers , so we divide 128/2 > set 1 bit more ..10000000, and 11000000 , allocate first 1 to lab 1 and second needs more division. The mask over here will be 192 (as 6 empty boxes)
- Lab 3 and 4 needs 28 and 20 comps : 64/2 :32 should cater to both. 11000000 and 11100000 >> 224 (5 empty boxes)

- Lab 2 needs 5 and we cant split these without messing requiremenets!

An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:
a. The first group has 64 customers; each needs 256 addresses.
b. The second group has 128 customers; each needs 128 addresses.
c. The third group has 128 customers; each needs 64 addresses.
Design the subblocks and find out how many addresses are still available after these allocations.

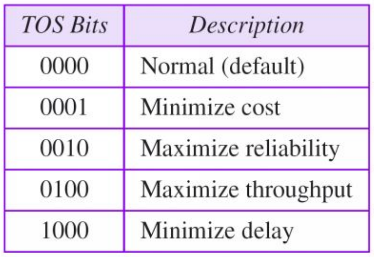
Group number	Bits free	Number of divisions	First address	Last address	Total number of addresses
Group1 (64c, 256)	Log 256/log2 =8 bits free → /24	1	190.100.0.0/24 → 190.100.0.255/24	190.100.63.0/24-->190.100.63.255/24	64 X256
Group2 (128c, 128)	Log 256/log2 =7 bits free → /25	2	190.100.64.0/25 → 190.100.64.127/25; 190.100.64.128/25→ 190.100.64.255/25	Last address is 128/2 → 64 : first address+64; 63+64 -->127 190.100.127.128 →190.100.127.255	128X128
Group3 (128c, 64)	Log 256/log2 =6 bits free → /26	4	190.100.128.0/26 →190.100.128.63/26	Last address is 128/4 → 32 : first address+32; 128+32-1 -->159	128X64
Group4			190.100.160.0	190.100.255.255	


ISP
Granted addresses: 190.100.0.0 to 190.100.255.255
Group 1: 190.100.0.0 to 190.100.63.255
Customer 001: 190.100.0.0/24
Customer 064: 190.100.63.0/24
Group 2: 190.100.64.0 to 190.100.127.255
Customer 001: 190.100.64.0/25
Customer 128: 190.100.127.128/25
Group 3: 190.100.128.0 to 190.100.159.255
Customer 001: 190.100.128.0/26
Customer 128: 190.100.159.192/26
Available 190.100.160.0 to 190.100.255.255

19. How to connect different networks together ?
    a. Diff networks have diff addressing, QOS, pkt size,security and service model
    b. IP (narrow waist of internet)
20. IPV4 datagram (20)
    a. The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols.
    b. The total length field defines the total length of the datagram including the header.
    c. Header | MTU(max length of dgram in the frame) | Trailer
    d. 

    e. FIELDS :
        i. Version → ipv4 or ipv4 , 4 bits
        ii. Header Length → where the data will begin , 4 bits
        iii. TOS → what kind of service is provided (more reliable, less delay , high thorughput) , 4 bits

Table 20.1 *Types of service*



TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

iv. Datagram Length (header +data); 16 bits

v. Identification

vi. Flags

vii. Fragmentation offset

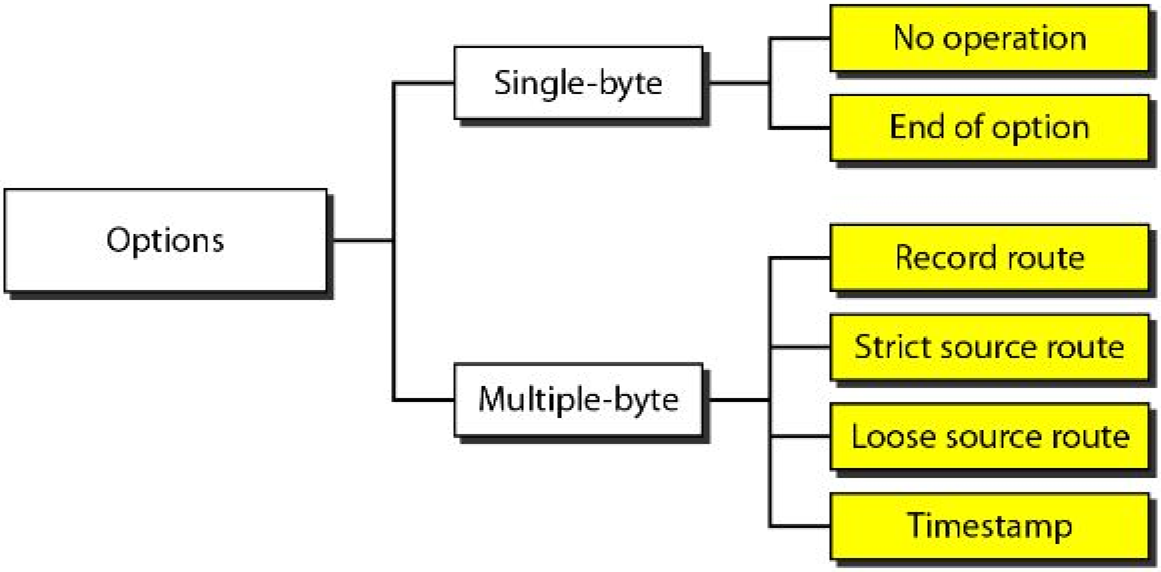
viii. TTL → (prevents routing loop) ; 8 bits

ix. Protocol →which protocol you are passing to, analogous to port number ;8bits

x. Checksum → contains the ones complement of the sum of the data, checks for errors in data ; 16 bits

xi. Source and Destination IP ; 32 bits each

xii. Options → helps to extend header length, increases time at router



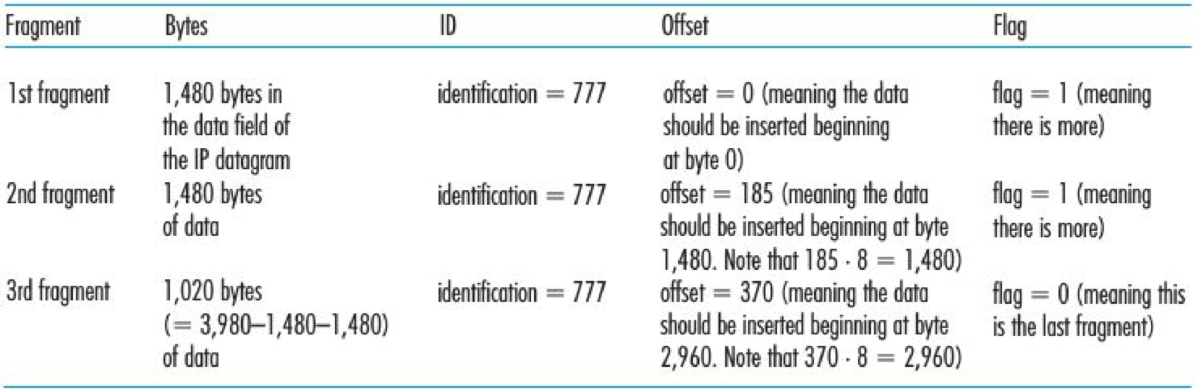
f. The **protocol number** is the glue that binds the network and transport layers together, whereas the **port number** is the glue that binds the transport and application layers together.

g. why does TCP/IP perform error checking at both the transport and network layers?.

        i. First, note that only the IP header is checksummed at the IP layer while the TCP/UDP checksum is computed over the entire TCP/UDP segment.
        ii. Second, TCP/UDP and IP do not necessarily both have to belong to the same protocol stack. TCP can, in principle, run over a different protocol (for example,ATM) and IP can carry data that will not be passed to TCP/UDP.

    h. Fragmentation :
        i. Link layer protocol will implement hard limit on size of IP datagram because this will be encapsulated in link layer frame and sent to other router
        ii. Fragmentation will occur when outgoing link has lower MTU capacity than incoming
        iii. Datagram reassembly is not done in router but done at end system, to allow host to do all this , in the dgram we have the fields id, frag offset and flags which allow it to decide if dgram is fragment and if it is which one.
            1. same id ? fragment!
            2. How to determine if last frag sent ? Flag set to 0 else all set to 1
            3. Offset : decides where in dgram frag fits

4000 bytes of data : 3980(payload) +20 (H)



Fragment	Bytes	ID	Offset	Flag
1st fragment	1,480 bytes in the data field of the IP datagram	identification = 777	offset = 0 (meaning the data should be inserted beginning at byte 0)	flag = 1 (meaning there is more)
2nd fragment	1,480 bytes of data	identification = 777	offset = 185 (meaning the data should be inserted beginning at byte 1,480. Note that 185 · 8 = 1,480)	flag = 1 (meaning there is more)
3rd fragment	1,020 bytes (= 3,980–1,480–1,480) of data	identification = 777	offset = 370 (meaning the data should be inserted beginning at byte 2,960. Note that 370 · 8 = 2,960)	flag = 0 (meaning this is the last fragment)

Actual Payload Length = 4000 - 20 = 3980

Now the packet is fragmented owing to the fact that the length is greater than the MTU (1500 Bytes).

Thus the 1st packet contains 1500 Bytes which includes IP header + Payload Fraction.

1500 = 20 (IP header) + 1480 (Data Payload)

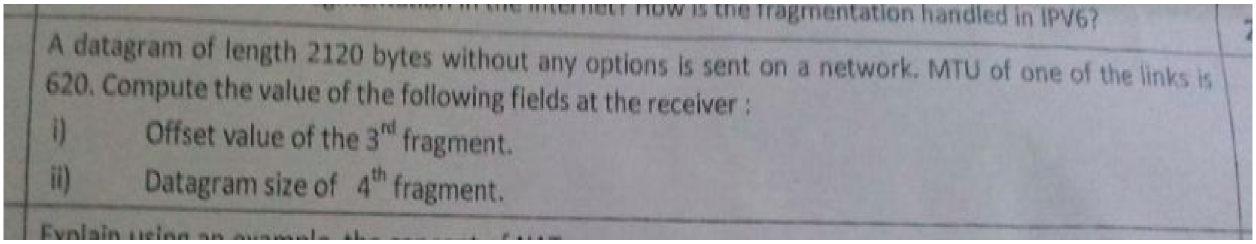
Similarly for the other packet.

The third packet shall contain remaining left over data (3980 - 1480 -1480) = 1020

Thus length of the packet is 20 (IP Header) + 1020 (payload) = 1040

There is a 20 byte header in each packet. So the original packet contains 3,980 bytes of data.
The fragments contain 1480, 1480, and 1020 bytes of data. 1480 + 1480 + 1020 = 3980
Every bit in the header is precious. Dividing the offset by 8 allows it to fit in 13 bits instead of 16.
This means every packet but the last must contain a number of data bytes that is a multiple of 8, which isn't a problem

Problem on fragmenting



internet? How is the fragmentation handled in IPV6?

A datagram of length 2120 bytes without any options is sent on a network. MTU of one of the links is 620. Compute the value of the following fields at the receiver :

i) Offset value of the 3rd fragment.

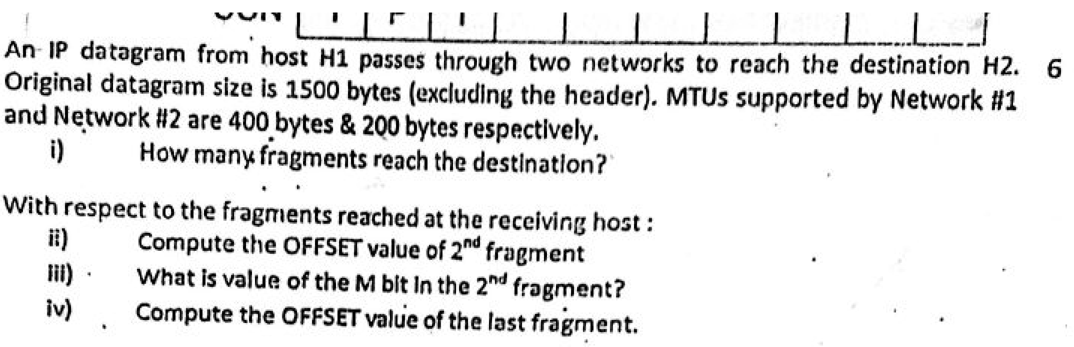
ii) Datagram size of 4th fragment.

Explain using an example, the concept of NAT

	Offset start	size	Flag
of1	0	600	1
of2	75	600	1
of3	150	600	1
of4	225	300	0

Total length =2120
Payload : 2100 + header =20
MTU on link = 620

So in each case , 600 + 20 (H)
Therefore number of fragments :3 +1
600 X3 = 1800 (2100-1800 = 300) , last packet has 280+20 of the data remaining



An IP datagram from host H1 passes through two networks to reach the destination H2. Original datagram size is 1500 bytes (excluding the header). MTUs supported by Network #1 and Network #2 are 400 bytes & 200 bytes respectively. 6

i) How many fragments reach the destination?

With respect to the fragments reached at the receiving host :

ii) Compute the OFFSET value of 2nd fragment

iii) What is value of the M bit in the 2nd fragment?

iv) Compute the OFFSET value of the last fragment.

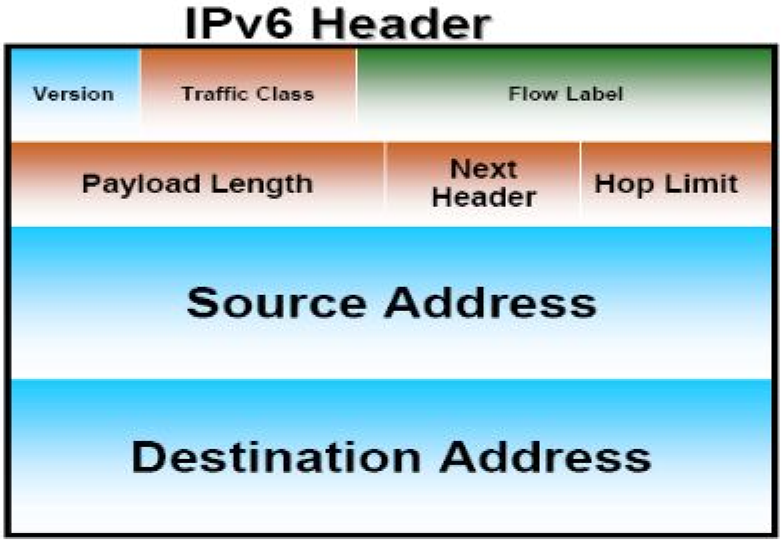
20 bytes should be for header..so, remaining 380 bytes..but data should have byte boundaries..

So, every frame can carry only 376(which is divisible by 8) and not 380(not div by 8)..

So, 1500=>376*3+372

Stage 2: 376=> 176*2+24

Total: 10 fragments

21. Problems in Fragmentation :
    a. Lethal DOS attack
    b. Load on router
22. IPV6 Datagram (40)
    a. 

23. IPV6 vs IPV4
    a. Support billions of hosts, even with inefficient address space allocation
    b. Reduce the size of the routing tables
    c. Simplify the protocol, to allow routers to process packets faster
    d. Provide better security (authentication and privacy) than current IP
    e. Pay more attention to type of service, particularly for real-time data
    f. Provide multicasting by allowing scopes to be specified
    g. Make it possible for a host to roam without changing its address
    h. allow the protocol to evolve in the future

i. Permit the old and new protocols to co-exist for years

24. NAT

a. Violates end to end principle as it connects home network to public network

b. Will do the following

i. all datagrams leaving local network have same single source NAT IP address. (range of addresses not needed from ISP: just one IP address for all devices)

ii. can change addresses of devices in local network without notifying outside world

iii. can change ISP without changing addresses of devices in local network

iv. devices inside local net not explicitly addressable, visible by outside world (a security plus)

v. NAT TABLE

Source ip (priv)	Port number(16-bit)	Global address (pub)

vi. Q.1. Is it possible to have the same address space e.g. 10.0.0.0/8 for all the 3 campuses ?

1. 3 NATS

vii. Q.2. Suppose PES campus is allotted an IP address 200.200.200.0/24 (which means only 254 hosts can be connected), is there any way to connect 1000 users?

c. Tunnelling :

i. Private device sends pkt , makes nat entry and gets global address n port

ii. Device learns this global address (DNS) and creates tunnels

d. Advantages :

i. No more ip address pressure

ii. Easy to deploy

iii. Easy functionality and security (put firewall in nat)

iv. NAT traversal deals with incoming traffic

e. Problems in NAT :

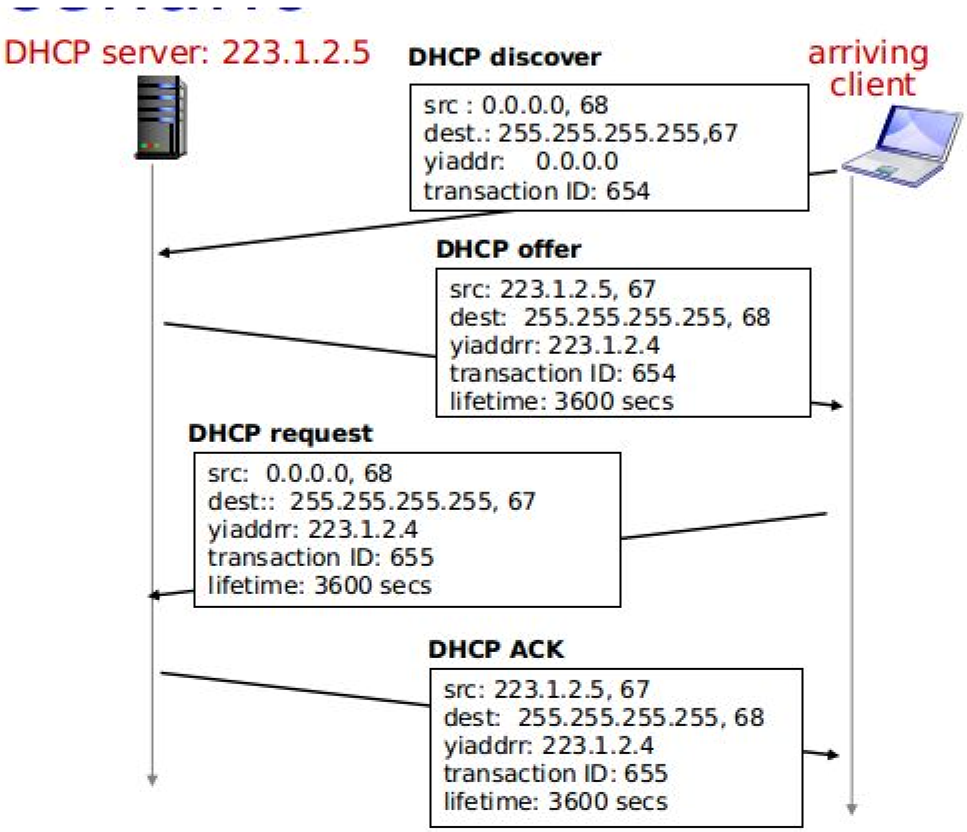
i. Nat table filled only when req made from private to outside

ii. Difficult to run peer to peer services like Skype

iii. Breaks apps that expose IP address (FTP)

iv. When peer to peer connection needed via tcp and receiver peer is behind nat, it cant get connection. Peer A can first contact Peer B through an intermediate Peer C, which is not behind a NAT and to which B has established an ongoing TCP connection. Peer A can then ask Peer B, via Peer C, to initiate a TCP connection directly back to Peer A. Once the direct P2P TCP connection is established between Peers A and B, the two peers can exchange messages or files. T**his hack, called connection reversal, is actually used by many P2P applications for NAT traversal**. If both Peer A and Peer B are behind their own NATs, the situation is a bit trickier but can be handled using application relays, as we saw with Skype relays in Chapter 2.

25. Disadvantages of Middle boxes(router)
    a. Break layering principle
    b. More functionality difficult at ip level (intrusion detection)
26. Discovery protocols : DHCP & ARP
27. DHCP(Dynamic Host Configuration Protocol)
    a. A macromobility solution to manage IP addresses dynamically
    b. Why not reuse/share ip addresses when not being used ?
    c. PLUG and PLAY protocol , automatically allocated address
    d. DHCP encapsulated in UDP
    e. Features :[DORA]
        i. host broadcasts “DHCP discover” msg [optional]
        ii. DHCP server responds with “DHCP offer” msg [optional]
        iii. host requests IP address: “DHCP request” msg
        iv. DHCP server sends address: “DHCP ack” msg



DHCP discover
src : 0.0.0.0, 68
dest.: 255.255.255.255,67
yiaddr: 0.0.0.0
transaction ID: 654

DHCP offer
src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddrr: 223.1.2.4
transaction ID: 654
lifetime: 3600 secs

DHCP request
src: 0.0.0.0, 68
dest:: 255.255.255.255, 67
yiaddrr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

DHCP ACK
src: 223.1.2.5, 67
dest: 255.255.255.255, 68
yiaddrr: 223.1.2.4
transaction ID: 655
lifetime: 3600 secs

    f. DHCP returns :
        i. address of first-hop router for client

ii. name and IP address of DNS sever
iii. network mask (indicating network versus host portion of address)
iv. Ip address on subnet

28. ARP(Address Resolution Protocol)

a. At **Link layer** level, a frame has to be prepared and to be sent to adjacent node. Frame must have Source MAC address and Destination MAC address. This mapping done by ARP(used to get datagram to destination IP subnet)
b. 32 bit
c. network-layer address (MAC) 48 bit MAC address (for most LANs)
d. MAC flat address ➔ portability (can move LAN card from one LAN to another unlike IP which depends on subnet)
e. PLUG and PLAY
    i. A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
        - soft state: information that times out (goes away) unless refreshed

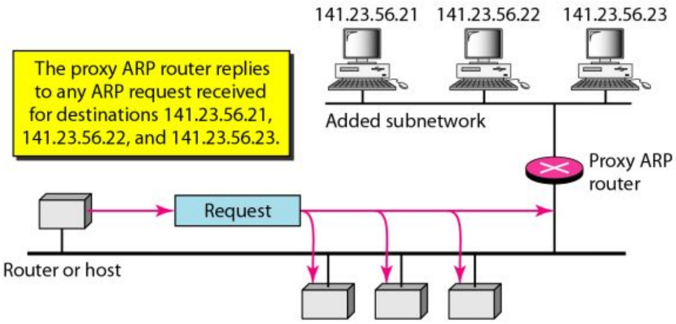
f. ARP table

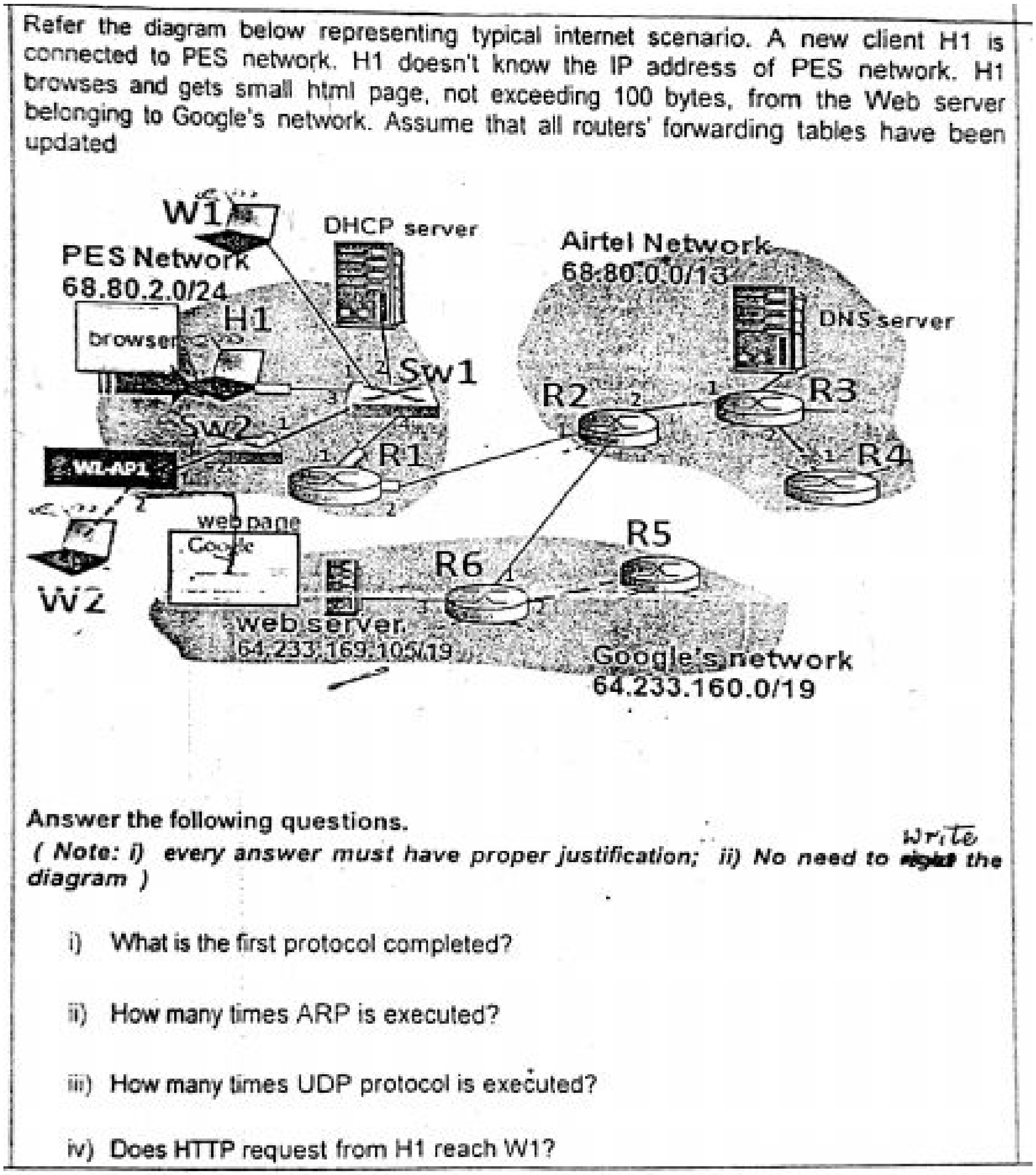
IP	MAC address	TTL

g. Frame

Source mac	Dest mac	Source ip	Dest ip	TTL	payload

h. Broadcasts dest address, dest will unicast and info will stay in source's arp table till TTL
i. Proxy ARP


141.23.56.21
141.23.56.22
141.23.56.23
The proxy ARP router replies to any ARP request received for destinations 141.23.56.21, 141.23.56.22, and 141.23.56.23.
Added subnetwork
Proxy ARP router
Request
Router or host



Refer the diagram below representing typical internet scenario. A new client H1 is connected to PES network. H1 doesn't know the IP address of PES network. H1 browses and gets small html page, not exceeding 100 bytes, from the Web server belonging to Google's network. Assume that all routers' forwarding tables have been updated

Answer the following questions.

(Note: i) every answer must have proper justification; ii) No need to write the diagram)

i) What is the first protocol completed?

ii) How many times ARP is executed?

iii) How many times UDP protocol is executed?

iv) Does HTTP request from H1 reach W1?

29.

First protocol-dhcp

Arp-3 times-once in PES, once in google network,once in airtel network

Udp-once for getting ip address(DNS) and 1 times for DHCP

If somebody else has browsed the internet before, the switch has router's mac address associated with the corresponding port and it wont broadcast the http request. Here, if H1 didn't know the ip address of google, it would have sent one dns query..the moment the response comes, the switch will register the router's mac to that link and it wont broadcast the http request!

30. ICMP

a. Companion protocol with IP

Ip header	Icmp header(type,code,chksum)	payload

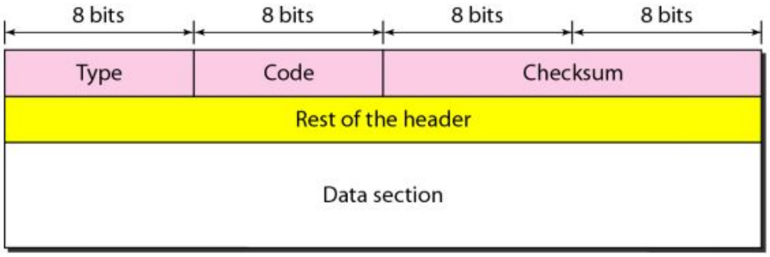
b.

c. The IP protocol has no error-reporting or **error-correcting** mechanism. The IP protocol also lacks a mechanism for **host and management queries**. The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol.

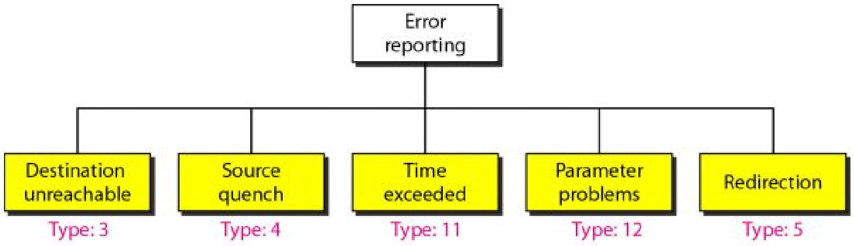
d. used by hosts & routers to communicate network-level information error reporting: unreachable host, network, port, protocol echo request/reply (used by ping)

e. Also used in path MTU discovery

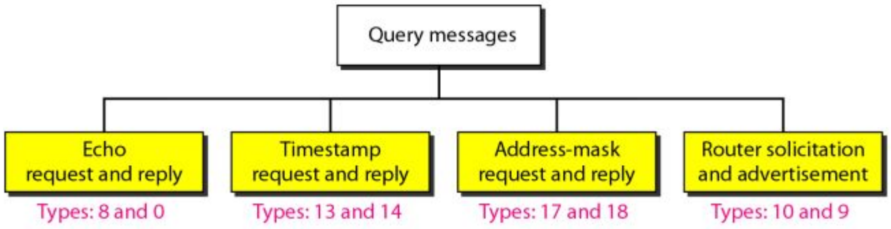
f. ICMP message format

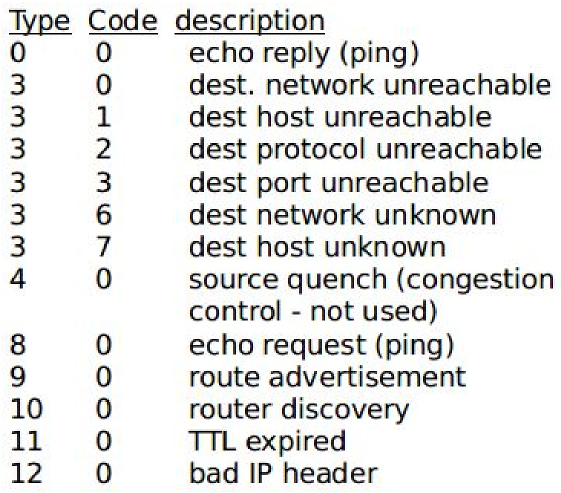


g. Types of errors that can occur



h. Types of queries that can occur



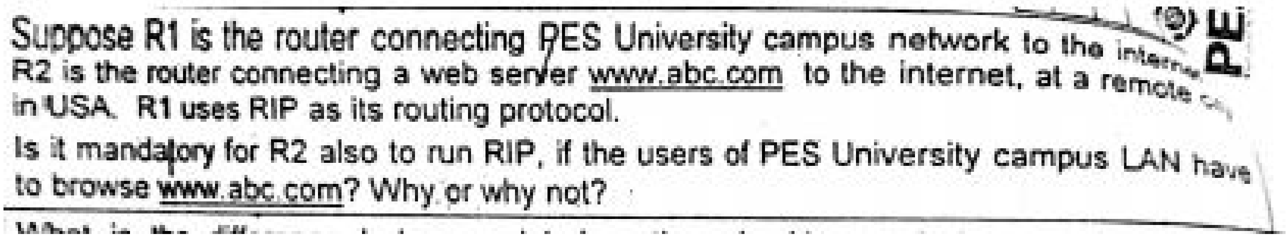


Type	Code	description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

i.

T2 : Network Layer continued

1. Params influencing Routing :
    a. Hop count
    b. Bandwidth
    c. Load in network
2. In which case DVR/ LS is sizeof msg sent more and why ?
    a. in distance vector, we send the entire distance matrix..but in LS, we send only info about neighbors..



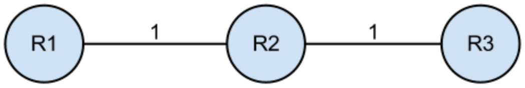
Suppose R1 is the router connecting PES University campus network to the interne
R2 is the router connecting a web server www.abc.com to the internet, at a remote ci
in USA. R1 uses RIP as its routing protocol.
Is it mandatory for R2 also to run RIP, if the users of PES University campus LAN have to browse www.abc.com? Why or why not?

3.
    a. no..both belong to different AS..hence, they can run own routing protocols..BGP will synchronize..
4. If no user accesses internet is there still traffic on internet ?
    a. yes..RIP will keep on exchanging routing messages every 30sec..this is in accordance to the RIP protocol which will assume neighbor is not there/link is down if there's no message from that neighbor within 180 sec..(not really sure of the time)
5. Complexity of LS ?
    a. n(n-1)/2 searches done so O(n square) → can be reduced by using a heap for finding minimum at each level which makes sure it is done in log time
6. Why is LS Global , while DV is Distributed ?
    a. Cuz flooding of LS packets done, such that everyone in the network has a global view of topology (centralised setting)
    b. After obtaining the LS packet from everyone , each node is capable of doing the Dijkstra calculation to get node-next hop table (Forwarding table).
    c. In the case of DV (distributed setting)
        i. Distributed ? gets info from neighbours and redistributes after calc
        ii. asynchronous ? all nodes don't need to work together
        iii. Iterative ? Process continues till no more info exchanged
7. Convergence is the time required for the routers to update their routing tables after a topology change has occurred.
8. DV / LS comparison

Property	**DV**	**LS**

Nature of Algo	Asynchronous, distributed and iterative	Global, centralised, synchronous
Message Complexity	Here we can send only to neighbors	Everyone gets message so O(NE) messages sent
Convergence Time	Link cost propgated only if its cost is less than original least cost path	New link cost sent to all nodes. Flood and compute. (faster)
Speed of Convergence	Slow convergence due to count to infinity and routing problems faced in case of cost increase in links. Usually complexity is O(VE)	O(N square)
Robustness	Incorrect calculation is propagated throughout the network	Every node independantly calculates so only malfunctioning node will have wrong forwarding table. MORE robust
Implementation	Bellman Ford	Djikstra
Scalability	Only at node level computation (better)	Too much computation

9. Complexity of DV : O(VE)
10. Contributions of Bellman Ford Equation to DV :
    a. It will give next hop entries in forwarding table.For x to update its FTable to destination Y it needs to know, the next hop neighbour in the shortest path to Y. This neighbor is the neighbor which satisfies the bellman ford equation and is the minimum value.
    b. Suggests the form of neighbor-neighbor interaction that should take place
11. What is the count to infinity problem ?
    a. Counting-to-infinity occurs when one router feeds another old information, which continues to propagate through the network toward infinity. This can definitely occur when a link is removed.



So in this example, the Bellman-Ford algorithm will converge for each router, they will have entries for each other. R2 will know that it can get to R3 at a cost of 1, and R1 will know that it can get to R3 via R2 at a cost of 2.

If the link between R2 and R3 is disconnected, then R2 will know that it can no longer get to R3 via that link and will remove it from its table. Before it can send any updates it's possible that it will receive an update from R1 which will be advertising that it can get to R3 at a cost of 2. R2 can get to R1 at a cost of 1, so it will update a route to R3 via R1 at a cost of 3. R1 will then receive updates from R2 later and update its cost to 4. They will then go on feeding each other bad information toward infinity. NOTE : the same problem can happen when cost increases also, doesn't happen when cost of link decreases.

12. In DV what happens if the connection breaks ?
    a. That nodes updation is done , in the next iteration only the nodes connected to this node will be updated. In the iteration after that the nodes connected to these updated nodes will be changed and so on the change will be propagated. CLEARLY this is slow :P
13. What is poisoned reverse case of DV algo ?
    a. indicate to other routers that a route is no longer reachable and should not be considered from their routing tables. Unlike the split horizon with poison reverse, route poisoning provides for sending updates with unreachable hop counts immediately to all the nodes in the network.When the protocol detects an invalid route, all of the routers in the network are informed that the bad route has an infinite (∞) route metric. This makes all nodes on the invalid route seem infinitely distant, preventing any of the routers from sending packets over the invalid route.

14. Intra Domain Routing : here they follow only one type of routing algorithm, and this AS is owned by some organisation and rules of that organisation will be followed.

15. Need for Hierarchical Routing and solution :

PROBLEM	**SOLUTION**
Scale : Route loops + Broadcast not leaving any b/w left for sending data only	Intra AS router needs to know only about routers within its AS
Administrative consideration	Within an AS you can run whatever intra AS you need, between two AS you need to fix upon the inter As protocol you want to run.

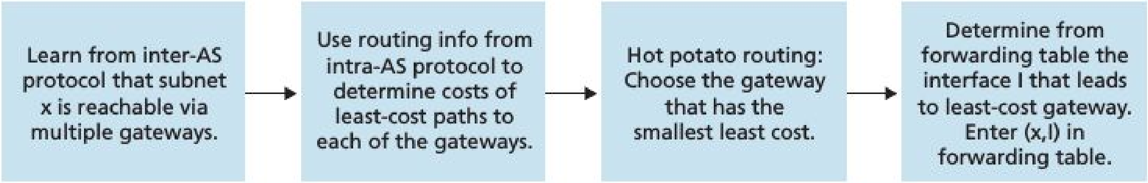
16. Cases in Hierarchical Routing :
    a. 1 gateway router per AS
        i. Info within As follow intra , else send to gateway which has one outlet to external
    b. More than 1 gateway router per AS

        i. Which AS has the subnet we need ? The gateway to that subnet becomes the destination and everyone in the subnet learns that they should divert to this gateway . They add (x, interface to gateway) to their forwarding table

    c. More than two AS have connections to the subnet

        i. In this case they can reach in more than 1 way, so whichever is easiest to reach or HPR.

17. Steps in adding outside AS address to forwarding table

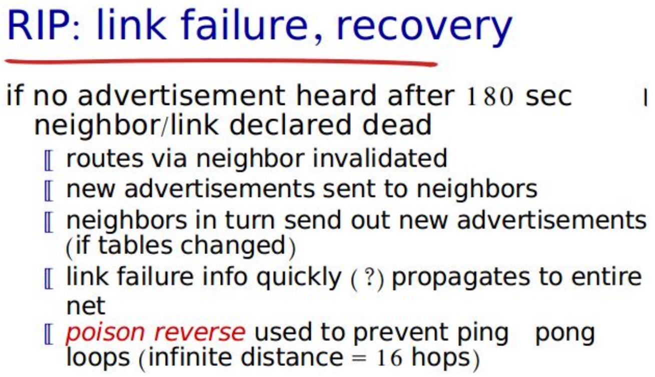

Learn from inter-AS protocol that subnet x is reachable via multiple gateways.
Use routing info from intra-AS protocol to determine costs of least-cost paths to each of the gateways.
Hot potato routing: Choose the gateway that has the smallest least cost.
Determine from forwarding table the interface I that leads to least-cost gateway. Enter (x,I) in forwarding table.

18. Hot potato Routing (HPR) : route the information from router to the gateway using the least cost path between router and gateway. “Get Rid of the hot potato fast”
19. An AS can learn about transitive connections via other AS’s also. (BGP). Every AS has the flexibility to decide which As its gonna advertise to other AS’s.
20. RIP VS OSPF

	RIP	**OSPF**
Type of Protocol	DV	LS(Djikstra)
Metric	Hop count	Set by network admin : hopcount/links weighted so that traffic does not use less /w link
Advertisement	Every 30 s	Every 30 minutes as well as on change
Checks for Link damage/operation	If within 180s advertisement not achieved then the router is dead or link broke , update and merge routing tables !	HELLO message to neighbour router.
Loop Prevention mechanism	RIP can send packets upto 15th hop, 16th router in path is therefore infinity.In the case of RIP, the maximum hop count is 15, so to perform route poisoning on a route its hop count is changed to 16,	Flooding/broadcast will help, as topographical map of network maintained by router with router as source and source tree generated to all other hosts in AS

	deeming it unreachable, and a routing update is sent.	
Implementation	RIP is implemented as an APPLICATION LAYER PROTOCOL over UDP(transport) over IP(network) through port 520 to implement routing algo which is network layer function.	OSPF implemented through IP, and takes care of its own Reliability functionality as well as link state broadcast.

21. Routing table : dest subnet, next hop router, no of hops to destination

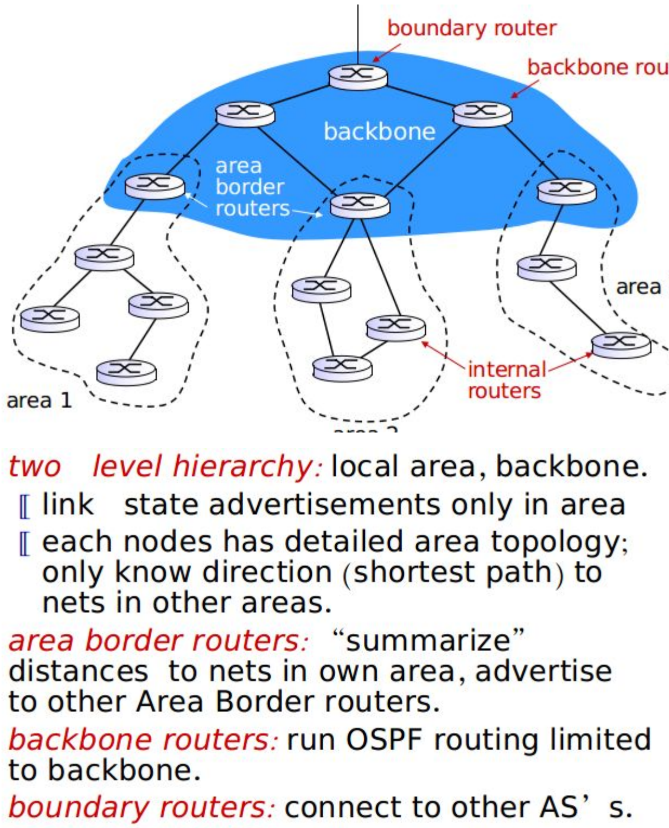


RIP: link failure, recovery

if no advertisement heard after 180 sec
neighbor/link declared dead

- routes via neighbor invalidated
- new advertisements sent to neighbors
- neighbors in turn send out new advertisements (if tables changed)
- link failure info quickly (?) propagates to entire net
- *poison reverse* used to prevent ping pong loops (infinite distance = 16 hops)

22. OSPF Better Features :
    a. Security
        i. Simple (plain text password shared) : meh
        ii. MD5 (every router shares a secret key, sender router will get hash of content+key and send with OSPF packet, dest router will do hash and compare, we can even send seqno with MD5 to protect against replay attack)
    b. Multiple same cost path
    c. Support for Uni and multicast
    d. Hierarchy support within AS
        i. Backbone area
        ii. Area Border Routers



two level hierarchy: local area, backbone.

- link state advertisements only in area
- each nodes has detailed area topology; only know direction (shortest path) to nets in other areas.

area border routers: "summarize" distances to nets in own area, advertise to other Area Border routers.

backbone routers: run OSPF routing limited to backbone.

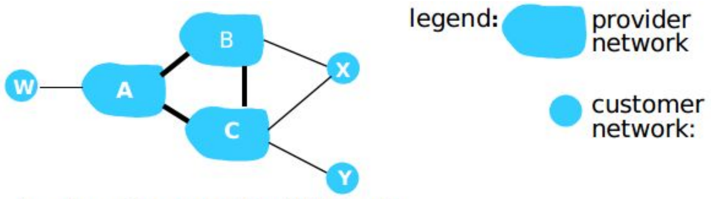
boundary routers: connect to other AS' s.

23. BGP Job
    a. Tell internet about existence of this subnet
    b. Obtain subnet reachability information from neighboring ASs.(eBGP)
    c. Propagate the reachability information to all routers internal to the AS.(iBGP)
    d. Determine "good" routes to subnets based on the reachability information and on AS policy.
24. BGP Basics

https://www.youtube.com/watch?v=hP5D5iShwXE&index=47&list=PLkHsKoi6eZnzJl1qTzmvBwTxrSJW4D2Jj
https://www.youtube.com/watch?v=3HEFFsfQzpI&index=49&list=PLkHsKoi6eZnzJl1qTzmvBwTxrSJW4D2Jj

    a. Across two AS we have a eBGP session , where prefix reachability info is passed on through messages.
    b. If there is a new prefix , router adds it to the forwarding table
    c. Route : Advertised prefix + BGP attributes (ASpath till now + next hop within AS)
    d. Within an AS to broadcast the information we have iBGP session
25. BGP Route selection
    a. Policy
    b. Shortest AS path
    c. HPR

26. BGP Messages sent via **TCP**
    a. OPEN
    b. UPDATE
    c. NOTIFICATION
    d. KEEP ALIVE while acking OPEN
27. BGP Routing Policy



A advertises path AW to B

B advertises path BAW to X

Should B advertise path BAW to C?

- No way! B gets no "revenue" for routing CBAW since neither W nor C are B's customers
- B wants to force C to route to w via A
- B wants to route *only* to/from its customers!

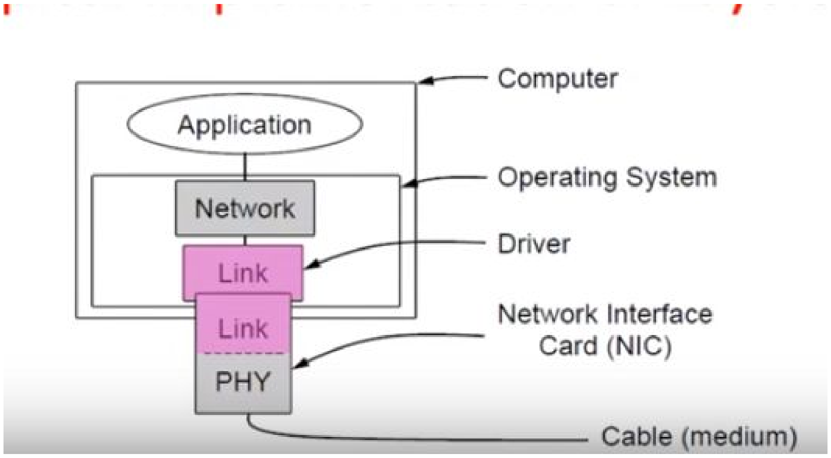
28. Why different inter AS and intra AS policies ?
    a. Policy(inter :needed , intra : single admin , not needed)
    b. Scale (table size reduced)
    c. Performance (intra : cares about performance, inter : policy)
29. Broadcast as a N Way unicast
    a. Inefficient : as N copies passes through same link, instead duplication can be done at next hop
    b. Broadcast recipients how to know ? you should have extra protocols like broadcast membership or destination registration which makes things complicated.
    c. when the goal is to setup unicast paths, how can you use broadcasting which rely on unicast paths?!
30. Other broadcasting Techniques
    a. Uncontrolled Flooding
        i. At each level make copies and pass on to neighbor
        ii. Problems are cycles and broadcast storm which occurs if node has more than one connection and redundant broadcast packets
    b. Controlled Flooding (avoid broadcast storm)
        i. SEQUENCE NUMBER CONTROLLED : Seqno of broadcast +source address sent in pkt, every node maintains list of source +broadcast number, if there in list , drop else flood (Gnutella protocol)
        ii. REVERSE PATH FORWARDING:When u get a packet From some source (Name it A)U choose whether u will forward the packet or not,: U will forward the packet only if u received the packet on the interface that connects with A along the shortest path ,So how do we decide?

We just look up A's IP address in the forwarding table ,Find which interface would lead us to A along the shortest path If we received the packet along that interface then broadcast, Else drop

c. Spanning Broadcast(avoid broadcast storm + redundant pkt)

31. Revise 404 and 405

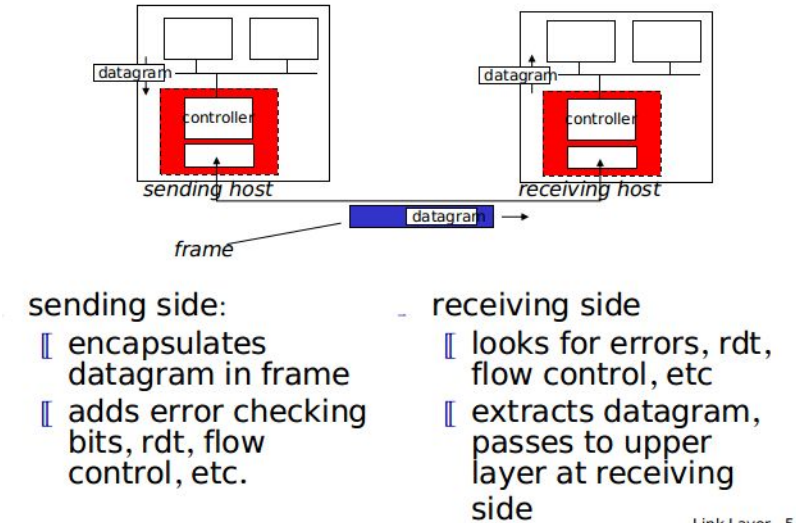
LINK LAYER



1. **Link Layer**
   a. Link : connection between two nodes
   b. Types of Link: Wireless, Wired , LAN
   c. Types of Channel in Link Layer:
      i. Broadcast >> MAP (decides the coordination of frames)
      ii. Point to Point >>PPP
   d. Responsibility : transfer data from 1 node to another node over link using some sort of link protocol, which may vary between nodes.
   e. Service provided:
      i. Framing : convert dgram to frame
         1. Physical layer often helps in finding the frame boundaries in cases where Physical and Link implemented together
         2.
      ii. Link access : MAP for shared or PPP for single
      iii. Reliable delivery : To correct errors locally
      iv. Flow control : To manage congestion
      v. Error check and correct : (because of emag noise, hardware problems, signal attenuation), not only will it say error occurred, will pinpoint where in frame occured
      vi. Half duplex and Full duplex (half : both sides can send not at same time)
2. Why both link-level and end-end reliability?

a. In wireless u can have probs in transmission so u correct locally but wired medium u can have only tcp as correcting all these link layer is overhead.

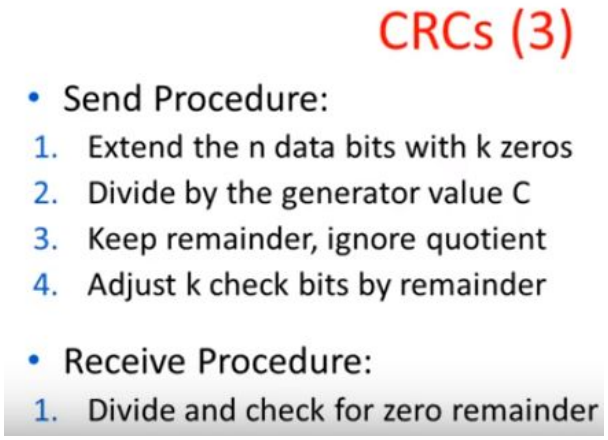
3. Where is Link Layer implemented ?
   a. NIC (Ethernet card attaches into system bus)



sending side:
- encapsulates datagram in frame
- adds error checking bits, rdt, flow control, etc.

receiving side
- looks for errors, rdt, flow control, etc
- extracts datagram, passes to upper layer at receiving side

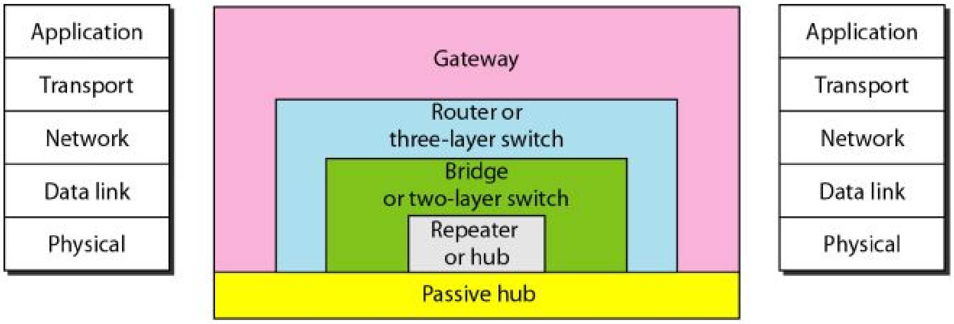
4. Error Detection and Correction Techniques
   a. Parity Check (1 error)
      i. Databits | parity
      ii. parity=sum of databits modulo 2
   b. Checksum (burst errors)
      i. 16bit words arrange
      ii. Sum them with 0
      iii. Negate
      iv. Resultant append and send
      v. At receivers end again do (i-iii)
      vi. After negation should yield 0
   c. CRC



CRCs (3)

- Send Procedure:
  1. Extend the n data bits with k zeros
  2. Divide by the generator value C
  3. Keep remainder, ignore quotient
  4. Adjust k check bits by remainder
- Receive Procedure:
  1. Divide and check for zero remainder

5. Channel Partitioning Protocol : CsMA/CD



6. Link layer addressing
7. ARP
8. Link layer switches
9. Spanning Tree Algorithm
10. VLAN
11. Retrospective
12. Danger of loops in Switched LANS ?
    a. if we have loops in switched lans, the mac table will keep on changing continuously..
13. Purpose of ARP ?
    a. IP-to-MAC
14. Advantage of Linked Layer Switch vs Hub- Switch
    a. helps in collisionless transport..and switch also helps in connecting links of different capacity through buffering..