Sub :

Day

Time : Date : / /

- Directory services are network services that identify every resource such as email address, peripheral devices and computers on the network, and make these resources accessible to users and applications.

2018-7(d):

Elaborate the following terms : DHCP, ARP, DNS, SMTP
(P-570)-1

Ans: DHCP : ~~The~~

The Dynamic Host Configuration Protocol (DHCP) is a client/server protocol designed to provide the four pieces of information for a diskless computer or a computer that is booted for the first time.

ARP:

The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.

Sub : Day Time : Date : / /

2018-7(a): 2

What is directory server? Explain its job.

Ans: Directory Server:

Directory services or name services are software systems that store, organize and provide access to directory information in order to unify network resources. A directory server or name server is a server which provides such a service.

Its Job:

- Directory services map the network names of network resources to network addresses and define a naming structure for networks.

- The directory service provides transparency to protocols and network topology, permitting users to access resources without having to be aware of the physical location of the devices.

- It's an important component of the network operating system and is a central information repository for a service delivery platform.

This type of data compression is used for organic data like audio signals and images.

2018-7(b):

Explain how the run length encoding compression technique works ? 2.75

Ans: Run-Length Encoding (RLE):

Run-Length Encoding (RLE) is a very simple form of data compression in which a stream of data is given as the input (i.e., "AAABBCCCC") and the output is a sequence of counts of consecutive data values in a row (i.e., "3A2B4C").

This type of data compression is lossless, meaning that when decompressed, all of the original data will be recovered when decoded. Simplicity in both the encoding (compression) and decoding (decompression) is one of the most attractive features of this algorithm.

Sub :

Day

Time : Date : / /

2018-7(a):

Can you explain the lossless and lossy compression mechanism?

Ans: Lossless Compression:

Lossless compression is a group of data compression algorithms that permits the original data to be accurately rebuild from the compressed data. The quality of the data is not compromised. This technique allows a file to restore its original form. It is normally used in text or program, images and sound.

Lossy Compression:

The lossy compression method eliminates some amount of data that is not noticeable. This technique does not allow a file to restore in its original form but significantly reduces the size.

The lossy compression technique is beneficial if the quality of the data is not our priority. It slightly degrades the quality of the file or data but is convenient when one wants to send or store the data.

Sub :

Day

Time :

Date : / /

Connectionless Communication:

Connectionless communication, often referred to as CL-mode communication, is a data transmission method used in packet switching networks in which each data unit is individually addressed and routed based on information carried in each unit, rather than in the setup information of a prearranged, fixed data channel as in connection-oriented communication.

See page- 386 (2)

2018-6(b):

What is meant by connection oriented and connectionless communication?

1.75

Ans: Connection Oriented Communication:

Connection-oriented communication is a network communication mode in telecommunications and computer networking, where a communication session or a semi-permanent connection is established before any useful data can be transferred, and where a stream of data is delivered in the same order as it was sent.

There is a sequence of operation to be followed by the users of connection oriented service. These are:

1. Connection is established.
2. Information is sent.
3. Connection is released.

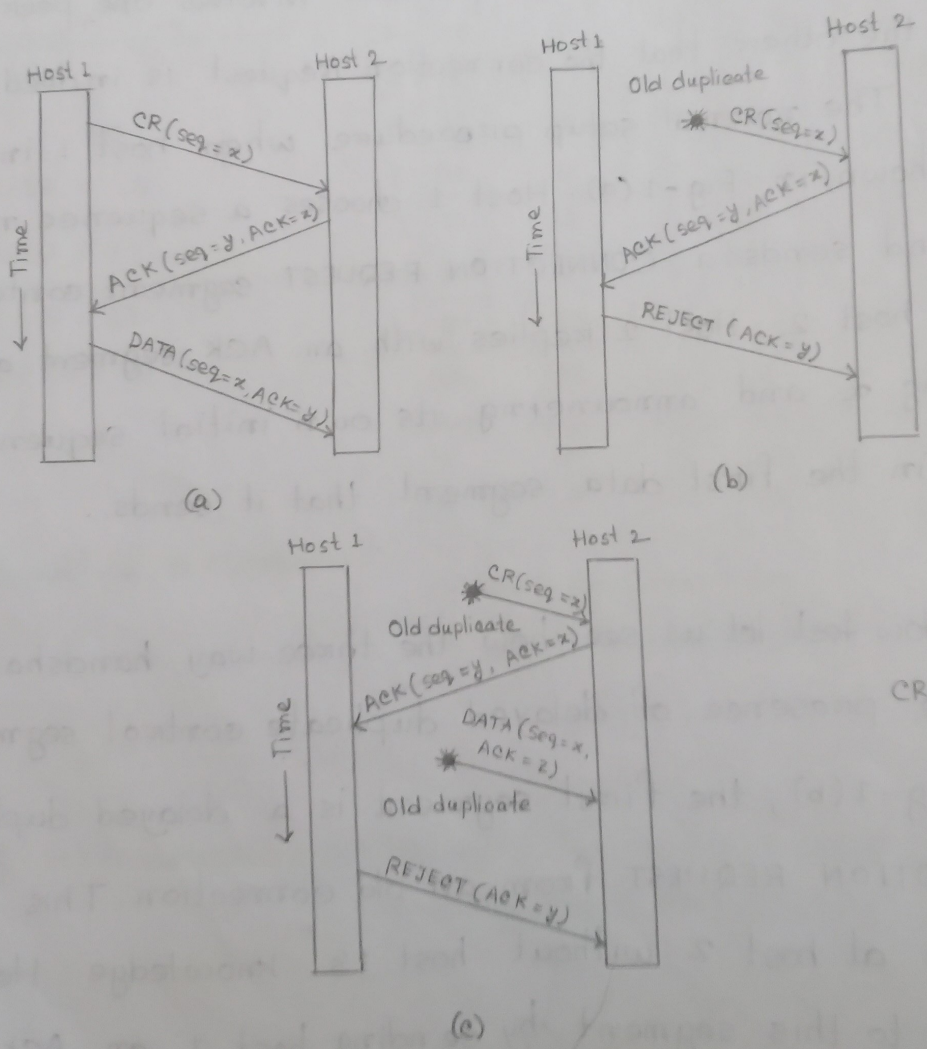
Sub :

Day

Time : Date : / /

The worst case is when both ~~del~~ a delayed CONNECTION REQUEST and an ACK are floating around in the subnet. This case is shown in Fig - 6.1 (c).

trying to set up a new connection. When host 1 rejects host 2's attempt to establish a connection, host 2 realizes that it was ~~trit~~ tricked by a delayed duplicate and abandon's the connection. In this way, a delayed duplicate does no damage.



CR = CONNECTION REQUEST

Fig-1: Three protocol scenarios for establishing a connection using a three-way handshake. (a) Normal operation, (b) Old duplicate CONNECTION REQUEST appearing out of nowhere. (c) Duplicate CONNECTION REQUEST and duplicate ACK.

Sub :

Day

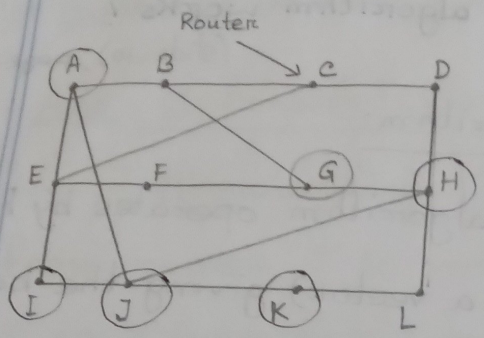
Time : Date : / /

2018-6(a):

Can you explain the three-way handshake mechanism for establishing a connection in TCP? (P-560)-1, Slide-11, (P-516)-1 (P-442)-2

Ans: The three-way handshake was introduced by Tomlinson (1975). This establishment protocol involves one peer checking with the other that the connection request is indeed ~~ee~~ current. The normal setup procedure when host 1 initiates is shown in Fig-1(a). Host 1 chooses a sequence number, x, and sends a CONNECTION REQUEST segment containing it to host 2. Host 2 replies with an ACK segment acknowledging x and announcing its own initial sequence number in the first data segment that it sends.

Now ~~test~~ let us see how the three-way handshake works in the presence of delayed duplicate control segments. In Fig-1(b), the first segment is a delayed duplicate CONNECTION REQUEST from an old connection. This segment arrives at host 2 without host 1's knowledge. Host 2 reacts to this segment by sending host 1 an ACK segment, in effect asking for verification that host 1 was indeed



(a)

8+18 = 26

10+31 = 41

12+6 = 18

6+31 = 37

G: Send via A - 18 ms

To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	-
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is	JI delay is	JH delay is	JK delay is		New routing table for J
	8	10	12	6		

Vectors received from J's four neighbors

(b)

Fig: (a) A network, (b) Input from A, I, H, K and the new routing table for J.

Sub :

Day

Time : Date : / /

until every station has had a chance and the bit-map has come around again.

- Protocols like this in which the desire to transmit is broadcast before the actual transmission are called reservation protocols because they reserve channel ownership in advance and prevent collisions.

See Page- 271 (1), Slide-6 → Token passing.

- No other station is allowed to transmit during this slot.

- Regardless of what station 0 does, station 1 gets the opportunity to transmit a 1 bit during slot 1, but only if it has a frame queued.

- In general, station j may announce that it has a frame to send by inserting a 1 bit into slot j.

- After all N slots have be passed by, each station has complete knowledge of which stations wish to transmit.

- At that point, they begin transmitting frames in numerical order (see Fig.).

- Since everyone agrees on who goes next, there will never be any collisions.)

- After the last ready station has transmitted its frame, an event all stations can easily monitor, another N-bit contention period is begun.

- If a station becomes ready just after its bit slot has passed by, it is out of luck and must remain silent

Sub :

Day

Time : Date : / /

2018 - 3(c):

Explain the basic bitmap protocol as a collision free protocol with necessary figures. 4.75

Ans: Bitmap Protocol :

Bit-map protocol is a collision free protocol that operates in the Medium Access Control (MAC) layer of the OSI model. It resolves any possibility of collisions while multiple stations are contending for acquiring a shared channel for transmission.

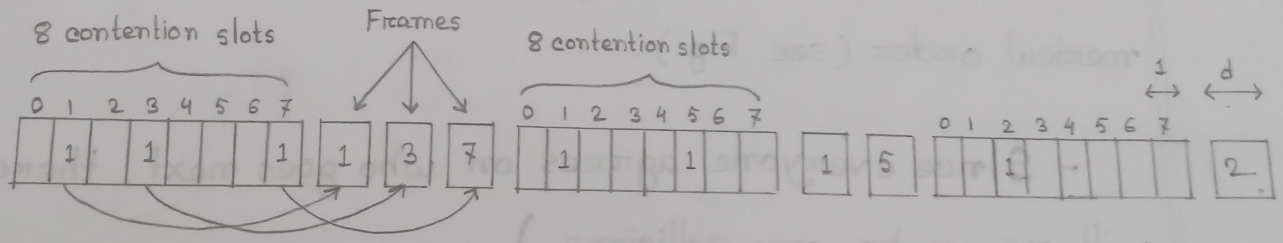


Fig : The basic bit-map protocol.

- In the basic bit-map method, each contention period consists of exactly N slots.

- If station 0 has a frame to send, it transmits a 1 bit during the slot 0.

Sub :

Day

Time : Date : / /

5. Carrier Sense or No Carrier Sense:

- With the carrier sense assumption, stations can tell if the channel is in use before trying to use it.

- No station will attempt to use the channel while it is sensed as busy.

- If there is no carrier sense, stations can not sense the channel before trying to use it.

- They just go ahead and transmit.

- Only later can they determine whether the transmission was successful.

Sub :

Day

Time : Date : / /

2018-3(b):

What are the assumptions of dynamic channel allocation? (P-260)-1

Ans: There are 5 key assumptions of dynamic channel allocation:

1. Independent Traffic:

- The model consists of N independent stations (e.g., computers, telephones), each with a program or user that generates frames for transmission.)

- The expected number of frames generated in an interval of length Δt is $\lambda \Delta t$, where λ is a constant (the arrival rate of new frames).

- Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.

2. Single Channel:

- A single channel is available for all communication.

- All stations can transmit on it and all can receive from it.

See Page-123 (1)

2018 - 2(c):

Can you explain the mechanism of ~~a~~ data transfer of Relaying in space and Relaying on ground for satellite communication ? 1

Ans: Like in a relay race, where runners pass the baton to the next runner to run the next leg of the race, the Tracking and Data Relay Satellite (TDRS) works similarly with satellite's information to transfer data between the ground and space.

Satellites in orbit cannot pass along their information to the ground stations on Earth if the satellite does not have a clear view of the ground station. Therefore, TDRS serves as a way to pass along the satellite's information.

10 TDRS sit about 35,400 Km above the earth and are able to forward information from a satellite until it reaches the appropriate ground station in view, to that TDRS at either White Sands, New Mexico or Guam Island. TDRS can also send information from the

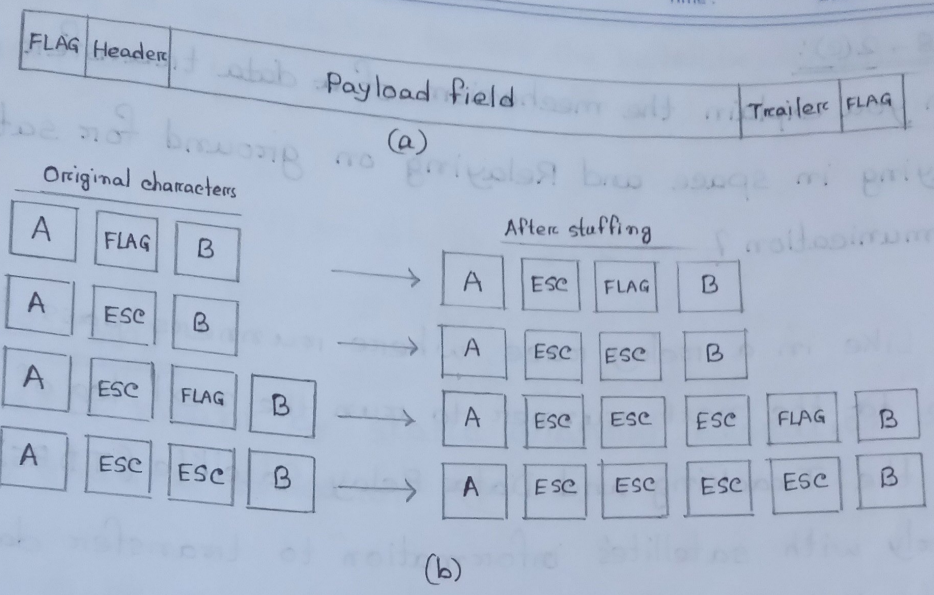


Fig-1: (a) A frame delimited by flag bytes.

(b) Four examples of byte sequences before and after byte stuffing.

2018- 2(b):

Explain how Hamming Code can be used as error correction mechanism.

Ans: Solved → 2017-3(a)

Flag bytes with byte stuffing mechanism : Slide-7

- In this method, start and end of frame are recognized with the help of flag bytes. Each frames starts with and ends with a flag byte. Two consecutive flag bytes indicate the end of one frame and start of the next one. The flag bytes used in the Fig-1 ~~is~~ is named as "ESC" flag byte.

- A frame delimited by flag bytes. This framing method is only applicable in 8-bit character codes which are a major disadvantage of this method as not all character codes use 8-bit characters e.g., Unicode.

- Four example of byte sequences before and after stuffing :

Sub :

Day

Time : Date : / /

2018-2(a):

What is framing? Explain the Flag bytes with byte stuffing mechanism for framing. (P-197)-1 3

Ans: Framing:

Frames are the units of digital transmission particularly in computer networks and communications.

Framing is a point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information. Framing is a function of the data link layer.

It provides a way for a sender to transmit a set of bits that are meaningful to the receiver.

5. The Internet :

In general, a collection of interconnected networks is called internetwork or internet. It covers larger area (almost the planet) than WAN.

2018-1(d):

Write the name of the layers suggested by OSI reference model in appropriate order.

Ans: Name of the layers suggested by OSI refercence model in appropriate order:

L7	1. Application Layer	Software Layers
L6	2. Presentation Layer	
L5	3. Session Layer	
L4	4. Transport Layer	→ Heart of OSI
L3	5. Network Layer	Hardware Layers
L2	6. Data Link Layer	
Layer1	7. Physical Layer	

Sender ↓ ↑ Receiver

2. Local Area Network:

A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory. LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information. Traditional LANs run at speeds of 10 Mbps to 100 Mbps, have low delay, and make very few errors. Newer LANs operate at up to 10 Gbps.

3. Metropolitan Area Network:

It covers a larger geographical area than LAN, ranging from several blocks of buildings to entire ~~city~~ cities. MANs can also depend on communications channels of moderate-to-high data rates. MAN can span up to 50 Km, devices used are modem and wire/cable.

4. Wide Area Network:

It covers a large geographical area, often a country or continent. (any network whose communications links cross metropolitan, regional, or national boundaries).

Interprocessor distance	Processors located in same	Example
1m	Square meter	Personal Area Network
10 m	Room	Local Area Network
100 m	Building	
1 Km	Campus	
10 Km	City	Metropolitan Area Network
100 Km	Country	Wide Area Network
1000 Km	Continent	
10,000 Km	Planet	The Internet

Fig: Classification of interconnected processors by scale.

1. Personal Area Network (PAN):

The interconnection of devices within the range of an individual person, typically within a range of maximum 10 meters. For example, a wireless network connecting a computer with its keyboard, mouse or printer is a PAN.

Sub :

Day

Time : Date : / /

- Distributed system appear as a single system to user.
- A distributed system is a software system built on top of a network.

2018 - 1(c) :

Can we classify computer network by its' scale? How? (P-18)

Ans: Classification of computer network by its scale:

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Metropolitan Area Network (MAN)
4. Wide Area Network (WAN)
5. The Internet

Sub :

Day

Time : Date : / /

2018 - 1(b) :

Is computer Network different from Distributed System ? Explain how. 3

Ans: Yes, computer Network is different from Distributed System.

Computer Networks:

- A computer Network is an interconnected collection of autonomous computers able to exchange information.

- A computer Network usually requires users to explicitly login onto one machine, explicitly submit jobs remotely, explicitly move files/data around the network.

Distributed System:

- The existence of multiple autonomous computers in a computer network is transparent to the user.

- The operating system automatically allocates jobs to processors, moves files among various computers without explicit user intervention.

Sub :

Day 36

Time : Date : / /

```
1001 ) 1101100 ( 1100
       1001
       ----
        1001
        1001
        ----
        0000
        0000
        ----
        0000
        0000
        ----
        000
```

Sub :

Day

Time :

Date : / /

2017-3(b):

Find out the CRC encoded codeword for the dataword 1101. You can choose any Generator polynomial G(x) as you like for CRC encoding.

Ans: For divisor, suppose,

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

$G(x) = x^3 + 1 = 1001$

For encoded data,

$$
\begin{array}{r|l}
1001 & 1101000 \;\big)\; 1100 \\
 & 1001 \\
\hline
 & 1000 \\
 & 1001 \\
\hline
 & 0010 \\
 & 0000 \\
\hline
 & 0100 \\
 & 0000 \\
\hline
 & 100
\end{array}
$$

$\therefore$ Encoded ~~data~~ codeword will be = 1101100

Sub :

Day 34

Time : Date : / /

2017 – 2(e) :

What is Ethernet's exponential backoff ? In what situations contention based MAC protocols are suitable? 2

Ans: Ethernet's Exponential Backoff :

Whenever there is a collision, the exponential back-off algorithm is used to determine when each station will retry its transmission. Backoff here is called exponential because the range from which the backoff value is chosen is doubled after every successive collision involving the same packet.

Exponential backoff is an algorithm that uses feed-back to multiplicatively decrease the rate of some process, in order to gradually find an acceptable rate.

Contention based MAC protocols are suitable for bursty nature of traffic under light to moderate load. These techniques are always decentralized, simple and easy to implement.

Sub :

Day

Time : Date : / /

2017-2(a) : (P-55)-1

Standard Ethernet.

Characteristics	10Base5	10Base2	10Base-T	10Base-F
Medium	Thick coax	Thin coax	2 UTP	2 Fiber
Maximum length	500m	185m	100m	2000 m

In the nomenclature 10Base-X, the number defines the data rate (10 Mbps), the term Base means baseband (digital) signal, and X approximately defines either the maximum size of the cable in 100 meters (for example 5 for 500 or 2 for 185 meter) or the type of the cable. T for unshielded twisted pair cable (UTP) and F for fiber-optic.

Sub : Day Time : Date : / /

2017 - 2(d):

Suppose a 100 Mbps CSMA/CD protocol in which the maximum one-way propagation delay between any two hosts is 100×10^{-6} sec. What will be the minimum size of a transmitted frame if the transmitting node to detect a collision before completing the transmission of the frame. (P-54)-2

Ans: We Know,

the frame transmission time, $T_{fr} = 2 \times T_p$.

Here, $T_p = 100 \times 10^{-6}$ sec

$\therefore T_{fr} = 2 \times 100 \times 10^{-6} = 200 \times 10^{-6}$ sec

∴The minimum size of a transmitted frame

$= T_{fr} \times 100 \times 10^6$

$= 200 \times 10^{-6} \times 100 \times 10^6$

$= 20000$ bits

$= 2500$ bytes

Sub :

Day

Time : Date : / /

2017-2(e):

What are the different types of cabling supported by Ethernet standard ? (P-292, 295, 297) -1

Ans: Different types of cabling supported by Ethernet standard :

1. The original fast Ethernet cabling :

Name	Cable	Max. segment
100 Base-T4	Twisted pair	100 m
100 Base-TX	Twisted pair	100 m
100 Base-FX	Fiber optics	2000 m

2. Gigabit Ethernet Cabling :

Name	Cable	Max. segment
1000 Base-SX	Fiber optics	550 m
1000 Base-LX	Fiber optics	5000 m
1000 Base-CX	2 pairs of STP	25 m
1000 Base-T	4 Pairs of UTP	100 m

3. 10- Gigabit Ethernet cabling

Name	Cable	Max. segment
10G Base - SR	Fiber optics	Up to 300 m
10 GBase - LR	Fiber optics	10 Km
10GBase - ER	Fiber optics	40 Km
10 GBase - CX4	4 Pairs of twinax	15 m
10 GBase - T	4 Pairs of UTP	100 m

Day

Sub :

Time : Date : / /

2017-2(b):

How throughput is improved in slotted ALOHA over pure ALOHA ? (Page-264) [1]

1

Ans: The formula to calculate the throughput of the pure ALOHA is $S = G \times e^{-2G}$. The throughput is maximum when $G = 1/2$ which is 18 % of the total transmitted data frames.

The formula to calculate the throughput of the Slotted ALOHA is $S = G \times e^{-G}$. The throughput is maximum when $G = 1$ which is 37% of the total transmitted data frames. In Slotted ALOHA, 37 % of the time slot is empty, 37 % successes and 26% collision.

In pure ALOHA, vulnerable period is 2λ.

So, $S/G = e^{-2G}$ or throughput $S = Ge^{-2G}$, where G is the total number of packets.

Maximum value of $G = 0.5$ or maximum throughput $S_{max} = 1/2e$.

In slotted ALOHA, vulnerable period is λ and $S/G = e^{-G}$ or throughput $S = Ge^{-G}$.

Here, maximum value of G is 1 and maximum throughput $S_{max} = 1/e$.

Sub :

Day

Time : Date : / /

CSMA/CD, (as well as many other LAN protocols), uses the conceptual model of Fig-1.

- At the point marked t_0, a station has finished transmitting its frame. Any other station having a frame to send may now attempt to do so.

- If two or more stations decide to transmit simultaneously, there will be a collision.

- If a station detects a collision, it aborts its transmission, waits a random period of time, and then tries again (assuming that no other station has started transmitting in the meantime).

- Therefore, our model for CSMA/CD will consists of alternating contention and transmission periods, with idle periods ~~occuring~~ occurring when all stations are quiet (e.g., for lack of work).

Sub : Day 28

Time : Date : / /

2017 - 2(a):

What is vulnerable period ? Explain how Ethernet's carrier sense multiple access with collision detection (CSMA/CD) works. (Page - 268) [1] 2.75

Ans: Vulnerable Period:

The total period of time when collision may occur for a packet is called vulnerable ~~point~~ period.

CSMA/CD working procedure:

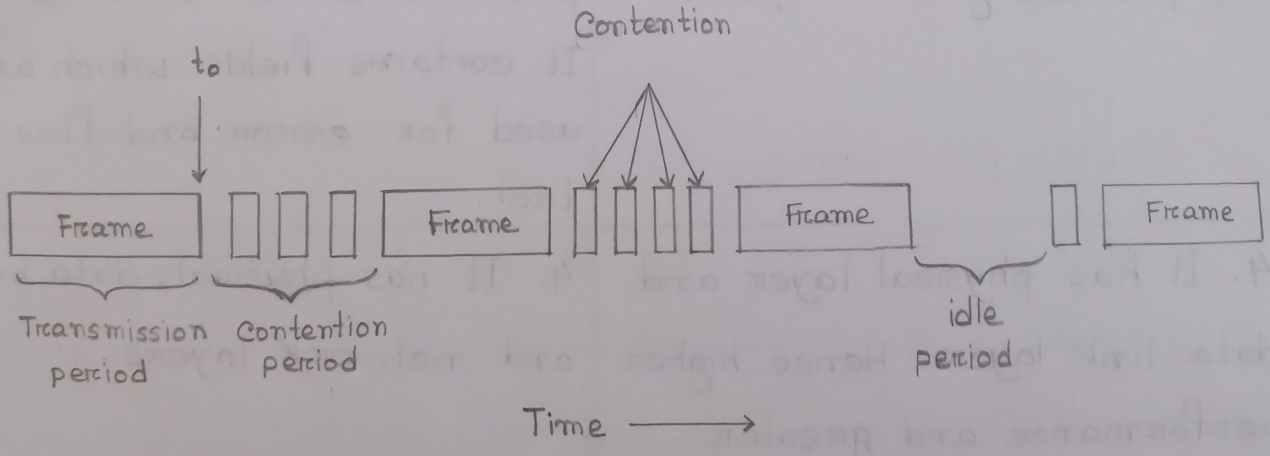


Fig-1: CSMA/CD can be in contention, transmission, or idle state.

Sub :

Day

Time : Date : / /

2017 - 1(d) :

Distinguish between Frame Relay and X.25 protocol. 2

Ans: Differences between Frame Relay and X.25 protocol:

Frame Relay	X.25
1. offers higher performance and greater transmission efficiency.	1. Lower than frame relay.
2. Frame relay is a Layer 2 protocol suite.	2. X.25 provides services at Layer 3.
3. No error detection hence it provides greater speeds.	3. Error detection hence it provides error free delivery. It contains fields which are used for error and flow control.
4. It has physical layer and data link layer. Hence higher performance and greater transmission rate is achieved.	4. It has physical, data link and network layers.
5. It can dynamically allocate bandwidth.	5. Fixed bandwidth is available in X.25 network.

Sub :

Day

Time :

Date : / /

3. Packet Layer :

This layer defines the format of data packets and the procedures for control and transmission of the data packets. It provides external virtual circuit service. Virtual circuits may be of two types : virtual call and permanent virtual circuit.

Sub :

Day

Time : Date : / /

2017-1(e):

What is X.25 protocol ? Explain the functionality of X.25 . 3

Ans: X.25 Protocol:

X.25 defines how a node terminal could be interfaced to the network for communication in Packet Mode.

Key terms here used here are : DTE (Data Terminal Equipment) and DCE (Data Circuit-terminating Equipment).

It defines how DTE's communicates with network and how packets are sent over that network using DCEs. It is also known as Subscriber Network Interface (SNI) Protocol.

- Presently it is used for networks for ATMs and credit card verification.

- It allows multiple logical channels to use the same physical line.

Sub :

Day

Time : Date : / /

2017-1(a) → Page-42 (1)

2017-1(b) :

What are the reasons for using layered protocols ? 2

Ans: The layered protocol is defined as the protocol that has been separated into layered pattern to make the tasks as simple. The reasons for using layered protocols are:

1. This architecture offers an abstract framework to exchange the information among hosts by a simple way.

2. It divides the complex tasks into simple tasks.

3. Each layers in the protocols is interacted with each other to transfer the information.

Sub :

Day 22

Time : Date : / /

128 168 254 0

10000000 . 10101000 . 11111110 . 00000000 (Network IP, Suppose)

(AND) 11111111 . 11111111 . 11111110 . 00000000 (Default mask)

10000000 . 10101000 . 1111111 0 . 0000 0000 (subnet 1)

0 . 1000 0000 (subnet 2)

1 . 0000 0000 (subnet 3)

1 . 1000 0000 (subnet 4)

Subnet No.	Range	Bit	Network IP	Broadcast IP	First Host IP	Last Host IP
1	128.168.254.0 - 128.168.254.127	25	128.168.254.0	128.168.254.127	128.168.254.1	128.168.254.126
2	128.168.254.128 - 128.168.254.255	25	128.168.254.128	128.168.254.255	128.168.254.129	128.168.254.254
3	128.168.255.0 - 128.168.255.127	25	128.168.255.0	128.168.255.127	128.168.255.1	128.168.255.126
4	128.168.255.128 - 128.168.255.255	25	128.168.255.128	128.168.255.255	128.168.255.129	128.168.255.254

Sub :

Day

Time : Date : / /

2018 - 4(b):

For the above scenario ~~to~~ described in question 4(a), if we want to increase PCs up to 100 per subnet and decrease sub network into 4, then what type of IP addressing scheme might work best. Explain your argument.

Ans: According to the question,

We ~~need~~ need 4 sub network each containing upto 100 PCs. Total no. of PCs = (100×4) = 400. This number 400 is not a power of 2. The next number that is a power of 2 is 512 (2^9). ~~(So, we need 9 zero's (0s) in the subnet mask).~~ So ~~weed~~ we need (32 - 9) = 23 number of 1s in the default mask.

255 255 254 0
1111 1111. 1111 1111. 1111 1110, 0000 0000 (default mask)

So, the network will belong to class B.

The 1st byte of network ~~#~~ will be any number ~~re~~ range between 128 - 191. The 2nd byte needs no change. The 3rd byte will be the number ranging 254 - 255. Since we need 4 subnetwork (2^2), So, the total no. of 0s will be {32 - (23 + 2)} = 7.

Sub :

Day

Time : Date : / /

2018-4(c):

Differentiate between subnetting and supernetting.

Ans: Differences between sub netting and super netting:

Sub netting	Super netting
1. A process of dividing a network into the subnetworks.	1. A process of combining small networks into a larger network.
2. The number of bits of network addresses is increased.	2. The number of bits of host addresses is increased.
3. Mask bits are moved towards right of the default mask.	3. Mask bits are moved towards left of the default mask.
4. Sub netting is implemented using VLSM (Variable Length Subnet Mask).	4. Super netting is implemented using CIDR (Classless Inter Domain Routing).
5. The objective is to reduce the address depletion.	5. The objective is to simplify and fasten the routing process.

Sub :

Day

Time :

Date : / /

2018-4(a):

We are going to establish a computer network with 6 subnets and each subnet will contain at least 30 PCs. Let network ID is 192.168.2.0. Design the IP addressing for the proposed network.

Ans: Here, 6 subnets are required for a computer network. This number 6 is not a power of 2. The next number that is a power of 2 is 8 (2^3). So, we need 3 more 1s in the subnet mask. The given network ID 192.168.2.0 ~~is~~ belongs to class C.

~~Then~~, The number of 1s in the default mask for class C is 24.

Now, the number of 1s for this particular mask will be (24 + 3) = 27 and the number of 0s will be (32 - 27) = 5.

Sub :

Day

Time : Date : / /

- Remaining 4 bits are used for the identification of hosts in the networks.

2015 - 3(c):

What are the differences between IPv4 and IPv6 ?

Ans: Differences between IPv4 and IPv6 :

IPv4	IPv6
1. IPv4 addresses are 32 bit length.	1. IPv6 addresses are 128 bit length.
2. IPv4 addresses are binary numbers represented in decimals.	2. IPv6 addresses are binary numbers represented in hexadecimal.
3. IPSec Support is only optional.	3. Inbuilt IPSec support.
4. No packet flow identification.	4. Packet flow identification is available.
5. Broadcast messages are available.	5. Broadcast messages are not available.

2017-4(b):

Define classless IP addressing with example.

Ans: Classless IP addressing :

Classless Addressing is an improved IP addressing system. It makes the allocation of IP addresses more efficient. It is also known as classless Inter-Domain Routing (CIDR). It allows the user to use VLSM or Variable Length Subnet Masks.

In CIDR, subnet masks are denoted by /x. For example, a subnet of 255.255.255.0 would be denoted by /24.

An example on CIDR IP address is :

182.0.1.2/28

It suggests -

- 28 bits are used for the identification of network.

Sub :

Day

Time : Date : / /

From the dotted decimal notation :

- Class A : IP address range from 0-127 in the 1st byte.
- Class B : IP address range from 128 - 191 in the 1st byte.
- Class C : IP address range from 192 - 223 in the 1st byte.
- Class D : IP address range from 224 - 239 in the 1st byte.
- Class E : IP address range from 240 - 255 in the 1st byte.

Day

Sub :

Time : Date : / /

Finding class of an address using dotted decimal notation :

To make the IPv4 address more compact and easier to read, an IPv4 address is usually written in decimal form with a decimal point (dot) separating the bytes. This format is referred to as dotted-decimal notation. Fig-1 shows an IPv4 address in dotted decimal notation. Each number in the dotted-decimal notation is between 0 and 255.

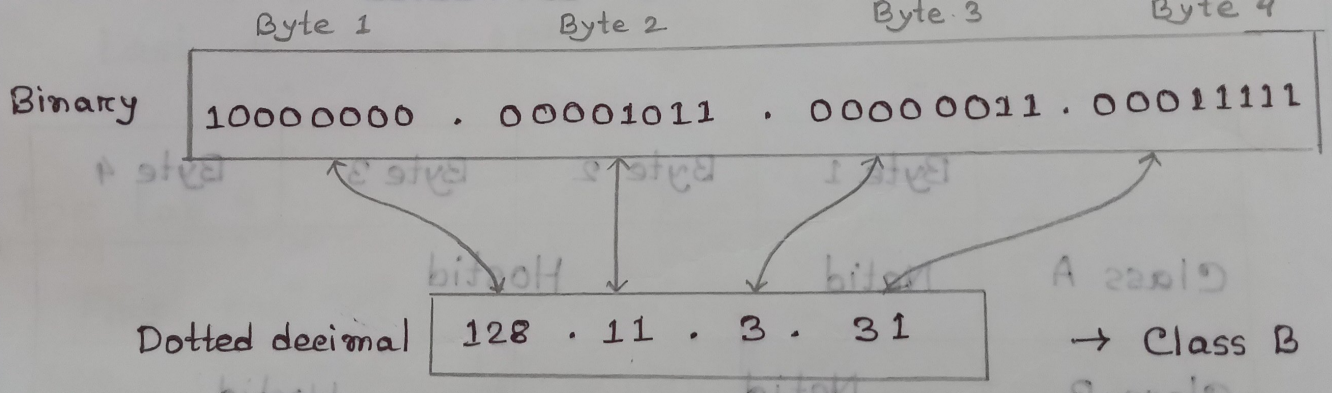


Fig-1: Dotted decimal notation.

In classful addressing, the IP address space is divided into 5 classes: A, B, C, D and E.

Sub :

Day

Time : Date : / /

2017 - 4(a):

What do you mean by ~~NetIt~~ Netid and Hostid? How can we find the class of an address when the address is given in dotted decimal notation?

Ans: Netid and Hostid:

In classful addressing, an IP address of class A, B and C is divided into Netid and Hostid. The Netid determines the network address while the Hostid determines the host connected to that network.

	Byte 1	Byte 2	Byte 3	Byte 4
Class A	Netid	Hostid		
Class B	Netid		Hostid	
Class C	Netid			Hostid
Class D	Multicast Address			
Class E	Reversed for future use			

Sub :

Day

Time :

Date : / /

For Lab 1 :

First host IP = 201.70.64.1

Last " " = 201.70.64.30

~~Fat~~ For Lab 2 :

First host IP = 201.70.64.33

Last " " = 201.70.64.62

For Lab 3 :

First host IP = 201.70.64.~~64~~65

Last " " = 201.70.64.94

For Lab 4 :

First host IP = 201.70.64.97

Last " " = 201.70.64.126

For Lab 5 :

First host IP = 201.70.64.129

Last " " = 201.70.64.158

Sub :

Day

Time : Date : / /

201 70 64 0

11001001 . 01000110 . 01000000 . 00000000

(classe ~~B~~ C default mask) 255 255 255 0

11111111 . 11111111 . 11111111 . 00000000 (AND)

~~11111111 . 01~~

11001001 . 01000110 . 01000000 . 00000000 = .0 (1)

So, NID = 201.70.64.0

01100000 = .32 (2)

01000000 = .64 (3)

01100000 = .96 (4)

10000000 = .128 (5)

~~10100000~~

Subnet No.	Range	Bit	Network IP	Broadcast IP
1 (Lab 1)	201.70.64.0 - 201.70.64.31	27	201.70.64.0	201.70.64.31
2 (Lab 2)	201.70.64.32 - 201.70.64.63	27	201.70.64.32	201.70.64.63
3 (Lab 3)	201.70.64.64 - 201.70.64.95	27	201.70.64.64	201.70.64.95
4 (Lab 4)	201.70.64.96 - 201.70.64.127	27	201.70.64.96	201.70.64.127
5 (Lab 5)	201.70.64.128 - 201.70.64.159	27	201.70.64.128	201.70.64.159

Sub :

Day

Time : Date : / /

2014-3 (b) :

Assign IP address to the subnets of different labs of CSE department using a class C private IP block. Let, the CSE department has five labs, there are 11 PCs in Lab 1, 7 PCs in Lab 2, 44 PCs in Lab 3, 64 PC in lab 4 and 3 PCs in Lab 5. List the network IP, broadcast IP, first host IP and last host IP of each lab.

Ans: Let the CSE department is granted site address 201.70.64.0 (class C). The CSE department needs 5 subnets. This number 5 is not a power of 2. The next number that is a power of 2 is 8 (2^3). So, we need 3 more 1s in the subnet mask.

The number of 1s in the default mask is 24 (class C). The total number of 0s is (32-27)=5.

2^{3-4} 6

Sub :

Day

Time : Date : / /

2014 - 3(a):

Given the IP address of 193.243.12.93 and a subnet mask of 255.255.255.128, what is the network address?

Ans: Given the IP address

193.243.12.93

It belongs to class C.

Subnet mask:

255.255.255.128

Last byte of given IP addesress and subnet mask in binary form:

01011101 = 93

10000000 = 128 (AND operation)

00000000 = 0

∴ Network address = ~~193~~. 193.243.12.0

Sub :

Day

Time : Date : / /

Network address :

~~Using~~ Last byte of given IP address and subnet mask are :

$$\begin{array}{lll} 01111011 & = & 123 \\ 11110000 & = & 240 \quad \text{(AND operation)} \\ \hline 01110000 & = & 112 \end{array}$$

∴ Network address = 192.168.12.112

Broadcast address :

Last byte of network address :

$$\begin{array}{lll} 01110000 & = & 112 \\ 01111111 & = & 127 \end{array}$$

[Performing 1's complement for last 4 bits]

∴ Broadcast address = 192.168.12.~~112~~ 127

∴ First host address = 192.168.12.113

∴ Last " " = 192.168.12.126

∴ Default gateway " = 192.168.12.~~112~~ 113 (= First host address)

Sub :

Day

Time :

Date : / /

2015-3(a):

Suppose, the IP address of a host of a network is 192.168.12.123 and a subnet mask of that network is 255.255.255.240. What are the network address, default gateway IP, ~~bra~~ broadcast IP, IP of the first host and last of that network?

Ans: Given IP address is:

192.168.12.123

So, this IP address belongs to class C.

The subnet mask for the ~~add~~ address is

255.255.255.240

In binary:

1111 1111 . 1111 1111 . 1111 1111 . 1111 0000

[So, the last 4 bits are 0's]

Here, only the last byte will be affected.

Sub :

Day

Time : Date : / /

Net B belongs to class B.

Here, the last two bytes:

128.0 = 1000 0000 . 0000 0000

So, last 15 bits are 0's.

∴ Total number of hosts = $2^{15} - 2$

= 32766

Net C belongs to class A.

Here, the last three bytes:

230.0.0 = 111 00 110 . 0000 0000 . 0000 0000

So, the last 17 bits are 0's. [Prefix notation = 15]

∴ Total number of hosts = $2^{17} - 2$

= 131070

Day

Sub :

Time : Date : / /

2016 - 4(a):

A novice network engineer (NNE) is thinking to set the following subnet masks to three networks on an internet. What is the maximum number of hosts each network will be able to handle? Give proper explanation of your answer.

NetA : 255.255.255.240, NetB : 255.255.128.0

~~Ans:~~

and of NetC : 255.230.0.0

Ans: NetA belongs to class C.

Here, last byte :

$$240 = 1111.0000$$

So, last 4 bits are 0's.

$\therefore$ Total number of hosts $= 2^4 - 2$

$= 14$

Sub :

Day

Time : Date : / /

∴ Network address = 192 . 168 . 3 . 192

Broadcast address :

Last byte : 11000000

for mid

11011111 = 223

[Changing the last 5 bits as 1s or performing 1's complement]

∴ Broadcast address : 192 . 168 . 3 . 223

∴ Total no. of hosts = $2^5 - 2$

= 30

Sub : Day Time : Date : / /

2017 - 4(c):

Suppose, A host is given the 192.168.3.219/27 IP address. Indicate the network address, the broadcast address and the total number of hosts available in the network?

Ans: Given IP address is,

192.168.3.219

So, this id belongs to class C.

The subnet mask for the address is

1111 1111 . 1111 1111 . 1111 1111 . 11100000

Or, 255.255.255.224

[Since the prefix length is 27, hence we must change the ~~last~~ remaining 5 bits to 0s.]

Here, only the last byte is affected.

Network address:

219	=	11011011	
224	=	11100000	[AND operation]
		11000000	

Sub :

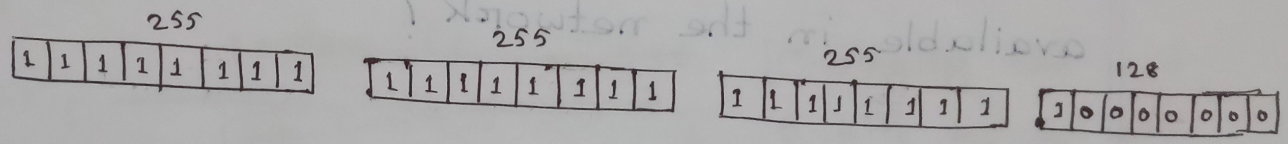
Day

Time : Date : / /

2014-3(a) :

Given the IP address of 193.243.12.93 and a subnet mask of 255.255.255.128, what is the network address?

Ans:



Number of network : $2^1 = 2$

Number of IP address on each network

$= (2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0) = 127$

Number of host on each network

$= 2^7 - 2 = 126$

On every network, first IP address is network ID and last IP address is a broadcast ID.

Network No :

1	193.243.12.0 (Network ID)
2	193.243.12.127 (Broadcast ID)

Sub :

Day

Time :

Date : / /

2017-7(e):

What is the difference between end-to-end delay and packet jitter? What are the causes of packet Jitter?

P- 196

Sub : Day Time : Date : / /

2017-5(d):

How is the 16-bit IP checksum field calculated ?

Ans: The checksum is calculated by forming the one's complement of the one's complement sum of the header's 16-bit words. The result of summing the entire IP header, including checksum, should be zero if there is no corruption.

See Page - 78(N1)

Sub :

Day

Time : Date : / /

2015-6 (c):

What are the purposes of using IHL and type of service fields in IPv4 header?

Ans: IHL (Internet Header Length):

The IHL field is used to specify the total length of the header and is represented in 32 bit words. The minimum valid value for the IHL field is 5 (5×32 = 160 bits) which accounts for the Version, IHL, TOS, Length, Identification, Flags, Fragment Offset, TTL, Protocol, Checksum, and the Source and Destination Addresses, which are all mandatory.

Sub :

Day

Time : Date : / /

DNS

DNS stands for Domain Name System. DNS is a ~~dir~~ directory service that provides a mapping between the name of a host on the network and its numerical address.

SMTP:

SMTP stands for Simple Mail Transfer Protocol. SMTP is a communication protocol for electronic mail transmission.

Sub :

Day

Time : Date : / /

Example:

Input data:

AAAAAAFDDeeeeeeeeAEEEEEEEEEEEEEEEE

Output data:

6A1F2D7e1A17E

In this example, we are able to compress the data from 34 characters down to 13.

Sub :

Day

Time : Date : / /

2018 - 5(c) :

How the distance vector routing algorithm works ? 4

(Slide-10), Page- 370(1)

Ans: Distance vector routing algorithm:

- A distance vector routing algorithm operates by having each router maintain a table (i.e, a vector) giving the best known distance to each destination and which link to use to get there.

- These tables are updated by exchanging information with the neighbors. Eventually, every router knows the best link to reach each destination.

- As an example, assume that delay is used as a metric and that the router knows the delay to each of its neighbors.

Sub :

Day

Time :

Date : / /

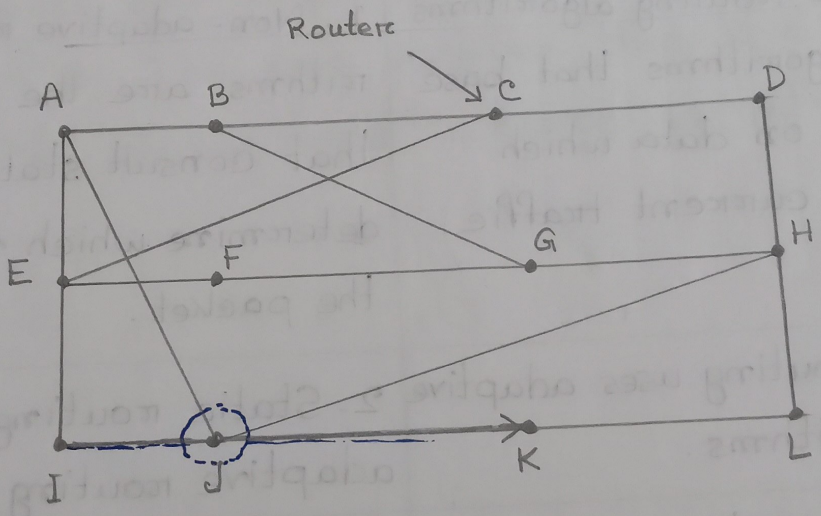
2

2018-5(b):

Explain Optimality Principle. (Slide-10) (P-364)-1

Ans: Optimality Principle:

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



Sub :

Day

Time : Date : / /

2018-5(a):

Distinguish between adaptive and non-adaptive routing algorithm. (Slide-10)

2.75

Ans: Differences between adaptive and non-adaptive routing algorithm:

Adaptive Algorithm ~~Routing~~	Non-adaptive Algorithm
1. Adaptive routing algorithms are the algorithms that base its decisions on data which reflects the current traffic conditions.	1. Non-adaptive routing algorithms are the algorithms that consult static tables to determine which node to send the packet.
2. Dynamic routing uses adaptive routing algorithms.	2. Static routing uses non-adaptive routing algorithms.
3. In these algorithms, the basis of routing decisions are the network traffic and topology.	3. In these algorithms, the basis of routing decisions are static tables.
4. Centralized, isolated and distributed are the types of adaptive routing algorithms.	4. Flooding and random walks are the types of non-adaptive routing algorithms.
5. These algorithms are more complex.	5. These algorithms are simple.

Sub :

Day

Time : Date : / /

3. Observable Collisions:

- If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled.

- This event is called a collision.

- All stations can detect that a collision has occurred.

- A collided frame must be transmitted again later. No errors other than those generated by collisions occur.

4. Continuous or Slotted Time:

- Time may be assumed continuous, in which case frame transmission can begin at any instant.

- Alternatively, time may be slotted or divided into discrete intervals (called slots).

- Frame transmissions must then begin at the start of a slot.

- A slot may contain 0, 1 or more frames, corresponding to an idle slot, a successful transmission, or a collision, respectively.

Sub :

Day

Time : Date : / /

Advantages :

1. This scheme allots channels as needed. This results in optimum utilization of network resources.

2. There are less chances of denial of services and call blocking in case of voice transmission.

3. These schemes adjust bandwidth allotment according to traffic volume, and so are particularly suitable for bursty traffic.

Disadvantage :

This scheme increases the computational as well as storage load on the system.

See page- 260 (Slide - 6)

- Assumptions for Dynamic Channel Allocation

Sub :

Day

Time : Date : / /

Dynamic Channel Allocation :

Dynamic channel allocation encompasses the channel allocation schemes where channels are allotted to users dynamically as per their requirements, from a central pool.

In dynamic channel allocation schemes, frequency channels are not permanently allotted to any user. Channels are assigned to the user as needed depending upon the network environment. The available channels are kept in a queue or a spool. The allocation of the channels is temporary. Distribution of the channels to the contending users is based upon distribution of the users in the network and offered traffic load. The allocation is done so that transmission interference is minimized.

Sub :

Day

Time : Date : / /

Disadvantages :

1. If the value of N is very large, the bandwidth available for each user will be very less.

2. This will reduce the throughput if the user needs to send a large volume of data once in a while.

3. The badwidth allocated to non-communicating users lies wasted.

4. If the number of users is more than N, then some of them will be denied service, even if there are unused frequencies.

Sub :

Day

Time : Date : / /

Working Principle:

Suppose that there are N competing users. Here, the total bandwidth is divided into N discrete channels using frequency division multiplexing (FDM). In most cases, the size of the channels is equal. Each of these channels is assigned to one user.

Advantages:

1. This scheme is particularly suitable for situations where there are a small number of fixed users having a steady flow of uniform network ~~to~~ traffic.

2. The allocation technique is simple and so the additional overhead of a complex algorithm need not be incurred.

3. There is no interferences between the users since each user is assigned a fixed channel which is not shared with others.

ground to the satellite to tell the satellite what to do (take a pe picture, turn a sensor on/off etc.)

2018 - 3(a):

What is meant by static channel allocation and dynamic channel allocation ? (P - 258) - 1 2

Ans: ~~Static Channel Alloca~~

When there are more than one users who desire to access a shared network channel, an algorithm is deployed for channel allocation among the competing users.

Static Channel Allocation:

Static channel allocation is a traditional method of channel allocation in which a fixed portion of the frequency channel is allotted to each users, who may be base stations, access points or terminal equipment. This scheme is also referred to as fixed channel allocation or fixed channel assignment.

Sub :

Day

Time : Date : / /

2018-1(a):

How the term Computer Network is defined in literature?

Ans: Computer Network:

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.

In simple words, computer network is a collection of autonomous computers interconnected by a single technology.

Sub :

Day 39

Time : Date : / /

2017-5(a):

Differentiate between routing and forwarding. Why link state protocol is not used for interdomain routing, ~~for the~~ or routing for the entire Internet ? 2.75

Ans: Differences between routing and forwarding :

1. Forwarding does not transmit data on outgoing links, but routing does.

2. Forwarding finds suitable path for a packet than routing.

3. Forwarding is a part of decision making while routing is not.

4. Forwarding is used ~~to~~ in telephony while routing is used in all networks.

Sub :

Day

Time : Date : / /

2017- 3(c) :

Briefly explain the difference between single-bit errors and burst errors ?

Ans: Difference between single-bit errors and burst errors:

Single bit error means only one bit of data unit is changed from 1 to 0 or from 0 to 1.

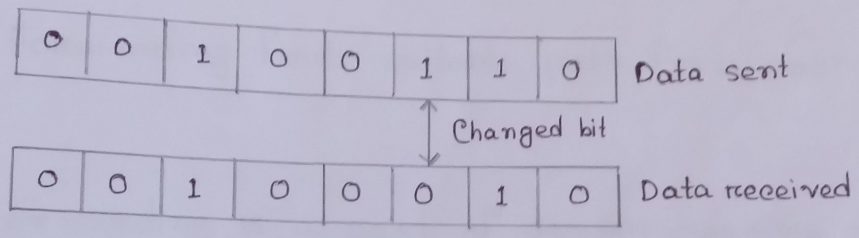


Fig-1: Single-bit error

Burst error means two or more bits in data unit are changed from 1 to 0 ~~from~~ or 0 to 1.

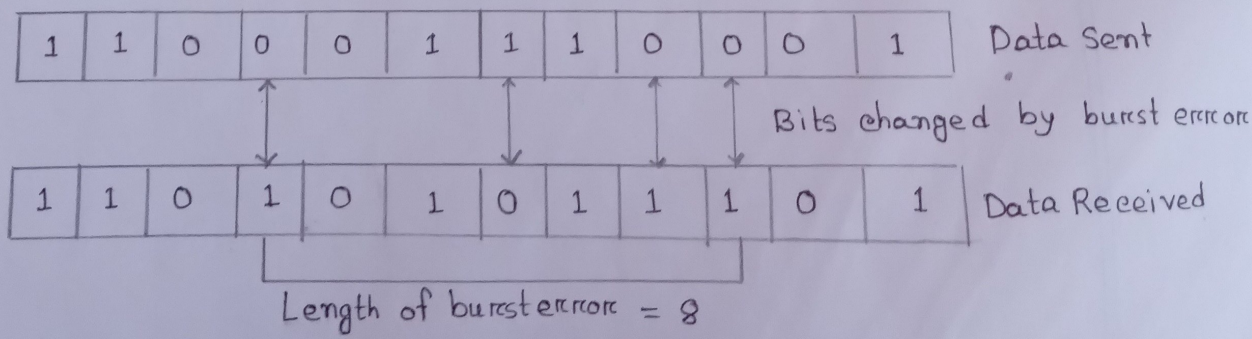


Fig-2 : Burst Error.

Sub :

Day

Time : Date : / /

- It also permits data exchange between terminals with different communication speeds.

We can understand the functionality of X.25 by discussing its three protocol layers:

1. Physical Layer:

It lays out the physical, electrical and functional characteristics that interface between the computer terminal and the link to the packet switched node. X.21 physical implementer is commonly used for the linking.

2. Data Link Layer:

It comprises the link access procedures for exchanging data over the link. Here, control information for transmission over the link is attached to the packets from the packet layer to form the LAPB frame (Link Access Procedure Balanced). This service ensures a bit-oriented, error-free, and ordered delivery of frames.

Sub :

Day

Time : Date : / /

192 168 2 0

11000000 . 10101000 . 00000010 . 00000000

(Class c default mask) 11111111 . 11111111 . 11111111 . 00000000 (AND)

11000000 . 10101000 . 00000010 . 00000000 = .0 (1)

00100000 = .32 (2)

01000000 = .64 (3)

01100000 = .96 (4)

10000000 = .128 (5)

10100000 = .160 (6)

∴ Network ID = 192.168.2.0

Subnet No.	Range	Bit	Network IP	Broadcast IP	First Host IP	Last Host IP
1	192.168.2.0 - 192.168.2.31	27	192.168.2.0	192.168.2.31	192.168.2.1	192.168.2.30
2	192.168.2.32 - 192.168.2.63	27	192.168.2.32	192.168.2.63	192.168.2.33	192.168.2.62
3	192.168.2.64 - 192.168.2.95	27	192.168.2.64	192.168.2.95	192.168.2.65	192.168.2.94
4	192.168.2.96 - 192.168.2.127	27	192.168.2.96	192.168.2.127	192.168.2.97	192.168.2.126
5	192.168.2.128 - 192.168.2.159	27	192.168.2.128	192.168.2.159	192.168.2.129	192.168.2.158
6	192.168.2.160 - 192.168.2.191	27	192.168.2.160	192.168.2.191	192.168.2.161	192.168.2.190