**course Code : MCS-042**
**Course Title : Data Communication and Computer Network**
**Assignment Number : MCA (4)/042/Assign/13**
**Maximum Marks :**
**100 Weightage : 25%**
**Last Dates for Submission : 15th October, 2013 (For July 2013 Session) 15th April, 2014 (For January 2014 Session)**
**This assignment has eight questions. Answer all questions. Rest 20 marks are for viva-voce. You may use illustration and diagrams to enhance the explanations. Please go through the guidelines regarding assignments given in the Programme Guide for the format of presentation.**

**Q. 1** (i) Construct the Hamming Code for the bit sequence **(5 marks)** 10011010

A byte of data: 10011010
Create the data word, leaving spaces for the parity bits: _ _ 1 _ 0 0 1 _ 1 0 1 0
Calculate the parity for each parity bit (a ? represents the bit position being set):
Position 1 checks bits 1,3,5,7,9,11: **? _ 1 _ 0** 0 **1 _ 1** 0 **1** 0. Even parity so set position 1 to a 0: **0 _ 1 _ 0** 0 **1 _ 1** 0 **1** 0
Position 2 checks bits 2,3,6,7,10,11: 0 **? 1** _ 0 **0 1** _ 1 **0 1** 0. Odd parity so set position 2 to a 1: 0 **1 1** _ 0 **0 1** _ 1 **0 1** 0
Position 4 checks bits 4,5,6,7,12: 0 1 1 **? 0 0 1** _ 1 0 1 **0**. Odd parity so set position 4 to a 1: 0 1 1 **1 0 0 1** _ 1 0 1 **0**
Position 8 checks bits 8,9,10,11,12: 0 1 1 1 0 0 1 **? 1 0 1 0**. Even parity so set position 8 to a 0: 0 1 1 1 0 0 1 **0 1 0 1 0**
Code word: 011100101010.

(ii) If a binary signal is sent over 3 MHZ and whose signal to noise **(5 marks)**
ratio is the30 db,maximumwhat achievableis channel capacity

The Nyquist Limit can be disregarded as this is not a noiseless channel (faster signal = more noise, this channel's s/n ratio is provided as 20dB)

thus we use Shannon's result which says the maximum data rate of a noisy channel is X = H $Log_2$(1 + S/N) bps using 10$Log_{10}$ S/N as our standard quality 2
= $Log_{10}$ S/N --> S/N = $10_2$ --> S/N = 100 X =
3000 $Log_2$ (1 + 100) bps which gives you x = 19,974 63bps

**Q.4** (i) Explain Backoff algorithm in CSMA/CD. **(5 marks)**

```
procedure putFrameCSMA/CD/persistent/expBackoff( . s : frame )

variable collided? : boolean; w, max : integer

begin collided? := true; max := 1

while collided? loop begin waitWhileBusy()

broadcastQuitOnCollision( s, collided? )

if collided? then begin w := random( 0, max )

wait( w ); if max<_finalLimit then double( max )

end
end
end
```

➔ CD = Collision Detection, enables to abandon further frame transmission immediately when collision is detected, which results in a considerable increase of channel utilization

➔ Exponential backoff = low start, rapid exponential increase in waiting time limit max which is restricted by a given final limit.Copes efficiently with varying load situations.

(ii) What are the reasons for having a minimum length frame is **(5 marks)**
Ethernet?

Ethernet has a minimum frame size of 64 bytes. The reason for having a minimum size frame is to prevent a station from completing the transmission of a frame before the first bit has reached the far end of the cable, where it may collide with another frame. Therefore, the minimum time to detect a collision is the time it takes for the signal to propagate from one end of the cable to the other. This minimum time is called the *Slot Time*

By defining the minimum ethern et frame size, you ensure that all neces sary information is being transferred at each transmission.

The minimum frame size breaks down like this: Size is 64 bytes.
→Destination Address (6 bytes)
→Source Address (6 bytes)
→Frame Type (2 bytes)
→Data (46 bytes)
→CRC Checksum (4 bytes)

46 bytes must be transmitted a t a minimum, with additional pad bytes added to meet frame requirements.

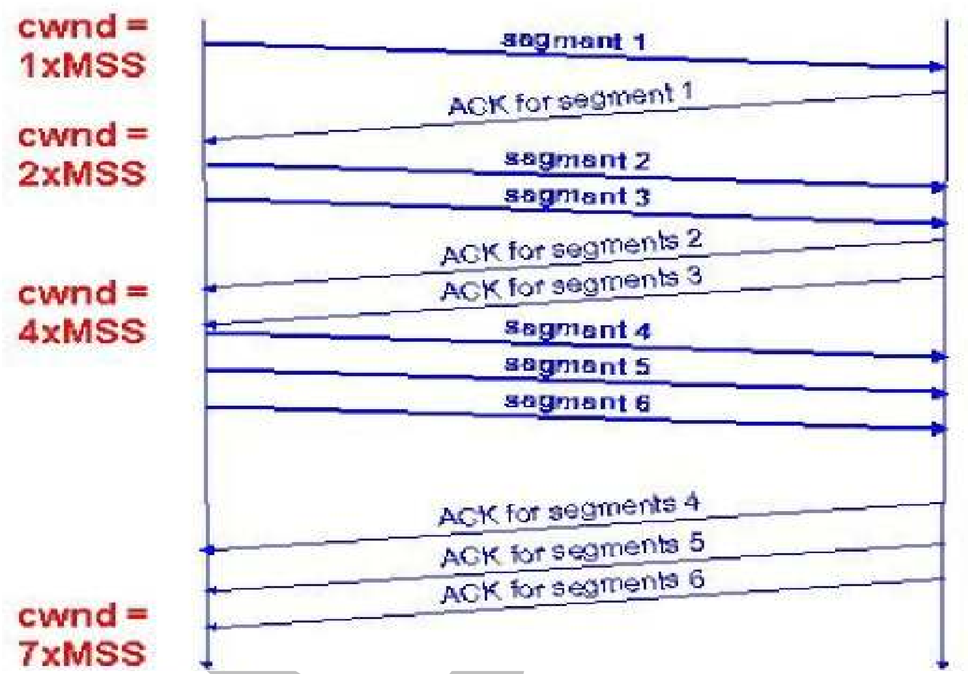
**Q.5** (i) How does TCP's congestion control mechanism work? Explain **(5 marks)** through an illustration.

- TCP has a mechanism for congestion control. The mechanism is implemented at the sender
- The window size at the sender is set as follows:

where

- flow control window is adverti sed by the receiver
- congestion window is adjusted based on feedback from the network
- The sender has two additional parameters:
  - **Congestion Window** ( **cwnd**)
    Initial value is 1 MSS (=maximum segment size) counted as bytes
  - **Slow-start threshold V alue (ssthresh)**
    Initial value is the advertised window size)
  - Congestion control wor ks in <u>two modes</u>:
  - **slow start** (cwnd < ssth resh)
  - **congestion avoidance** (cwnd >= ssthresh)
- Initial value:

- **cwnd = 1 segment**
- **Note: cwnd is actually measured in bytes:**
  **1 segment = MSS bytes**
- Each time an ACK is received, the congestion window is increased by MSS bytes.
  - **cwnd = cwnd + MSS**
  - If an ACK acknowledges two segments, cwnd is still increased by only 1 segment.
  - Even if ACK acknowledges a segment that is smaller than MSS bytes long, cwnd is increased by MSS.
    - Does Slow Start increment slowly? Not really. In fact, the increase of cwnd can be exponential
- The congestion window size grows very rapidly
  - For every ACK, we increase cwnd by 1 irrespective of the number of segments ACK'ed
- TCP slows down the increase of *cwnd* when
  ***cwnd > ssthresh***

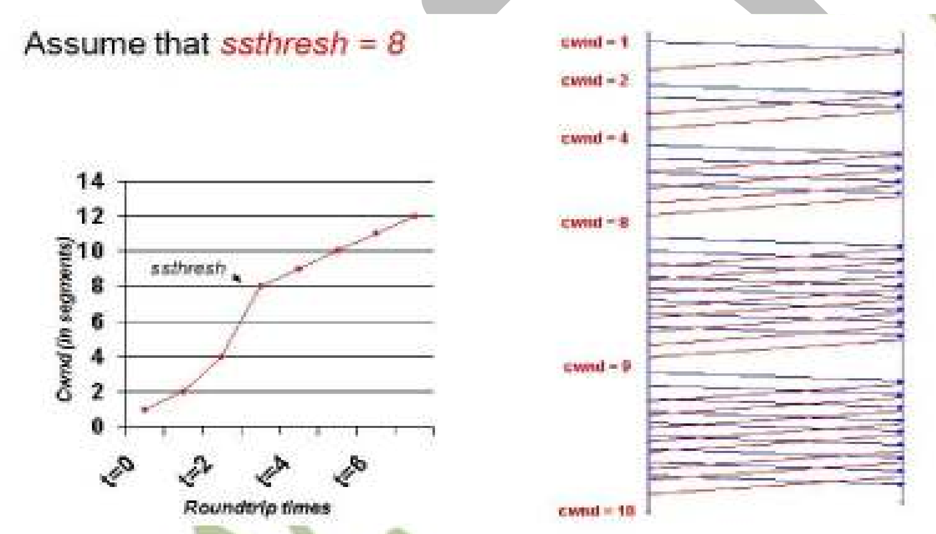



**Congestion Avoidance**

- Congestion avoidance phase is started if cwnd has reached the slow-start threshold value

- If cwnd >= ssthresh then each time an ACK is received, increment cwnd as follows:
    - cwnd = cwnd + MSS(MSS/ cwnd)
    - So *cwnd* is increased by one segment (=MSS bytes) only if all segments have been acknowledged.
- Here we give a more accurate version than in our earlier discussion of Slow Start:

**If** *cwnd* <= *ssthresh* **then**
Each time an Ack is received:
cwnd = cwnd + *MSS*
**else** /* *cwnd* > *ssthresh* */
Each time an Ack is received :
*cwnd = cwnd + MSS. MSS / cwnd*
**endif**




**Responses to Congestion**

- Most often, a packet loss in a network is due to an overflow at a congested router (rather than due to a transmission error)
- So, TCP assumes there is congestion if it detects a packet loss
- A TCP sender can detect lost packets via:
    - Timeout of a retransmission timer
    - Receipt of a duplicate ACK
- When TCP assumes that a packet loss is caused by congestion it reduces the size of the sending window

- Congestion is assumed if sender has timeout or receipt of duplicate ACK
- Each time when congestion occurs,
  - cwnd is reset to one:

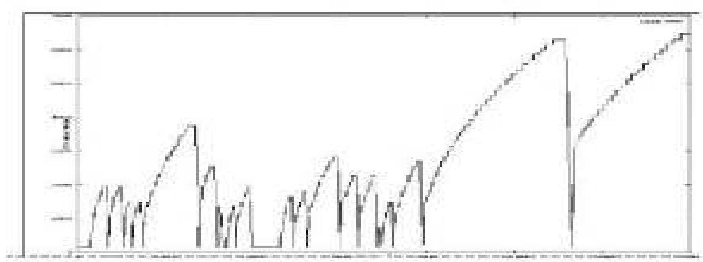
cwnd = MSS

  - ssthresh is set to half the current size of the congestion window:

ssthressh = cwnd / 2

  - and slow-start is entered

- A typical plot of cwnd for a TCP connection (MSS = 1500 bytes) with TCP Tahoe:



(ii) Describe Silly window**(5 marks)**problem. How it can b

Silly window syndrome is a problem in computer ne serious problem can arise in the sliding window o slowly, thepplicatreceivingonprogram consumes data slowly, process all incoming data, it requests that its cl setting on a TCP packeesto) .beIfunabletheservertoprocesscontinuall smaller and smaller, sometimes to the point that t data transmission extremely inefficientwindow. sizThe nameshrin value.

Since there is a certain amount of overhead assoc packets means increased overhead to process a decr

# Solution

➔When there is no synchronization between the send size of the packet, the window syndrome problem is sender, Nagle's algorithm is used. Nagle's solution r small one, then the sender waits until an ACK is r When the silly windowtedbysyndromethereceiver,iscreaDavid D Clar the window until another segment of maximum segmen

➔There are 3 reasons for SWS:
➔If the server announces,this leadsEmpty tospaceSWS.as 0
➔When client is able to generate only 1 byte at a
➔When server is able to consume only 1 byte at a t
➔During SWS, efficiency of communication .is almost

## Send-side silly window avoidance[

A heuristic method where the send TCP must allow data transferred in each call beforeng TCPtransmittingdelaysse until it can accumulate reasonable amounts of data

## Receive-side silly window avoidance[

A heuristic method that a receiver uses to maint advertising a decrease in window size to the sende on the receiver'saximb**u**mffersegmentsize sizeand .m By using thi advertisements where received applications extract

**Q.**Explain**6** Ethernet**(10 marks)**frame format.

Ethernet wasdevelopedoriginallytorun on a long coaxial cable This type of network topology is called a bus. Wh Ethernet was designed uldassuminghear **th**eseat allbroadcastsstationst connect them. This is where the terms 'wire segme includes all the wire and computers that trc**an**smitthear wire segment is the piece of wire used to connect

Because Ethernet networks are composed of broadcas connections often have. Instead,if Ethernetwire isystemsinus data to enable the remote station to allow it to with the ability to detect other computersl c**a**ttll**e**mpd Sense Multip-Coll**e**isionAccessDetect (CSMA/CD).

## IEEE 803.2 / 802.2

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 7 bytes | 1 byte | 2 or 6 bytes | 2 or 6 bytes | 2 bytes | 4-1500 bytes | | | | 4 bytes |
| Preamble | Start Frame Delimiter | Dest. MAC address | Source MAC address | Length | (Data / Pad) | | | | FCS |
| | | | | | DSAP | SSAP | CTRL | NLI | |

**Preamble**
This is a stream of bits used to allow the trans preamble is an alternating pattern of binary 56 on Frame Delimter.

***Start Fraterme Delim***
This is always 10101011 and is used to indicate th
***Destination MAC***
This is the MAC address of the machine receiving d is checking ownthisMACfieldadressfor.it's

***Source MAC***
This is the MAC address of the machine transmittin
***Length***
This is the length of the entire Ethernet frame i 65,534, it is rarely largerallythethanmaximum1500 astransmissiothat connections. Ethernet networks tend to use serial

***Data/Padding (a.k.a. Payload)***
The data is inserted here. This is nningwhere IPtheoverIP hE field contains IPX information if you are running

IEEE 803.2 frame are four specific fields: DSAP-Destination Service Access Point

SSAP-Source ServPoiceontAccess
CTRL-Control bits for Ethernet communication NLI-Network Layer Interface

FCS
This field contains the Frame Check Sequence (FCS) FCS allows Ethernet toframedetectande rrorsejectinthetheframeEthernif

**Q.7** (i) Why is traffic shaping needed? **(5 marks)**

Traffic shaping (also known as "packet shaping") is a computer network traffic management technique which delays some or all datagrams to bring them into compliance with a desired traffic profile.[1][2] Traffic shaping is a form of rate limiting.
Traffic shaping is used to optimize or guarantee performance, improve latency, and/or increase usable bandwidth for some kinds of packets by delaying other kinds.

Functionality

If a link becomes saturated to the point where there is a significant level of contention (either upstream or downstream) latency can rise substantially. Traffic shaping can be used to prevent this from occurring and keep latency in check. Traffic shaping provides a means to control the volume of traffic being sent into a network in a specified period (bandwidth throttling), or the maximum rate at which the traffic is sent (rate limiting), or more complex criteria such as GCRA. This control can be accomplished in many ways and for many reasons; however traffic shaping is always achieved by delaying packets. Traffic shaping is commonly applied at the network edges to control traffic entering the network, but can also be applied by the traffic source (for example, computer or network card[3]) or by an element in the network. Traffic policing is the distinct but related practice of packet dropping and packet marking.[4] The technique of selecting or categorising traffic into different types or classes is traffic classification.

Uses[edit source | editbeta]

Traffic shaping is sometimes applied by traffic sources to ensure the traffic they send complies with a contract which may be enforced in the network by a policer.

It is widely used for network traffic engineering, and appears in domestic ISPs' networks as one of several Internet Traffic Management Practices (ITMPs).[5]

Nodes in an IP network which buffer packets before sending on a link which is at capacity result in a traffic shaping effect. This can appear at for example a low bandwidth link (such as dial-up), a particularly expensive WAN link or satellite hop.

Traffic shaping is often used in combination with:

➔Differentiated services, Integrated services — including traffic classification and prioritization.

➔Weighted round robin (WRR)

➔Random early detection (RED), Weighted RED (WRED) and RED In/Out (RIO) — Lessens the possibility of port queue buffer tail drops and this lowers the likelihood of TCP global synchronization.

➔A number of port queue buffers.

➔VLAN tagging IEEE 802.1q