GATEFREAKS

GATE/NET/PSU

COMPUTER SCIENCE

Computer Network : Shortnotes

Sachin Michu
Alumnus IIT DELHI

Neha Michu
Alumna IIT DELHI

August 6, 2018

Key concepts on Computer Networking

1. Throughput for sliding window=$\frac{W \times L}{t_t + 2 * t_p}$
   W:Window size.
   L:Data size.
   t_t:Transmission time.
   t_p:Propagation time.

2. Transmission time(t_t) =$\frac{L}{B}$
   L:Data size.
   B:Bandwidth.

3. Propagation time(t_p) = $\frac{\text{distance}}{\text{speed}} = \frac{d}{v}$

4. Efficiency(utilization) for sliding window = $\frac{W \times t_t}{(t_t + 2 \times t_p)}$

5. Size of (sender window + receiver window)=2^n
   n:Number of bits used for sequence number.

6. Sender Window size in case of Go-Back-N=$2^n - 1$

7. Receiver Window size in case of Go-Back-N=1

8. 'N' in Go-back-N defines the window size.

9. Sender/Receiver Window size in case of Selective Repeat=2^{n-1}

10. Number of Retransmission in case of error=$\frac{1}{\text{Probability of Success}}$ = $\frac{1}{1-p}$ p:Probability of Error/Failure.

11. Hamming distance is the minimum hamming distance among the given Codewords.

12. If hamming distance is d+1 then d bits errors can be detected.

13. If hamming distance is 2d+1 then d bits error can be corrected.

14. Number of bit corrections:=$\left\lfloor \frac{(\text{Hamming Distance} - 1)}{2} \right\rfloor$

15. Parity check can detect Odd bits error in the message.

16. CRC can detect all burst errors of length <r
    r: Degree of polynomial Generator.

17. Checksum detect all odd bits errors, but it may not detect even number of errors.

18. In case of collision station waits for random amount of time , which can be calculated using Binary(exponential) backoff algorithm.

19. Throughput in Pure-Aloha = $G \times e^{-2G}$=18.4%(when G=0.5)

20. Throughput in Slotted-Aloha = $G \times e^{-G}$=36.8(when G=1)
    G:Load on the channel.

21. G=Slot time $\times$ Number of requests

22. Number of slots/s=$\frac{1}{\text{slot time}}$

23. Minimum frame size > $2t_p$* Bandwidth

24. Preamble in the ethernet frame format is used for bit-synchronization which is not the part of frame . Bit-synchronization is the responsibility of physical layer.

25. Virtual circuit is connection oriented service, X.25 is the example of Virtual circuit.

26. Datagram is connection less service , IP packet on internet is example of datagram.

27. Maximum no. of hosts = $2^{(\text{no. of 0-bits in hostId})} - 2$

28. As per old convention :
    Maximum number of subnets possible,if k bits are used for subnetting =$2^k - 2$
    Maximum number of hosts possible , if k bits are used for hostID=$2^k - 2$
    As per new convention:
    Maximum number of subnets possible,if k bits are used for subnetting =2^k
    Maximum number of hosts possible , if k bits are used for hostID=$2^k - 2$

29. ARP is a used with the IP for mapping a 32-bit Internet Protocol address to a MAC

30. RARP is a used for mapping MAC address to IP address.

31. ICMP is network layer protocol which is used for error reporting in the network.

32. Distance Vector routing (DVR) is an intradomain/ Interior Gateway, adaptive,Distributed,Decentralized, dynamic routing algorithms which uses bellman-ford algorithm . RIP and IGRP are the protocol used in DVR.

33. DVR is very slow as it has very high convergence time, Also count to infinity is related to DVR.

34. In DVR , router exchange information with their neighbour only.

35. Solution of count to infinity problem are split horizon and poisoned reverse.

36. Link State routing(LSR) is an intradomain/ Interior Gateway, adaptive,Distributed protocol. LSR uses Dijkstras algorithm for finding the shortest path and reliable flooding to send information to all the routers on the network.

37. LSR uses OSPF(Open Shortest Path First) Protocol, which can directly send data packet to IP without having Payload of UDP(Unlike RIP, Which Uses UDP).It also support multi-casting and Sub-netting.

38. Table size in hierarchal routing : {No. of routers within the region + No. of regions-1 + No. of clusters -1 }, Size of table will be optimal if number of clusters=number of regions=number of routers.

39. TCP is byte stream in which 1 byte transferred at a time.

40. Maximum burst time(t) in leaky bucket(Token Bucket) $=\frac{C}{(\rho - r)}$
C:Capacity of the token bucket
ρ:Maximum possible transmission rate
r:Rate at which New tokens are added

41. Token bucket follow the following relationship:
ρ*t=r*t+C.

42. Bandwidth delay product = Bandwidth*RTT

43. Wrap Around Time = (Possible sequence no. in TCP)/ Given Bandwidth

44. In Asynchronous serial Transmission , baud rate =bit rate.

45. In Manchester Encoding , bits rate is half of the baud rate.

46. $S = N \times \frac{1}{r}$
$r = \log_2 L$
Where,
S:Baud rate
N:Bit rate
r: Data elements in each signal.
L:signal elements.

47. TCP is full duplex,reliable,statefull, connection oriented,Byte oriented protocol which uses Selective acknowledgement. TCP is used with HTTP, FTP , SMTP.TCP uses IP for routing of Data , So data packets may follow different paths .

48. TCP does not use negative acknowledgment for lost packets but uses Timeout .

49. Timeout value is always greater than round trip time , which is also calculated in every round.

50. TCP uses 3-way handshaking for connection establishing, TCP also uses selective acknowledgment.

51. Admission control and Leaky bucket(Token Bucket) is used for open loop congestion control. while for closed loop congestion control "additive increase Multiplication decrease with slow start" is used.

52. When congestion window size is less than threshold value, then slow start algorithm is used.

53. When congestion window(congWin) size is greater than threshold value then congestion avoidance algorithm is used.

54. 3 Duplication acknowledgment indicate there is congestion in the network and threshold value is set to congWin/2 and congWin is set to threshold value.

55. When timeout occur , threshold set to congWin/2 and congWin is set to 1MSS.

56. IP address and socket address pair is known as Socket.

57. Congestion window increase exponetially during the slow start phase and linearly during the congestion control phase.

58. HTTP is stateless protocol which uses TCP connection, works on port 80.

59. FTP is statefull file transfer protocol which uses TCP and works on port 20/21.

60. SMTP is statefull mail transfer protocol which uses POP and IMAP and works with TCP at port 25.

61. In public key(asymmetric key) cryptology 2n keys are required for encryption and decryption, example RSA.

62. In public key cryptology sender encrypt message using the public key of the receiver and receiver decrypt it using its own private key.

63. In digital signature sender encrypt message using the private key of itself , and receiver decrypt/verify it using the public of sender.

64. In private key cryptology(symmetric key) n*(n-1)/2 keys are required , where n are number of users.example AES , DES.

65. In AES, size of key is 128 bits then the number of rounds are 10 whereas it is 12 and 14 for 192 and 256 bits respectively.

66. The AES design is based on a substitution-permutation network (SPN) and Data Encryption Standard (DES) is based on Feistel network.

67. MD5, SHA-1, CRC32 are hash functions which are used for message digest.

68. MD5 produce 128 bits massage digest whereas SHA-1 and CRC-32 produce 160 bit and 32 bits digest respectively.

69. physical layer or below : Hubs, Repeaters, Cables, Fibers, Wireless.
Data-link layer: Bridges, Modems, Network cards, 2-layer switches.
Network layer: Routers, Brouters, 3-layer switches.
Transport layer: Gateways, Firewalls.
Session layer: Gateways, Firewalls, PCs.
Presentation layer : Gateways, Firewalls, PCs.
Application layer: Gateways,Firewalls, all end devices like PCs, Phones, Servers.

70. Application Layer: Provides Applications with access to network services. It supporting network applications: FTP, SMTP, HTTP.

71. Presentation Layer(not used in tcp/ip model): Determines the format used to exchange data among networked computers.
    1. Translation
    2. Compression and decompression
    3. Encryption and decryption

72. Session Layer(not used in tcp/ip model): Allows two applications to establish, use and disconnect a connection between them called a session. Provides for name recognition and additional functions like security, which are needed to allow applications to communicate over the network. This layer also provides synchronisation, check parity.

73. Transport Layer: Ensures that data is delivered error free, in sequence and with no loss, duplications or corruption.
    (a) process-process data transfer: TCP, UDP
    (b) End-to-end reliable communication
    (c) Congestion and flow control
    (d) Fragmentation and Defragmentation of data .
    (e) Multiplexing /demultiplexing

74. Network Layer:
operation of the subnet
routing of packets source to destination
static / dynamic routing;
provide IP addressing
-Fragmentation and Defragmentation of data . The main responsibility of Network Layer is transmission of packets from source to destination

75. Data link layer :
    1. Error control
    2. Flow control
    3. Framing
    4. Access control to shared channel.
    5. The main responsibility of the data link layer is hop to hop transmission of frames

76. Physical layer:
    1. Electrical and mechanical specification of data (number of pins on Network connector and use of each pin on the connector)
    1. Modulation and demodulation
    2. Encoding and decoding .
    3. Bit synchronization.

Gatefreaks believe in providing quality. Qualifying any exam is not difficult if you have proper guidance and quality material. Our focus is to provide you the best error free content. We provide complete material including short notes, detailed notes, previous year solved papers and practice tests as a part of our intensive classroom program.For further details visit www.gatefreaks.com