IGNOU | BCA

2023-2024

FREE

SOLVED ASSIGNMENT

All In One

BCS-041

Fundamentals of Computer Networks

Prepared by

730-339-3555

www.ignoustudymentor.com

@ism_ignoustudymentor_

ISM - IGNOU STUDY MENTOR

Youtube Channel and

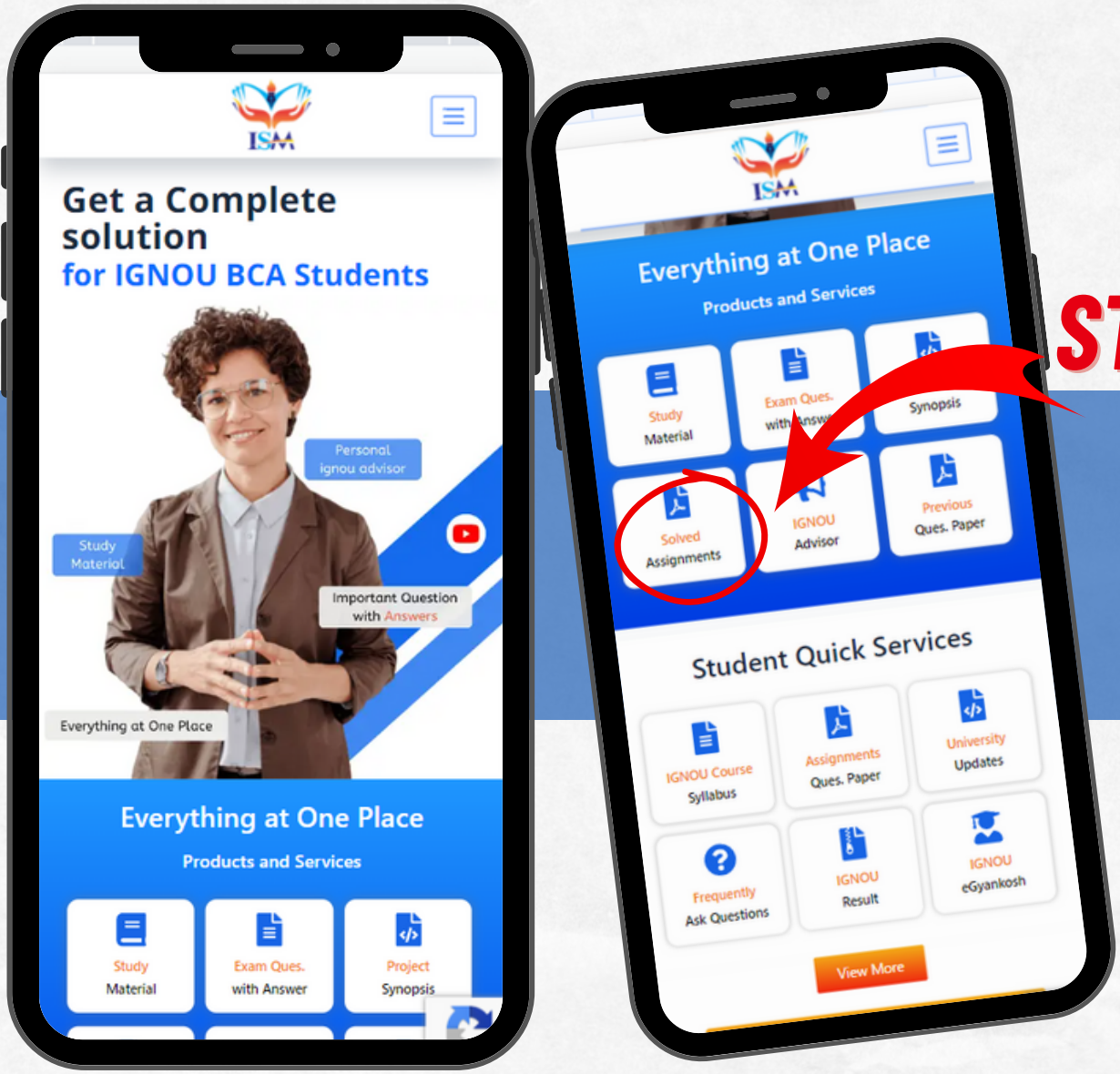
Get a Complete Solution

for IGNOU Students

www.ignoustudymentor.com

STEP 1

www.ignoustudymentor.com



STEP 2

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]

Ques.6(a) Explain POP and IMAP. How does POP work? What are the advantages of IMAP over POP?

Ans. POP Protocol: POP stands for Post Office Protocol. It provides a standard mechanism for retrieving emails from a remote server for a mail recipient. For instance, suppose that a home user A usually connects to the Internet using a dial-up connection to an ISP

ICMP: Internet Control Message Protocol (ICMP) is a network layer protocol used to diagnose communication errors by performing an error control mechanism. Since IP does not have an inbuilt mechanism for sending error and control messages. It depends on Internet Control Message Protocol(ICMP) to provide error control.

Advantages of POP3

1. Emails are downloaded to the user's computer. Messages can be read when user is offline.
2. Opening attachments is quick and easy as they are already downloaded.
3. Less server storage space is required; all emails are stored on local machine.
4. The storage capacity of emails is limited by the size of your hard disk. Very popular, easy to configure and use.

Benefits of ICMP: A great example is that of either a gateway or destination host sending an ICMP message to the source host if there is an error or a change in network connectivity that requires notification – such as a destination host or networking being unreachable, packet loss during transmission, etc.

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]

Ques.6(b) Assume two prime numbers p and q are 3 and 5 respectively. Calculate private key and public key using RSA algorithm.

Ans. Calculation of private and public key using RSA algorithm:

Given:

p=3 and q=5

Step 1: Calculate n = p*q n = 3*5=15

Step 2:calculate ϕ(n) ϕ(n) =(p - 1) * (q - 1) =(3 - 1) * (5 - 1)=2*4=8

Step 3: choose e such that 1 < e < ϕ(n) and e and ϕ (n) are coprime. Let e = 3

Step 4: Compute a value for d such that (d * e) % ϕ(n) = 1

Extended Euclidean algorithm:

8=3*2+2

3=1*2+1

2=2*1+0

Working of backward:

1=3-1*2

1=3-1*(8-2*3)

1=3*3-1*8

Therefore, (8 * 3) % ϕ(n) = 3

Step 5: Public key and Private key The public key is (n, e): (15, 3) The public key is (n, d): (15, 3)

Therefore, the public key is (15, 3) and private key is (15, 3)

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]

Ques.7(a) Compare between CSMA/CD and token passing methods in Ethernet. Also, explain how collisions are handled by CSMA/CD. Ans. Difference between CSMA And Token Passing

Ans. CSMA Carrier Sense Multiple Access is a listen-before-talking system. Each member of the network may transmit only if it does not detect another member using the network. This method works like a meeting in which each person waits for the others to finish talking before speaking But what if the network is "quiet," and two stations begin to transmit at once? If two (or more) computers transmit messages or data at the same time, the information will become distorted and unusable. One way of taking care of this situation is CSMA/CA (collision avoidance). In this scheme, when data get garbled, the sending station does not get an acknowledgment from the receiving station. Then the transmitting computer retransmits. The transmissions take place in fractions of a second, so the likelihood of a second collision in succession is very low. CSMA/CD (collision detection) does not wait for an acknowledgment. Instead, it has the stations listen before transmission to see whether the system is free, and listen during transmission to see whether two or more stations are transmitting at once. If a collision does take place, each transmitting station stops and waits for a fraction of a second before retransmitting. The amount of waiting time is chosen by each computer at random. Thus, it is unlikely that two stations will wait precisely the same amount of time before trying again. Remember that each transmission takes only a fraction of a second to complete..

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]

Token-passing: Token-passing is a protocol used in ring networks. It avoids collisions altogether because two or more stations cannot transmit at the same time. Token-passing is much like a children's game. The token is a pattern of bits, or a message that goes around the ring to each computer in turn. A computer can transmit only when it is "in possession" of the token. The computer then changes the bit pattern from "free" to "busy." It transmits a block of data or information called a frame immediately after the "busy" token. Part of the transmission also carries the "address" of the receiving computer. The token and frame pass through each computer on the network until they reach the one that is supposed to receive the frame. The receiver copies the data or message in the frame. The token and frame continue around the ring back to the transmitting computer. The transmitting computer then clears the frame and generates a new "free" token.Today most LANs are developed for PCs so that individual workers can communicate with each other. The connections in a PC network are made with various types of cables. Depending on the type of network hardware used, the cabling may be ordinary telephone wire, coaxial cable, fiber-optic cable, or twisted-pair cable (copper wires twisted to reduce electromagnetic induction). The most popular type of LAN today is Ethernet carried over twisted-pair cable.

Handling of collisions by CSMA/CD: Suppose a collision is detected from each station while broadcasting the packets. In that case, the CSMA CD immediately sends a jam signal to stop transmission and waits for a random time context before transmitting another data packet. If the channel is found free, it immediately sends the data and returns it.

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]

Ques.7(b) What is round robin technique for transmission? How does polling differ from token passing?

Ans. Round-robin technique for transmission: The round robin algorithm uses its scheduling techniques to assign processing time slices and transfer queued data packets. Network devices such as routers and switches implement special round robin algorithm buffer queues, which exist in device memory and store incoming and overloaded data for future processing. The term is also used in load balancing for servers. For example, a front end load balancer on a webfarm could distribute Internet traffic among a group of webservers based on a round-robin process.

Polling: The polling method primarily works with those topologies where one device acts as the primary station and the other as the secondary station. All data exchange must be made through the primary device even though the secondary device's final destination. Thus, to impose order on a network of independent users and establish one station that will act as a controller and periodically polls over all other stations, this is called polling. The Primary device controls the link while the secondary device follows the instructions of the primary device. The responsibility is on the primary device to determine which device is allowed to use the channel at a given time. Therefore, the primary devices are always an initiator of the session. Efficiency Assume Tpoll be the time for polling and Tt be the time required for data transmission. Then,

Efficiency = Tt/(Tt + Tpoll)

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]

Token Passing: In token-passing methods, we organize all the stations in a logical ring. We can also say that each station has a predecessor and a successor.

- A predecessor is a station that is logically before the station in the ring, while the successor is after the station in the ring. The station that is accessing the channel is the current station.
- A unique bit pattern or a small message circulating from one station to the next in some predefined order is called a token.
- Possessing the token gives the station the right to access the channel and send its data.
- Whenever a station has some data to send, it waits until it acquires a token from its predecessor. After obtaining the token, it holds it and then sends its data. When a station has no more data to send, it frees the token and passes the token to the next logical station in the ring.
- Furthermore, the station cannot transmit the data until it receives the token again in the next round.
- In Token passing, when a station acquires the token and has no data to send, it passes it to the next station.
- The problem due to the Token passing technique is the duplication of tokens or the loss of tokens. The insertion & removal of a station also needs to be tackled.

Note: A token can only work in that channel, for which it is generated, and not for any other.

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]

Ques.8(a) What is distance vector routing? Briefly discuss the problem of distance vector routing.

Ans. Distance Vector Routing Algorithm: The Distance vector algorithm is iterative, asynchronous and distributed. Distributed: It is distributed in that each node receives information from one or more of its directly attached neighbours, performs calculation and then distributes the result back to its neighbours.

Iterative: It is iterative in that its process continues until no more information is available to be exchanged between neighbours.

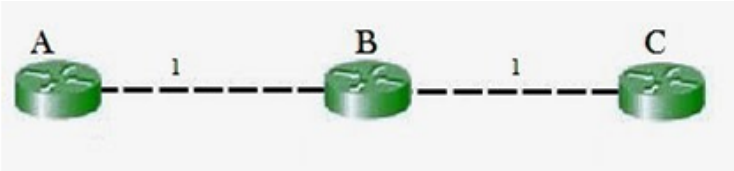
Asynchronous: It does not require that all of its nodes operate in the lock step with each other.

The Distance vector algorithm is a dynamic algorithm. It is mainly used in ARPANET, and RIP. Each router maintains a distance table known as Vector.

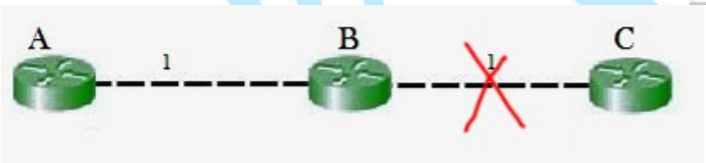
problem of distance vector routing: The main issue with Distance Vector Routing (DVR) protocols is Routing Loops since Bellman-Ford Algorithm cannot prevent loops. This routing loop in the DVR network causes the Count to Infinity Problem. Routing loops usually occur when an interface goes down or two routers send updates at the same time.

Counting to infinity problem:

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]



So in the example, the bellman-Ford algorithm will converge for each router, they will have entries for each other. B will know that it can get to C at a cost of 1, and A will know that it can get to C via B at a cost of 2.



If the link between B and C is disconnected, then B will know that it can no longer get to C 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 A which will be advertising that it can get to C at a cost of 2. B can get to A at a cost of 1, so it will update a route to C via A at a cost of 3. A will then receive updates from B later and update its cost to 4. They will then go on feeding each other bad information toward infinity which is called as Count to Infinity problem.

Ques.8(b) What do you understand by the term Quality of Services (QoS). Discuss the techniques to improve QoS.

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]

Ans. Quality of Services (QoS): Quality of Service (QOS) determines a network's capability to support predictable service over various technologies, containing frame relay, Asynchronous Transfer Mode (ATM), Ethernet, SONET IP-routed networks. The networks can use any or all of these frameworks. The QOS also provides that while supporting priority for one or more flows does not create other flows fail. A flow can be a combination of source and destination addresses, source and destination socket numbers, session identifier, or packet from a specific application or an incoming interface. The QOS is primarily used to control resources like bandwidth, equipment, wide area facilities etc. It can get more efficient use of network resources, provide tailored services, provide coexistence of mission-critical applications, etc

Reliability: Reliability is the degree to which a network guarantees delivering data packets, regardless of a node/link failure or any other network disruption. We measure reliability with the error and loss rates.

3.2. Delay or Latency

This metric shows how much time a data packet needs to travel from its source to its destination. Applications such as file transfer and emailing tolerate high latency. However, video gaming and conferencing require low latency. Otherwise, they would have so poor quality that users would be very dissatisfied

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]

3.3. Jitter: The jitter refers to the scenario when packets aren't delivered at regular intervals of time. It is the change in the amount of latency for a set of packets delivering a singular service. This parameter is crucial in real-time applications as it can totally damage the reception of a video or a phone call. Its causes are typically path changes and traffic congestion.

3.4. Bandwidth

The bandwidth refers to the transmission capacity of the network, i.e., how much data we can transfer at a given time. We estimate it as the maximum number of bits we can transfer per second. When the network throughput (the actual load of data it needs to handle) exceeds the bandwidth, the traffic will suffer from congestion, and the QoS will degrade.

4. Techniques to Improve the QoS

We can apply several mechanisms to improve the QoS in a network. They rely mainly on organizing data routing based on their sensitivity to real-time traffic.

4.1. Classification and Marking

Here, we split the network traffic into different classes. Grouping distinct packets having the same class (video, audio, web browsing, etc.) helps us know what types of data streams flow across the network and how to assign priorities.

classification and marking

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]

4.2. Queuing and Scheduling

When a router (switch) receives packets from different flows, it stores them in different buffers we call queues. We differentiate the traffic in queues by order of priority. Packets belonging to the same type of class form a singular queue. Based on the result of classification, each traffic receives a specific type of treatment.

4.3. Policing and Shaping

When the traffic load exceeds the link capacity in the network, it leads to deteriorating QoS. Policing and shaping are bandwidth-modeling techniques to manage the amount and rate of traffic.

5. Conclusion

In this article, we explained QoS in networking and introduced different metrics and tools used to improve network performance. Packet loss and delay are the two most significant metrics to consider when evaluating QoS and user experience.

Techniques to improve Quality of Services (QoS):

There are several techniques that businesses can use to guarantee the high performance of their most critical applications. These include:

BCS-041
FUNDAMENTALS OF COMPUTER NETWORKS [SEM-4]

Prioritization of delay-sensitive VoIP traffic via routers and switches: Many enterprise networks can become overly congested, which sees routers and switches start dropping packets as they come in and out faster than they can be processed. As a result, streaming applications suffer. Prioritization enables traffic to be classified and receive different priorities depending on its type and destination. This is particularly useful in a situation of high congestion, as packets with higher priority can be sent ahead of other traffic.

Resource reservation: The Resource Reservation Protocol (RSVP) is a transport layer protocol that reserves resources across a network and can be used to deliver specific levels of QoS for application data streams. Resource reservation enables businesses to divide network resources by traffic of different types and origins, define limits, and guarantee bandwidth.

Queuing: Queuing is the process of creating policies that provide preferential treatment to certain data streams over others. Queues are high-performance memory buffers in routers and switches, in which packets passing through are held in dedicated memory areas. When a packet is assigned higher priority, it is moved to a dedicated queue that pushes data at a faster rate, which reduces the chances of it being dropped. For example, businesses can assign a policy to give voice traffic priority over the majority of network bandwidth. The routing or switching device will then move this traffic's packets and frames to the front of the queue and immediately transmit them.

Traffic marking: When applications that require priority over other bandwidth on a network have been identified, the traffic needs to be marked. This is possible through processes like Class of Service (CoS), which marks a data stream in the Layer 2 frame header, and Differentiated Services Code Point (DSCP), which marks a data stream in the Layer 3 packet header.

Follow :

ism_ignoustudymentor_

Join Telegram Group :

ism_ignoustudymentor

Youtube Channel

ISM - IGNOU Study MENTOR

Website

www.ignoustudymentor.com

730-339-3555