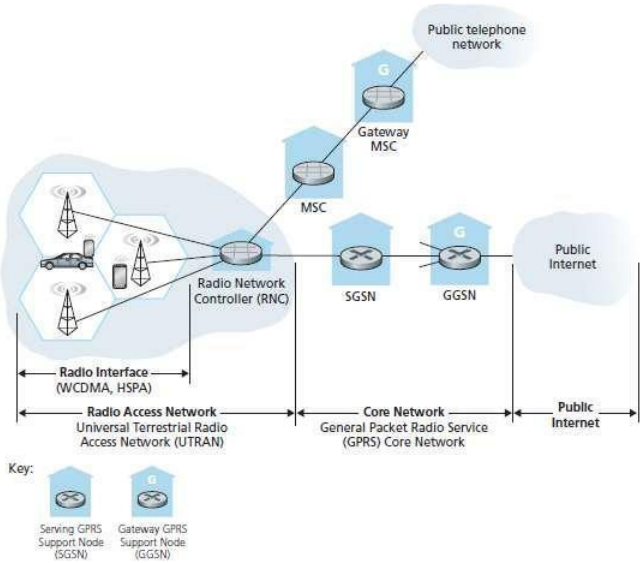
USN | | | | | | | | | | |

Internal Assessment Test III Solutions – Nov. 2018

Sub:	**Computer Networks**					Sub Code:	**15CS52**	Branch:	CSE	
Date:	19/11/2018	Duration:	90 min's	Max Marks:	50	Sem / Sec:	V / A,B,C		OBE	

Answer any FIVE FULL Questions

		MARKS	CO	RBT
Q1.	With a diagram, explain various components of 3G system architecture.	[10]	CO5	L2



(Fig: 4 Marks)

Main responsibilities of the core-network: (1 Mark)

1) Connects radio access-networks (RANs) to the public Internet.
2) Interoperates with components of the existing voice-network.

• Two types of nodes in the core-network: (3 Marks)
1) Serving GPRS Support Node (SGSN) and
2) Gateway GPRS Support Node (GGSN).

1) SGSN
• An SGSN is responsible for delivering data to/from the mobile-nodes in the RAN.
• Main responsibilities of the SGSN:
1) Interacting with the MSC of voice-network.
2) Providing user authorization and handoff.
3) Maintaining location information about active mobile-nodes.
4) Performing data forwarding between a GGSN & mobile-nodes in the RAN.

2) GGSN
• A GGSN acts as a gateway.
• The GGSN is used to connect multiple SGSNs into the larger Internet.
• To the outside world, the GGSN looks like any other router.
• The mobility of the nodes within the GGSN's network is hidden from the outside world.

3G Radio Access Network: The Wireless Edge (2 Marks)

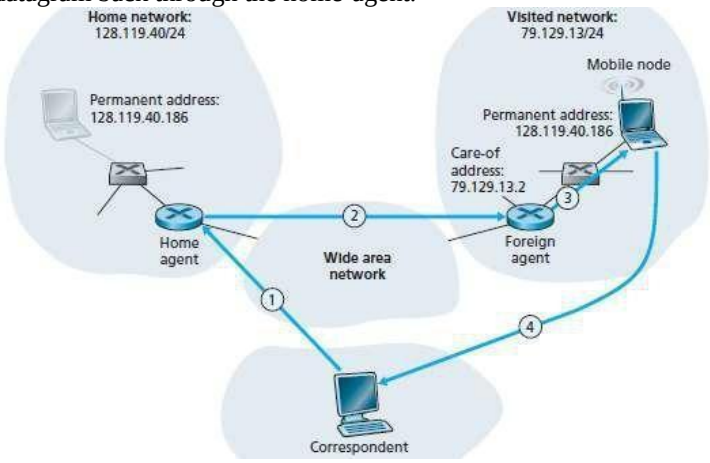
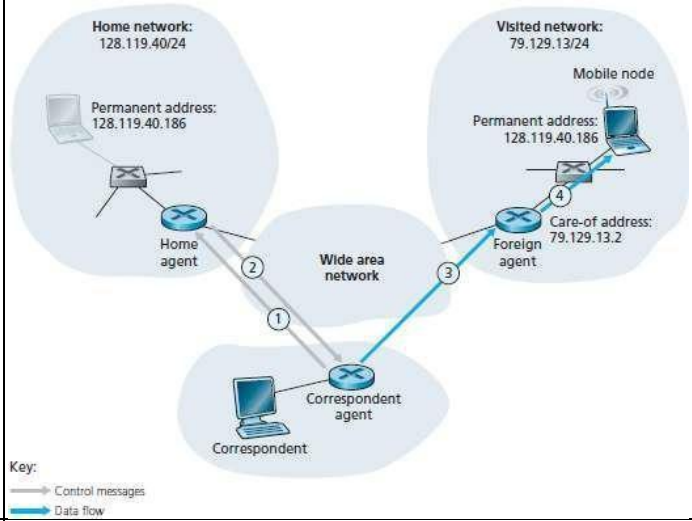
• The RAN is the wireless first-hop network that the 3G user sees.
• The RNC (Radio Network Controller) typically controls several cell BTSs
• Each cell's wireless-link operates between the mobile-nodes and a BTS.
• The RNC connects to both the circuit-switched voice-network and the packet-switched Internet.

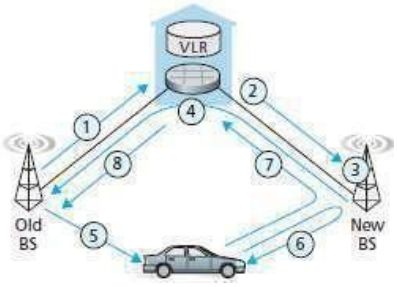
Q2.	With relevant diagrams, explain the approaches for routing to a mobile node.	[10]	CO5	L2

Routing to a Mobile Node:
• Two approaches are 1) indirect routing and 2) direct routing.

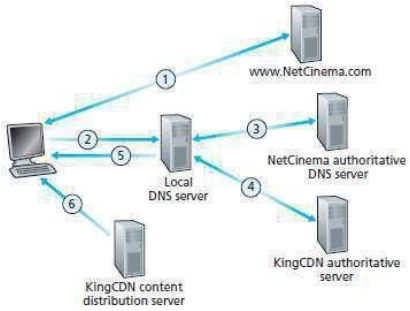
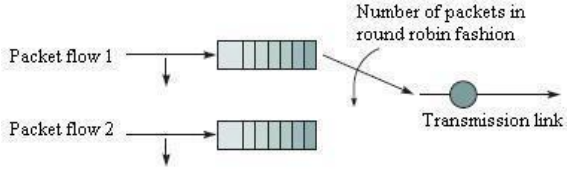
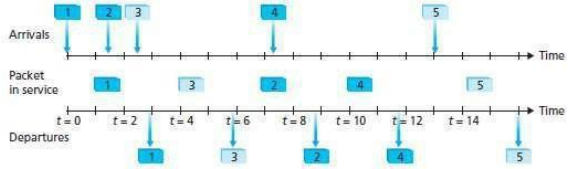
Indirect Routing to a Mobile Node
• Four steps are involved. (5 Marks)

Step 1:
The correspondent
→ addresses the datagram to the mobile-node's permanent-address and

	→ routes the datagram to the mobile-node's home-network. Step 2: Home-agent encapsulates the correspondent's original datagram within a larger datagram. This larger datagram is addressed & delivered to the mobile-node's COA. Step 3: The foreign-agent receives and decapsulates the datagram. The foreign-agent forwards the original datagram to the mobile-node. Step 4: The mobile-node directly routes the datagram to the correspondent. There is no need to route the datagram back through the home-agent.  **Disadvantage of Indirect Routing:** Suffers from triangle routing problem: The datagrams addressed to the mobile-node must be routed first to the home-agent and then to the foreign-network, even when an efficient route exists b/w the correspondent and the mobile-node. (2 Marks) • Solution: Use direct routing. **Direct Routing to a Mobile Node** (3 Marks) • Four steps are involved. Figure 4.6 illustrates the 4 steps. Steps 1 & 2 A correspondent-agent in the correspondent's n/w first learns the COA of the mobile-node. This can be done by having the correspondent-agent query the home-agent. Steps 3 & 4 Then, the correspondent-agent forwards datagrams directly to the mobile-node's COA  			
Q3.	Define Handoff. Explain the steps accomplishing handoffs in GSM. A handoff occurs when a mobile-station moves from one base-station to another during a call. (1 Mark) 1) Before handoff, a call is initially routed to the mobile through old base-station. 2) After handoff, the call is routed to the mobile through another new base-station. (1 Mark) Eight steps are involved. Figure illustrates the steps involved when a hand off occurs. (8 Marks) 1) Old base-station (BS) informs both visited M C & new BS that a handoff is about to happen. 2) The visited MSC performs following tasks: i) Initiates path setup to the new BS. ii) Allocates the resources needed to carry the rerouted call.	[10]	CO5	L2

	iii) Signals the new BS that a handoff is about to occur. 3) The new BS allocates and activates a radio-channel for the mobile. 4) The new BS informs both visited MSC and old BS that the new path is set up. 5) The mobile is informed to perform a handoff. 6) The mobile & new BS exchange signaling messages to fully activate the new channel. 7) The mobile sends a handoff complete message to the new BS. ¤ This message is then forwarded to the visited MSC. ¤ The visited MSC then reroutes the ongoing-call to the mobile via the new BS. 8) The resources allocated along the path to the old BS are released.  Fig: A handoff between base stations with a common MSC			
Q4.	With a diagram, explain the following with respect to mobile IP: a) Agent Discovery A mobile-node arriving to a new network must learn the identity of the corresponding foreign or home- agent. This process is known as agent discovery. (1 Mark) • Two methods to perform agent discovery: 1) Via agent advertisement and 2) Via agent solicitation. **Agent Advertisement** (3 Marks) • A foreign or home-agent advertises its services using a router discovery protocol. • The agent periodically broadcasts a router discovery message on all links. • The router discovery message contains 1) IP address of the agent and 2) A mobility agent advertisement extension. Five main fields in the extension: 1) Home Agent (H) This bit indicates that the agent is a home-agent for the network in which it resides. 2) Foreign Agent (F) This bit indicates that the agent is a foreign-agent for the network in which it resides. 3) Registration required (R) This bit indicates that a mobile-user in this network must register with a foreign-agent. 4) M, G Encapsulation These bits indicate whether an encapsulation other than IP-in-IP encapsulation will be used. 5) Care-of-address (COA) Fields This field indicates a list of one or more care-of-addresses provided by the foreign-agent. **Agent Solicitation** (2 marks) • A mobile-node wanting to learn about agents can broadcast an agent solicitation message. • An agent receiving the solicitation will unicast an agent advertisement directly to the mobile-node. b) Registration with the home agent Address must be registered with the home-agent. This can be done in 2 ways: 1) Via the foreign-agent who then registers the COA with the home-agent. 2) By the mobile IP node itself. Four steps are involved. (4 Marks) 1) When a mobile receives a foreign-agent advertisement, the mobile sends a registration-request to the foreign-agent. The registration-request contains i) COA advertised by the foreign-agent ii) address of the home-agent (HA) iii) permanent-address of the mobile (MA) iv) registration identification and	[6] [4]	CO5	L2

	v) requested lifetime of the registration. The requested registration lifetime indicates number of seconds the registration is valid. If registration is not renewed within the specified lifetime, the registration will become invalid. 2) When the foreign-agent receives the registration-request, the foreign-agent records the mobile's permanent IP address. The foreign-agent then sends a registration-request to the home-agent. 3) When home-agent receives the registration-request, the home-agent checks for correctness. The home-agent binds the mobile's permanent IP address with the COA. The home-agent sends a registration-reply. 4) The foreign-agent receives and forwards the registration-reply to the mobile-node.			
Q5.	Briefly explain the following streaming stored video applications: a) Dynamic Adaptive Streaming over HTTP (DASH) The video is encoded into several different versions. • Each version has a different bit-rate and a different quality level. • Two main tasks: (2 Marks) 1) The client dynamically requests video-chunks from the different versions: low & high. i) When the available bandwidth is high, the client selects chunks from a high-rate version. For ex: Fiber connections can receive a high-quality version. ii) When the available bandwidth is low, the client naturally selects from a low-rate version. For ex: 3G connections can receive a low-quality version. 2) The client adapts to the available bandwidth if end-to-end bandwidth changes during session. This feature is particularly important for mobile-users. The mobile-users see their bandwidth fluctuate as they move with respect to base-stations. • HTTP server stores following files: 1) Each video version with a different URL. 2) Manifest file provides a URL for each version along with its bit-rate. • Here is how it works: (3 Marks) 1) First, the client requests the manifest file and learns about the various versions. 2) Then, the client selects one chunk at a time by specifying → URL and → byte range in an HTTP GET request message. 3) While downloading chunks, the client → measures the received bandwidth and → runs a rate determination-algorithm. i) If measured-bandwidth is high, client will choose chunk from high-rate version. ii) If measured-bandwidth is low, client will choose chunk from low-rate version 4) Therefore, DASH allows the client to freely switch among different quality-levels. b) Streaming stored video over HTTP/TCP. The video is stored in an HTTP server as an ordinary file with a specific URL. • Here is how it works: (5 Marks) 1) When a user wants to see the video, the client → establishes a TCP connection with the server and → issues an HTTP GET request for that URL. 2) Then, the server responds with the video file, within an HTTP response message. 3) On client side, the bytes are collected in a client application buffer. 4) Once no. of bytes in this buffer exceeds a specific threshold, the client begins playback.	[5+5]	CO6	L2
Q6.	With a neat diagram, explain CDN operation. A CDN (2 Marks) → manages servers in multiple geographically distributed locations → stores copies of the videos in its servers, and → attempts to direct each user-request to a CDN that provides the best user experience. • The CDN may be a private CDN or a third-party CDN. A private CDN is owned by the content provider itself. For example: Google"s CDN distributes YouTube videos A third-party CDN distributes content on behalf of multiple content providers CDNs. **CDN Operation: (6 Marks+ fig: 2 marks)** • When a browser wants to retrieve a specific video, the CDN intercepts the request. • Then, the CDN 1) determines a suitable server-cluster for the client and 2) redirects the client"s request to the desired server. • Most CDNs take advantage of DNS to intercept and redirect requests.	[10]	CO6	L2

	• CDN operation is illustrated in Figure 5.2.  Figure 5.2: DNS redirects a user‟s request to a CDN server • Suppose a content provider “NetCinema” employs the CDN company ”KingCDN” to distribute videos. • Let URL = http://video.netcinema.com/6Y7B23V • Six events occur as shown in Figure 5.2: 1) The user visits the Web page at NetCinema. 2) The user clicks on the following link: Then, the user‟s host sends a DNS query for “video.netcinema.com”. 3) The user‟s local-DNS-server (LDNS) forwards the DNS-query to an authoritative-DNS-server “NetCinema”. The server “NetCinema” returns to the LDNS a hostname in the KingCDN‟s domain. For example: “a1105.kingcdn.com”. 4) The user‟s LDNS then sends a second query, now for “a1105.kingcdn.com”. Eventually, KingCD „s D S system returns the IP addresses of a “KingCDN” server to LDNS. 5) The LDNS forwards the IP address of the “KingCDN" server to the user‟s host. 6) Finally, the client → establishes a TCP connection with the server → issues an HTTP GET request for the video.			
Q7.	Describe RRQ and WFQ scheduling mechanisms with diagrams. **RRQ** (Round Robin Queuing) is illustrated in Figure 5.16 & Figure 5.17. • The transmission bandwidth is divided equally among the buffers. • Each user flow has its own logical buffer. • Round-robin scheduling is used to service each non-empty buffer one bit at a time. • In the simplest form, a class 1 packet is transmitted, followed by a class 2 packet, followed by a class 1 packet, followed by a class 2 packet, and so on. • RRQ is a work-conserving queuing discipline. • Thus, RRQ will immediately move on to the next class when it finds an empty queue. • Disadvantage: Extensive processing at the destination.  Figure 5.16: Round-robin queuing  Figure 5.17: Operation of the two-class round robin queue **WFQ** • WFQ (Weighted Fair Queuing) is illustrated in Figure 5.18. • Each user flow has its own buffer, but each user flow also has a weight that determines its relative share of the bandwidth. • If buffer 1 has weight 1 and buffer 2 has weight 3, then buffer 1 will receive 1/4 of the bandwidth and buffer 2 will receive 3/4 of the bandwidth. • In each round, each non-empty buffer would transmit a number of packets proportional to its weight. • WFQ systems are means for providing QoS guarantees. • WFQ is also a work-conserving queuing discipline. • Thus, WFQ will immediately move on to the next class when it finds an empty queue.	[5+5]	CO6	L2

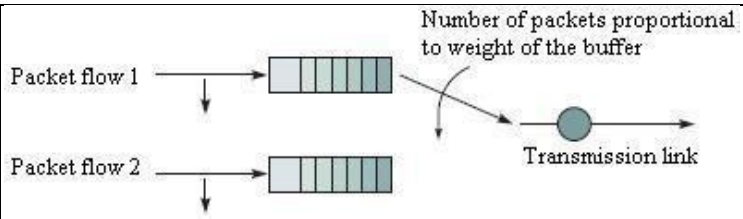
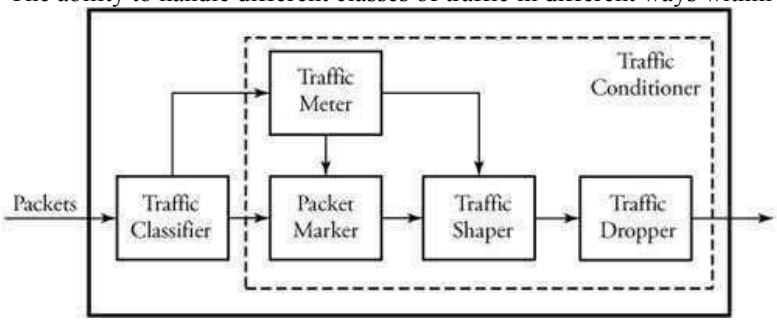


Figure 5.18: Weighted fair queuing

Q8.a)	Describe the Diffserv Internet Architecture. This provides QoS support to a broad class of applications. • This provides service differentiation. • Differentiation is defined as "The ability to handle different classes of traffic in different ways within the Internet".	[6]	CO6	L2



(2 Marks)

• The Diffserv architecture consists of 2 functional elements:

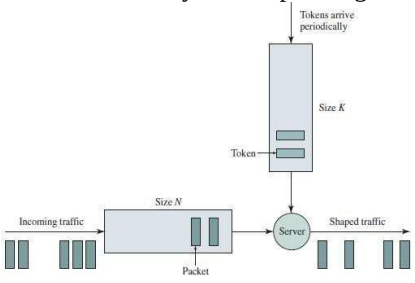
1) Packet Classification & Traffic Conditioning **(2 marks)**

• The traffic-classifier routes packets to specific outputs, based on the values of one or more header-fields.
• The traffic-profile contains a limit on the peak-rate of the flow.
• The traffic-conditioner detects and responds if any packet has violated the negotiated traffic-profile.
•The traffic-conditioner has 4 major components:
i) Meter
The meter measures the traffic to make sure that packets do not exceed their traffic profiles ii) Marker
The marker marks or unmarks packets in order to keep track of their situations in the Diffserv node.
iii) Shaper
The shaper delays any packet that is not complaint with the traffic-profile
iv) Dropper
The dropper discards any packet that violates its traffic-profile

2) Core Function: Forwarding **(2 marks)**

• The per-hop behavior (PHB) is performed by Diffserv-capable routers.
• A router forwards marked-packet onto its next hop according to the PHB (per-hop behavior).
• PHB influences how network-resources are shared among the competing classes of traffic.
• Two types of PHB are: i) expedited forwarding and ii) assured forwarding.
i) Expedited Forwarding (EF) PHB
This specifies that the departure rate of a class of traffic from a router must equal or exceed a configured rate.
ii) Assured Forwarding (AF) PHB
This divides traffic into 3 classes: good, average and poor.
Here, each class is guaranteed to be provided with some minimum amount of bandwidth and buffering.

b)	Describe the leaky bucket policing mechanism.	[4]	CO6	L2



(1 Mark)

Policing-device can be implemented based on the concept of a leaky bucket.
• Tokens are generated periodically at a constant rate.
• Tokens are stored in a bucket.
• A packet from the buffer can be taken out only if a token in the bucket can be drawn.
• If the bucket is full of tokens, additional tokens are discarded.

	• If the bucket is empty, arriving packets have to wait in the buffer until a sufficient no. of tokens is generated. (3 Marks)			