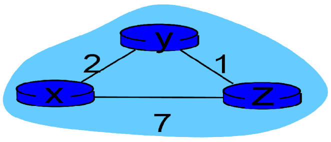
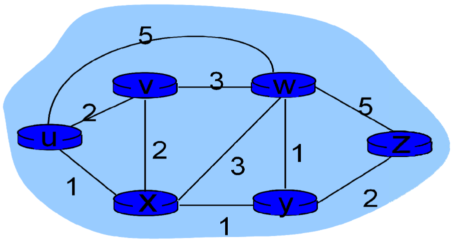
USN □□□□□□□□□□

CELEBRATING 25 YEARS
CMRIT
CMR INSTITUTE OF TECHNOLOGY, BENGALURU.
ACCREDITED WITH A+ GRADE BY NAAC

Internal Assessment Test 4 – February 2022

Sub:	Computer Networks and Security				Sub Code:	18CS52	Branch:	ISE
Date:	1/2/2022	Duration:	90 min's	Max Marks:	50	Sem/Sec:	V A, B & C	OBE

	Answer any FIVE FULL Questions	MARKS	CO	RBT
1	Illustrate the structure of AES and describe the steps in AES encryption process with example.	[10]	CO4	L2
2	Describe the working of following protocols. i)RTP ii)SIP	[10]	CO5	L2
3a)	Describe UDP streaming stored video application.	[5]	CO5	L1
3b)	List the types of security attacks and explain any 4 such attacks.	[5]	CO4	L1
4	Discuss the FEC mechanisms and interleaving with neat diagrams.	[10]	CO5	L1
5	Explain about CDN types, operations and cluster selection strategies.	[10]	CO5	L1
6(a)	Consider there is a network consisting of 3 routers. The weights are mentioned on the edges. Weights could be distances or costs or delays. Find out the final routing tables for all the routers using Bellman-ford algorithm.  	[5]	CO3	L3
6 (b)	Deduce the shortest path tree using Dijkstra's algorithm for the following network. Assume source node as ***u***.  5 v 3 w 5 2 u 2 3 1 z 1 x y 2 1	[5]	CO3	L3

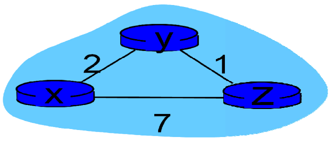
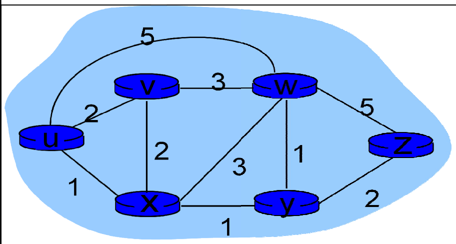
Scheme of Evaluation
Internal Assessment Test 4 – FEB 2022

Sub:	Computer Networks and Security						**Code:**	18CS52
Date: 1/2/2022	Duration:	90mins	Max Marks:	50	**Sem:**	V	**Branch:**	ISE

Note: **Answer Any five full questions.**

Question #		**Description**	**Marks Distribution**		**Max Marks**
1		Illustrate the structure of AES and describe the steps in AES encryption process with example. **Diagram** **Steps**	3M+7M	10M	10M
2		Describe the working of following protocols. i)RTP ii)SIP **Diagram** **Explanation**	5M+5M	10M	10M
3	a)	Describe UDP streaming stored video application. **Explanation** **Limitations**	3M +2 M	5M	10M

3	b)	List the types of security attacks and explain any 4 such attacks. **List** **Explanation**	1M+4M	5M	
4		Discuss the FEC mechanisms and interleaving with neat diagrams. **Diagram** **Explanation**	4M 6M	10M	10M
5		Explain about CDN types, operations and cluster selection strategies.	3M+4M+3M	10M	10M

6	a)	Consider there is a network consisting of 3 routers. The weights are mentioned on the edges. Weights could be distances or costs or delays. Find out the final routing tables for all the routers using Bellman-ford algorithm.  **Steps** **MST**	5M	5M	10M
6	b)	 u v w x y z 5 3 2 5 2 3 1 1 1 2 Deduce the shortest path tree using Dijkstra's algorithm for the following network. Assume source node as ***u***. **Steps** **Show off of Final Table**	5M	5M	

Scheme Of Evaluation Internal Assessment Test 4 – FEB 2022

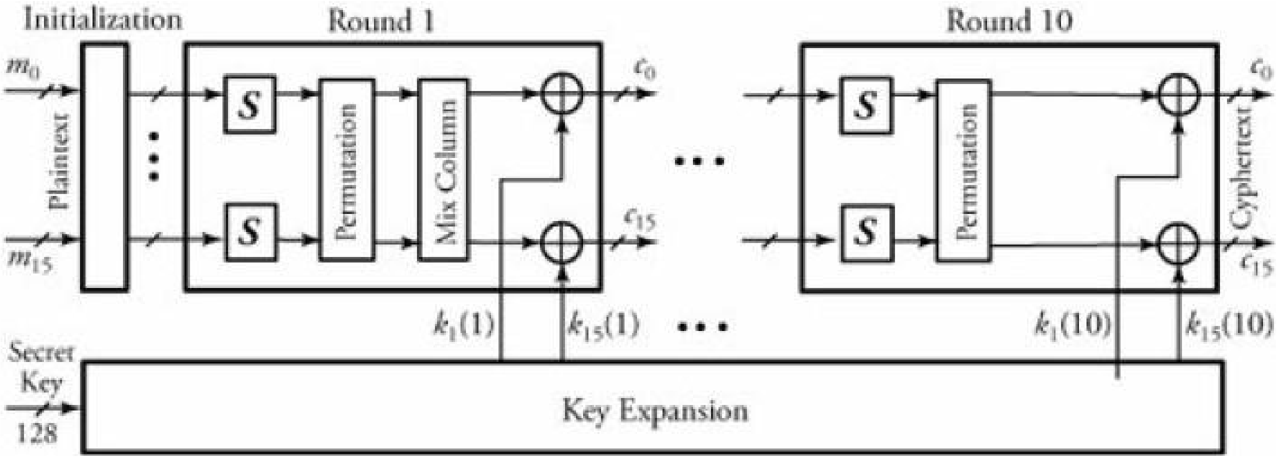
Sub:	Computer Networks and Security							**Code:**	18CS52
Date:	1/2/2022	Duration:	90mins	Max Marks:	50	**Sem:**	V	**Branch:**	ISE

Note: **Answer Any full five questions**

Q1. Illustrate the structure of AES and describe the steps in AES encryption process with example.

AES has better security strength than DES.

- In AES message is divided into 128-bit block, and it uses 128 or 192 or 256 bit key.
- Based on the key size number of rounds can be 10,12 or 14.
- The plaintext is formed as 16 bytes m0 through m15 and is fed into round 1 after an initialization stage.
- In this round, substitute-units(S) perform a byte-by-byte substitution of blocks.
- The ciphers move through a permutation-stage to shift rows to mix-columns.
- At the end of this round, all 16 blocks of ciphers are Exclusive-ORed with the 16 bytes of round 1 key k0(1) through k15(1).



Q2. Describe the working of following protocols. i)RTP ii)SIP

RTP

- RTP can be used for transporting common formats such as
→ MP3 for sound and
→ MPEG for video
- It can also be used for transporting proprietary sound and video formats.
- Today, RTP enjoys widespread implementation in many products and research prototypes.
- It is also complementary to other important real-time interactive protocols, such as SIP.

RTP Basics

- RTP runs on top of UDP.
- The RTP packet is composed of i) RTP header & ii) audio chunk
- The header includes

i) Type of audio encoding
ii) Sequence number and
iii) Timestamp.

- The application appends each chunk of the audio-data with an RTP header.
- Here is how it works:

1) At sender-side:
i) A media chunk is encapsulated within an RTP packet.
ii) Then, the packet is encapsulated within a UDP segment.
iii) Finally, the UDP segment is handed over to IP.
2) At receiving-side:
i) The RTP packet is extracted from the UDP segment.
ii) Then, the media chunk is extracted from the RTP packet.
iii) Finally, the media chunk is passed to the media-player for decoding and rendering

- If an application uses RTP then the application easily interoperates with other multimedia applications
- For example:

If 2 different companies use RTP in their VoIP product, then users will be able to communicate.

- What RTP does not provide?

i) It does not provide any mechanism to ensure timely delivery of data.
ii) It does not provide quality-of-service (QoS) guarantees.
iii) It does not guarantee delivery of packets.
iv) It does not prevent out-of-order delivery of packets.

- RTP encapsulation is seen only at the end systems.
- Routers do not distinguish between

i) IP datagrams that carry RTP packets and
ii) IP datagrams that don‟t carry RTP packets.

- RTP allows each source to be assigned its own independent RTP stream of packets.
- For example:

1) For a video conference between two participants, four RTP streams will be opened
i) Two streams for transmitting the audio (one in each direction) and
ii) Two streams for transmitting the video (again, one in each direction).
2) Encoding technique MPEG bundles audio & video into a single stream.
□□In this case, only one RTP stream is generated in each direction.

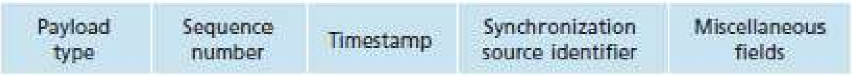
- RTP packets can also be sent over one-to-many and many-to-many multicast trees.

RTP Packet Header Fields

- Four header fields of RTP Packet (Figure 5.6):

1) Payload type
2) Sequence number
3) Timestamp and
4) Source identifier.

- Header fields are illustrated in Figure 5.6.



Payload type	Sequence number	Timestamp	Synchronization source identifier	Miscellaneous fields

Figure 5.6: RTP header fields

1) Payload Type

i) For an audio-stream, this field is used to indicate type of audio encoding that is being used.

□□For example: PCM, delta modulation.

□□Table 5.1 lists some of the audio payload types currently supported by RTP.

ii) For a video stream, this field is used to indicate the type of video encoding.

□□For example: motion JPEG, MPEG.

□□Table 5.2 lists some of the video payload types currently supported by RTP.

2) Sequence Number

• This field increments by one for each RTP packet sent.

• This field may be used by the receiver to detect packet loss and to restore packet sequence.

3) Timestamp

• This field reflects the sampling instant of the first byte in the RTP data packet.

• The receiver can use timestamps

→ to remove packet jitter in the network and

→ to provide synchronous playout at the receiver.

• The timestamp is derived from a sampling clock at the sender.

4) Source Identifier (SRC)

• This field identifies the source of the RTP stream.

• Typically, each stream in an RTP session has a distinct SRC.

SIP

• SIP (Session Initiation Protocol) is an open and lightweight protocol.

• Main functions of SIP:

1) It provides mechanisms for establishing calls b/w a caller and a callee over an IP network.

2) It allows the caller to notify the callee that it wants to start a call.

3) It allows the participants to agree on media encodings.

4) It also allows participants to end calls.

5) It provides mechanisms for the caller to determine the current IP address of the callee.

6) It provides mechanisms for call management, such as

→ adding new media streams during the call

→ changing the encoding during the call

→ inviting new participants during the call,

→ call transfer and

→ call holding.

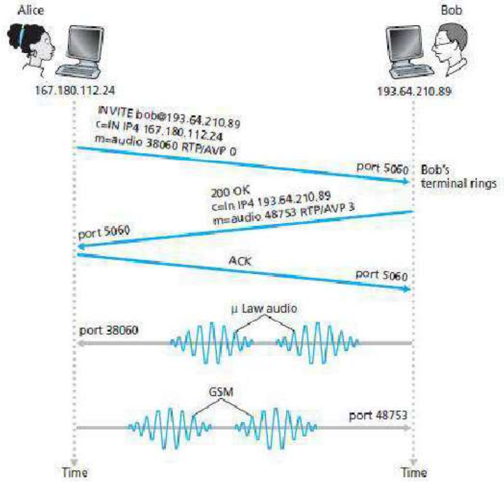


Figure 5.7: SIP call establishment when Alice knows Bob‟s IP address

• Consider an example: Alice wants to call Bob.

• Alice‟s & Bob‟s PCs are both equipped with SIP-based software for making and receiving phone calls.

• The following events occur:

1) An SIP session begins when Alice sends Bob an INVITE message.

□□This INVITE message is sent over UDP to the well-known port 5060 for SIP.

□□The INVITE message includes

i) An identifier for Bob (bob@193.64.210.89)

ii) An indication of Alice‟s current IP address

iii) An indication that Alice desires to receive audio, which is encoded in format AVP 0.

2) Then, Bob sends an SIP response message (which resembles an HTTP response message).

□□The response message is sent over UDP to the well-known port 5060 for SIP.

□□The response message includes

i) 200 OK

ii) An indication of Bob‟s current IP address

iii) An indication that Bob desires to receive audio, which is encoded in format AVP 3.

3) Then, Alice sends Bob an SIP acknowledgment message.

4) Finally, Bob and Alice can talk.

Q3a) Describe UDP streaming stored video application.

With UDP streaming, the server transmits video at a rate that matches the client’s video consumption rate by clocking out the video chunks over UDP at a steady rate.

□ For example, if the video consumption rate is 2 Mbps and each UDP packet carries 8,000 bits of video, then the server would transmit one UDP packet into its socket every (8000 bits)/(2 Mbps) = 4 msec.

□ UDP does not employ a congestion-control mechanism, the server can push packets into the network at the consumption rate of the video without the rate-control restrictions of TCP.

□ Before passing the video chunks to UDP, the server will encapsulate the video chunks within transport packets specially designed for transporting audio and video, using the Real-Time Transport Protocol (RTP).

□ The client and server also maintain, in parallel, a separate control connection over which the client sends commands regarding session state changes (such as pause, resume, reposition,

Limitation:

 Due to the unpredictable and varying amount of available bandwidth between server and client, constant-rate UDP streaming can fail to provide continuous playout.

 It requires a media control server, such as an RTSP server, to process client-to-server interactivity requests and to track client state for each ongoing client session.

 Many firewalls are configured to block UDP traffic, preventing the users behind these firewalls from receiving UDP video.

Q 3b) List the types of security attacks and explain any 4 such attacks.

Internet infrastructure attacks are broadly classified into 4 categories

1) DNS hacking
2) Routing table poisoning
3) Packet mistreatment
4) Denial of Service (DOS)

DNS HACKING ATTACKS

• DNS server is a distributed hierarchical and global directory that translates domain names into numerical IP address.

• DNS is a critical infrastructure, and all hosts contact DNS to access servers and start connections.

• Name-resolution services in the modern Internet environment are essential for email transmission, navigation to web sites, or data transfer. Thus, an attack on DNS can potentially affect a large portion of the Internet.

ROUTING TABLE POISONING

• This is the undesired modification of routing tables. This results in a lower throughput of the network.

• Two types of attacks are: i) link attack and ii)router attack.

Link Attack

• Link attack occurs when a hacker gets access to a link and thereby intercepts, interrupts or modifies routing messages. This act similarly on both the link-state and the distance-vector protocols.

• If an attacker succeeds in placing an attack in a link-state routing protocol, a router may send incorrect updates about its neighbors or remain silent even if the link state of its neighbor has changed

Router Attack

• Router Attack may affect the link-state protocol or even the distance-vector protocol.

• In link-state protocol, if routers are attacked, they become malicious. As a result, routers may add a non existing link to a routing table delete an existing link or change the cost of a link.

• In the distance-vector protocol, an attacker may cause routers to send wrong updates about any node in the network, thereby misleading a router and resulting in network problems

PACKET MISTREATMENT ATTACKS

• Packet mistreatment attacks can occur during any data transmission.

• A hacker may capture certain data packets and mistreat them.

- The attack may result in congestion lowering throughput & DOS attacks

- Link-attack causes interruption, modification or replication of data packets. Whereas, a router-attack can misroute all packets and may result in congestion or DOS

DOS ATTACKS (DENIAL OF SERVICE)

- DOS is a type of security breach that prohibits a user from accessing normally provided services.

- DOS can cost the target person a large amount of time and money.

- DOSaffects the destination rather than a data-packet or router.

- They take important servers out of action for few hours, thereby denying service to all users. Two types of attacks are: 1) *Single-source:* An attacker sends a large number of packets to a target system to overwhelm & disable it

2) *Distributed:* A large number of hosts are used to flood unwanted traffic to a single target. The target cannot then be accessible to other users in the network.

Q4. Discuss the FEC mechanisms and interleaving with neat diagrams.

FEC

- The basic idea of FEC: Redundant information is added to the original packet stream.
- The redundant information can be used to reconstruct approximations of some of the lost-packets.
- Two FEC mechanisms:

1) Block Coding

➢ A redundant encoded chunk is sent after every n chunks.
➢ The redundant chunk is obtained by exclusive OR-ing the n original chunks.
➢ If any one packet in a group is lost, the receiver can fully reconstruct the lost-packet.
➢ Disadvantages:
1) If 2 or more packets in a group are lost, receiver cannot reconstruct the lost-packets.
2) Increases the playout delay. This is because
→ receiver must wait to receive entire group of packets before it can begin playout.

2) Lower Resolution Redundant Information

➢ A lower-resolution audio-stream is sent as the redundant information.
➢ For example: The sender creates
→ nominal audio-stream and
→ corresponding low-resolution, low-bit-rate audio-stream.
➢ The low-bit-rate stream is referred to as the redundant-stream.
➢ As shown in Figure 5.4, the sender constructs the nth packet by
→ taking the nth chunk from the nominal stream and
→ appending the nth chunk to the (n−1)st chunk from the redundant-stream
➢ Advantage:
Whenever there is packet-loss, receiver can hide the loss by playing out low-bit-rate chunk.

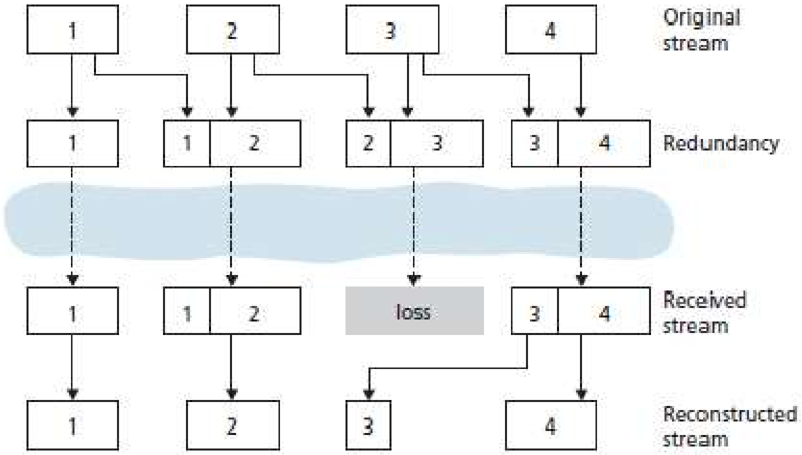


Figure 5.4: Piggybacking lower-quality redundant information

Interleaving

- A VoIP application can send interleaved audio.
- The sender resequences units of audio-data before transmission.
- Thus, originally adjacent units are separated by a certain distance in the transmitted-stream.
- Interleaving can mitigate the effect of packet-losses.
- Interleaving is illustrated in Figure 5.5.
- For example:

If units are 5 msecs in length and chunks are 20 msecs (that is, four units per chunk), then
→ the first chunk contains the units 1, 5, 9, and 13
→ the second chunk contains the units 2, 6, 10 & 14 and so on.

- Advantages:

1) Improves the perceived quality of an audio-stream.
2) Low overhead.
3) Does not increase the bandwidth requirements of a stream.

- Disadvantage:

1) Increases latency. This limits use for VoIP applications.

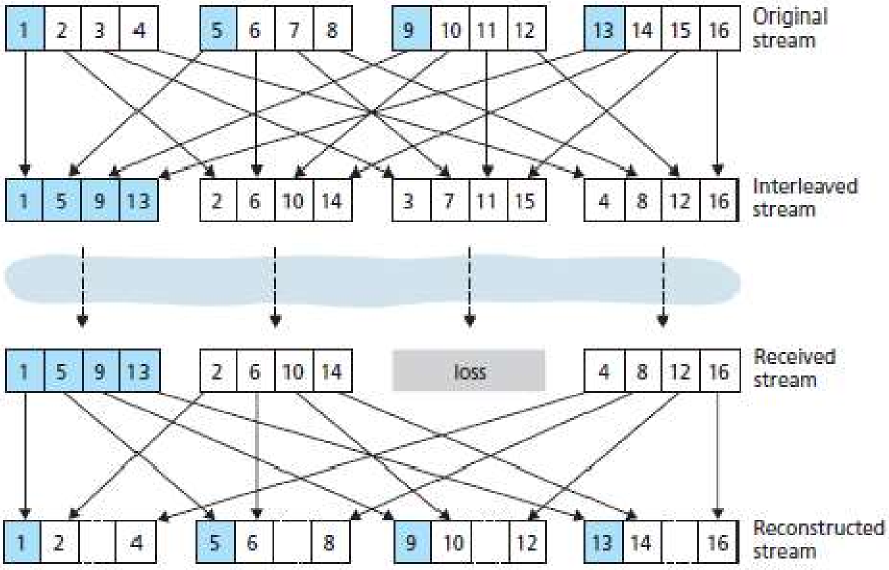


Figure 5.5: Sending interleaved audio

Q5. Explain about CDN types, operations and cluster selection strategies.

• A CDN
→ 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.

1) Private CDN

➢ A private CDN is owned by the content provider itself.
➢ For example:
Google"s CDN distributes YouTube videos

2) Third Party CDN

➢A third-party CDN distributes content on behalf of multiple content providers CDNs.
➢ Two approaches for server placement:

i) Enter Deep

¤ The first approach is to enter deep into the access networks of ISPs.
¤ Server-clusters are deployed in access networks of ISPs all over the world.
¤ The goal is to get close to end users.
¤ This improves delay/throughput by decreasing no. of links b/w end user & CDN cluster

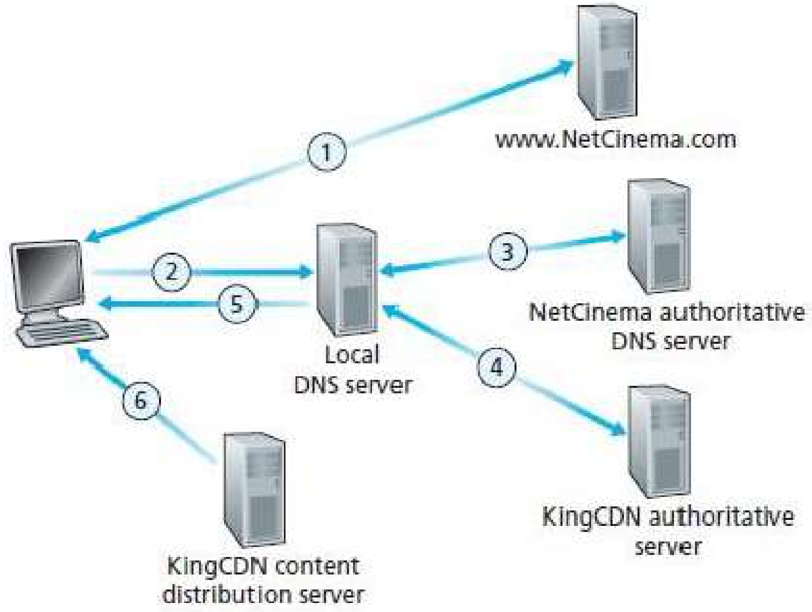
ii) Bring Home

¤ The second approach is to bring the ISPs home.
¤ Large clusters are built at a smaller number of key locations.
¤ These clusters are connected using a private high-speed network.
¤ Typically, clusters are placed at a location that is near the PoPs of many tier-1 ISPs.
For example: within a few miles of both Airtel and BSNL PoPs in a major city.

➔ CDN Operation

When a browser in a user's host is instructed to retrieve a specific video (identified by a URL), the CDN must intercept the request so that it can
(1) Determine a suitable CDN server cluster for that client at that time.

(2) Redirect the client's request to a server in that cluster.



www.NetCinema.com
1
2
5
3
NetCinema authoritative DNS server
Local DNS server
4
6
KingCDN authoritative server
KingCDN content distribution server

1. The user visits the Web page at NetCinema.

2. When the user clicks on the link http://video.netcinema.com/6Y7B23V, the user’s host sends a DNS query for video.netcinema.com.

3. The user’s Local DNS Server (LDNS) relays the DNS query to an authoritative DNS server for NetCinema, which observes the string ―video‖ in the hostname video.netcinema.com. To ―hand over‖ the DNS query to KingCDN, instead of returning an IP address, the NetCinema authoritative DNS server returns to the LDNS a hostname in the KingCDN’s domain, for example, a1105.kingcdn.com.

4. From this point on, the DNS query enters into KingCDN’s private DNS infrastructure. The user’s LDNS then sends a second query, now for a1105.kingcdn.com, and KingCDN’s DNS system eventually returns the IP addresses of a KingCDN content server to the LDNS. It is thus here, within the KingCDN’s DNS system, that the CDN server from which the client will receive its content is specified.

5. The LDNS forwards the IP address of the content-serving CDN node to the user’s host.

6. Once the client receives the IP address for a KingCDN content server, it establishes a direct TCP connection with the server at that IP address and issues an HTTP GET request for the video. If DASH is used, the server will first send to the client a manifest file with a list of URLs, one for each version of the video, and the client will dynamically select chunks from the different versions.

➔ Cluster Selection Strategies

 Cluster Selection Strategies is a mechanism for dynamically directing clients to a server cluster or a data center within the CDN.

 The CDN learns the IP address of the client’s LDNS server via the client’s DNS lookup. After learning this IP address, the CDN needs to select an appropriate cluster based on this IP address.

 One simple strategy is to assign the client to the cluster that is geographically closest. Using commercial geo-location databases each LDNS IP address is mapped to a geographic location. When a DNS request is received from a particular LDNS, the CDN chooses the geographically closest cluster.

 For some clients, the solution may perform poorly, since the geographically closest cluster may not be the closest cluster along the network path.

 In order to determine the best cluster for a client based on the current traffic conditions, CDNs can instead perform periodic real-time measurements of delay and loss performance between their clusters and clients.

 An alternative to sending extraneous traffic for measuring path properties is to use the characteristics of recent and ongoing traffic between the clients and CDN servers.

 Such solutions, however, require redirecting clients to (possibly) suboptimal clusters from time to time in order to measure the properties of paths to these clusters.

 A very different approach to matching clients with CDN servers is to use IP anycast. The idea behind IP anycast is to have the routers in the Internet route the client’s packets to the ―closest‖ cluster, as determined by BGP.

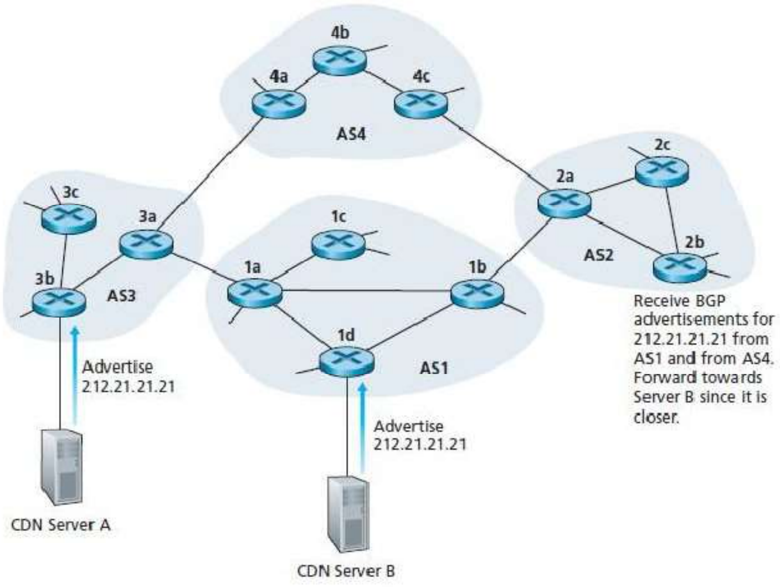
During the IP-anycast configuration stage, the CDN company assigns the same IP address to each of its clusters, and uses standard BGP to advertise this IP address from each of the different cluster locations.

 When a BGP router receives multiple route advertisements for this same IP address, it treats these advertisements as providing different paths to the same physical location.

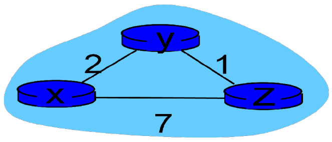
□ Following standard operating procedures, the BGP router will then pick the —best‖ route to the IP address according to its local route selection mechanism.

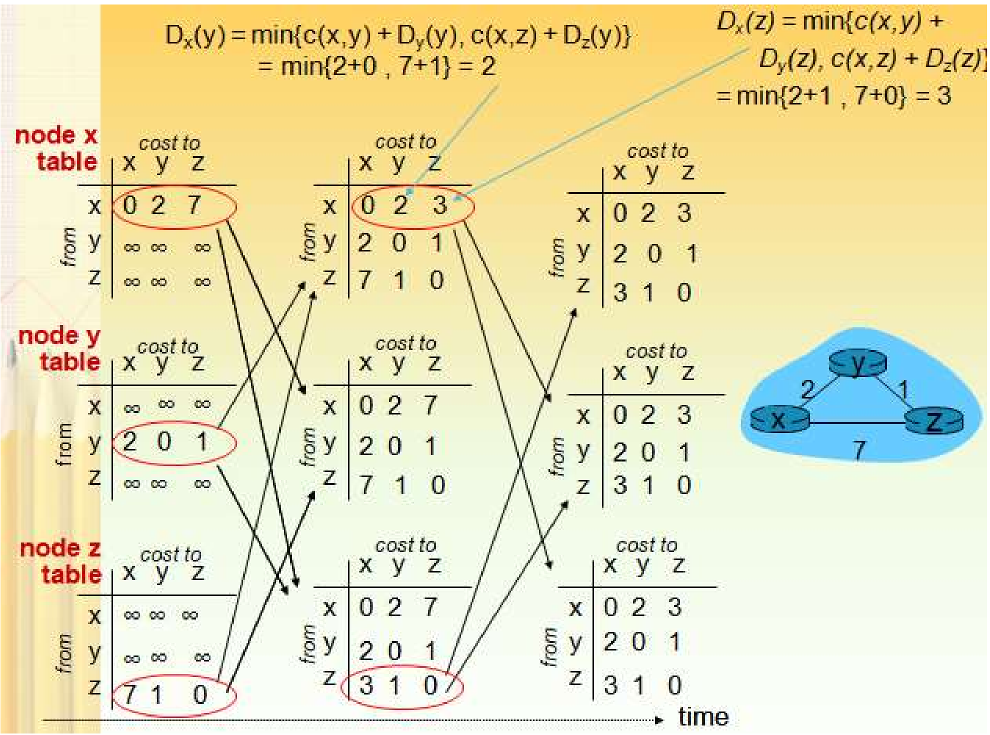
□ After this initial configuration phase, the CDN can do its main job of distributing content. When any client wants to see any video, the CDN’s DNS returns the anycast address, no matter where the client is located.

□ When the client sends a packet to that IP address, the packet is routed to the —closest‖ cluster as determined by the preconfigured forwarding tables, which were configured with BGP.


4b
4a
4c
AS4
2c
2a
3c
3a
1c
2b
AS2
1a
1b
3b
AS3
1d
AS1
Receive BGP advertisements for 212.21.21.21 from AS1 and from AS4. Forward towards Server B since it is closer.
Advertise 212.21.21.21
Advertise 212.21.21.21
CDN Server A
CDN Server B

Q6 a)Consider there is a network consisting of 3 routers. The weights are mentioned on the edges. Weights could be distances or costs or delays. Find out the final routing tables for all the routers using Bellman-ford algorithm.





$D_x(y) = \min\{c(x,y) + D_y(y), c(x,z) + D_z(y)\}$
$= \min\{2+0 , 7+1\} = 2$

$D_x(z) = \min\{c(x,y) +$
$D_y(z), c(x,z) + D_z(z)\}$
$= \min\{2+1 , 7+0\} = 3$

node x table

from \ cost to	x	y	z
x	0	2	7
y	∞	∞	∞
z	∞	∞	∞

from \ cost to	x	y	z
x	0	2	3
y	2	0	1
z	7	1	0

from \ cost to	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

node y table

from \ cost to	x	y	z
x	∞	∞	∞
y	2	0	1
z	∞	∞	∞

from \ cost to	x	y	z
x	0	2	7
y	2	0	1
z	7	1	0

from \ cost to	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

node z table

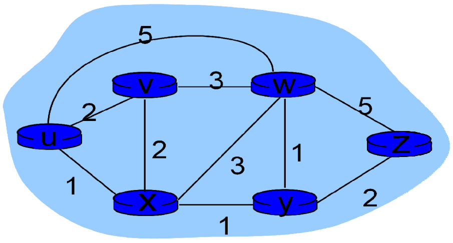
from \ cost to	x	y	z
x	∞	∞	∞
y	∞	∞	∞
z	7	1	0

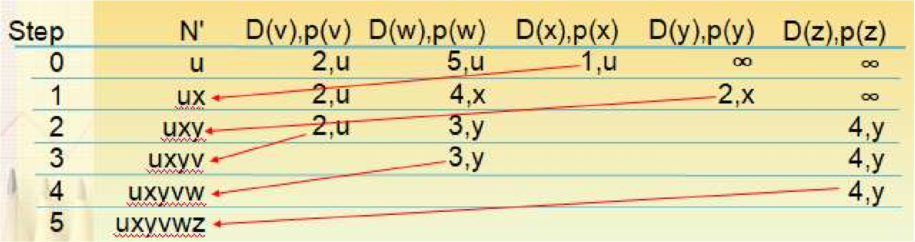
from \ cost to	x	y	z
x	0	2	7
y	2	0	1
z	3	1	0

from \ cost to	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

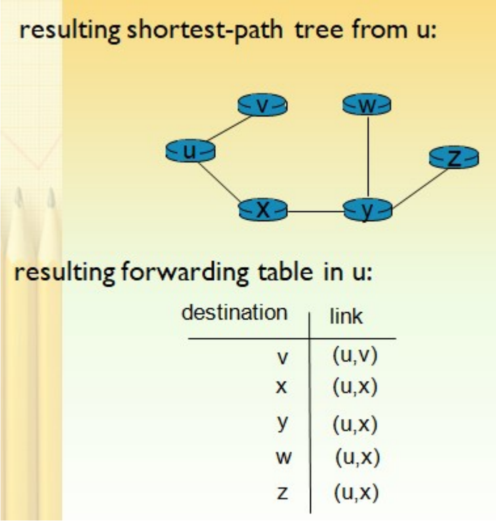
time

Q6 b)Deduce the shortest path tree using Dijkstra's algorithm for the following network. Assume source node as *u*.





Step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					



resulting shortest-path tree from u:

resulting forwarding table in u:

destination	link
v	(u,v)
x	(u,x)
y	(u,x)
w	(u,x)
z	(u,x)

****