[6003]-349 ENS (2023)

Q1a)

CIRCUIT SWITCHING	PACKET SWITCHING
→ There is physical connection between transmitter & receiver	→ No physical path is established between transmitter & receiver
→ All packets use same path	→ packet travels independently.
→ Needs an end to end path before data transmission	→ No need of end to end path before data transmission
→ Reverse the entire bandwidth in advance	→ Does not reserve bandwidth in advance
→ wastage of bandwidth	→ No wastage of bandwidth.
→ Recording of packet never happens	→ Recording of packet is possible

b)

→ In RIP routing updates are exchanged between neighbours approximately every 30 sec called as RIP response message.

→ response message sent by router or contains list of upto 25 destination networks within an autonomous system. Response messages are known as RIP advertisements.

→ RIP routers exchange info. advertisements approximately every 30 sec. if router does not hear from its neighbour at least once every 180 seconds then neighbour is considered no longer reachable i.e either neighbour has died or connecting link has gone down. when this happens RIP modifies local forwarding table & then propagates this info by sending advertisements to neighbouring routers.

→ router can also request info. about its neighbours cost to a given destination using RIP request message. Routers send RIP request & response message to each other using UDP port no. 520

c) Given:

IP address : 192.168.5.71

subnet: /26

i) Subnet mask.

/26 means 26 bits → network part

6 bits → host part

Hence subnet mask is:

255.255.255.192

ii) First IP address.

range of IP address for /26 network → 64

first IP address in series for this range → 192.168.5.0

∴ first IP address: → 192.168.5.64

iii) last IP address

set all host bits to 1

∴ last IP address:

192.168.5.127

Q49

→ RTP header size is 32bits

→ fields in headers are version P, X, CC, M, payload type sequence number, timestamp, synchronization source identifier & contributing source identifier.

1) Version: size of version field is 2 bits. It indicates version number. the current version is 2

2) P bits: size is 1 bit P bit indicates that the packet has been padded to multiple of 4 bytes.

3) X bit. Size is again 1bit indicates extension header is present.

4) CC field: size of CC field is 4 bits. used for indicating no. of source present. range 0 to 15

5) M bit. marker bit is of 1 bit. this bit used to indicate start of the frame. it may be video frame. start of word in an audio channel.

6) payload type: size of payload type field is 7 bits. used for indicating encoding algorithm has been used determine interpretation by application.

7) Sequence no: 16 bit field incremented by one each time RTP packet is sent. no. can be used by receiver to detect packet loss & to recover packet sequence. initial value is selected at random.

8) Time stamp: 32 bits no. specifies sampling instant of first byte in the RTP data packet. value helps to reduce jitter at receiver by decoupling playback from packet arrival time.

9) Synchronisation source identifier: tells which stream packet belongs.

10) Contributing source identifier: This is use of 0 to 15 thirty two bit item specifies contributing sources for payload contained in packet.

Q4b Services provided by Transport layer.

1) Segmentation & Reassembly:
- Segmentation: breaks larger messages into small segments. each segment assigned a sequence no. to be reassembled correctly.
- Reassembly: reassembles original message based on sequence no.

2) error detection & correction.
→ use checksums to detect any corruption during transmission In case of error, it may request retransmission.

3) Flow control:
→ ensures sender does not overwhelm receiver with too much data. it uses sliding windows to manage
- rate of transmission of data.

4) multiplexing & demultiplexing
→ allows multiple applications/process on device to use network simultaneously. & demultiplexing: the receiving TS uses these port no. to deliver data to correct process.

5) Congestion control:
→ also monitors network condition & regulates rate at which data is sent to avoid congestion.

6) Reliable data transfer:
→ protocols like TCP provide reliability through features such as acknowledgements, timeouts & retransmission

Q4c) Given: 06 32 00 0D 00 1C E2 17

i) Source port no: $(0632)^{16}$ = 1586

ii) Destn port no: $(000D)^{16}$ = 13

iii) Total length: $(001C)^{16}$ = 28 bytes.

Q5a)

HTTP

→ HyperText Transfer Protocol used for transferring hypertext & other types of data on the web.

→ Functioning: facilitates communication between clients & servers. allowing users to access web pages & resources.

→ Stateless protocol: each request response pair is independent with no retained state b/w transactions

→ Transport layer: typically operated over TCP to ensure reliable data transmission.

HTTP Request message.

Structure

→ Request Line: contains method (GET, POST), resource URL & HTTP version.

→ Headers: provide additional information (Host, Accept)

→ optional body: present in methods like (POST / PUT, containing data sent to server.

Response message.

Structure.

- Status line: contain HTTP version, status code (200 OK)
- Headers: include metadata about response (content-type, content length)
- optional body: contains requested resource (HTML content, images)

Q5b

MIME

→ stands for multipurpose internet mail extensions.

⇒ It is supplementary protocol allows non ASCII data to be sent through SMTP.

→ MIME designed by IETF allow transmission of non ASCII data via email

→ allows arbitrary data to be encoded in ASCII for normal transmission.

→ All media types sent/recieved over world wide web are encoded using different MIME types.

→ Messages sent using MIME encoding include info the describes type of data & encoding that was used.

Links

→ MIME has five headers.
1) MIME version
2) content type
3) content - transfer - encoding
4) content - id
5) content - description.

→ MIME types & subtypes.
content type must contain a identifier.
- content type
- content subtype.

→ There are seven standardised content types that can appear in MIME content-type declaration

SMTP
→ simple mail transfer protocol.
→ transfers message from sender's mail server to recipients mail servers.

→ interacts with local mail system & not user.

→ uses TCP socket on port 25 to transfer email reliably from client to server.

→ email is temporarily stored on local & eventually transferred directly to receiving server.

→ mail client application interacts with local SMTP server to initiate delivery of email message.

→ There is input & output queue at interface b/w local mail system & client & server parts of SMTP.

→ client is considered with initiating transfer of mail to another system while server concerned with receiving mail. Before email message can be transferred application process must be set up. TCP connection to local SMTP server. local mail system retains mailbox for each user into which user can deposit / retrieve mail. mail handling system must use unique addressing system.

→ Addressing system had 2 parts A local part & global part, local part is username & is uniquely only within local mail system. global part of address is domain name (identifying of host)

Symmetric key cryptography	Assymetric key cryptography
→ same key is used for encryption	→ one key for encryption & other key for decryption.
→ very fast	→ slower
→ key exchange is big problem	→ key exchange not a problem
→ Also called secret key encryption	→ also called public key encryption.
→ key must be kept secret	→ one of the 2 keys must be kept secret.
→ cannot be used for digital signatures	→ can be used for digital signatures

Q7b

→ message is to be transferred from source to destination across some sort of internet. Both sides must cooperate for exchange of data.

→ logical information channel is established by defining route through internet from source to destination.

→ All techniques for providing security have 2 components.

1) security related transformation on information to be sent.

2) Some secret info shared by 2 principles hoped unknown to opponents

Basic tasks designing a particular security service.

1) design algorithm for performing security related transformation.

2) Generate secret info to be used with algorithm.

3) Develop methods for distribution & sharing of secret info.

4) Security protocol to be used by 2 principles that makes use of security algorithm & secret info to achieve a particular security service.

Q7 c)

various securing mechanism are encipherment, digital signature, access control, data integrity, etc.

1) encipherment: use of mathematical algo. to transform data into form that is not readily intelligible.

2) digital signature: allows recipient of data unit to prove source & integrity of data unit & protect against forgery.

3) Access control: variety of mechanisms enforce access to rights to resources

4) data integrity: variety of mechanisms used to ensure integrity of data unit or stream of data units.

5) Authentication exchange: mechanism intended to ensure identity of an entity by means of info exchange.

6) Traffic padding:
insertion of bits into gaps in data stream to frustrate traffic analysis attempts.