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

Internal Assessment Test 5 – Feb 2022

Sub:	Computer Networks and Security					Sub Code:	18CS52	Branch:	ISE	
Date:	05/02/2022	Duration:	90 min's	Max Marks:	50	Sem/Sec:	V A, B & C		OBE	
Answer any FIVE FULL Questions								MARKS	CO	RBT
1	Identify the protocol using the port numbers 20 and 21 used for communication and explain its command and replies.							[10]	CO1	L3
2a)	Explain HTTP with persistent connection and non-persistent connection.							[5]	CO1	L2
2b)	Explain about DNS Records and Messages.							[5]	CO1	L2
3a)	Explain about Distributed Hash Table (DHT)							[5]	CO1	L2
3b)	Explain about multiplexing and de-multiplexing concepts in transport layer							[5]	CO2	L2

P.T.O.

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

Internal Assessment Test 5 – Feb 2022

Sub:	Computer Networks and Security					Sub Code:	18CS52	Branch:	ISE	
Date:	05/02/2022	Duration:	90 min's	Max Marks:	50	Sem/Sec:	V A, B & C		OBE	
Answer any FIVE FULL Questions								MARKS	CO	RBT
1	Identify the protocol using the port numbers 20 and 21 used for communication and explain its command and replies.							[10]	CO1	L3
2a)	Explain HTTP with persistent connection and non-persistent connection.							[5]	CO1	L2
2b)	Explain about DNS Records and Messages.							[5]	CO1	L2
3a)	Explain about Distributed Hash Table (DHT)							[5]	CO1	L2
3b)	Explain about multiplexing and de-multiplexing concepts in transport layer							[5]	CO2	L2

P.T.O.

4 (a)	Explain about Fairness in UDP and TCP	[05]	CO2	L1
4 (b)	Discuss HTTP and its commands and replies.	[05]	CO2	L1
5	Identify the suitable protocol for error control mechanism to satisfying the following conditions and explain its working with a neat flow diagram It is allows the receiver to accept & buffer the data packets following a damaged or lost one and then retransmits only those data packets which were lost or damaged in the network channel during transmission.	[10]	CO2	L3
6	Design a FSM for the RDT which handles garbled ACK/NAKs	[10]	CO2	L2

Faculty Signature CCI Signature HOD Signature

4 (a)	Explain about Fairness in UDP and TCP	[05]	CO2	L1
4 (b)	Discuss HTTP and its commands and replies.	[05]	CO2	L1
5	Identify the suitable protocol for error control mechanism to satisfying the following conditions and explain its working with a neat flow diagram It is allows the receiver to accept & buffer the data packets following a damaged or lost one and then retransmits only those data packets which were lost or damaged in the network channel during transmission.	[10]	CO2	L3
6	Design a FSM for the RDT which handles garbled ACK/NAKs	[10]	CO2	L2

Faculty Signature CCI Signature HOD Signature

Scheme of Evaluation Internal Assessment Test 5 – Feb 2022

Sub:	Computer Networks and Security							Code:	18CS52
Date:	01/02/2022	Duration:	90mins	Max Marks:	50	Sem:	V	Branch:	ISE

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

Question #		Description	Marks Distribution		Max Marks
1		Identify the protocol using the port numbers 20 and 21 used for communication and explain its command and replies. **Protocol Identification** **Commands and replies** **Explanation**	 1M 6M 3M	10M	10M
2	a)	Explain HTTP with persistent connection and non-persistent connection. **Persistent Connection** **Non- Persistent Connection** **Explanation**	 2M 2M 1M	5M	10M
2	b)	Explain about DNS Records and Messages. **Records** Messages **Explanation**	 2M 2M 1M	5M	

3	a)	Explain about Distributed Hash Table (DHT) **Definition** **Explanation** **Example**	 1M 2M 1M	5M	10M
3	b)	Explain about multiplexing and de-multiplexing concepts in transport layer **Multiplexing** **De-multiplexing** **Explanation**	 2M 2M 1M	5M	
4	a)	Explain about Fairness in UDP and TCP **Explanation UDP** **Explanation TCP**	 2.5M 2.5M	5M	10M
4	b)	Discuss HTTP and its commands and replies. **Explanation** **Commands**	 2M 3 M	5M	

5		Identify the suitable protocol for error control mechanism to satisfying the following conditions and explain its working with a neat flow diagram It is allows the receiver to accept & buffer the data packets following a damaged or lost one and then retransmits only those data packets which were lost or damaged in the network channel during transmission. **Identification of Protocol** **Explanation** **Steps** **Diagram**	1M 5M 1M 3M	10 M	10M
6		Design a FSM for the RDT which handles garbled ACK/NAKs **FSM with all proper states and events**	**10M**	**10M**	**10M**

Scheme Of Evaluation Internal Assessment Test 5 – Feb 2022

Sub:	Computer Networks and Security							Code:	18CS52
Date:	01/02/2022	Duration:	90mins	Max Marks:	50	Sem:	V	Branch:	ISE

Note: **Answer Any full five questions**

Q. 1 Identify the protocol using the port numbers 20 and 21 used for communication and explain its command and replies.

- FTP is used for transferring file from one host to another host.
- In order for the user to access the remote account, the user must provide user identification and a password. After providing this authorization information, the user can transfer files from the local file system to the remote file system and vice versa.
- The user first provides the hostname of the remote host, causing the FTP client process in the local host to establish a TCP connection with the FTP server process in the remote host.
- The user then provides the user identification and password, which are sent over the TCP connection as part of FTP commands.
- Once the server has authorized the user, the user copies one or more files stored in the local file system into the remote file system (or vice versa).
- FTP uses two parallel TCP connections to transfer a file, a control connection and a data connection.
- The control connection is used for sending control information between the two hosts—information such as user identification, password, commands to change remote directory, and commands to "put" and "get" files.
- The data connection is used to actually send a file.
- When a user starts an FTP session with a remote host, the client side of FTP (user) first initiates a control TCP connection with the server side (remote host) on server port number 21.
- The client side of FTP sends the user identification and password over this control connection. The client side of FTP also sends, over the control connection, commands to change the remote directory.
- When the server side receives a command for a file transfer over the control connection (either to, or from, the remote host), the server side initiates a TCP data connection to the client side.

FTP Commands and Replies

Some of the more common commands are given below:

• USER username: Used to send the user identification to the server.

• PASS password: Used to send the user password to the server.

• LIST: Used to ask the server to send back a list of all the files in the current remote directory. The list of files is sent over a (new and non-persistent) data connection rather than the control TCP connection.

• RETR filename: Used to retrieve (that is, get) a file from the current directory of the remote host. This command causes the remote host to initiate a data connection and to send the requested file over the data connection.

• STOR filename: Used to store (that is, put) a file into the current directory of the remote host.

Each command is followed by a reply, sent from server to client. The replies are three-digit numbers, with an optional message following the number.

• 331 Username OK, password required

• 125 Data connection already open; transfer starting

• 425 Can't open data connection

• 452 Error writing file

Q2) Explain HTTP with persistent connection and non-persistent connection.

If Separate TCP connection is used for each request and response, then the connection is said to be non persistent. If same TCP connection is used for series of related request and response, then the connection is said to be persistent.

HTTP with Non-Persistent Connections

Let's suppose the page consists of a base HTML file and 10 JPEG images, and that all 11 of these objects reside on the same server.

Further suppose the URL for the base HTML file is

http://www.someSchool.edu/someDepartment/home.index

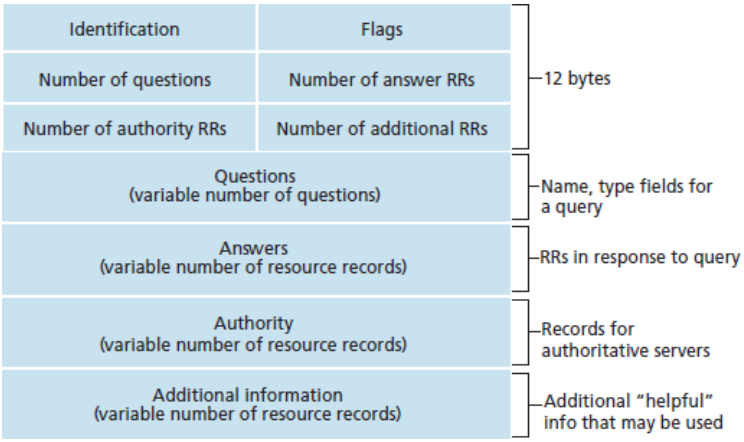
Here is what happens:

1. The HTTP client process initiates a TCP connection to the server www.someSchool.edu on port number 80, which is the default port number for HTTP. Associated with the TCP connection, there will be a socket at the client and a socket at the server.
2. The HTTP client sends an HTTP request message to the server via its socket. The request

message includes the path name /someDepartment/home.index.

3. The HTTP server process receives the request message via its socket, retrieves the object /someDepartment/home.index from its storage (RAM or disk), encapsulates the object in an HTTP response message, and sends the response message to the client via its socket.
4. The HTTP server process tells TCP to close the TCP connection.
1. The HTTP client receives the response message. The TCP connection terminates. The message indicates that the encapsulated object is an HTML file. The client extracts the file from the response message, examines the HTML file, and finds references to the 10 JPEG objects.
2. The first four steps are then repeated for each of the referenced JPEG objects.

Q2b)Explain about DNS Records and Messages.



- The first 12 bytes is the header section, which has a number of fields.
- The first field is a 16-bit number that identifies the query. This identifier is copied into the reply message to a query, allowing the client to match received replies with sent queries.
- There are a number of flags in the flag field.

  A 1-bit query/reply flag indicates whether the message is a query (0) or a reply (1). A1-bit authoritative flag is set in a reply message when a DNS server is an authoritative server for a queried name.

  A 1-bit recursion-desired flag is set when a client (host or DNS server) desires that the DNS server perform recursion when it doesn't have the record.

  A 1-bit recursion available field is set in a reply if the DNS server supports recursion.
- In the header, there are also four number-of fields. These fields indicate the number of occurrences of the four types of data sections that follow the header.

- For the primary authoritative server for networkutopia.com, the registrar would insert the following two resource records into the DNS system:
- (networkutopia.com, dns1.networkutopia.com, NS)

  (dns1.networkutopia.com, 212.212.212.1, A)

Q3 a) Explain about Distributed Hash Table (DHT)

distributed hash table (DHT) is a distributed system that provides a lookup service similar to a hash table: key-value pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. The main advantage of a DHT is that nodes can be added or removed with minimum work around re-distributing keys. Keys are unique identifiers which map to particular values, which in turn can be anything from addresses, to documents, to arbitrary data.[1] Responsibility for maintaining the mapping from keys to values is distributed among the nodes, in such a way that a change in the set of participants causes a minimal amount of disruption. This allows a DHT to scale to extremely large numbers of nodes and to handle continual node arrivals, departures, and failures.

Because of the decentralization, fault tolerance, and scalability of DHTs, they are inherently more resilient against a hostile attacker than a centralized system

Open systems for distributed data storage that are robust against massive hostile attackers are feasible

A DHT system that is carefully designed to have Byzantine fault tolerance can defend against a security weakness, known as the Sybil attack, which affects most current DHT designs. Whanau is a DHT designed to be resistant to Sybil attacks.

Petar Maymounkov, one of the original authors of Kademlia, has proposed a way to circumvent the weakness to the Sybil attack by incorporating social trust relationships into the system design. The new system, codenamed Tonika or also known by its domain name as 5ttt, is based on an algorithm design known as "electric routing" and co-authored with the mathematician Jonathan Kelner. Maymounkov has now undertaken a comprehensive implementation effort of this new system. However, research into effective defences against Sybil attacks is generally considered an open question, and wide variety of potential defences are proposed every year in top security research conferences.

Q.3 b) Explain about multiplexing and de-multiplexing concepts in transport layer

A process can have one or more sockets.
• The sockets are us.ed to pass data from the network to the process and vice versa.
1) multlplexing
x At the sender, the transport layer
.gathers data chunks at the source-host from different sockets
—• encapsulates data-chunk with header to create s.egments and
— passes the segments to the network-layer.
The job of combining the data-chunks from different sockets to create a segment is called
muItlp[exfng.
2) Demultlplexlng

At the receiver, the transport layer
examines the fields in the segments to identify the receiving -socket and directs the segment to the receiving socket.
» The job of delivering the data in a segment to the correct socket is called demuloplexing.
In the m.lddle host, the transport layer musr demultiplex segments arriving from the network-
layer to either process P1 or P2.
4 The arriving segment's data is directed to the corresponding process's socket.
4.A) Explain Diffie-Hellman key exchange algorithm in detail.HTTP Request Message:

4. B) Explain about Fairness in UDP and TCP.

TCP is a connection-oriented protocol, whereas UDP is a connectionless protocol. A key difference between TCP and UDP is speed, as TCP is comparatively slower than UDP. Overall, UDP is a much faster, simpler, and efficient protocol, however, retransmission of lost data packets is only possible with TCP.

TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.

UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.

5. Identify the suitable protocol for error control mechanism to satisfying the following conditions and explain its working with a neat flow diagram, It is allows the receiver to accept & buffer the data packets following a damaged or lost one and then retransmits only those data packets which were lost or damaged in the network channel during transmission.

2.4.4 Selective Repeat (SR)

- Problem with GBN:
  - ➢ GBN suffers from performance problems.
  - ➢ When the window-size and bandwidth-delay product are both large, many packets can be in the pipeline.
  - ➢ Thus, a single packet error results in retransmission of a large number of packets.
- Solution: Use Selective Repeat (SR).

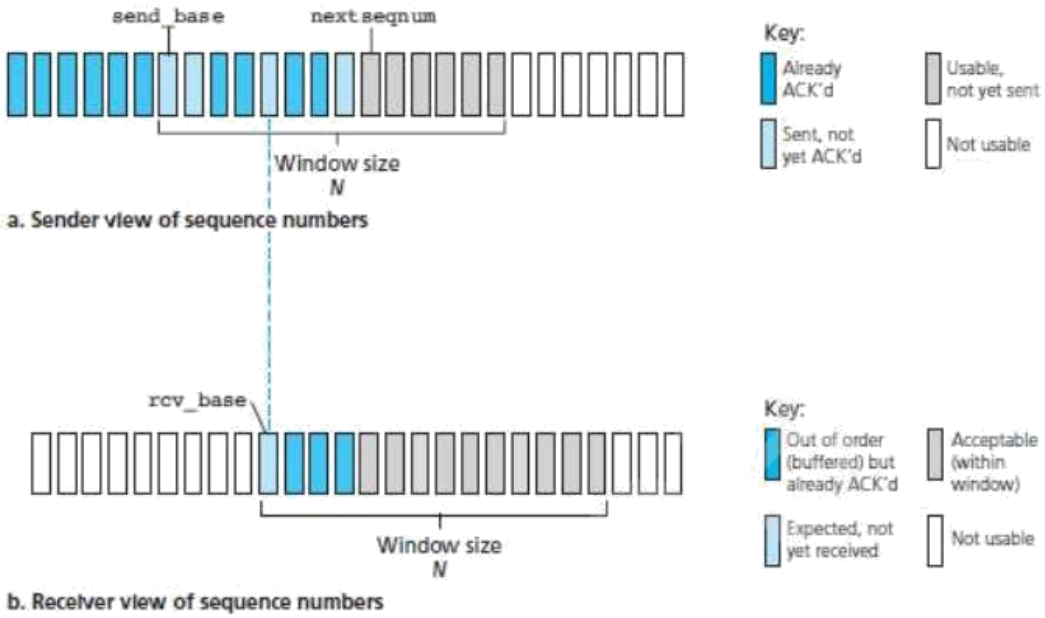


Figure 2.21: Selective-repeat (SR) sender and receiver views of sequence-number space

- The sender retransmits only those packets that it suspects were erroneous.
- Thus, avoids unnecessary retransmissions. Hence, the name "selective-repeat".
- The receiver individually acknowledge correctly received packets.
- A window-size N is used to limit the no. of outstanding, unacknowledged packets in the pipeline.
- Figure 2.21 shows the SR sender's view of the sequence-number space.

2.4.4.1 SR Sender

- The various actions taken by the SR sender are as follows:

1) Data Received from above.

➢ When data is received from above, the sender checks the next available sequence-number for the packet.

➢ If the sequence-number is within the sender's window;

Then, the data is packetized and sent;

Otherwise, the data is buffered for later transmission.

2) Timeout.

➢ Timers are used to protect against lost packets.

➢ Each packet must have its own logical timer. This is because

→ only a single packet will be transmitted on timeout.

3) ACK Received.

➢ If an ACK is received, the sender marks that packet as having been received.

➢ If the packet's sequence-number is equal to send_base, the window base is increased by the smallest sequence-number.

➢ If there are untransmitted packets with sequence-numbers that fall within the window, these packets are transmitted.

2.4.4.2 SR Receiver

- The various actions taken by the SR receiver are as follows:

1) Packet with sequence-number in [rcv_base, rcv_base+N-1] is correctly received.

- In this case,
  - → received packet falls within the receiver's window and
  - → selective ACK packet is returned to the sender.
- If the packet was not previously received, it is buffered.
- If this packet has a sequence-number equal to rcv_base, then this packet, and any previously buffered and consecutively numbered packets are delivered to the upper layer.
- The receive-window is then moved forward by the no. of packets delivered to the upper layer.
- For example: consider Figure 2.22.
  - ¤ When a packet with a sequence-number of rcv_base=2 is received, it and packets 3, 4, and 5 can be delivered to the upper layer.

2) Packet with sequence-number in [rcv_base-N, rcv_base-1] is correctly received.

- In this case, an ACK must be generated, even though this is a packet that the receiver has previously acknowledged.

3) Otherwise.

- Ignore the packet.

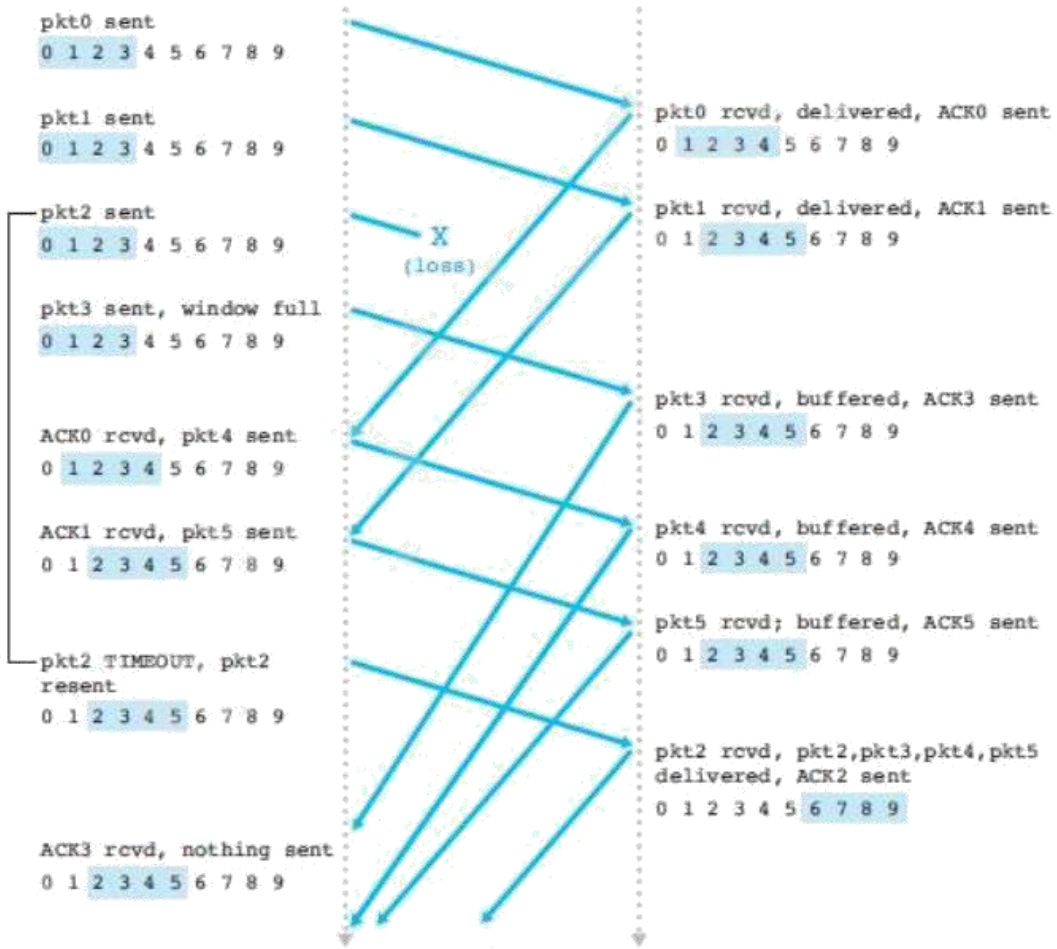


Figure 2.22: SR operation