NETWOK PROTOCOLS (CS E77)
FINAL YEAR / SEVENTH SEMESTER (2022-2023)
ANSWER KEY
PART A – (10*2=20)

1. **What is the use of BOOT?**

The Bootstrap Protocol (BOOTP) is a UDP/IP-based protocol which allows a booting host to configure itself dynamically and without user supervision.

BOOTP provides a means to notify a host of its assigned IP address, the IP address of a boot server host and the name of a file to be loaded into memory and executed.

Other configuration information such as the local subnet mask, the local time offset, the addresses of default routers and the addresses of various Internet servers, can also be communicated to a host using BOOTP.

2. **What are the management components of SNMP?**
   - SNMP Manager
   - SNMP agent
   - Management Information Base
3. **List the services that are offered by TCP to the processes at the application layer.**
   - Stream delivery service
   - Sending and receiving buffers
   - Bytes and segments
   - Full Duplex Service
   - Connection Oriented Service.
   - Reliable Service

4. **What is the use of Lightweight Presentation Protocol?**

Lightweight Presentation Protocol (LPP) describes an approach for providing “stream- lined” support of OSI application services on top of TCP/IP-based network for some constrained environments. LPP was initially derived from a requirement to run the ISO Common Management Information Protocol (CMIP) in TCP/IP-based networks.

5. **What is DVMRP?**

Distance Vector Multicast Routing Protocol (DVMRP) is an Internet routing protocol that provides an efficient mechanism for connectionless message multicast to a group of hosts across an internetwork. DVMRPis an –interior gateway protocol‖ (IGP); suitable for use within an autonomous system, but not between different autonomous systems. DVMRP is not currently developed for use in routing non- multicast datagram’s, so a router that routes both multicast and unicast datagram’s must run two separate routing processes.

6. **Define IP. List some of the common internet protocols.**

The Internet Protocol (IP) is a network- layer (Layer 3 in the OSI model) protocol that contains addressing information and some control information to enable packets to be routed in a network. IP is the primary network- layer protocol in the TCP/IP protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols. IP is equally well suited for both LAN and WAN communications.

Common internet protocols:

- TCP/IP
- UDP/IP
- HTTP
- FTP

7. **What are the major problems of Mobile IP?**
   It seems to be inefficient due to the extra distance that a message has to travel.

8. **Why do we need HDLC?**
   The High Level Data Link Control (HDLC) protocol, an ISO data link layer protocol based on the IBM SDLC, ensures that data passed up to the next layer has been received exactly as transmitted (i.e. error free, without loss and in the correct order). Another important function of HDLC is flow control, which ensures that data is transmitted only as fast as the receiver can receive it. There are two distinct HDLC implementations: HDLC NRM (also known as SDLC) and HDLC Link Access Procedure Balanced (LAPB). The later is the more popular implementation. HDLC is part of the X.25 stack.

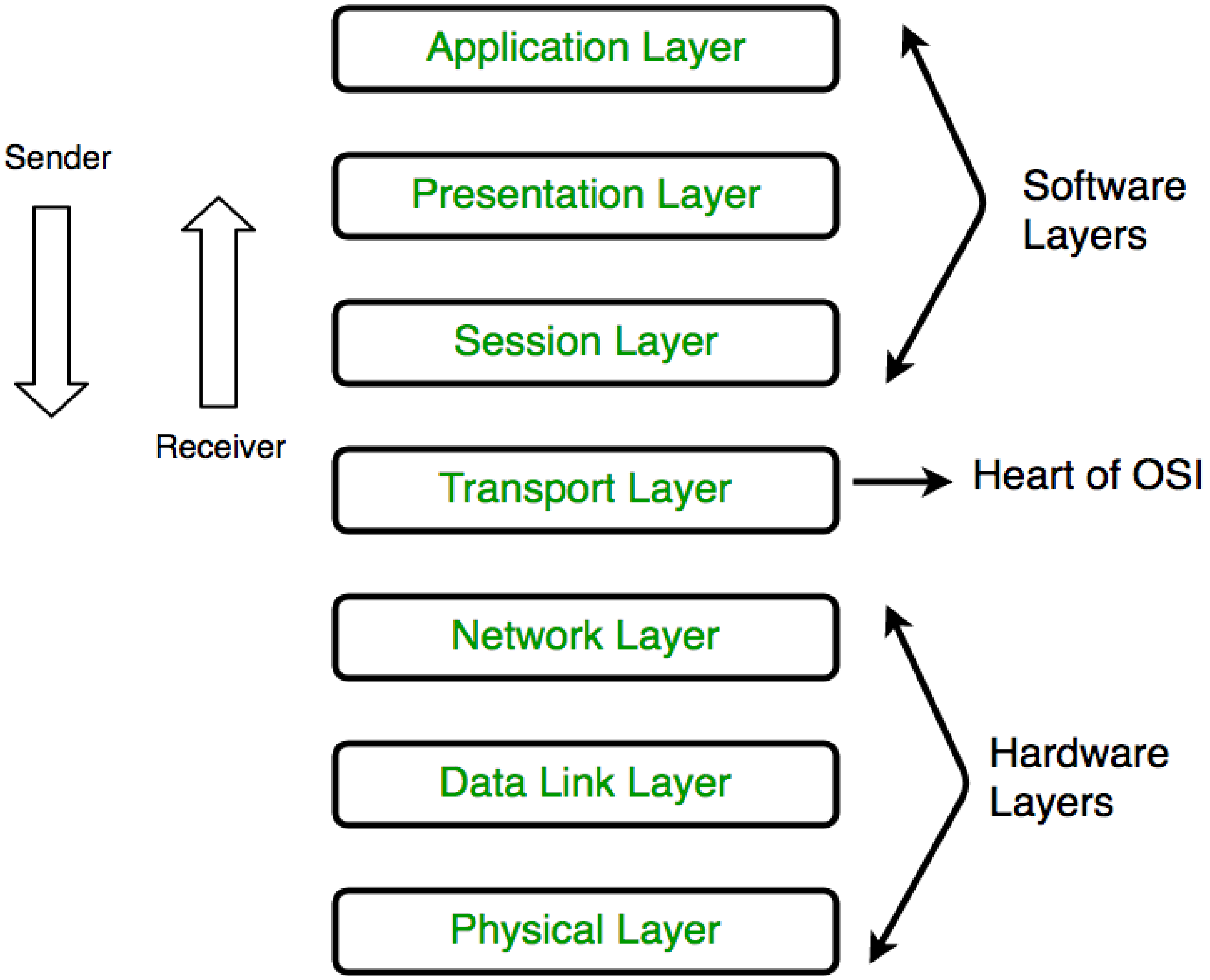
9. **What is IPSec?**
   Internet Security architecture (IPsec) defines the security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPsec can be used to protect one or more “paths” between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

10. **Define IP telephony.**
    Voice over IP (VOIP) uses the Internet Protocol (IP) to transmit voice as packets over an IP network. Using VOIP protocols, voice communications can be achieved on any IP network regardless whether it is Internet, Intranet or Local Area Networks (LAN). In a VOIP enabled network, the voice signal is digitized, compressed and converted to IP packets and then transmitted over the IP network. VOIP signaling protocols are used to set up and tear down calls, carry information required to locate users and negotiate capabilities.

PART A – (11*5=55)

UNIT –I

11. Discuss in detail about the OSI model with a neat diagram.



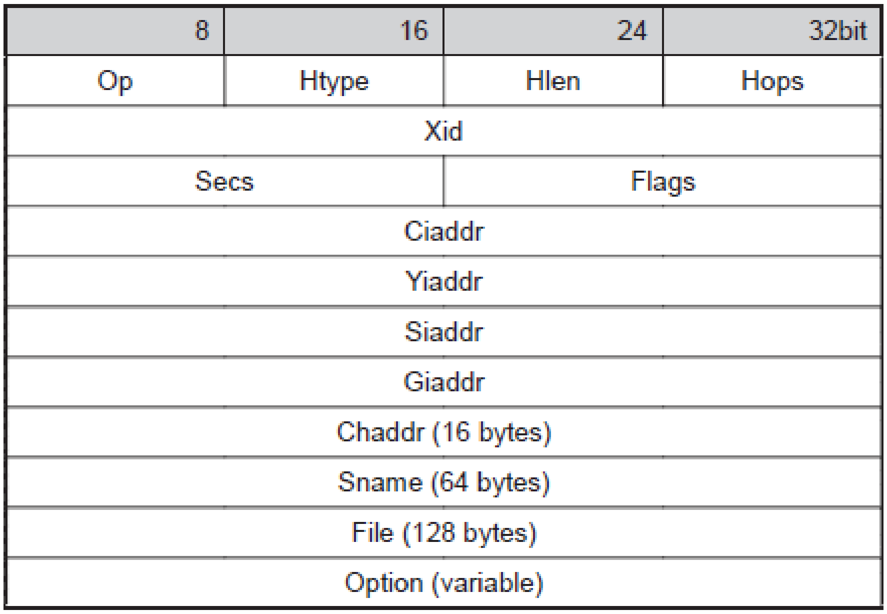
12. Write short notes on:

A) DHCP

Protocol Description

Dynamic Host Configuration Protocol (DHCP) is a communications protocol enabling network administrators manage centrally and to automate the assignment of IP addresses in a network. In an IP network, each device connecting to the Internet needs a unique IP address. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

Protocol Structure



8	16	24	32bit
Op	Htype	Hlen	Hops
Xid			
Secs		Flags	
Ciaddr			
Yiaddr			
Siaddr			
Giaddr			
Chaddr (16 bytes)			
Sname (64 bytes)			
File (128 bytes)			
Option (variable)			

B) SMTP

Protocol Description

Simple Mail Transfer Protocol (SMTP) is a protocol designed to transfer electronic mail reliably and efficiently. SMTP is a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and provides notification regarding incoming mail.

SMTP is independent of the particular transmission subsystem and requires only a reliable ordered data stream channel. An important feature of SMTP is its capability to transport mail across networks, usually referred to as “SMTP mail relaying”. A network consists of the mutually- TCP-accessible hosts on the public Internet, the mutually-TCP-accessible hosts on a firewall- isolated TCP/IP Intranet, or hosts in some other LAN or WAN environment utilizing a non-TCP transport- level protocol. Using SMTP, a process can transfer mail to another process on the same network or to some other network via a relay or gateway process accessible to both networks.

Protocol Structure

Command	Description
DATA	Begins message composition.
EXPN <string>	Returns names on the specified mail list.
HELO <domain>	Returns identity of mail server.
HELP <command>	Returns information on the specified command.
MAIL FROM <host>	Initiates a mail session from host.
NOOP	Causes no action, except acknowledgement from server.
QUIT	Terminates the mail session.
RCPT TO <user>	Designates who receives mail.
RSET	Resets mail connection.
SAML FROM <host>	Sends mail to user terminal and mailbox.
SEND FROM <host>	Sends mail to user terminal.
SOML FROM <host>	Sends mail to user terminal or mailbox.
TURN	Switches role of receiver and sender.
VRFY <user>	Verifies the identity of a user.

UNIT –II

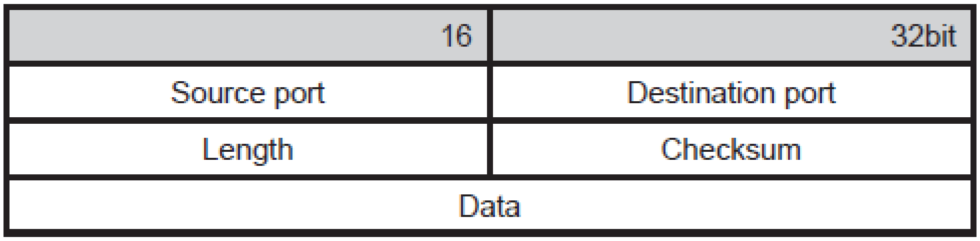
13. Explain About User Datagram Format,Udp operations and also discuss how checksum is computed in udp.

Protocol Description

UDP is a connectionless transport layer (layer 4) protocol in the OSI model which provides a simple and unreliable message service for transaction-oriented services. UDP is basically an interface between IP and upper- layer processes. UDP protocol ports distinguish multiple applications running on a single device from one another.

Since many network applications may be running on the same machine, computers need something to make sure the correct software application on the destination computer gets the data packets from the source machine and some way to make sure replies get routed to the correct application on the source computer. This is accomplished through the use of the UDP “port numbers”

Protocol Structure



16	32bit
Source port	Destination port
Length	Checksum
Data	

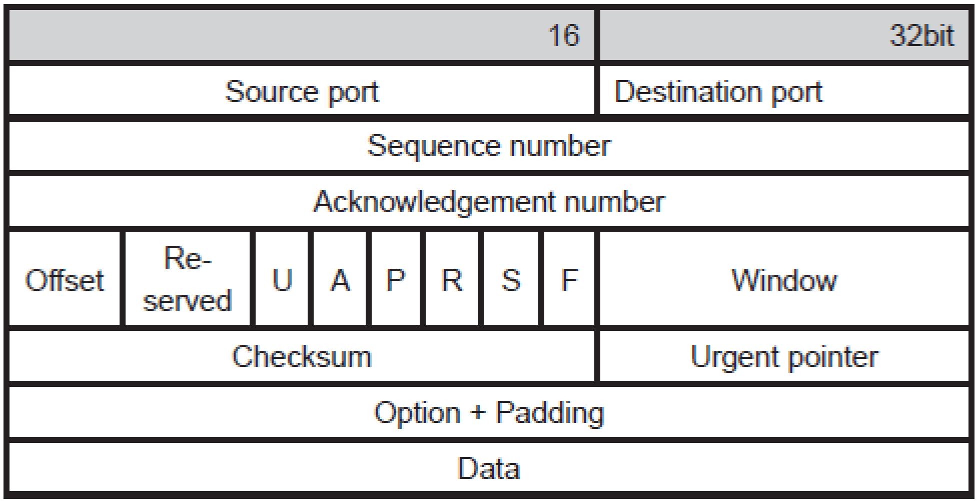
14..Discuss the functionally of TCP along with its message format.also discuss about the connection establishment procedure using TCP.

Protocol Description

Transmission Control Protocol (TCP) is the transport layer protocol in the TCP/IP suite, which provides a reliable stream delivery and virtual connection service to applications through the use of sequenced acknowledgment with retransmission of packets when necessary. Along with the Internet Protocol (IP), TCP represents the heart of the Internet protocols.

Since many network applications may be running on the same machine, computers need something to make sure the correct software application on the destination computer gets the data packets from the source machine and some way to make sure replies get routed to the correct application on the source computer. This is accomplished through the use of the TCP “port numbers”. The combination of IP address of a network station and its port number is known as a “socket” or an “endpoint”. TCP establishes connections or virtual circuits between two “endpoints” for reliable communications.

Protocol Structure



16								32bit
Source port								Destination port
Sequence number								
Acknowledgement number								
Offset	Re-served	U	A	P	R	S	F	Window
Checksum								Urgent pointer
Option + Padding								
Data								

UNIT –III

15.Explain the salient features of IPv6 in detail.

Protocol Description

IPv6 is the new version of Internet Protocol (IP) based on IPv4, a network-layer (Layer 3) protocol that contains addressing information and some control information enabling packets to be routed in the network. There are two basic IP versions: IPv4 and IPv6. IPv6 is also called next generation IP or IPng. IPv4 and IPv6 are de- multiplexed at the media layer. For example, IPv6 packets are carried over Ethernet with the content type 86DD (hexadecimal) instead of IPv4’s 0800. This document describes the IPv6 details. The IPv4 is described in a separate document.

Protocol Structure

4	**12**		**16**	**24**	**32bit**
Version	**Priority**		**Flow label**		
Identification				**Flags**	**Fragment offset**
Payload length		**Next header**		**Hop limit**	
Source address(128 bits)					
Destination address(128 bits)					

16.Describe ICMP and its message format with examples.How is eror reporting and error detection done using ICMP ?

Protocol Description

Internet Control Message Protocol (ICMP) is an integrated part of the IP suite. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation or mis-operation. ICMP packet delivery is unreliable, so hosts can’t count on receiving ICMP packets for any network problems. The key ICMP functions are:

- Announce network errors,
- Announce network congestion.
- Assist Troubleshooting.
- Announce Timeouts.

The Internet Control Message Protocol (ICMP) was revised during the definition of IPv6. In addition, the multicast control functions of the IPv4 Group Membership Protocol (IGMP) are now incorporated in the

ICMPv6.

Protocol Structure

8	**16**	**32bit**
Type	**Code**	**Checksum**
Identifier		**Sequence number**
Address mask		

UNIT –IV

17.What is ARP and RARP ? Explain in detail.

Address Resolution Protocol (ARP) performs mapping of an IP address to a physical machine address (MAC address for Ethernet) that is recognized in the local network. For example, in IP Version 4, an address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the rules for making this correlation and providing address conversion in both directions.

Reverse Address Resolution Protocol (RARP) allows a physical machine in a local area network to request its IP address from a gateway server‘s Address Resolution Protocol (ARP) table or cache. A network administrator creates a table in a local area network‘s gateway router that maps the physical machines‘ (or Media Access Control - MAC) addresses to corresponding Internet Protocol addresses. When a new machine is set up, its RARP client program requests its IP address from the RARP server on the router. Assuming that an entry has been set up in the router table, the RARP server will return the IP address to the machine, which can store it for future use. RARP is available for Ethernet, Fiber Distributed-Data Interface, and Token Ring LANs.
The protocol header for RARP is the same as for ARP:

16		32 bit
Hardware type		Protocol type
HLen	PLen	Operation
Sender Hardware address		
Sender Protocol Address		
Target Hardware Address		
Target Protocol Address		

18.Illustrate IEEE 802.11 architecture with a neat diagram.

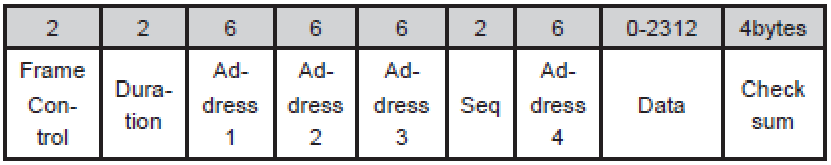
Protocol Description

The Wireless Local Area Network (WLAN) technology is defined by the IEEE 802.11 family of specifications. There are currently four specifications in the family: 802.11, 802.11a, 802.11b, and 802.11g. All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance instead of CSMA/CD) for path sharing.

- 802.11 -- applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band usingeither frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
- 802.11a -- an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in

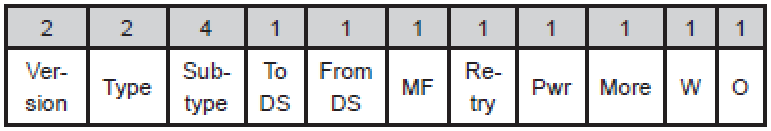
the 5GHz band.802.11a uses an orthogonal frequency division multiplexing (OFDM) encoding scheme rather than FHSS or DSSS. The 802.11a specification applies to wireless ATM systems and is used in access hubs.

- 802.11b (also referred to as 802.11 High Rate or Wi-Fi) -- an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b is a modification of the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- 802.11g -- offers wireless transmission over relatively short distances at 20 – 54 Mbps in the 2.4 GHz band. 801.11 protocol family MAC frame structure:



2	2	6	6	6	2	6	0-2312	4bytes
Frame Con-trol	Dura-tion	Ad-dress 1	Ad-dress 2	Ad-dress 3	Seq	Ad-dress 4	Data	Check sum

- Frame Control Structure:



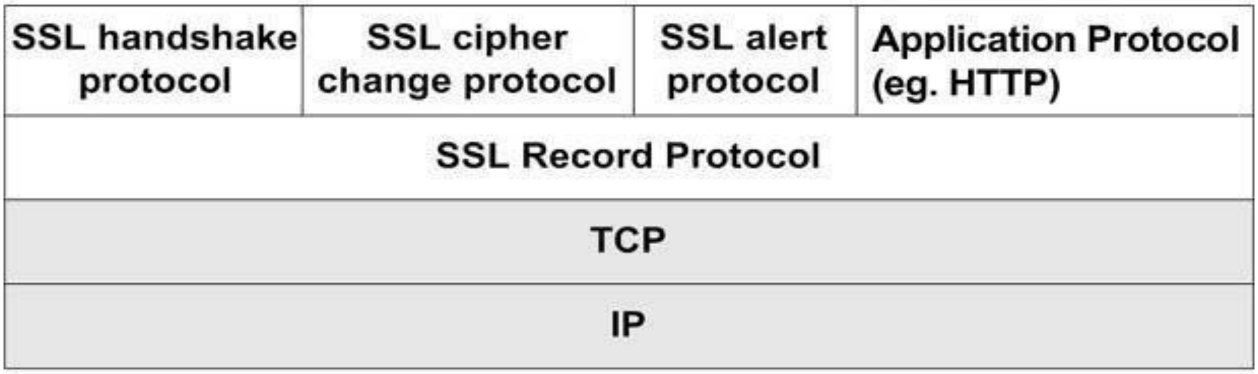
2	2	4	1	1	1	1	1	1	1	1
Ver-sion	Type	Sub-type	To DS	From DS	MF	Re-try	Pwr	More	W	O

UNIT –V

19.What is SSL/TLS ?Discuss in detail about the SSL services,protocols and IETF standard version of SSL with a neat diagram.

SSL and the Protocol Stack

- SSL between Transmission Control Protocol (TCP) layer and Application layer
- Actually 2 layers
  - Record
  - Secure Application
- Can run under any protocol that relies on TCP, including HTTP, LDAP, POP3, FTP



SSL handshake protocol	SSL cipher change protocol	SSL alert protocol	Application Protocol (eg. HTTP)
SSL Record Protocol			
TCP			
IP			

The Four Upper Layer Protocols

- Handshaking Protocol
  - Establish communication variables
- ChangeCipherSpec Protocol
  - Alert to a change in communication variables
- Alert Protocol
  - Messages important to SSL connections

- Application Encryption Protocol
  - Encrypt/Decrypt application data

Record Layer

- Frames and encrypts upper level data into one protocol for transport through TCP
- 5 byte frame
  - 1st byte protocol indicator
  - 2nd byte is major version of SSL
  - 3rd byte is minor version of SSL
  - Last two bytes indicate length of data inside frame, up to 2^{14}
- Message Authentication Code (MAC)

Message Authentication Code

- MAC secures connection in two ways
  - Ensure Client and Server are using same encryption and compression methods
  - Ensure messages sent were received without error or interference
- Both sides compute MACs to match them
- No match = error or attack

TLS Protocol Description

Transport Layer Security (TLS) Protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. At the lowest level, layered on top of some reliable transport protocol (TCP) is the TLS Record Protocol. The TLS Record Protocol provides connection security that has two basic properties:

- Private - Symmetric cryptography is used for data encryption (DES, RC4, etc.) The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol). The Record Protocol can also be used without encryption.
- Reliable - Message transport includes a message integrity check using a keyed MAC. Secure hash functions (SHA, MD5, etc.) are used for MAC computations. The Record Protocol can operate without a MAC, but is generally only used in this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters.

20. Write a detailed note on :

a) SSH

Protocol Description

SSH is a protocol for secure remote login and other secure network services over an insecure network. SSH consists of three major components:

The Transport Layer Protocol [SSH-TRANS] provides server authentication, confidentiality, and integrity. It may optionally also provide compression. The transport layer will typically be run over a TCP/IP connection, but might also be used on top of any other reliable data stream. SSH-Trans provides strong encryption, cryptographic host authentication, and integrity protection. Authentication in this protocol level is host-based; this protocol does not perform user authentication. A higher level protocol for user authentication can be designed on top of this protocol.

The User Authentication Protocol [SSH-USERAUTH]

The Connection Protocol [SSH-CONNECT]

b) Kerberos.

Kerberos is a network authentication protocol. Kerberos is designed to provide strong authentication for client/server applications by using secret-key cryptography. This is accomplished without relying on authentication by the host operating system, without basing trust on host addresses, without requiring physicalsecurity of all the hosts on the network, and under the assumption that packets traveling along the network canbe read, modified, and inserted at will. Kerberos performs authentication under these conditions as a trusted third-party authentication service by using conventional cryptography, i.e., shared secret key.

The Client/Server Authentication
ExchangeMessage direction
Message type

1. Client to Kerberos	KRB_AS_REQ
2. Kerberos to client	KRB_AS_REP or KRB_ERROR

The Client/Server Authentication Exchange

Message direction	**Message type**
Client to Application server	KRB_AP_REQ
[optional] Application server to client	KRB_AP_REP or KRB_ERROR

The Ticket-Granting Service (TGS)
Exchange Message direction
Message type

1. Client to Kerberos	KRB_TGS_REQ
2.	Kerberos to client

KRB_TGS_REP or KRB_ERRORThe KRB_SAFE Exchange
The KRB_PRIV
Exchange The
KRB_CRED Exchange