MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

IQAC

MUST KNOW CONCEPTS

MKC

CSE

2020-21

Course Code & Course Name : 19CSC07/Computer Networks

Year/Sem/Sec : II/IV/A&B

S.No.	Term	Notation (Symbol)	Concept / Definition / Meaning / Units / Equation / Expression	Units
			Unit-I : Introduction	
1.	**Computer Network**		A Computer Network is a set of computers connected together for the purpose of sharing resources	
2.	**Link**		A link of a network is one of the connections between the nodes of the network	
3.	**Node**		Any system or device connected to a network is also called a node	
4.	**Data Communication**		Data communication is the exchange of data (in the form of 1s and 0s) between two devices	
5.	**Router**		A node that is connected to two or more networks is commonly called as router or Gateway	
6.	**Protocols**		A network protocol is a set of rules followed by the network	
7.	**Local Area Network**	**LAN**	A local area network (LAN) is a computer network within a small geographical area.	
8.	**Metropolitan Area Network**	**MAN**	A metropolitan area network, or MAN.A MAN is larger than a LAN, which is typically limited to a single building or site	
9.	**Wide Area Network**	**WAN**	A wide area network (WAN) is a network that exists over a large-scale geographical area. A WAN connects different smaller networks	
10.	**Network Topology**		Network topology refers to the physical or logical layout of a network	
11.	**Mesh Topology**		Mesh topology is a type of networking where all nodes cooperate to distribute data amongst each other	
12.	**Ring Topology**		A ring topology is a network configuration in which device connections create a circular data path	
13.	**Bus Topology**		A bus topology is a network setup where each computer and network device is connected to a single cable or backbone	

14.	**Simplex**		Simplex is a communication channel that sends information in one direction only	
15.	**Half duplex**		In half duplex mode, data can be transmitted in both directions on a signal carrier but not at the same time	
16.	**Full duplex**		A full duplex communication channel is able to transmit data in both directions on a signal carrier at the same time.	
17.	**OSI Model**		OSI (Open Systems Interconnection) is a reference model for how applications communicate over a network	
18.	**Physical Layer**		Physical layer is the lowest layer of the OSI reference model. It is responsible for sending bits from one computer to another	
19.	**Data Link Layer**		Data link layer performs the most reliable node to node delivery of data	
20.	**Network Layer**		The main aim of this layer is to deliver packets from source to destination across multiple links (networks)	
21.	**Transport Layer**		The transport layer is the layer in the open system interconnection (OSI) model responsible for end-to-end communication over a network	
22.	**Session Layer**		The main aim is to establish, maintain and synchronize the interaction between communicating systems	
23.	**Presentation Layer**		• The Presentation Layer deals with the syntax and semantics of the information being exchanged	
24.	**Application Layer**		This layer is responsible for accessing the network by user	
25.	**TCP/IP Protocol**		TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet	
Unit-II : Data Link Layer				
26.	**Digital Signals**		A digital signal refers to an electrical signal that is converted into a pattern of bits	
27.	**Hub**		A hub, also called a network hub, is a common connection point for devices in a network	
28.	**Repeaters**		A repeaters is an electronic device that receives a signal and retransmits it	
29.	**Bridges**		A bridge is a type of computer network device that provides interconnection with other bridge networks that use the same protocol	
30.	**Redundancy**		shorter group of bits or extra bits may be appended at the destination of each unit	
31.	**Single bit error**		The term single bit error means that only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.	
32.	**Burst error**		Means that 2 or more bits in the data unit have changed	

			from 1 to 0 from 0 to 1	
33.	**Responsibilities of data link layer**		a) Framing b) Physical addressing c) Flow control d) Error control e) Access control	
34.	**LRC**		In longitudinal redundancy check (LRC), a block of bits is divided into rows and a redundant row of bits is added to the whole block	
35.	**CRC**		A cyclic redundancy check (CRC) is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data	
36.	**Checksum**		The error detection method used by the higher layer protocol is called checksum. Checksum is based on the concept of redundancy	
37.	**Error Correction**		It is the mechanism to correct the errors	
38.	**Error Correcting Methods**		a) Single bit error correction b) Burst error correction	
39.	**Hamming Code**		Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver	
40.	**flow control**		Flow control refers to a set of procedures used to restrict the amount of data. The sender can send before waiting for acknowledgment	
41.	**buffer**		Each receiving device has a block of memory called a buffer, reserved for storing incoming data until they are processed	
42.	**Stop and wait**		Send one from at a time	
43.	**Sliding window**		Send several frames at a time	
44.	**Data Link Control**		DLC (data link control) is the service provided by the Data Link layer of function defined in the Open Systems Interconnection (OSI) model for network communication	
45.	**HDLC**		High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes.	
46.	**PPP**		Point - to - Point Protocol (PPP) is a communication protocol of the data link layer that is used to transmit multiprotocol data between two directly connected (point-to-point) computers	
47.	**MAC**		MAC is responsible for the transmission of data packets to and from the network-interface card, and to and from another remotely shared channel	
48.	**Ethernet**		Ethernet (pronounced "eether net") is a computer network technology which is used in different area networks like LAN, MAN, WAN. Ethernet connecting computers together with	

			cable so the computers can share information	
49.	**IEEE 802.11**		IEEE 802.11 refers to the set of standards that define communication for wireless LANs (wireless local area networks, or WLANs). The technology behind 802.11 is branded to consumers as Wi-Fi	
50.	**Bluetooth**		Bluetooth technology essentially works by using short-range wireless communication technology to connect two devices together	
Unit-III : Network Layer				
51.	**IPV4 addressing**		The IP address in IPV4 is 32 bits. It is represented in 4 blocks of 8 bits. It uniquely defines the connection of a device	
52.	**IPV6 addressing**		An IPv6 address is a 128-bits.Pv6 has the capability to provide unique addresses to each and every device or node attached to the Internet.	
53.	**subnetting**		When a bigger network is divided into smaller networks, in order to maintain security, then that is known as Subnetting	
54.	**CIDR**		Classless inter-domain routing (CIDR) is a set of Internet protocol (IP) standards that is used to create unique identifiers for networks and individual devices	
55.	**Internetworking**		Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices	
56.	**Responsibilities of Network Layer**		The network layer is responsible for routing, which is moving packets (the fundamental unit of data transport on modern computer networks) across the network using the most appropriate paths	
57.	**Dual Stack Routers**		A router's interface is attached with Ipv4 and IPv6 addresses configured is used in order to transition from IPv4 to IPv6	
58.	**Tunneling**		Tunneling is used as a medium to communicate the transit network with the different ip versions	
59.	**NAT**		NAT(Network Address Translation) is an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic	
60.	**ARP**		ARP stands for address resolution protocol. It is used to transform an IP address to its corresponding physical network address	
61.	**RARP**		RARP stands for Reverse Address resolution protocol, maps a MAC address to an IP address	
62.	**DHCP**		A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to	

			broadcast queries by clients	
63.	**ICMP**		Internet Control Message Protocol is a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully	
64.	**BGP Messages**		• OPEN • UPDATE • KEEPALIVE • NOTIFICATION	
65.	**Local sub-network**		Addresses in the range of 224.0.0.0 to 224.0.0.255 are individually assigned by IANA and designated for multicasting on the local subnetwork only	
66.	**peer-peer process**		The processes on each machine that communicate at a given layer are called peer-peer process	
67.	**Round Trip Time**		The duration of time it takes to send a message from one end of a network to the other and back, is called RTT	
68.	**Unicasting**		If the message is sent from a source to a single destination nod	
69.	**Multicasting**		If the message is sent to some subset of other nodes	
70.	**Broadcasting**		If the message is sent to all the m nodes in the network	
71.	**Server-based network**		It provide centralized control of network resources and rely on server computers to provide security and network administration	
72.	**Router**		A router is a device that forwards data packets along networks	
73.	**Circuit Switching**		When two nodes communicate with each other over a dedicated communication path, it is called circuit switching	
74.	**Message Switching**		This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety	
75.	**Packet Switching**		Packet switching is a method of grouping data that is transmitted over a digital network into packets	
Unit-IV : Routing and Transport Layer				
76.	**IGMP**		The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships	
77.	**Properties of Routing Algorithm**		Correctness, simplicity, robustness, stability, fairness, and optimality	
78.	**Shortest Path Routing**		A technique to study routing algorithms: The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph	

			representing a communication line	
79.	**Flooding**		Another static algorithm is flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on	
80.	**Multicasting**		Multicast is group communication where data transmission is addressed to a group of destination computers simultaneously. Multicast can be one-to-many or many-to-many distribution	
81.	**User Datagram**		User Datagram UDP packets, called user datagram, have a fixed-size header of 8 bytes made of four fields, each of 2 bytes	
82.	**Process-to-Process Communication**		UDP provides process-to-process communication using socket addresses, a combination of IP addresses and port numbers	
83.	**Connectionless Services**		This means that each user datagram sent by UDP is an independent datagram. There is no relationship between the different user data grams even if they are coming from the same source process and going to the same destination program	
84.	**SCTP**		SCTP is a new transport-layer protocol that combines the features of UDP and TCP	
85.	**Routing protocols**		Routing protocols are configured on routers with the purpose of exchanging routing information. Their types are 1. Distance vector (RIP, IGRP) 2. Link state (OSPF, IS-IS)	
86.	**Distance-Vector Routing**		A distance-vector routing (DVR) protocol requires that a router inform its neighbors of topology changes periodically	
87.	**Link State Routing**		It is a dynamic routing algorithm in which each router shares knowledge of its neighbors with every other router in the network. A router sends its information about its neighbors only to all the routers through flooding	
88.	**RIP**		Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network	
89.	**OSPF**		Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS).	
90.	**BGP**		Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reach ability information among autonomous systems (AS) on the Internet. The protocol is classified as a path vector protocol	

91.	**UDP**		UDP (User Datagram Protocol) is an alternative communications protocol to Transmission Control Protocol (TCP) used primarily for establishing low-latency and loss-tolerating connections between applications on the internet	
92.	**TCP Flow Control**		Flow Control basically means that TCP will ensure that a sender is not overwhelming a receiver by sending packets faster than it can consume. ... Congestion control is about preventing a node from overwhelming the network	
93.	**Error Control in TCP**		TCP is a reliable transport layer protocol. Error control includes mechanisms for detecting corrupted segments, lost segments, out-of-order segments, and duplicated segments. Error control also includes a mechanism for correcting errors after they are detected	
94.	**Congestion control**		Congestion control is a network layer issue, and is thus concerned with what happens when there is more data in the network than can be sent with reasonable packet delays, no lost packets, etc. Flow control is a local, congestion control is global	
95.	**QoS**		Quality of service (QoS) refers to any technology that manages data traffic to reduce packet loss, latency and jitter on the network	
96.	**Elements of transport protocols**		1. Addressing 2. Connection Establishment. 3. Connection Release. 4. Error control and flow control 5. Multiplexing	
97.	**Multiplexing**		In networks that use virtual circuits within the subnet, each open connection consumes some table space in the routers for the entire duration of the connection	
98.	**TPDU**		Transmissions of message between 2 transport entities are carried out by TPDU	
99.	**Window management in TCP**		Window management in TCP decouples the issues of acknowledgement of the correct receipt of segments and receiver buffer allocation	
100.	**Sliding Window protocol**		Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames	
Unit-V : Application Layer and Security				
101.	Security in CN		Network security is the security provided to a network from unauthorized access and risks	
102.	WWW		It is an internet application that allows users to view web pages and move from one web page to another	
103.	Aspects of Security		• Privacy • Authentication	

			• Integrity • Non-repudiation	
104.	Web Browser		Web browser is a software program that interprets and displays the contents of HTML web pages	
105.	URL		URL is a string identifier that identifies a page on the World Wide Web	
106.	TELNET		TELNET is used to connect remote computers and issue commands on those computers	
107.	HTTP		It is used mainly to access data on the World Wide Web	
108.	FTP		It is a standard mechanism provided by the internet for copying a file from one host to another	
109.	Electronic Mail		Email operates across computer networks, which today is primarily the Internet	
110.	Telnet		Telnet is an application protocol used on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection	
111.	SSH		Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network	
112.	DNS		DNS is a client/server application that identifies each host on the internet with a unique user friendly name	
113.	SMTP		Simple Mail Transfer Protocol is a standard and reliable host to host mail transport protocol that operates over the TCP port 25	
114.	SNMP		The primary purpose of SNMP is to allow the network administrator to monitor and configure devices on the network, remotely via the network	
115.	POP		Post Office Protocol, version3 (POP3)	
116.	Cryptographic Algorithms		The technology comes in many forms, with key size and strength generally being the biggest differences in one variety from the next.	
117.	Authentication		Authentication is the process of verifying the identity of a person or device	
118.	Confidentiality		Keeps the information away from an unauthorized person	
119.	Integrity		Identifying any alteration to the data	
120.	Non repudiation		An entity cannot refuse the ownership of a previous action or commitment	
121.	Symmetric key encryption		Same keys are used for encrypting and decrypting	
122.	Asymmetric Key Encryption		Different keys are used for encrypting and decrypting the information	
123.	Public Key Cryptography		Public key cryptography is a method of encrypting data with two different keys and making one of the keys,	

			the public key, available for anyone to use.	
124.	X. 509		An X. 509 certificate is a digital certificate that uses the widely accepted international X	
125.	Firewall		A Firewall is software that blocks unauthorized users from connecting to your computer	
Placement Questions				
126.	Message		The Protocol Data Unit for Application layer in the Internet Stack (or TCP/IP) is called Message	
127.	Layers of the OSI reference model		There are 7 OSI layers: Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer and Application Layer	
128.	Backbone network		A backbone network is a centralized infrastructure that is designed to distribute different routes and data to various networks	
129.	Point to Point Link		A point to point connection does not need any other network devices other than connecting a cable to the NIC cards of both computers	
130.	Subnet Mask		A subnet mask is combined with an IP address in order to identify two parts	
131.	Maximum length allowed for a UTP cable		A single segment of UTP cable has an allowable length of 90 to 100 meters. This limitation can be overcome by using repeaters and switches	
132.	Data encapsulation		Data encapsulation is the process of breaking down information into smaller manageable chunks before it is transmitted across the network	
133.	VPN		VPN means Virtual Private Network, a technology that allows a secure tunnel to be created across a network such as the Internet	
134.	NAT		NAT is Network Address Translation	
135.	NIC		NIC is short for Network Interface Card	
136.	Layers under TCP/IP		There are four layers: the Network Layer, Internet Layer, Transport Layer and Application Layer	
137.	Proxy servers		Proxy servers primarily prevent external users who identifying the IP addresses of an internal network	
138.	Function of the OSI Session Layer		This layer provides the protocols and means for two devices on the network to communicate with each other by holding a session	
139.	Fault Tolerance System		A fault tolerance system ensures continuous data availability. This is done by eliminating a single point of failure	
140.	10Base-T		The 10 refers to the data transfer rate, in this case is 10Mbps	
141.	private IP address		Private IP addresses are assigned for use on intranets	
142.	NOS		NOS, or Network Operating System, is specialized software whose main task is to provide network connectivity to a computer in order for it to be able to communicate with other computers and connected	

			devices	
143.	DoS		DoS, or Denial-of-Service attack, is an attempt to prevent users from being able to access the internet or any other network services. Such attacks may come in different forms and are done by a group of perpetuators	
144.	Crosstalks		Crosstalks are electromagnetic interferences or noise that can affect data being transmitted across cables	
145.	MAC Address		MAC, or Media Access Control, uniquely identifies a device on the network	
146.	Star topology		Star topology consists of a central hub that connects to nodes. This is one of the easiest to setup and maintain	
147.	SLIP		SLIP, or Serial Line Interface Protocol, is actually an old protocol developed during the early UNIX days	
148.	Tracert		Tracert is a Windows utility program that can used to trace the route taken by data from the router to the destination network	
149.	Ping		Ping is a utility program that allows you to check connectivity between network devices on the network	
150.	Ipconfig		Ipconfig is a utility program that is commonly used to identify the addresses information of a computer on a network	

Faculty Prepared By

1. **M.Buvaneswari**
2. **S.R.Sridhar**

Signatures

HoD