DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CS3591– COMPUTER NETWORKS

Question Bank

III YEAR – V SEM

BATCH: 2021 -2025

SYLLABUS

CS3591 COMPUTER NETWORKS L T P C 3 0 2 4

UNIT I INTRODUCTION AND APPLICATION LAYER 10

Data Communication - Networks - Network Types - Protocol Layering - TCP/IP Protocol suite - OSI Model - Introduction to Sockets - Application Layer protocols: HTTP - FTP - Email protocols (SMTP - POP3 - IMAP - MIME) - DNS - SNMP

UNIT II TRANSPORT LAYER 9

Introduction - Transport-Layer Protocols: UDP - TCP: Connection Management - Flow control - Congestion Control - Congestion avoidance (DECbit, RED) - SCTP - Quality of Service

UNIT III NETWORK LAYER 7

Switching: Packet Switching - Internet protocol - IPV4 - IP Addressing - Subnetting - IPV6, ARP, RARP, ICMP, DHCP

UNIT IV ROUTING 7

Routing and protocols: Unicast routing - Distance Vector Routing - RIP - Link State Routing - OSPF - Path-vector routing - BGP - Multicast Routing: DVMRP - PIM.

UNIT V DATA LINK AND PHYSICAL LAYERS 12

Data Link Layer - Framing - Flow control - Error control - Data-Link Layer Protocols - HDLC - PPP - Media Access Control - Ethernet Basics - CSMA/CD - Virtual LAN - Wireless LAN (802.11)
- Physical Layer: Data and Signals - Performance - Transmission media- Switching - Circuit Switching.

45 PERIODS

COURSE OUTCOMES:

At the end of this course, the students will be able to:

CO 1: Explain the basic layers and its functions in computer networks.
CO 2: Understand the basics of how data flows from one node to another.
CO 3: Analyze different routing algorithms.
CO 4: Describe protocols for various functions in the network.
CO 5: Analyze the working of various application layer protocols.

TEXT BOOKS

1. James F. Kurose, Keith W. Ross, Computer Networking, A Top-Down Approach Featuring the Internet, Eighth Edition, Pearson Education, 2021.
2. Behrouz A. Forouzan, Data Communications and Networking with TCP/IP Protocol Suite, Sixth Edition TMH, 2022

REFERENCES

1. Larry L. Peterson, Bruce S. Davie, Computer Networks: A Systems Approach, Fifth Edition, Morgan Kaufmann Publishers Inc., 2012.
2. William Stallings, Data and Computer Communications, Tenth Edition, Pearson Education, 2013.
3. Nader F. Mir, Computer and Communication Networks, Second Edition, Prentice Hall, 2014.
4. Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, "Computer Networks: An Open Source Approach", McGraw Hill, 2012.

CS3591: Computer Networks

Corresponding Lab, with code (If any): Nil

Course Prerequisites: -

Course Outcomes

On successful completion of this course, the student will be able to

C301.1	Understand the concept of layering in networks and basic application layer protocols
C301.2	Familiar with the Transport layer protocols like UDP, TCP and SCTP and their functions
C301.3	Understand switching in Internet, IP addressing protocol versions 4 and 6, Supporting
C301.4	Intra domain routing and Inter domain routing protocols and multicast routing protocols
C301.5	Familiar with the services provided by Datalink layer and Physical Layer.

MAPPING BETWEEN CO AND PO, PSO WITH CORRELATION LEVEL 1/2/3

CS3591	Pos												PSOs			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
C301.1	-	2	-	-	-	-	-	-	-	-	-	-	3	2	2	2
C301.2	-	1	-	-	2	-	-	-	-	-	-	2	2	2	2	2
C301.3	-	2	-	-	3	-	-	-	-	-	-	-	3	3	2	2
C301.4	-	-	-	1	2	-	-	-	-	3	-	-	3	3	2	1
C301.5	-	1	-	-	1	-	-	-	-	1	-	-	2	1	2	2

RELATION BETWEEN COURSE CONTENT WITH Cos

UNIT I-INTRODUCTION AND APPLICATION LAYER

S. No	Topic	Knowledge level	No. of Hrs to be handled	Books Referred
1.	Data Communication - Networks	L2	1	T2
2.	Network Types	L2	1	T2
3.	Protocol Layering	L2	1	T2
4.	TCP/IP Protocol suite	L2	1	T2
5.	OSI Model	L2	2	T2
6.	Introduction to Sockets	L1, L2	2	T2
7.	Application Layer Protocols - HTTP - FTP	L2	2	T2
8.	Email Protocols (SMTP - POP3 - IMAP - MIME)	L2	1	T2
9.	DNS - SNMP	L2	2	T2

UNIT II-TRANSPORT LAYER

S. No	Topic	Knowledge level	No. of Hrs to be handled	Books Referred
1.	Introduction - Transport Layer Protocols	L1, L2	1	T2
2.	UDP	L2	2	T2
3.	TCP: Connection Management, Flow control	L2	2	T2
4.	Congestion Control	L2	2	T2
5.	Congestion Avoidance - DECbit, RED	L2	1	R1
6.	SCTP	L2	1	T2
7.	Quality of Service	L2	1	T2

UNIT III-NETWORK LAYER

S. No	Topic	Knowledge level	No. of Hrs to be handled	Books Referred
1.	Switching - Packet switching	L2	2	T2
2.	Internet Protocol - Ipv4	L1,L2	1	T2
3.	IP Addressing	L2	2	T2
4.	Subnetting	L1,L2,L3	1	T2
5.	IPv6	L2	2	T2
6.	APR, RARP	L2	1	T2
7.	ICMP, DHCP	L2	2	T2

UNIT IV-ROUTING

S. No	Topic	Knowledge level	No. of Hrs to be handled	Books Referred
1.	Routing and Protocols	L1,L2	1	T2
2.	Unicast Routing - Distance Vector Routing	L2	1	T2
3.	RIP	L2	1	T2
4.	Link State Routing - OSPF	L2	2	T2
5.	Path Vector Routing	L2	1	T1
6.	BGP	L2	1	R1
7.	Multicast Routing: DVMRP, PIM	L2	2	T2

UNIT V-DATALINK AND PHYSICAL LAYER

S. No	Topic	Knowledge level	No. of Hrs to be handled	Books Referred
1.	Datalink Layer - Framing	L2	1	T2
2.	Flow control, Error control	L2	2	T2
3.	Datalink layer Protocols - HDLC, PPP	L2	2	T2
4.	Media Access Control - Ethernet Basics	L2	1	T2
5.	CSMA/CD, Virtual LAN	L2	2	T2
6.	Wireless LAN (IEEE802.11)	L2	2	T2
7.	Physical Layer - Data and Signals,	L2	1	T2
8.	Transmission Media	L2	2	T2
9.	Switching - Circuit Switching	L2	2	T2

L1- Remember; L2- Understand; L3- Apply; L4- Analyze; L5- Evaluate; L6- Create

S. No	Content beyond syllabus	PO Mapping	PSO Mapping
1.	Network Security - Cryptography	PO5	PSO2

UNIT I INTRODUCTION AND APPLICATION LAYER

Data Communication - Networks - Network Types - Protocol Layering - TCP/IP Protocol suite - OSI Model - Introduction to Sockets - Application Layer protocols: HTTP - FTP - Email protocols (SMTP - POP3 - IMAP - MIME) - DNS - SNMP

<table>
<tr><th colspan="3">PART-A</th><th>CO Stmt</th><th>Knowledge Level(R/U/Ap /An/E/C)</th></tr>
<tr><td>1</td><td colspan="2">Compare LAN and WAN.
<table><tr><th>LAN</th><th>WAN</th></tr><tr><td>Scope of Local Area Network is restricted to a small/ single building</td><td>Scope of Wide Area Network spans over large geographical area country/ Continent</td></tr><tr><td>LAN is owned by some organization.</td><td>A part of network asserts is owned or not owned.</td></tr><tr><td>Data rate of LAN 10-.10-100mbps.</td><td>Data rate of WAN is Gigabyte.</td></tr></table></td><td>C301.1</td><td>BL2</td></tr>
<tr><td>2</td><td colspan="2">Define Full Duplex and simplex transmission system.
With Full duplex transmission, two stations can simultaneously send and receive data from each other. This mode is known as two-way simultaneous. The signals are transmitted in only one direction. One is the sender and another is the receiver.</td><td>C301.1</td><td>BL1</td></tr>
<tr><td>3</td><td colspan="2">Define networks. (Nov 12)
A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Networks are commonly categorized based on their characteristics.</td><td>C301.1</td><td>BL1</td></tr>
<tr><td>4</td><td colspan="2">Why do we need a Domain Name System? What role does the DNS Resolver play in the DNS system? (Nov 12)
Domain Name System can map a name to an address and conversely an address to name. The Domain Name System converts domain names into IP numbers. IP numbers uniquely identify hosts on the Internet</td><td>C301.1</td><td>BL2</td></tr>
<tr><td>5</td><td colspan="2">What are the four fundamental characteristics that the data communication system depends on?
The four fundamental characteristics are: Delivery, Accuracy, Timeliness and Jitter.</td><td>C301.1</td><td>BL2</td></tr>
<tr><td>6</td><td colspan="2">What are the five components of data communications system?
The five components are Message, Sender, Receiver, Transmission Medium and Protocol.</td><td>C301.1</td><td>BL2</td></tr>
</table>

7	**Define link and state the types of connection.** A link is the communication pathway that transfers data from one device to another. The two possible types of connections are point to point and multipoint	**C301.1**	**BL1**
8	**Define point to point and Multipoint.** **Point to point:** A point to point connection provides a dedicated link between two devices. **Multipoint:** A multipoint connection is one in which more than two specific devices share a single link.	**C301.1**	**BL1**
9	**What is Network topology? List its types.** Network topology is the interconnected pattern of network elements. A network topology may be physical, mapping hardware configuration, or logical, mapping the path that the data must take in order to travel around the network. The types are Bus topology, Star topology, Mesh topology and Ring Topology.	**C301.1**	**BL1**
10	**What are the four main properties of HTTP?** • Global Uniform Resource Identifier. • Request-response exchange. • Statelessness. • Resource metadata.	**C301.1**	**Bl1**
11	**What is a protocol? What are the key elements of a protocol?** ***(Nov 15)*** Protocol is the set of rules governing the exchange of data between two entities. It defines what is communicated, how it is communicated, when it is communicated. The Key elements of a Protocol are as follows, • Syntax - It refers to the structure or format of data meaning the order in which they are presented. • Semantics - It refers to the meaning of each section of bit. How to do interpretation. • Timing - When data should be sent and how fast they can be sent.	**C301.1**	**BL1**
12	**Define File Transfer Protocol.** ***(Nov 21)*** The File Transfer Protocol is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client-server model architecture using separate control and data connections between the client and the server.	**C301.1**	**BL1**
13	**What is WWW and SMTP?** ***(Nov 10,15) (May 15)*** World Wide Web is an internet application that allows user to view pages and move from one web page to another.	**C301.1**	**R**

<table>
<tr><td></td><td>It helps to store and share data across varied distances. The TCP/IP protocol that supports electronic mail on the Internet is called Simple Mail Transfer (SMTP). It is a system for sending messages to other computer users based on e-mail addresses.</td><td></td><td></td></tr>
<tr><td>14</td><td>List the two types of DNS message. (May 16)
There are two types of DNS messages - Query and Response
• Query message - consists of the header and question records.
• Response message - consists of header, question record, authoritative record and additional record.</td><td>C301.1</td><td>BL1</td></tr>
<tr><td>15</td><td>What is a layered Network Architecture?
A layer is created when a different level of abstraction occurs at protocol. Each layer should perform a well-defined function. Function of each layer should be chosen using internationality standardized protocols. Boundaries between should be chosen to minimize information flow across the interfaces.</td><td>C301.1</td><td>BL1</td></tr>
<tr><td>16</td><td>Compare OSI and TCP/IP models.
<table>
<tr><th>OSI Model</th><th>TCP / IP Model</th></tr>
<tr><td>It distinguishes between Service, Interface, Protocol</td><td>It does not distinguish between Service, Interface, Protocol</td></tr>
<tr><td>Protocols are well hidden</td><td>Protocols are not just hidden</td></tr>
<tr><td>Dejure standard Fit Model</td><td>Defacto standard Fit Model</td></tr>
<tr><td>In transport layer only connection-oriented services are available</td><td>In Transport layer choice is for connection oriented and connectionless</td></tr>
<tr><td>Contains 7 layers</td><td>Contains 5 layers</td></tr>
</table></td><td>C301.1</td><td>BL2</td></tr>
<tr><td>17</td><td>How do layers of the internet model correlate to the layers of the OSI model?
<table>
<tr><th>OSI</th><th>TCP/IP</th></tr>
<tr><td>Physical Layer</td><td>Physical Layer</td></tr>
<tr><td>Data Link Layer</td><td>Network Access Layer</td></tr>
<tr><td>Network Layer</td><td>IP Layer</td></tr>
<tr><td>Transport Layer</td><td>TCP Layer</td></tr>
<tr><td>Session Layer</td><td rowspan="3">Application Layer</td></tr>
<tr><td>Presentation Layer</td></tr>
<tr><td>Application layer</td></tr>
</table></td><td>C301.1</td><td>BL2</td></tr>
<tr><td>18</td><td>Describe why HTTP is defined as a stateless protocol.
Maintaining state across request - Response connections significantly increases the initial interactions in a connection, since the identity of each party needs to be established and any saved state much be retrieved. HTTP is therefore stateless to ensure that</td><td>C301.1</td><td>BL2</td></tr>
</table>

	internet is scalable since state is not contained in a HTTP request / response pair by default.		
19	**What are the four groups of HTTP Headers? What are the two methods of HTTP?** ***(May 15)*** ***(Nov 15)*** The four groups of HTTP headers are • General headers • Entity Headers • Request Headers • Response Headers. Two methods of HTTP are Get Method( ) Post Method( )	**C301.1**	**BL1**
20	**Justify the need for layer five in the OSI model.** ***(Nov 21)*** Layer 5 of the OSI Model: Session Layer is the layer of the ISO Open Systems Interconnection (OSI) model that controls the dialogues (connections) between computers. It establishes, manages, and terminates the connections between the local and remote application.	**C301.1**	**BL2**
21	**What are the functions of Application Layer?** ***(Apr 11)*** It enables the user (human/software) to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management and other types of distributed information services. Services provided by the application layer are Network Virtual terminal, File transfer, access and management. Mail services, Directory services.	**C301.1**	**BL1**
22	**Define anonymous FTP.** ***(May / June 2021)*** An anonymous FTP is where users are given access to a distributed file where they do not need to sign in with a specific username and password.	**C301.1**	**BL1**
23	**What are the transmission modes of FTP?** Stream mode: Default mode and data is delivered from FTP to TCP as a continuous stream of data. Block mode: Data is delivered from FTP to TCP in terms of blocks. Each data block follows the three-byte header. Compressed mode: File is compressed before transmitting if size is big. Run length encoding method is used for compression.	**C301.1**	**BL1**
24	**Why is an application such as POP needed for electronic messaging?** ***(May 12)*** Workstations interact with the SMTP host, which receives the mail on behalf of every host in the organization, to retrieve messages by using a client-server protocol such as Post Office Protocol. Although POP3 is used to download messages from the server, the	**C301.1**	**BL2**

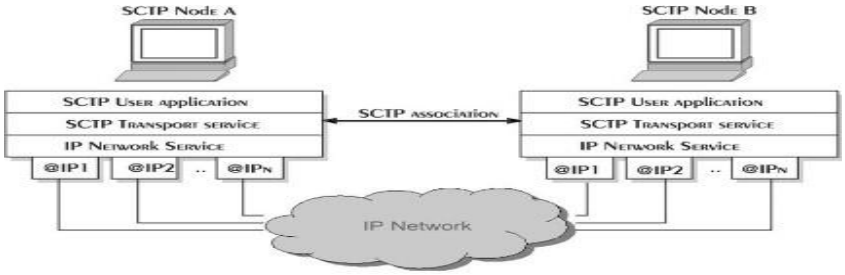
<table>
<tr><td></td><td>SMTP client still needed on the desktop to forward messages from the workstation user to its SMTP mail server.</td><td></td><td></td></tr>
<tr><td>25</td><td>What is the difference between IMAP and POP? (May / June 2021)
<table>
<tr><th>POP</th><th>IMAP</th></tr>
<tr><td>POP allows downloading messages from your Inbox to your local computer</td><td>IMAP allows the user to see all the folders on the mail server.</td></tr>
<tr><td>The mail can only be accessed from a single device at a time.</td><td>Messages can be accessed across multiple devices</td></tr>
<tr><td>To read the mail it has to be downloaded on the local system</td><td>The mail content can be read partially before downloading.</td></tr>
<tr><td>The user cannot organize mails in the mailbox of the mail server.</td><td>The user can organize the emails directly on the mail server.</td></tr>
</table></td><td>C301.1</td><td>BL2</td></tr>
<tr><td>26</td><td>What is the use of MIME Extension?
Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME transforms non-ASCII data at the sender site to NVT ASCII data and deliverers it to the client SMTP to be sent through the Internet. MIME converts binary files, executed files into text files. Then only it can be transmitted using SMTP</td><td>C301.1</td><td>BL2</td></tr>
<tr><td>27</td><td>How are the subgroups of the OSI model layers segregated by their functions? (May / June 2021)
The lower 4 layers (transport, network, data link and physical) are concerned with the flow of data from end to end through the network and hence are called as network support layers. The upper four layers of the OSI model (application, presentation and session) are orientated more toward services to the applications and hence are called user support layers.</td><td>C301.1</td><td>BL1</td></tr>
<tr><td>28</td><td>Identify the Port number of Hyper Text Transfer Protocol and Telnet. (Nov 21)
By default, these two protocols are on their standard port number of 80 for HTTP and 443 for HTTPS. For telnet port number is 23.</td><td>C301.1</td><td>BL1</td></tr>
<tr><td>29</td><td>Discuss the three main division of the domain name space. (May 12)
Domain name space is divided into three different sections: generic domains, country domains & inverse domain.
• Generic domain: Define registered hosts according to their generic behavior, uses generic suffixes.</td><td>C301.1</td><td>BL1</td></tr>
</table>

	• Country domain: Uses two characters to identify a country as the last suffix. Inverse domain: Finds the domain name given the IP address.		
30	**Define SNMP.** ***(May 12)*** **Simple Network Management Protocol** (**SNMP**) is an "Internet-standard protocol for managing devices on IP networks". Devices that typically support SNMP include routers, switches, servers, workstations, printers, & modem. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.	**C301.1**	BL1
31	**List the two types of DNS message.** ***(May 16)*** There are two types of DNS messages, • Query • Response **Query message** - consists of the header and question records. **Response message** - consists of header, question record, authoritative record and additional record.	**C301.1**	BL1
	PART-B		
1	Explain different types of networks in detail with neat diagram ***(Nov/Dec 2021)***	**C301.1**	BL1
3	Discuss in detail about the layers in OSI model. ***(Nov 10,11,12,15,19) (May 12) (May / June 2021)***	**C301.1**	BL2
4	Explain in detail about the TCP/IP protocol suite with neat diagram	**C301.1**	BL1
5	Discuss how the Simple Mail Transfer Protocol (SMTP) is useful in electronic mail. (***May 12,15) (Nov 13,15) (Nov 19) (May/June 2021) (Nov 21)***	**C301.1**	BL2
6	Explain the role of a DNS on a computer network, including its involvement in the process of a user accessing a web page. ***(May 13) (Nov 15, 19) (Nov 21)***	**C301.1**	BL1
7	Explain about HTTP. Give their uses, state strengths and weaknesses. ***(Nov 10,13)***	**C301.1**	BL1
8	Explain about FTP. ***(Nov 12, 13, 19), May 13)***	**C301.1**	BL1
9	Explain in detail about SNMP.	**C301.1**	BL1
10	Explain in detail about sockets with an example.	**C301.1**	BL1
UNIT II	**TRANSPORT LAYER** Introduction - Transport-Layer Protocols: UDP - TCP: Connection Management - Flow control - Congestion Control - Congestion avoidance (DECbit, RED) - SCTP - Quality of Service		
	PART-A	**CO Stateme**	**Knowledge Level(R/U/Ap**

<table>
<tr><td></td><td></td><td>nt</td><td>/An/E/C)</td></tr>
<tr><td>1</td><td>Give any two Transport layer service. (Dec 12)
Multiplexing: Transport layer performs multiplexing/de-multiplexing function. Multiple applications employ same transport protocol, but use different port number. According to lower layer n/w protocol, it does upward multiplexing or downward multiplexing.
Reliability: Error Control and Flow Control.</td><td>C301.2</td><td>BL1</td></tr>
<tr><td>2</td><td>How IANA has divided port numbers?
IANA (Internet Assigned Number Authority) has divided port numbers into three ranges: 1) Well Known ports
2) Registered ports 3) Dynamic Ports.</td><td>C301.2</td><td>BL2</td></tr>
<tr><td>3</td><td>List few well known ports for UDP.
<table>
<tr><th>Port</th><th>Protocol</th><th>Description</th></tr>
<tr><td>7</td><td>Echo</td><td>Echoes a received datagram back to the sender</td></tr>
<tr><td>9</td><td>Discard</td><td>Discards any datagram received</td></tr>
<tr><td>11</td><td>Users</td><td>Active Users</td></tr>
<tr><td>13</td><td>Daytime</td><td>Returns Date and Time</td></tr>
</table></td><td>C301.2</td><td>BL1</td></tr>
<tr><td>4</td><td>How congestion occurs in a network? (May / June 2021)
The routers / switches in a network have a limited buffer size to store the received packets. If the packets arrive at a faster rate than what the receiver can store, then the packets are dropped leading to congestion.</td><td>C301.2</td><td>BL2</td></tr>
<tr><td>5</td><td>What is a Port? (Nov 21)
In computer networking, a port is a communication endpoint. At the software level, within an operating system, a port is a logical construct that identifies a specific process or a type of network service.</td><td>C301.2</td><td>BL1</td></tr>
<tr><td>6</td><td>Give the datagram format of UDP?
The basic idea of UDP is for a source process to send a message to a port and for the destination process to receive the message from a port.
<table>
<tr><td>Source Port Address
16 bits</td><td>Destination Port Address
16 bits</td></tr>
<tr><td>Total Length
16 bits</td><td>Checksum
16 bits</td></tr>
</table></td><td>C301.2</td><td>BL1</td></tr>
</table>

<table>
<tr><td>7</td><td>What is the main difference between TCP & UDP?<table><tr><th>TCP</th><th>UDP</th></tr><tr><td>It provides connection-oriented service</td><td>Provides connectionless service.</td></tr><tr><td>Connection Establishment delay will be there</td><td>No connection establishment and no delay</td></tr><tr><td>Provides reliable service</td><td>Provides unreliable, but fast service</td></tr><tr><td>It is used by FTP, SMTP</td><td>It is used by DNS, SNMP, audio, video and multimedia applications.</td></tr></table></td><td>C301.2</td><td>BL2</td></tr>
<tr><td>8</td><td>Name the techniques and policies that can prevent (avoid) congestion.
Techniques to avoid congestion:
• DEC (Digital Equipment Corporation) bit.
• Random Early Detection (RED).
• Source based congestion avoidance.
The congestion may be avoided by two policies:
• BECN - Backward Explicit Congestion Notification
• FECN - Forward Explicit Congestion Notification.</td><td>C301.2</td><td>BL1</td></tr>
<tr><td>9</td><td>List out various congestion control techniques.
AIMD (Additive Increase Multiplicative Decrease), Slow start, Fast retransmit, Fast Recovery</td><td>C301.2</td><td>BL1</td></tr>
<tr><td>10</td><td>What are the advantages of using UDP over TCP? (Nov 10)
UDP is very useful for audio or video delivery which does not need acknowledgement. It is useful in the transmission of multimedia data. Connection Establishment delay will occur in TCP.</td><td>C301.2</td><td>BL1</td></tr>
<tr><td>11</td><td>What is the use of UDP’s Pseudo header?
The pseudo header consists of three field from the IP header protocol number, source IP address and destination IP address plus the UDP length field (which is included twice in checksum calculation). The pseudo header is used to check whether the message is delivered between 2 endpoints.</td><td>C301.2</td><td>BL1</td></tr>
<tr><td>12</td><td>What are the four aspects related to the reliable delivery of data? (May 12)
The four aspects are
(i) Error control,
(ii) Sequence control
(iii) Loss control
(iv) Duplication control.</td><td>C301.2</td><td>BL1</td></tr>
</table>

<table>
<tr><td>13</td><td>Outline Stop and Wait ARQ mechanism. (Nov 19)
In the stop-and-wait ARQ mechanism, sender sends one frame at a time; it is a special case of the general sliding window protocol with transmit and receive window sizes equal to one in both cases.</td><td>C301.2</td><td>BL1</td></tr>
<tr><td>14</td><td>What do you mean by slow start in TCP congestion? (May 16)
TCP slow start is an algorithm which balances the speed of a network connection. Slow start gradually increases the amount of data transmitted until it finds the network’s maximum carrying capacity.</td><td>C301.2</td><td>BL1</td></tr>
<tr><td>15</td><td>Differentiate congestion control and flow control. (Nov 13,15)
<table>
<tr><th>Congestion Control</th><th>Flow Control</th></tr>
<tr><td>Congestion control means preventing the source from sending data that will end up getting dropped by a router because its queue is full.</td><td>Flow control means preventing the source from sending data that the receiver will end up dropping because it runs out of buffer space.</td></tr>
<tr><td>This is more complicated, because packets from different sources travelling different paths can converge on the same queue.</td><td>This is fairly easy with a sliding window protocol</td></tr>
</table></td><td>C301.2</td><td>BL2</td></tr>
<tr><td>16</td><td>List the different phases used in TCP Connection. (May 16)
The different phases used in TCP connection are Connectio establishment Phase, Data transfer and Connection Terminatio Phase</td><td>C301.2</td><td>BL1</td></tr>
<tr><td>17</td><td>List the advantages of Connection oriented services over connectionless services. (May 17)
<u>Connection Oriented</u>:
Advantages:
1. Buffers can be reserved in advance
2. Sequencing can be guaranteed.
Short headers.</td><td>C301.2</td><td>BL1</td></tr>
<tr><td>18</td><td>How do fast retransmit mechanism of TCP works? (May 17)
Fast Retransmit is an enhancement to TCP that reduces the time sender waits before retransmitting a lost segment. A TCP sende uses a timer to recognize lost segments. If an acknowledgement i not received for a particular segment within a specified time (</td><td>C301.2</td><td>BL2</td></tr>
</table>

	function of the estimated round-trip delay time), the sender wil assume the segment was lost in the network, and will retransmit th segment.		
19	**Define SCTP** ***(Nov 21)*** SCTP (Stream Control Transmission Protocol) is a reliable, message-oriented transport layer protocol. It combines the best features of UDP and TCP. It is mostly designed for internet applications.	**C301.2**	**BL1**
20	**What is the use of SCTP Multiple stream service?** SCTP allows multi stream service in each connection, which is called association in SCTP terminology. If one of the streams is blocked, the other streams can still deliver their data. The idea is similar to multiple lanes on a highway. The figure shows the idea of multi stream delivery.	**C301.2**	**BL2**
21	**Define Multihoming Concept of SCTP** Multihoming is the ability of an SCTP association to support multiple IP paths to its peer endpoint. The benefit of multihoming associations is that it makes the association more fault-tolerant against physical network failures and other issues on the interfaces.  	**C301.2**	**BL1**
22	**What happens in a three-way handshaking between any 2 devices?** ***(May/June 2021)*** The three-way handshake involves the exchange of three messages between the client and the server. The client sends a segment to the server stating the initial sequence number it plans to use (Flags = SYN, Sequence Num = x). The server responds with a single segment that both acknowledges the client's sequence number (Flags = ACK, ACK = x +1) and states its own beginning sequence number, (Flags = SYN, Sequence Num = y). Both the SYN and ACK bits are set in the Flags field of this second message.	**C301.2**	**BL2**
23	**What are the two categories of QoS attributes?** User Oriented and Network Oriented. User related attributes are	**C301.2**	**BL1**

	SCR – Sustainable Cell Rate PCR – Peak Cell Rate MCR- Minimum Cell Rate CVDT – Cell Variation Delay Tolerance. The network related attributes are, Cell loss ratio (CLR), Cell transfer delay (CTD), Cell delay variation (CDV), Cell error ratio (CER).		
UNIT-II / PART-B			
1	Write short notes on ***(May 12) (Nov 19) (Nov 21)*** (i) **TCP segment format** (ii) Silly window syndrome (Or) discuss the silly window syndrome and explain how to avoid it.	**C301.2**	BL1
2	With neat architecture, Explain TCP and its sliding window algorithm for flow control. ***(Nov 15)***	**C301.2**	BL2
3	Describe with examples the three mechanisms by which congestion control is achieved in TCP. ***(Nov 13,15)(May 15,16)(Nov 19)***	**C301.2**	BL2
4	Discuss congestion avoidance algorithm like DEC bit method and random early detection in transport layer with an example.***(May 12,17)***	**C301.2**	BL2
5	What are the 2 broad categories of congestion control mechanisms? Briefly explain all the techniques. **(May / June 2021)**	**C301.2**	BL1
6	Explain connection establishment and connection closing in TCP (Or) Describe how reliable and ordered delivery is achieved through TCP. ***(Nov 13) (May 15)***	**C301.2**	BL2
7	Explain the significance of Clark's solution and Nagle's algorithm. (Or) What is the need for Nagle's algorithm? How does it determine when to transmit data? ***(May 13)***	**C301.2**	BL4
8	Define UDP. Discuss the operations of UDP. Explain UDP checksum with one example. ***(Nov 21)***	**C301.2**	BL2
9	Discuss the effectiveness of Go Back N and Selective Repeat ARQ among the Sliding window Protocols. ***(Nov 21)***	**C301.2**	BL2
10	Explain SCTP in Detail ***(May 17)***	**C301.2**	BL2
11	Explain the association establishment of SCTP through four-way handshake in detail.	**C301.2**	BL2
12	Furnish the packet format of Stream Control Transmission Protocol with its fields. How the data are transferred using 4-way handshaking? ***(May / June 2021)***	**C301.2**	BL1
13	Explain the various approaches to improve quality of services in a data transmission network.	**C301.2**	BL2

UNIT III **NETWORK LAYER**

Switching: Packet Switching - Internet protocol - IPV4 - IP Addressing - Subnetting - IPV6, ARP, RARP, ICMP, DHCP

	UNIT-III / PART-A	**CO Statement**	**Knowledge Level (R/U/Ap/An/E/C)**
1	**What is packet switching?** *(Nov 12)* In a packet-switched network, it's not necessary to dedicate transmission capacity along a path through the network. Rather, data are sent out in a sequence of small chunks, called packets.	**C301.3**	**BL1**
2	**What is subnetting?** *(Nov 11,15)* The whole network can't manage by single server, so that the entire network divided into small network in order to manage the network easily. Subnetting provides an elegantly simple way to reduce the total number of network numbers that are assigned. The idea is to take a single IP network number and allocate the IP address with that network to several physical networks, which are now referred to as subnets.	**C301.3**	**BL1**
3	**What is subnet mask?** A subnet mask is a number that defines a range of IP addresses available within a network. A single subnet mask limits the number of valid IPs for a specific network. Multiple subnet masks can organize a single network into smaller networks (called subnetworks or subnets).	**C301.3**	**BL1**
4	**Define CIDR?** CIDR, which stands for Classless Inter-Domain Routing, is an IP addressing scheme that improves the allocation of IP addresses. It replaces the old system based on classes A, B, and C. This helped to extend the life of IPv4 as well as slow the growth of routing tables.	**C301.3**	**BL1**
5	**How many network addresses and host addresses are supported by class A, class B networks?** Class A: Number of networks = 127 Number of hosts = 2^{24} -1 Class B: Number of networks = 2^{14} -1 Number of hosts = 2^{16} – 1 = 65,535	**C301.3**	**BL1**
6	**List out the functions of IP.** IP services are unreliable, best-effort, connectionless packet delivery system. Unreliable – delivery is not guaranteed, Connectionless – each pocket is treated independent from others,	**C301.3**	**BL1**

	Best-effort delivery - it makes an earnest attempt to deliver packets. It defines basic unit of data transfer through TCP/IP.		
7	**What do you mean by ICMP?** ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. The source must relate the error to an individual application program and take other actions to correct the problem.	**C301.3**	**BL1**
8	**To whom ICMP reports error message will be sent?** **ICMP** allows routers to send error messages to other router or hosts. ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. It is informing the source that the error has occurred and the source has to take actions to rectify the errors.	**C301.3**	**BL2**
9	**When ICMP redirect message is used? *(May 17)*** An ICMP redirect is an error message sent by a router to the sender of an IP packet Redirects are used when a router believes a packet is being routed sub optimally and it would like to inform the sending host that it should forward the subsequent packets to that same destination through a different gateway.	**C301.3**	**BL2**
10	**State the rules of non-boundary-level masking? *(May 12)*** • The bytes in the IP address that corresponds to 255 in the mask will be repeated in the sub network address. • The bytes in the IP address that corresponds to 0 in the mask will change to 0 in the sub network address. • For other bytes, use the bit-wise AND operator. Example- IP address 45 123 21 8 Mask 255 192 0 0 Subnet 45 64 0 0 123 0 1 1 1 1 0 1 1 192 1 1 0 0 0 0 0 0 64 0 1 0 0 0 0 0 0	**C301.3**	**BL3**
11	**How many network addresses and host addresses are supported by class A, class B networks?** Class A: Number of networks = 127 Number of hosts = 2^{24} -1 Class B: Number of networks = 2^{14} -1 Number of hosts = 2^{16} - 1 = 65,535	**C301.3**	**BL2**

12	**What is the network address in a class A subnet with the IP addresses of one of the hosts as 25.34.12.56 and mask 255.255.0.0?** ***(May 14)*** IP Address - 25.34.12.56 , Mask - 255.255.0.0 , Network Address - 25.34.0.0	**C301.3**	**BL2**
13	**What is IP address?** An Internet Address is made of four bytes (32 bits) that define a host's connection to a network. There are currently 5 different field lengths patterns, each define a class of addresses. These are designed to cover the needs of different types of organizations, class A, B, C, D, E.	**C301.3**	**BL1**
14	**Explain IPV6 protocol. Why IPV6 is preferred over IPV4?** ***(May / June 2021)*** IPv6 (Internet Protocol version 6) is a set of basics of IPv6 are similar to those of IPv4. The most obvious improvement in IPv6 over IPv4 is that IP addresses are lengthened from 32 bits to 128 bits. This extension anticipates considerable future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses.	**C301.3**	**BL2**
15	**What is DHCP?** ***(Nov 19)*** DHCP (Dynamic Host Configuration Protocol) is a protocol that provides quick, automatic, and central management for the distribution of IP addresses within a network. DHCP is also used to configure the subnet mask, default gateway, and DNS server information on the device.	**C301.3**	**BL1**
16	**Explain IPV4 protocol.** IPv4 (Internet Protocol Version 4) is the fourth revision of the Internet Protocol (IP) used to identify devices on a network through an addressing system. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks. IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bitaddress scheme	**C301.3**	**BL2**
17	**Present an outline of IPv6 addressing.** ***(Nov 19)*** An IPv6 address is 128 bits in length and consists of eight, 16-bit fields, with each field bounded by a colon. Each field must contain a hexadecimal number, in contrast to the dotted-decimal notation	**C301.3**	**BL2**

<table>
<tr><td></td><td>of IPv4 addresses. In the below figure, the x's represent hexadecimal numbers.</td><td></td><td></td></tr>
<tr><td>18</td><td><table><tr><td colspan="2">What are the differences between IPV4 and IPV6? (Nov 21)</td></tr><tr><td>IPV4</td><td>IPV6</td></tr><tr><td>A 32-bit numeric address in IPv4 is written in decimal as four numbers separated by periods. Each number can be zero to 255.
For eg,
1.160.10.240 could be an IP address.</td><td>IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons. An example IPv6 address could be written like this:
3ffe:1900:4545:3:200:f8ff:fe21:67cf</td></tr></table></td><td>C301.3</td><td>BL1</td></tr>
<tr><td>19</td><td>Identify the class of the following IP Address: (May / June 2021)
11000001 10000011 00011011 11111111 = Class C
252.5.15.111 = Class D</td><td>C301.3</td><td>BL2</td></tr>
<tr><td>20</td><td>Why is IPV4 to IPV6 transition required? (May 17)
IPv4 and IPv6 networks are not directly interoperable, transition technologies are designed to permit hosts on either network type to communicate with any other host.</td><td>C301.3</td><td>BL2</td></tr>
<tr><td>21</td><td><table><tr><td colspan="2">Compare ARP and RARP.</td></tr><tr><td>ARP</td><td>RARP</td></tr><tr><td>Address Resolution Protocol.</td><td>Reverse Address Resolution Protocol.</td></tr><tr><td>Retrieves the physical address of the receiver.</td><td>Retrieves the logical address for a computer from the server.</td></tr></table></td><td>C301.3</td><td>BL2</td></tr>
<tr><td>22</td><td>What is the need of ARP? (Nov/Dec 2015)
ARP is used to find the physical address of the node when its Internet address is known. Any time a host/router needs to find the physical address of another host on its network, it formats an ARP query packet that includes the IP address and broadcasts it. All hosts in the network process the ARP packet but only the required station sends back physical address.</td><td>C301.3</td><td>BL2</td></tr>
<tr><td>23</td><td>Define RARP.
Allows a host to discover its internet address when it knows only its physical address (a diskless computer). The host wishing to retrieve its internet address broadcasts an RARP query packet that contains its physical address to every host on its physical network.</td><td>C301.3</td><td>BL1</td></tr>
</table>

<table>
<tr><td></td><td>A server on the network recognizes the RARP packet and returns the host's internet address.</td><td></td><td></td></tr>
<tr><td>24</td><td>How many network addresses and host addresses are supported by class A, class B networks?
• Class A: Number of networks = 127
Number of hosts = 224 -1
• Class B: Number of networks = 214 -1
Number of hosts = 216 – 1 = 65,535</td><td>C301.3</td><td>BL1</td></tr>
<tr><td>25</td><td>List the difference between Packet Switching and Circuit Switching. (Apr/May 2011, Nov/Dec 2011, May/June 2014)
<table>
<tr><td>Issue</td><td>Packet switching</td><td>Circuit Switching</td></tr>
<tr><td>Circuit setup</td><td>Not Required</td><td>Required</td></tr>
<tr><td>Transmission path</td><td>No Transmission path</td><td>Dedicated path</td></tr>
<tr><td>Delay</td><td>Packet transmission delay</td><td>Call setup delay</td></tr>
<tr><td>Addressing</td><td>Each packet contains the full source and destination address</td><td>Only data is sent</td></tr>
<tr><td>Bandwidth</td><td>Dynamic Bandwidth</td><td>Fixed Bandwidth</td></tr>
<tr><td>Routing</td><td>Each packet is routed independently</td><td>Entire data is sent through the same path</td></tr>
<tr><td>Congestion control</td><td>Difficult</td><td>Easy if enough buffers can be located in advance for each VC set up</td></tr>
<tr><td>Complexity</td><td>In the transport layer</td><td>In the network layer</td></tr>
<tr><td>Suited for</td><td>Connection-oriented and connectionless service</td><td>Connection-oriented service</td></tr>
</table></td><td>C301.3</td><td>BL1</td></tr>
<tr><td colspan="4">UNIT-III / PART-B</td></tr>
<tr><td>1</td><td>Explain Packet Switching in detail.</td><td>C301.3</td><td>BL2</td></tr>
<tr><td>2</td><td>i) Discuss the IP addressing methods. (May/June2014)
ii) Write short notes on ARP. (May/June2014) or Explain in detail ARP. (Nov/Dec 2015)</td><td>C301.3</td><td>BL2</td></tr>
<tr><td>3</td><td>Explain in detail about DHCP. (Nov/Dec 2015)</td><td>C301.3</td><td>BL2</td></tr>
<tr><td>4</td><td>What is the need for ICMP? Mention ICMP MESSAGES and their purpose. (May/June 2013)</td><td>C301.3</td><td>BL1</td></tr>
<tr><td>5</td><td>Explain about IPV6? Compare IPV4 and IPV6 (May 16)(Nov 21)</td><td>C301.3</td><td>BL2</td></tr>
</table>

6	Discuss about address Resolution protocols. (Nov/Dec 2013)	**C301.3**	BL2
7	Explain in detail about: i) ICMP ii) ARP iii) RARP. ***(Nov 19)***	**C301.3**	BL2
8	Explain IPv4 packet format and how fragmentation is applied in datagram delivery.	**C301.3**	BL3
9	Draw an IPv4 datagram and explain about the fields present in it.	**C301.3**	BL2

UNIT IV ROUTING

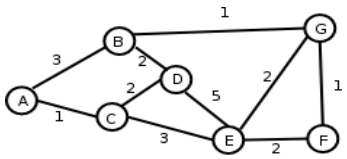
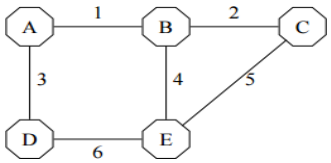
Routing and protocols: Unicast routing - Distance Vector Routing - RIP - Link State Routing - OSPF - Path-vector routing - BGP - Multicast Routing: DVMRP - PIM.

UNIT IV - PART A		**CO Statement**	**Knowledge Level(R/U/Ap/An/E/C)**
1	**Define routing.** ***(Nov12,15)*** It is the process of building up the tables that allow the collect output for a packet to be determined. It is a lot harder to create the forwarding tables in large, complex networks with dynamically changing topologies and multiple paths between destinations. Routing is a process that takes place in the background so that, when a data packet turns up, we will have the right information in the forwarding table to be able to forward, or switch, the packet.	**C301.4**	**BL1**
2	**Write on the packet cost referred in distance vector and link state routing.** ***(May 2012)*** In distance vector routing, cost refer to hop count while in case of link state routing, cost is a weighted value based on a variety of factors such as security levels, traffic or the state of the link.	**C301.4**	**BL1**
3	**What is source routing?** ***(Nov 13)*** Rotation, stripping off and using pointers are the different types of source routing approach.	**C301.4**	**BL1**
4	**What is the function of a router? (*Nov 10)(Nov 21*)** Routers relay packets among multiple interconnected networks. They route packets from one network to any of a number of potential destination networks on internet. A router operates at the physical, data link and network layer of the OSI model.	**C301.4**	**BL1**
5	**Write the difference between Distance vector routing and Link state routing.**	**C301.4**	**BL2**

Distance Vector Routing	**Link state routing**
Basic idea is each node sends its knowledge about the entire network to its neighbors.	Basic idea is every node sends its knowledge about its neighbors to the entire network
It is dynamic routing	It is dynamic routing
RIP uses Distance vector routing	OSPF uses link state routing

6	**What does a router do when it receives a packet with a destination address that it does not have an entry for, in its routing table?** **Default Router:** If IP Software is not able to find the destination, from routing table then it sends the datagram to default router. It is useful when a site has small set of local address connected to it and connected to the rest of the Internet.	**C301.4**	**BL1**
7	**What is piggybacking?** ***(Nov 19)*** The technique of temporarily delaying outgoing acknowledgment so that they can be hooked onto the next outgoing data frame is widely known as piggybacking.	**C301.4**	**BL1**
8	**Explain Multicast routing?** Multicast IP Routing protocols are used to distribute data for example, audio/video streaming broadcasts) to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients.	**C301.4**	**BL2**
9	**What is RIP?** RIP (Routing Information Protocol) is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network or an interconnected group of such LANs. Using RIP, a gateway host (with a router) sends its entire routing table (which lists all the other hosts it knows about) to its closest neighbor host every 30 seconds.	**C301.4**	**BL1**
10	**Explain about OSPF.** OSPF (Open Shortest Path First) is a router protocol used within larger autonomous system networks in preference to the Routing Information Protocol (RIP), an older routing protocol that is installed in many of today's corporate networks.	**C301.4**	**BL2**
11	**What is PIM?** **Protocol-Independent Multicast (PIM)** is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed *protocol-independent* because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other routing protocols. PIM Source-Specific Multicast, Bidirectional PIM PIM Dense Mode, PIM Sparse Mode	**C301.4**	**BL1**
12	**What is DVMRP?** **The Distance Vector Multicast Routing Protocol (DVMRP),** is a routing protocol used to share information between routers to facilitate the transportation of IP multicast packets among networks. The protocol is based on the RIP protocol. The router	**C301.4**	**BL1**

	generates a routing table with the multicast group of which it has knowledge with corresponding distances. When a multicast packet is received by a router, it is forwarded by the router's interfaces specified in the routing table.		
13	**What are the metrics used by routing protocols? (Apr/May 2015)** Path length, bandwidth, load, hop count, path cost, delay, Maximum Transmission Unit (MTU), reliability and communications cost.	**C301.4**	**BL1**
14	**Define Unicasting, Broadcasting and Multicasting. (Nov/Dec 2011)** Unicasting: Transmitting data from a single sender to a single receiver. Broadcasting: Transmitting data from a single source to all the other nodes in the network Multicasting: Transmitting data from a single source to a group of destination nodes.	**C301.4**	**BL1**
15	**Explain BGP.** BGP stands for Border Gateway Protocol. It can be defined as a standardized exterior gateway protocol which is developed to interchange routing information and reachability information between various autonomous systems (AS) on the Internet. It is classified as a path vector protocol as well as a distance-vector routing protocol.	**C301.4**	**BL2**
16	**What is a path vector routing protocol?** A path-vector routing protocol is a network routing protocol which maintains the path information that gets updated dynamically. Updates that have looped through the network and returned to the same node are easily detected and discarded.	**C301.4**	**BL1**
17	**What is count to infinity problem in distance vector routing?** 1. One of the important issues in Distance Vector Routing is County of Infinity Problem. 2. Counting to infinity is just another name for a routing loop. 3. In distance vector routing, routing loops usually occur when an interface goes down. 4. It can also occur when two routers send updates to each other at the same time.	**C301.4**	**BL2**
18	**What techniques are used to overcome the count to infinity issue in distance vector routing?** Split horizon technique and split horizon with poison reverse technique are used to overcome count to infinity issue in distance vector routing.	**C301.4**	**BL1**
19	**What are the contents of a link spate packet (LSP)?** LSP contains the following information: 1. The ID of the node that created the LSP 2. A list of directly connected neighbors of that node, with the	**C301.4**	**BL1**

	cost of the link to each one 3. A sequence number 4. A time to live for this packet		
20	**What is the main difference between BGP and Distance vector routing.** BGP differs from Distance Vector and Link State routings as it advertises complete paths as an enumerated list of ASs to reach a particular network.	**C301.4**	**R**
	UNIT IV - PART B		
1	Explain what is Distance Vector Routing and Demonstrate how distance table gives routing table ***(Nov 21)***	**C301.4**	BL2
2	Discuss about Link-state routing and routers. ***(Nov 12) (May 15)***	**C301.4**	BL2
3	Explain about the inter domain routing (BGP) routing algorithms.	**C301.4**	BL2
4	Explain the Routing Information protocol/Distance vector routing in detail. ***(Nov 13,15) (May 15,16)(Nov 19)***	**C301.4**	BL2
5	What are the different routing algorithms? List out their pros and cons. ***(May / June 2021)***	**C301.4**	BL1
6	Explain Link state routing with Dijkstra's algorithm for the following graph. 	**C301.4**	BL3
7	Explain Distance Vector Routing Algorithm for the graph given below. 	**C301.4**	BL3
8	Explain in detail the operation of OSPF protocol by considering a suitable network. ***(May 17)***	**C301.4**	BL3
9	Explain DVMRP multicast routing in detail	**C301.4**	BL2
10	Explain PIM multicast routing in detail.	**C301.4**	BL2
UNIT V	**DATA LINK AND PHYSICAL LAYERS** Data Link Layer - Framing - Flow control - Error control - Data-Link Layer Protocols - HDLC - PPP - Media Access Control - Ethernet Basics - CSMA/CD - Virtual LAN - Wireless LAN (802.11) - Physical Layer: Data and Signals - Performance - Transmission media- Switching - Circuit Switching.		
	UNIT V - PART A	**CO Statement**	**Knowledge Level(R/U/Ap/An/E/C)**
1	**List out the functions of data link layer** ***(May / June 2021)***	**C301.5**	**BL1**

	Data link layer deals with node-to-node delivery of data. The services provided by the data link layer include: framing, flow control, error control and access control.		
2	**What do you mean by framing? (Nov/Dec2013 and Nov/Dec 2014)** The data link layer divides the stream of bits received from the network layer into manageable data units called frames. The ways to address the framing problem are • Byte-Oriented Protocols (PPP) • Bit-Oriented Protocols (HDLC) • Clock-Based Framing (SONET)	**C301.5**	**BL1**
3	**What are the two types of errors occurred during data transmission? (May/June 2012)** Single bit error and burst error	**C301.5**	**BL1**
4	**Compare error detection and correction. (Nov/Dec 2012)** **Error Detection** | **Error Correction** Only the occurrence of an error is checked | The exact number of bits that are corrupted and location of error in the message are known.	**C301.5**	**BL2**
5	**Define bit stuffing. (Apr/May 2011)** HDLC denotes both the beginning and the end of a frame with the distinguished bit sequence 01111110. This sequence might appear anywhere in the body of the frame, it can be avoided by bit stuffing. On the sending side, any time five consecutive 1's has been transmitted from the body of the message (i.e., excluding when the sender is trying to transmit the distinguished 01111110 sequence), the sender inserts a 0 before transmitting the next bit.	**C301.5**	**BL1**
6	**What do you mean by Flow Control? (Nov/Dec 2011)** Flow control is a technique for assuring that a transmitting entity does not overwhelm a receiving entity with data. It is a feedback mechanism by which the receiver is able to regulate the sender. Such a mechanism is used to keep the sender from overrunning the receiver, i.e., from transmitting more data than the receiver is able to process	**C301.5**	**BL1**
7	**Why is flow control and error control duplicated in different layers?** Like the data link layer, the transport layer is responsible for flow and error control. Flow control and error control at data link layer	**C301.5**	**BL2**

<table>
<tr><td></td><td>is node-to-node level. But at transport layer, flow control and error control is performed end-end rather than across a single link.</td><td></td><td></td></tr>
<tr><td>8</td><td>Differentiate between lost frame and damaged frame?
<table>
<tr><th>Lost Frame</th><th>Damaged Frame</th></tr>
<tr><td>Lost frame is the frame that fails to arrive at the other side.</td><td>The damaged frame is a recognizable frame does arrive, but some of the bits are in error</td></tr>
</table></td><td>C301.5</td><td>BL2</td></tr>
<tr><td>9</td><td>What is the difference between stop and wait and sliding window protocol? (Nov/Dec 2012)
<table>
<tr><th>Stop and Wait Protocol</th><th>Sliding Window Protocol</th></tr>
<tr><td>In stop and wait protocol, we can send one frame at a time</td><td>In sliding window protocol, we can send multiple frames at a time.</td></tr>
<tr><td>Shows poor performance than Sliding Window Protocol, comparatively</td><td>As sliding window doesn't waste network bandwidth compared with stop-n-wait, both in normal and in congested condition, sliding window show better performance than stop-n-wait.</td></tr>
</table></td><td>C301.5</td><td>BL2</td></tr>
<tr><td>10</td><td>Why sliding window flow control is considered to be more efficient than stop and wait flow control?
In sliding window flow control, the transmission link is treated as a pipeline that may be filled with frames in transit. But with stop-and-wait flow control only one frame may be in the pipe at a time.</td><td>C301.5</td><td>BL1</td></tr>
<tr><td>11</td><td>Define Piggybacking?
The technique of temporarily delaying outgoing acknowledgment so that they can be hooked onto the next outgoing data frame is widely known as piggybacking.</td><td>C301.5</td><td>BL1</td></tr>
<tr><td>12</td><td>Find the hamming distance between the two pair of code words: A = 01011; B = 11110 (May / June 2021)
Hamming distance is the numbers of bits by which two codes differ. Here hamming distance = 3</td><td>C301.5</td><td>BL3</td></tr>
<tr><td>13</td><td>Define hidden node problem. (May 16)
In wireless networking, the hidden node problem or hidden terminal problem occurs when a node is visible from a wireless access point (AP), but not from other nodes communicating with that AP. This leads to difficulties in media access control sub layer.</td><td>C301.5</td><td>BL1</td></tr>
<tr><td>14</td><td>What is the access method used by wireless LAN? (May 14)</td><td>C301.5</td><td>BL1</td></tr>
</table>

	The access method used by wireless LAN is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)		
15	**What is meant by Exponential back of algorithm?** After first collision, each station waits either 0 or 1 slot time before trying again. If two stations collide and each one picks same random number 0/1. After second collision, each one picks 0, 1, 2 or 3 slot at random and waits. If collision occurs again, then next time the number of slots to wait is chosen at random from 0 to [2^3 – 1]. This algorithm is called binary exponential "back off algorithm".	**C301.5**	**BL1**
16	**What is High Level data link control?** ***(Nov 21)*** High-Level Data Link Control is a bit-oriented code-transparent synchronous data link layer protocol developed by the International Organization for Standardization. The standard for HDLC is ISO/IEC 13239:2002. HDLC provides both connection-oriented and connectionless service.	**C301.5**	**BL1**
17	**Give the format of Ethernet address.** Preamble 64 | Dest addr 48 | Src addr 48 | Type 16 | Body | CRC 32	**C301.5**	**BL1**
18	**Outline the use of cyclic redundancy check.** ***(Nov 19)*** 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.	**C301.5**	**BL2**
19	**What is CSMA/CD?** ***(Nov 11)*** Carrier Sense Multiple Access with Collision Detection is one of the methods of medium access. It is used to sense whether a medium is busy before transmission. If the medium is busy, it refrains from transmitting the data or else proceeds with the transmission. Also has the ability to check whether a transmission has collided with another.	**C301.5**	**BL1**
20	**Examine how Network Interface Card works.** ***(Nov 21)*** A Network Interface Card provides a computer with a dedicated, full-time connection to a network. It implements the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi.	**C301.5**	**BL2**
21	**List the rules for CSMA/CD.** 1. If the medium is idle, transmit; otherwise go to step 2. 2. If the medium is busy, continue to listen until the channel is idle, and then transmit immediately.	**C301.5**	**BL1**

	3. If a collision detected during transmission, transmit a brief jamming signal to all station to indicate collision has occurred and then cease transmission.		
22	**Mention some of the physical properties of Ethernet.** ***(May 11)*** The Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link. An Ethernet is like a bus that has multiple stations plugged into it.	**C301.5**	**BL1**
23	**Write the parameters used to measure network performance.** ***(May 2016)*** The parameters used to measure network performance are Latency, Throughput, Delay and Bandwidth.	**C301.5**	**BL1**
24	**Outline the need for switching.** ***(Nov 19)*** Switched communication networks are those in which data transferred from source to destination is routed between various intermediate nodes. Switching is the technique by which nodes control or switch data to transmit it between specific points on a network. There are three common switching techniques: Circuit Switching, message switching and packet switching.	**C301.5**	**BL2**
25	**List the types of Transmission media.** ***(Nov 21)*** Transmission Media is broadly classified into the following types: Guided Media: It is also referred to as Wired or Bounded transmission media. Common types are: (i) Twisted Pair Cable (ii) Coaxial Cable (iii) Optical Fiber Cable Unguided Media: Wireless Transmission. Common Types are: (i) Satellite (ii) Infrared (iii) Broadcast (iv)Wi-Fi	**C301.5**	**BL1**
26	**Define Bandwidth** Bandwidth refers to the number of bits per second that a channel, a link, or even a network can transmit.	**C301.5**	**BL1**
27	**What is Throughput?** It is a measure of how data can actually be sent through network.	**C301.5**	**BL1**
28	**What is meant by the contention period of Ethernet?** When several stations on an Ethernet have data to send, there are contention periods during which collisions happen and no data is successfully transmitted.	**C301.5**	**BL1**
29	**What does IEEE 10 Base 5 standard signify?** • 10 represents data rate 10 Mbps. • 5 refers to segment length 5* 100 m that can run without repeaters • Base represents Base band communication.	**C301.5**	**BL1**

30	**What do you mean by CSMA protocol? (Apr/May 2015)** Carrier sense multiple access (CSMA) is a media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium. Carrier sense means that a transmitter attempts to determine whether another transmission is in progress before initiating a transmission. If a carrier is sensed, the node waits for the transmission in progress to end before initiating its own transmission. In other words, CSMA is based on the principle "sense before transmit". Multiple access means that multiple nodes may send and receive on the medium. Transmissions by one node are generally received by all other nodes connected to the medium.	**C301.5**	**BL1**
	UNIT-V / PART-B		
1	Given a remainder of 111, a data unit of 10110011 and a divisor of 1001, is there an error in the data unit. Justify your answer with necessary principles. ***(May 14)***	**C301.5**	BL3
2	Explain the various error detection techniques with example. (Nov 10,12), (May 12,16)	**C301.5**	BL2
3	The message X5 + X4 + X 11001001 is to be transmitted, using CRC error detection algorithm. Assuming the CRC polynomial to be X3 + X2 + 1, determine the three-bit CRC code that should be appended to message. (May / June 2021)	**C301.5**	BL3
4	Discuss in detail about the HDLC protocol (Bit Oriented Protocol). ***(May 16) (Nov 19)***	**C301.5**	BL2
5	Explain various flow control mechanisms. i) Stop Wait protocol ii) Go Back-N iii) Selective Repeat (Nov 15)	**C301.5**	BL2
6	Discuss in detail about the PPP protocol (Byte Oriented Protocol).	**C301.5**	BL2
7	Describe the CSMA/CD protocol and comment on its performance for medium access. ***(May 11,14,17) (Nov 19)***	**C301.5**	BL4
8	Explain the functioning of wireless LAN in detail. ***(Nov 10,12,15) (May 15)***	**C301.5**	BL2
9	Explain how hidden node and exposed node problem is solved in IEEE 802.11 ***(Nov 13)***	**C301.5**	BL2
10	Explain Transmission media and its types in detail. ***(May / June 2021)***	**C301.5**	BL2
11	Explain the various performance metrics in detail.	**C301.5**	BL2
12	Explain Circuit Switching in detail. ***(Nov 19)(Nov/Dec 2021)***	**C301.5**	BL2