JEPPIAAR
ENGINEERING COLLEGE

JEPPIAAR NAGAR, CHENNAI - 600119

Department of Electronics & Communication Engineering

QUESTION BANK

EC3401 NETWORKS AND SECURITY

IV Semester ECE (Regulation 2021)

BATCH 2023-27

DEPARTMENT OF ECE

VISION OF

To build Jeppiaar Engineering College as an institution of academic excellence in technological and management education to become a world class University.

MISSION OF INSTITUTION

- To excel in teaching and learning, research and innovation by promoting the principles of scientific analysis and creative thinking.
- To participate in the production, development and dissemination of knowledge and interact with national and international communities.
- To equip students with values, ethics and life skills needed to enrich their lives and enable them to meaningfully contribute to the progress of society.
- To prepare students for higher studies and lifelong learning, enrich them with the practical and entrepreneurial skills necessary to excel as future professionals and contribute to Nation’s economy

PROGRAM OUTCOMES (POs)

PO1	**Engineering Knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and electronics engineering specialization to the solution of complex engineering problems.
PO2	**Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO3	**Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
PO4	**Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO5	**Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
PO6	**The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
PO7	**Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
PO8	**Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
PO9	**Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
PO10	**Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
PO11	**Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
PO12	**Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

VISION&MISSION, PEO & PSO OF THE DEPARTMENT

VISION OF ECE DEPT

To become a centre of excellence to provide quality education and produce creative engineers in the field of Electronics and Communication Engineering to excel at international level.

MISSION OF ECE DEPT

M1	Inculcate creative thinking and zeal for research to excel in teaching-learning process.
M2	Create and disseminate technical knowledge in collaboration with industries.
M3	Provide ethical and value based education by promoting activities for the betterment of the society.
M4	Encourage higher studies, employability skills, entrepreneurship and research to produce efficient professionals thereby adding value to the nation's economy.

PEO of ECE DEPT

PEO I	Produce technically competent graduates with a solid foundation in the field of Electronics and Communication Engineering with the ability to analyze, design, develop, and implement electronic systems.
PEO II	Motivate the students for successful career choices in both public and private sectors by imparting professional development activities.
PEO III	Inculcate in the students' ethical values, effective communication skills and develop the ability to integrate engineering skills to broader social needs.
PEO IV	Impart professional competence, desire for lifelong learning and leadership skills in the field of Electronics and Communication Engineering.

PSO of ECE DEPT

PSO I	Competence in using modern electronic tools in hardware and software co-design for networking and communication applications.
PSO II	Promote excellence in professional career and higher education by gaining knowledge in the field of Electronics and Communication Engineering
PSO III	Understand social needs and environmental concerns with ethical responsibility to become a successful professional.

EC3401 NETWORKS AND SECURITY

OBJECTIVES: The student should be made to:

- To learn the Network Models and data link layer functions.
- To understand routing in the Network Layer.
- To explore methods of communication and congestion control by the Transport Layer.
- To study the Network Security Mechanisms.
- To learn various hardware security attacks and their countermeasures**.**

UNIT I NETWORK MODELS AND DATALINK LAYER **9**

Overview of Networks and its Attributes – Network Models – OSI, TCP/IP, Addressing – Introduction to Data link Layer – Error Detection and Correction – Ethernet(802.3)- Wireless LAN – IEEE 802.11, Bluetooth – Flow and Error Control Protocols – HDLC – PPP.

UNIT II NETWORK LAYER PROTOCOLS **9**

Network Layer – IPv4 Addressing – Network Layer Protocols (IP, ICMP and Mobile IP) Unicast and Multicast Routing – Intradomain and Interdomain Routing Protocols – IPv6 Addresses – IPv6 – Datagram Format - Transition from IPv4 to IPv6.

UNIT III TRANSPORT AND APPLICATION LAYERS **9**

Transport Layer Protocols – UDP and TCP Connection and State Transition Diagram - Congestion Control and Avoidance(DEC bit, RED)- QoS - Application Layer Paradigms – Client – Server Programming – Domain Name System – World Wide Web, HTTP, Electronic Mail

UNIT IV NETWORK SECURITY **9**

OSI Security Architecture – Attacks – Security Services and Mechanisms – Encryption –Advanced Encryption Standard – Public Key Cryptosystems – RSA Algorithm – Hash Functions – Secure Hash Algorithm – Digital Signature Algorithm.

UNIT V HARDWARE SECURITY **9**

Introduction to hardware security, Hardware Trojans, Side – Channel Attacks – Physical Attacks and Countermeasures – Design for Security. Introduction to Block chain Technology

TOTAL:45 PERIODS

OUTCOMES:

Upon successful completion of the course the student will be able to

CO1: Explain the Network Models, layers and functions.
CO2: Categorize and classify the routing protocols.
CO3: List the functions of the transport and application layer.
CO4: Evaluate and choose the network security mechanisms.
CO5: Discuss the hardware security attacks and countermeasures

TEXT BOOK:

1. Behrouz A. Forouzan, ―Data communication and Networking‖, Fifth Edition, Tata McGraw – Hill, UNIT I – V)

REFERENCES

1. James F. Kurose, Keith W. Ross, ―Computer Networking - A Top-Down Approach Featuring the Internet‖, Seventh Edition, Pearson Education, 2016.

2. Nader. F. Mir,― Computer and Communication Networks‖, Pearson Prentice Hall Publishers, 2nd Edition, 2014.

3. Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, ―Computer Networks: An Open Source Approach‖, Mc Graw Hill Publisher, 2011.

UNIT I: NETWORK MODELS AND DATALINK LAYER

Overview of Networks and its Attributes – Network Models – OSI, TCP/IP, Addressing – Introduction to Data link Layer – Error Detection and Correction – Ethernet(802.3)- Wireless LAN – IEEE 802.11, Bluetooth – Flow and Error Control Protocols – HDLC

1. **Compare LAN and WAN.**

LAN	WAN
Scope of Local Area Network is restricted to a small/ single building	Scope of Wide Area Network spans over large geographical area country/ Continent
LAN is owned by some organization.	A part of n/w asserts are owned or not owned.
Data rate of LAN 10-100mbps.	Data rate of WAN is Gigabyte.

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.
3. **Why sliding window flow control is 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.
4. **What is OSI?**
OSI (Open Systems Interconnection) is reference model for how applications can communicate over a network. It is partitioned into seven layers. It was developed by the International Organization for Standardization (ISO).
5. **What is a protocol? What are the key elements of a protocol?**
Protocol is used for communications between entities in a system and must speak the same language. 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 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.
6. **What are the uses of transport layer?**
   - Reliable data exchange
   - Independent of network being used
   - Independent of application
7. **What is Protocol Data Unit (PDU)?**
At each layer, protocols are used to communicate and Control information is added to user data at each layer. Transport layer may fragment user data. Each fragment has a transport header added and header consists of destination SAP, sequence number and error detection code.
8. **What are the uses of internet layer in TCP/IP?**
   - Systems may be attached to different networks
   - Routing functions across multiple networks
   - Implemented in end systems and routers
9. **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.
   - A set of layers and protocol is called network architecture. A list of protocols used by a system is called protocol stack.
10. **Compare OSI and TCP.**

Open System Interconnection	Transmission Control Protocol
It distinguishes between Service, Interface, Protocol	It does not distinguish between Service, Interface, Protocol
Protocols are well hidden	Protocols are not just hidden
Dejure standard Fit Model	Defacto standard Fit Model
In transport layer only connection-oriented services are available	In Transport layer choice is for connection oriented and connectionless
Contains 7 layers	Contains 5 layers

11. **How do layers of the internet model correlate to the layers of the OSI model?**

OSI	TCP/IP
Physical Layer	Physical Layer
Data Link Layer	Network Access Layer
Network Layer	IP Layer
Transport Layer	TCP Layer
Session Layer	Application Layer

12. **What is the use of data link layer in OSI?**
    Frame **synchronization**: Data is divided by data link layer as frames, a manageable unit.
    Flow **Control**: Sending station does not overwhelm receiving station.
    Error **Control**: Any error in bits must be detected and corrected using some mechanism.
    Addressing: Two stations in a multi-point that involved in transmission must be specified using physical address
    Access **Control**: When two or more devices are connected to the same link, Access control mechanism is needed to determine which device has control over the link at any given time.
13. **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 is node-to-node level. But at transport layer, flow control and error control is performed end-end rather than across a single link.
14. **What are the functions of physical layer and presentation layer?**
    Functions of Physical Layer-
    - Encoding/ decoding of signals
    - Preamble generation/removal (for synchronization)
    - Bit transmission/ reception

    Functions of Presentation Layer-
    - Translation, Encryption / Decryption, Authentication and Compression
15. **What do you mean by Flow Control?**
    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 can process
16. **Define error detection and correction. (Nov 2011)**
    Error detection: Sender transmits every data unit twice. Receiver performs bit-by-bit comparison between those two versions of data. Any mismatch would indicate an error, which needs error correction. Error Correction is the process or analyzing and rectifying the errors and the code
17. **What are the functions of Application Layer? (May 2011)**
    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, and management. Mail services, Directory services.
18. **What do you mean by error control? (Nov 2010, May 2015)**
    Error control refers to mechanism to detect and correct errors that occur in the transmission of frames.
19. **What are the major duties of Network Layer? (May 2012)**
    It is used to send the data from source to destination with help of logical address.
20. **What are the two types of errors occurred during data transmission? (May 2012)**
    Single bit error and burst error
21. **Define networks. (Nov 2012)**
    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.
22. **Write the parameters used to measure network performance. (May 2016)**
    Latency, Throughput, Delay and Bandwidth.
23. **Compare error detection and correction. (Nov 2012)**

Error Detection	Error Correction
Only the occurrence of an error is checked	The exact number of bit that are corrupted and location of error in the message are known.

24. **What do you meant by framing? (Nov 2013 and Nov 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)

25. **What is the purpose of layering? (May 2013)**

- It decomposes the problem of building a network into more manageable components.
- It provides a more modular design.

26. **List the services provided by data link layer.(Nov 2016)**

The three major types of services offered by data link layer are:

1. Unacknowledged connectionless service 2. Acknowledged connectionless service.
3. Acknowledged connection-oriented service.

27. **Write the mechanism of stop and wait protocol. (Nov 2016)**

In this method of flow control, the sender sends a single frame to receiver & waits for an acknowledgment. The next frame is sent by sender only when acknowledgment of previous frame is received. This process of sending a frame & waiting for an acknowledgment continues as long as the sender has data to send. To end up the transmission sender transmits end of transmission (EOT)

28. **Give the format of Ethernet format. (Dec 2017)**

Preamble 64	Dest addr 48	Src addr 48	Type 16	Body (variable length)	CRC 32

29. Define routing

The process of determining systematically how to forward messages toward the destination node based on its address is called **routing.**

30. Distinguish between Packet Switched and Circuit Switched Networks. Apr/May 2017

Circuit switching	*Packet switching*
Source & destination are *physically* connected Switching takes place at the *physical* layer Resources are allocated in *advance*. Resources remain allocated for *entire* duration. *No delay* during data transfer. Data transferred is a *continuous* flow of signal Example: *Telephony*	No such physical connection exists Switching occurs at *network* / *data link* layer Resources are allocated on *demand* Resources can be *reallocated* when idle. *Delay* exists at each switch during data transfer Data is transferred as *discrete* packets Example: *Internet*

31. What is the basic idea behind STDM?

The idea of STDM is to divide time into equal-sized quanta and, in a round-robin fashion, give each flow a chance to send its data over the physical link. In other words, during time quantum 1, data from S1 to R1 is transmitted; during time quantum 2, data from S2 to R2 is transmitted; in quantum 3, S3 sends data to R3. At this point, the first flow (S1 to R1) gets to go again, and the process repeats.

32. What is the basic idea behind FDM?

The idea of FDM is to transmit each flow over the physical link at a different frequency, much the same way that the signals for different TV stations are transmitted at a different frequency on a physical cable TV link.

33. Define quality of service.

A network that attempts to allocate bandwidth to particular flows is sometimes said to support *quality of service (QoS)*.

Layering and protocols

34. Explain the Layering Characteristics and Features Layering Characteristics

- Each layer relies on services from layer below and exports services to layer above
- Hides implementation - layers can change without disturbing other layers

Features of Layering

a. First, it decomposes the problem of building a network into more manageable components, rather than implementing a monolithic piece of software
b. Second, it provides a more modular design.

35. *List* the advantages of layering.

a. It decomposes the problem of building a network into more manageable components.
b. It provides a more modular design. To add a new service, then it is only needed to modify the functionality at one layer, reusing the functions at all the other layers.
c. Uses abstraction to hide complexity of network from application.

36. What are the two interfaces provided by protocols?

a. Service interface
b. Peer interface

Service interface- defines the operations that local objects can perform on the protocol.

Peer interface- defines the form and meaning of messages exchanged between protocol peers to implement the communication service.

37. Why protocols needed?

In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

38. What is a protocol graph?

a. Suite of protocols that make up a network system is represented as a *protocol graph*.
b. Nodes correspond to protocols and edges represent a depends-on relation in the graph.

39. Define network architecture.

- Set of rules governing form and content of protocol graph is called network architecture.
- Network architecture guides the design and implementation of computer networks.
- Two commonly used architecture are
  - OSI Architecture
  - Internet or TCP/IP architecture

40. What purpose do header and trailer serve?

- A layer communicates control information to its peer, instructing it how to handle the message when it is received by attaching a header in front of the message.

- Trailer usually contains error control information.
- A header/trailer is a small data structure consists of a few bytes.

41. What is OSI?

A standard that specifies a conceptual model called Open systems Interconnection network interface model, which breaks networked communications into seven layers: Application, Presentation, Session, Transport, Network, Data link, Physical.

42. Define a layer.

a. The ISO defined a common way to connect computers, called the Open Systems Interconnection (OSI) architecture.
b. It defines partitioning of network functionality into seven layers as shown.
c. The bottom three layers, i.e., physical, data link and network are implemented on all nodes on the network including switches.

43. What are the issues in data link layer?

Specific responsibilities of data link layer include the following. a) Framing b) Physical addressing c) Flow control d) Error control e) Access control.

44. Group the OSI layers by function?

The seven layers of the OSI model belonging to three subgroups.

a. Physical, data link and network layers are the *network support layers*; they deal with the physical aspects of moving data from one device to another.
b. Session, presentation and application layers are the *user support layers*; they allow interoperability among unrelated software systems.

The transport layer ensures *end-to-end reliable data transmission Network software*

45. Explain the socket API for implementing network application.

- Network protocols are part of operating system and interface provided is known as *network application programming interface* (API).
- Network APIs provide *syntax* through which protocol services are invoked.
- Unix *socket* interface is widely used. Socket is an endpoint on the communication link between applications running on the network.
- Operations defined are socket creation, binding socket to network, send / receive messages and finally close the socket.

46. Explain the Socket Creation methods

- Socket is created using socket interface. A handle is returned on successful creation.

socket (*domain*, *type*, *protocol*)

  - *domain* argument specifies protocol family (PF_INET for Internet family, PF_PACKET for direct access to network, etc)
  - *type* argument specifies stream (SOCK_STREAM for byte stream, SOCK_DGRAM for message-oriented service, SOCK_RAW for raw sockets)
  - *protocol* argument specifies the protocol used (default value 0).

47. Explain the Server Process in network application

- Server processes perform *passive* open, i.e., it waits for client requests by invoking the following operations:

| bind (*socket*, *address*, *addr_len*) listen (*socket*, |

- bind operation attaches the socket to server host's IP address and port. Server port number is well-known, i.e., 0–1024 (for example, web servers use port 80).
- listen operation specifies number of pending connections. ○

accept operation blocks until a client establishes connection

48. Explain the Client Process in network application

- Client processes perform *active* open, i.e., it establishes connection with the server using connect operation.

- Client knows the remote server's logical address and port number and lets the system fill in detail such as client IP address and ephemeral port number.

Communication

- Communication between server and client process takes place after connection establishment using send and recv operation.

send (socket, message, msg_len,

- send operation is used to send message over the socket and recv operation is used to store the message received over the socket onto a buffer.

49. Define the term Bandwidth and Latency

- Bandwidth refers to number of bits that can be transmitted over the network within a certain period of time (*throughput*).
- Bandwidth also determines how *long* it takes to transmit each bit. For example, each bit on a 1-Mbps link is 1μs wide, wh ereas each bit on a 2-Mbps link is 0.5μs wide .

- Latency refers to how long it takes for the message to travel to the other end (*delay*). It is a factor of propagation delay, transmission time and queuing delay

Latency = Propagation + Transmit + Queue

- Speed of light propagation depends on medium and

distance. Propagation = Distance / Speed Of

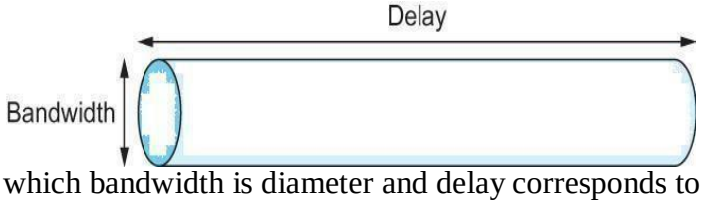
Light

- Transmission time depends upon bandwidth and packet

size. Transmit = Size / Bandwidth

- Queuing delay occurs at switches and routers, since packets are stored before forwarded.
- For applications that have minimal data transfer, latency dominates performance, whereas for bulk data transfers, bandwidth dominates performance.

50. Define Delay × Bandwidth Product



- Consider a pipe, in which bandwidth is diameter and delay corresponds to length.
- Delay × bandwidth product specifies the number of bits in transit. It corresponds to how much the sender should transmit before the first bit is received at the other end.
- For example, for a cross-country fiber with 10 Gbps bandwidth, distance of 4000 km, the RTT is 40 ms and RTT × bandwidth is 400 Mb.

51. Explain the High Speed Networks needs in the network performance

- High speed networks enhances the bandwidth for applications but latency remains fixed.
- For example, when a 1 MB file is transmitted over a 1 Mbps link takes 80 RTTs, whereas the same file over a 1 Gbps links falls short of 1 RTT.
- Effective end-to-end throughput that can be achieved is given as Throughput = TransferSize / TransferTime
- TransferTime includes latency as well as setup time.

52. Mention the Application Performance Needs

- Applications generally require as much bandwidth provided by the network.
- Average bandwidth of flow rates could be estimated, but instantaneous bursty traffic should also be handled.
- Latency varying from packet to packet is known as *jitter*. If receiver knows the latency that video packets may experience, then it delays playing first frame.

53. What are the three criteria necessary for an effective and efficient network?

The most important criteria are performance, reliability and security.

Performance of the network depends on number of users, type of transmission medium, and the capabilities of the connected h/w and the efficiency of the s/w.
Reliability is measured by frequency of failure, the time it takes a link to recover from the failure and the network's robustness in a catastrophe.
Security issues include protecting data from unauthorized access and viruses.

54. Explain how framing is done using bit and byte oriented protocols.

- Data link layer partitions message into smaller units called frames. When an error occurs, it affects only that small frame.
- Frame contains header (physical address of sender and destination), data and trailer (error control information). Frame length can be either fixed or variable.

55. What do you mean by framing? NOV/DEC 2013

A frame consists of one complete cycle of time slots, including one or more slot dedicated to each sending device.

56. Compare Byte-Oriented verses Bit-oriented protocol.

A bit-oriented protocol is a communications protocol that sees the transmitted data as an opaque stream of bits with no semantics, or meaning. Control codes are defined in terms of bit sequences instead of characters. Bit oriented protocol can transfer data frames regardless of frame contents.
Synchronous framing High-Level Data Link Control is a popular bit-oriented protocol.
Byte-oriented framing protocol is "a communications protocol in which full bytes are used as control codes. Also known as character-oriented protocol. UART communication is byte-oriented

57. What are the ways to address the framing problem?

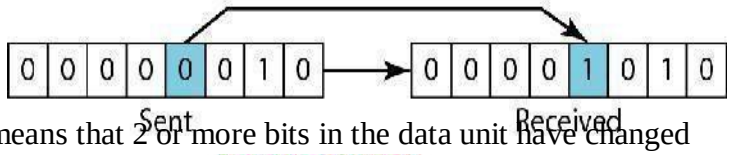
- Byte-Oriented Protocols(PPP)
- Bit-Oriented Protocols(HDLC)
- Clock-Based Framing(SONET)

58. How errors are introduced in the data?

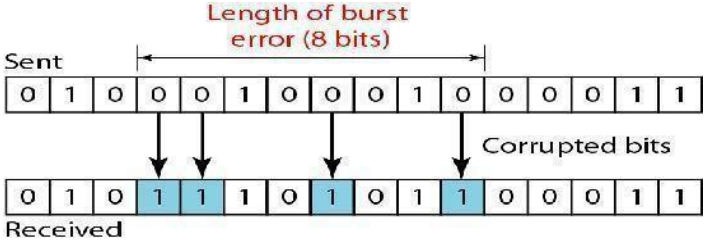
- Bit errors are introduced into frames because of electrical interference or thermal noise.
- This interference can change the shape of the signal, i.e. bit inversion.

59. List the types of error with an example.

- The two types of error are *single-bit* error and *burst* error
- *Single-bit* error means that only 1 bit of a given data unit is changed. Single-bit errors are the least likely type of error in serial data transmission.



- *Burst* error means that 2 or more bits in the data unit have changed



60. Mention the types of error correcting methods.

There are 2 error-correcting methods.

a. Single bit error correction
b. Burst error correction.

61. What is redundancy?

It is the error detecting mechanism, which means a shorter group of bits or extra bits may be appended at the destination of each unit.

62. Write short notes on error correction?

It is the mechanism to correct the errors and it can be handled in 2 ways.

- When an error is discovered, the receiver can have the sender retransmit the entire data unit.
- A receiver can use an error correcting coder, which automatically corrects certain errors.

63. What do you mean by error control? <u>NOV/DEC 2010, APR/MAY 2015</u>

Error control refers primarily to methods of error detection and retransmission. Anytime an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).

64. Define checksum.

The error detection method used by the higher layer protocol is called checksum. Checksum is based on the concept of redundancy.

65. What are the steps followed in checksum generator?

The sender follows these steps a) the units are divided into k sections each of n bits. b) All sections are added together using 2's complement to get the sum. c) The sum is complemented and become the checksum. d) The checksum is sent with the data

66. What is the purpose of hamming code?

A hamming code can be designed to correct burst errors of certain lengths. So the simple strategy used by the hamming code to correct single bit errors must be redesigned to be applicable for multiple bit correction

67. List out the available error detection methods.

Some of the redundancy checks that are used in data communication are:

a. Vertical redundancy checks (VRC).
b. Longitudinal redundancy checks (LRC).
c. Cyclic redundancy checks (CRC).
d. Checksum.

PART-B

1. **Eplain in detail the method of error detection and error correction**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 267
2. **Explain in detail about: HDLC**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 313
3. **Explain in detail about internet architecture**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 323
   Discuss in detail about the layers in OSI model.
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 33
4. **Explain the various flow control mechanisms.**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 35
5. **The message 11001001 is to be transmitted, using CRC error detection algorithm. Assuming the CRC polynomial to be x3+1, determine the message that should be transmitted. If the second left most bit is corrupted, show that it is detected by the receiver.**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 399
6. **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.**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 348
7. **Obtain the 4-bit CRC code for the data bit sequence 10011011111 using the polynomial $x^3 + x + 1$.**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 412
8. **Describe the architecture and protocol stack of Bluetooth technology.**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 434
9. **Explain in detail about the IEEE 802.11 protocol architecture, explain the physical layer and MAC layer.**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 421
10. **Explain sliding window flow control and stop and wait flow control in detail.**
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 318
11. **Discuss in detail about the network performance measures and selective-repeat ARQ flow control method.**
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 332
12. **Discuss in detail about the network performance measures (N/D-16)**
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 358
13. **Obtain the 4-bit CRC code for the data bit sequence 10011011100 using the polynomial x4+x2+1 (A/M-17)**
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no:357
14. **With a protocol graph, explain the architecture of internet (A/M-17)**
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 335
15. **Explain in detail about: PPP**
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 313

UNIT II
::0F53:6382:AB00:67DB:BB27:7
NETWORK LAYER PROTOCOLS

Network Layer – IPv4 Addressing – Network Layer Protocols (IP, ICMP and Mobile IP) Unicast and Multicast Routing – Intradomain and Interdomain Routing Protocols – IPv6

PART-A

1. **What is meant by ICMP? (May 2016)**

ICMP stands for Internet Control Message Protocol. It is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.

2. **List out the functions of IP.**

- IP stands for Internet Protocol. It performs routing function and finds a path from source to destination. IP includes a set of rules that provides unreliable, best-effort, connectionless packet delivery services.
- Unreliable – delivery is not guaranteed,
- Connectionless – each packet is treated independent from others,
- Best-effort delivery – it makes an earnest attempt to deliver packets. It defines basic unit of data transfer through TCP/IP.

3. **What is the network address in a class A subnet with the IP address of one of the hosts as 25.34.12.56 and mask 255.255.0.0? (May 2014)**

IP Address - 25.34.12.56
Mask - 255.255.0.0
Network Address - 25.34.0.0

4. **When is ICMP redirect message used?(May 2017)**

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 subsequently packets to that same destination through a different gateway.

5. **What details are provided by DHCP other than IP address? (NOV 2018)**

The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, and time servers

6. **List the difference between Packet Switching and Circuit Switching**. **(May14,May 17)**

Issue	**Packet switching**	**Circuit Switching**
Circuit setup	Not Required	Required
Transmission path	No Transmission path	Dedicated path
Addressing	Each packet contains the full source and destination address	Only data is sent
Bandwidth	Dynamic Bandwidth	Fixed Bandwidth
Routing	Each packet is routed independently	Entire data is sent through the same path
Congestion control	Difficult	Easy if enough buffers can be located in advance for each VC set up

7. **Differentiate Physical Address and Logical Address.**

Physical Address	**Logical Address**
It is implemented by data link layer	It is implemented by n/w layer
It contains 48 bits	It contains 32 bits
It is a local addressing system	It is an universal address system
Another name is MAC address	Another name is IP address
It is flat in nature	Hierarchical in nature
Does not give any clue for routing	Its structure gives clue for routing

8. **Define ARP. (Nov 2015)**

ARP stands for Address Resolution Protocol. It 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

9. Define RARP.

RARP stands for Reverse Address Resolution Protocol. It 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

10. Define routing. (Nov 2012, Nov 2015)

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another

11. 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, traffic, or the state of the link.

12. What is source routing? (Nov 2013)

A sender of a packet to partially or completely specify the route the packet takes through the network.

13. What is the function of a router? (Nov 2010)

The main purpose of a router is to connect multiple networks and forward packets destined either for its own networks or other networks. It has to determine the best possible transmission path among several available paths.

14. Write the difference between Distance vector routing and Link state routing.

Distance Vector Routing	Link state routing
Basic idea is each node sends its knowledge abou the entire network to its neighbors.	Basic idea is every node sends its knowledg 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

15. Identify the class of the following IP Address: (Nov /Dec2015)

(a) 110.34.56.45
(b) 212.208.63.23
(a) 110.34.56.45 – Class A
(b) 212.208.63.23- Class C

16. Define MTU.

A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet. The Internet's Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission

17. What does Border Gateway Protocol (BGP) mean? (Dec 2017)

Border Gateway Protocol (BGP) is a routing protocol used to transfer data and information between different host gateways, the Internet or autonomous systems. BGP is a Path Vector Protocol (PVP), which maintains paths to different hosts, networks and gateway routers and determines the routing decision based on that. It does not use Interior Gateway Protocol (IGP) metrics for routing decisions, but only decides the route based on path, network policies and rule sets. Sometimes, BGP is described as a reach ability protocol rather than a routing protocol.

18. Explain IPV6 protocol.

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. IPv6 also supports auto-configuration to help correct most of the shortcomings in version 4, and it has integrated security and mobility features.

19. 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.

20. Explain about OSPF. (May 2018)

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.Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information.

21. Explain Multicast routing? (May 2018)

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.

22. 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.

There are four variants of PIM:

- PIM Source-Specific Multicast
- Bidirectional PIM
- PIM Dense Mode
- PIM Sparse Mode

23. 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 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.

24. What are the differences between IPV4 and IPV6?

IPV4	IPV6
32-bit numeric address in IPv4 is written in decimal as four numbers separated by periods. Each number can be zero to 255.	IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons.
r example, **1.160.10.240** could be an IP address.	An example IPv6 address could be written like this: **3ffe:1900:4545:3:200:f8ff:fe21:67cf**
Checksum field is available in IPv4 header	No checksum field in IPv6 header.

25. Give the comparison of unicast, multicast and broadcast routing. (Nov16,May17)

No	icast	ulticast	oadcast
	e source and one destination	e source and group of destinations	e source and all destinations
	lationship is one to one	lationship is one to many	lationship is one to all

26. Check whether the following IPv6 address notations are correct? (NOV 2018)

a) ::0F53:6382:AB00:67DB:BB27:7332 - Incorrect

b) 7803:42F2:::88EC:D4BA:B75D:11CD - Incorrect

Why is IPv4 to IPv6 transition required? (May 2017)

The migration from IPv4 to IPv6 must be implemented node by node by using auto configuration procedures to eliminate the need to configure IPv6 hosts manually. This way, users can immediately benefit from the many advantages of IPv6 while maintaining the possibility of communicating with IPv4 users. The advantages are More Efficient Routing, More Efficient Packet Processing, Directed Data Flows, security.

27. What are the metrics used by routing protocols? (May 2015)

Metrics used by routing protocols are Hop count, Link cost , Delay , Bandwidth

28. State in brief the frequency hopping spread spectrum(FHSS) ?(N/D 19)

Frequency-hopping spread spectrum (FHSS) is a method of transmitting radio signals by rapidly changing the carrier frequency among many distinct frequencies occupying a large spectral band. The changes are controlled by a code known to both transmitter and receiver.

29. What is exposed station problem ?(N/D 19)

In wireless networks, the exposed node problem occurs when a node is prevented from sending packets to other nodes because of co-channel interference with a neighboring transmitter. ...
However note that R2 could still receive the transmission of S2 without interference because it is out of range of S1.

30. What is the need for fragmentation?(A/M 19)

Fragmentation is an Internet Protocol (IP) process that breaks packets into smaller pieces (fragments), so that the resulting pieces can pass through a link with a smaller maximum transmission unit (MTU) than the original packet size. The fragments are reassembled by the receiving host.

31. Draw the frame format of Ethernet. (A/M 19)

32. Define 802.11. (A/M-18)

Wireless LAN (WLAN) or Wi-Fi is designed for use in a limited area (office, campus, etc). It is standardized as IEEE 802.11

33. What do you meant by switching? (A/M-18)

- A switch is a *multi-input, multi-output* device, receives packets on one of its links and transmits them on one or more other links. This is known as *switching* or *forwarding*
- Hosts are connected to the switch using point-to-point link (star topology).
- Large networks can be built by *interconnecting* a number of switches, i.e., scalable.
- Switching is implemented by datagram or virtual circuit or source routing
- .

34. Suppose you are designing a sliding window protocol for a 1.5 Mbps point-to-point link, which has one way latency of 1.5 seconds. Assuming each frame carries 10 KB of data, what is the minimum number of bits required for the sequence number is SWS=RWS?(N/D 18)

find the window size based on delay-bw product, then find the max sequence number needed.

Delay BW Product= RTT * BW = 3 s * 1.5 Mbps = 4.5

No. of bits per frame= 10*1024*8 = 81,920 bits
Number of frames per window= 4.5 Mb / 81,920 bits per frame = 54.93
Approximate maximum sequence number = 110

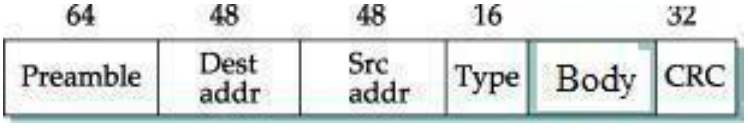
35. What details are provided by DHCP other than IP address? (N/D 18)

The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, and time servers

36. Show the Ethernet Frame Format**.** (N/D-17)

Ethernet is a multiple-access network, meaning that a set of nodes send and receive frames over a shared link.

Frame Format



- *Preamble*—alternating 0s and 1s that alerts the receiving node.
- *Destination address*—physical address of the destination host.
- *Source address*—physical address of the sender.
- *Type*—contains either type of upper layer protocol or frame length.
- *Body*—data (46–1500 bytes).
- *CRC*—error detection information (CRC-32).

37. Highlight the characteristics of datagram networks. (N/D-17)

In datagram approach, each packet is treated independently from all others. Even when one packet represents just a place of a multi packet transmission, the network treats it although it existed alone. Packets in this technology are referred to as datagram **.**

38. State the functions of Bridges. (A/M-17)

A bridge is a device that connects and passes packets between two network segments that use the same communications protocol. Bridges operate at the data link layer (layer 2) of the OSI reference model.

39. When is ICMP redirect message used? (A/M-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 subsequent packets tothat same destination through a different gateway.

40. What is meant by exponential backoff? .(N/D-16)

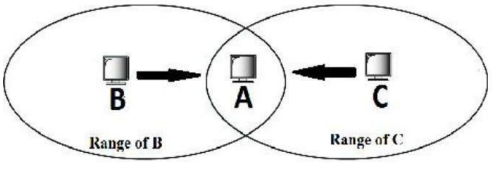
- When collision is detected, the node waits random amount of time and tries again.
- Each time it fails to transmit, the adaptor doubles the amount of time it waits for each reattempt. This is known as exponential back-off.

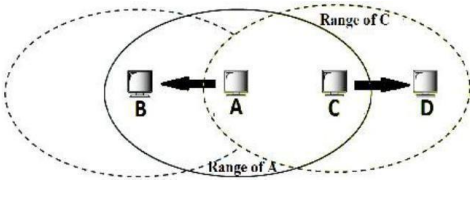
41. What is scatternet? .(N/D-16)

- Piconets can be combined to form *scatternet*. A node can be a part of two piconets, i.e., it can be slave in one and master in another piconet.
- Hardware and software is simple and inexpensive. Hence it is popular and widely used

42. Define hidden node problem (M/J-16)

- All nodes are not within the reach of each other.
- Carrier sensing may fail because of hidden node and exposed node problem.





- Suppose node *B* is sending data to *A*. At the same time, node *C* also wishes to send to *A*.
- Since node *B* is not within the range of *C*, *C* finds the medium free and transmits to *A*.

- Frames from nodes *B* and *C* sent to *A* collide with each other. Thus nodes *B* and *C* are *hidden* from each other.

43. What is Bluetooth? (M/J-16)

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs).

44. Expand ICMP and write the function**.** (M/J-16)

The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite.

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.

45. Define sub netting**.(**N/D-15)

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting. Computers that belong to a subnet are addressed with a common, identical, most-significant bit-group in their IP address.

46. What is the need of ARP? .(N/D-15)

ARP is a function of the IP layer of the TCP/IP protocol stack. It is necessary to translate a host.s software address (IP address) to a hardware address (MAC address). Typically, a host uses ARP to determine the hardware address of another host

47. What do you understand by CSMA protocol? (A/M-15)

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.

48. List the functions of bridges. (A/M-15)

- Pass data frames between networks using MAC address
- Break up collision domains
- Forwards all broadcast messages

49. Why is medium access control needed?

- If access to medium is not regulated, then multiple stations may transmit simultaneously resulting in collisions and retransmission.
- There will be little or no throughput on the network.
- Access to the medium could be either random or controlled or channelized.

50. Classify the various protocols used for medium access.

Random access	*Controlled access*	*Channelization*
➢ Aloha ➢ CSMA o CSMA/CA o CSMA/CD	➢ Reservation ➢ Polling ➢ Token passing	➢ FDMA ➢ TDMA ➢ CDMA

51. What is ALOHA protocol?

- ALOHA is a random access protocol. Station don't sense the medium before transmitting
- Resulted in high amount of collision with 18.4% throughput.
- When stations transmitted only at beginning of time slots, throughput doubled to 36.8%

52. Define 1-persistent, non-persistent and p-persistent sensing methods. 1-Persistent

- When a station finds the link idle, it sends frame immediately (with probability 1).
- High chances of collision because two or more stations may find the link idle and send frames immediately.

Non-persistent

- When a station senses the link to be idle, it sends immediately.

- If the link is not idle, it waits a random amount of time and then senses again.
- Reduces collision since it is unlikely that stations will wait same amount of time and retry
- Less efficient because the medium remains idle when there may be frames to send.

p-Persistent

- This method is used if channel has time slots equal to propagation time.
- If link is idle, with probability *p* station transmits frame, else waits for next time slot.
- If link is busy, back off procedure is adopted.
- Reduces collision and improves efficiency.

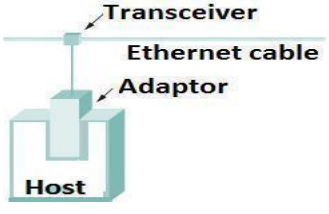
53. Brief the mechanism used in CSMA/CD?

- CSMA with collision detection (CSMA/CD) handles collisions over a wired medium.
- Station monitors the medium as it sends a frame
- If a collision is detected, it aborts transmission and broadcasts a jamming signal.
- Stations hearing jamming signal, refrain from transmitting frames.
- It waits for a random amount of time and attempts retransmission.

54. Explain IEEE 802.3 standard or Ethernet or CSMA/CD in detail.

- Ethernet was standardized as IEEE 802.3
- Standard Ethernet is the most successful LAN technology with a data rate of 10 Mbps.
- It has evolved into Fast Ethernet (100 Mbps) and Gigabit Ethernet (1Gbps, 10Gbps).

55. Explain the Physical Properties of Ethernet

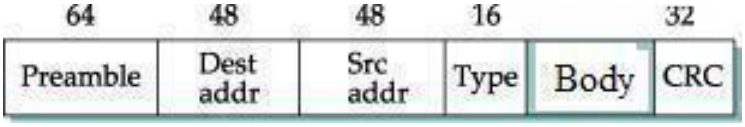


- Hosts are tapped on to the Ethernet segment, each at least 2.5 m apart.
- Transceiver is responsible for transmitting/receiving frames and collision detection.
- Protocol logic is implemented in the adaptor.
- Ethernet can support a maximum of 1024 hosts.
- Maximum length of Ethernet is 2500 m.
- Manchester encoding scheme is used with digital signaling at 10 Mbps.
- Various forms of Standard Ethernet are 10Base5 (thick ethernet), 10Base2 (thin ethernet), 10Base-T (twisted-pair) and 10Base-F (fiber-optic).
- Ethernet segments can be connected using *repeater or a hub*.

56. Draw the **Ethernet** Media Access Control (MAC) protocol format.

- Ethernet MAC protocol regulates access to the shared Ethernet link.

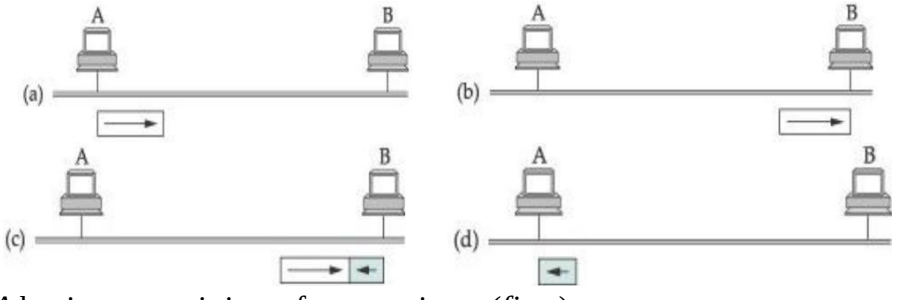
Frame Format



- *Preamble*—alternating 0s and 1s that alerts the receiving node.
- *Destination address*—physical address of the destination host.
- *Source address*—physical address of the sender.
- *Type*—contains either type of upper layer protocol or frame length.
- *Body*—data (46–1500 bytes).
- *CRC*—error detection information (CRC-32).

57. Why the minimum frame length in Ethernet should be at least 64 bytes (512 bits)?

- Consider the following worst case scenario in which hosts *A* and *B* are at either ends.



- Host *A* begins transmitting a frame at time *t* (*fig a*).
- It takes link latency *d* for the frame to reach host *B*. Thus, the first bit of *A*'s frame arrives at *B* at time *t* + *d* (*fig b*)
- Suppose an instant before host *A*'s frame arrives, *B* senses it idle and begins to transmit.
- *B*'s frame collides with *A*'s frame, and this collision will be detected by host *B* (*fig c*)
- Host *B* aborts its transmission and sends a runt frame.
- Host *A* knows about collision only when *runt* frame reaches it, at time *t* + 2*d* (*fig d*)
- RTT for Ethernet with maximum distance (2500 m) is 51.2µ s. It corresponds to 512 bits (64 bytes) on 10 Mbps standard Ethernet. Thus frame length of 512 bits is required for a host to detect collision before it transmits the last bit of that frame.

58. List the advantages and disadvantages of Ethernet.

- Easy to administer and maintain.
- Relataively inexpensive.
- Produces better output only when lightly loaded (< 200 hosts).
- It is an unreliable medium

59. List the function of a repeater?

- A repeater is a device that connects LAN segments and extends length of the LAN.
- It reconstructs a weak digital signal and forwards on all outgoing segments.
- Utmost four repeaters can be placed between a pair of hosts.
- It operates in the physical layer.

60. Give the features of 10Base5, 10Base2, 10BaseT and 10BaseF.

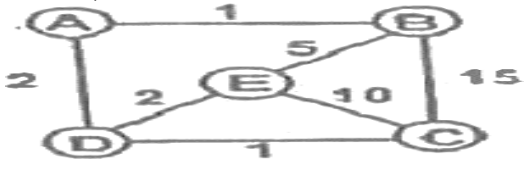
- *10Base5*—uses thick coax cable up to 500 m with bus topology (*Thick Ethernet*)
- *10Base2*—uses thin coax cable up to 200 m with bus topology (*Thin Ethernet*)
- *10BaseT*—uses twisted-pair cable up to 100 m with star topology (*Switched Ethernet*)
- *10BaseF*—uses fiber-optic cable up to 2000 m with star topology.

PART-B

1. **What is the need for ICMP? Mention ICMP MESSAGES and their purpose.**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 621
2. **Briefly explain the Border Gateway Protocol used for Inter domain routing in internetwork. (NOV 2018)**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 676
3. **Explain in detail about IP v4 addressing methods. (Nov 2012).**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 549
4. **Explain about IPV6. Compare IPV4 and IPV6. (May 2016) (May 2018)**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 335
5. **Explain the Routing Information protocol/Distance vector routing in detail. (Nov 2013) (May 2018)**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 665
6. **Explain the shortest path algorithm with suitable illustrations. (May 2015)**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 669
7. **Explain in detail the operation of OSPF protocol by considering a suitable network.(Nov 2016,May 2017)**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 671
8. **Outline the need of Distance Vector Multicasting Routing Protocol (May 18, Nov 2018)**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 1080

i) Explain the link-state algorithm in details.

ii) Consider the network shown in Fig. Compute the shortest path from C to all other nodes using link-state algorithm. Also update the forwarding table of node C. (NOV 2018)

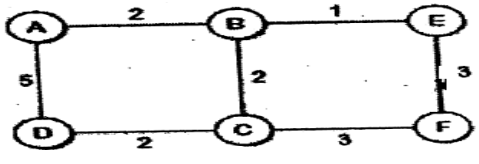


9. For the network given in Figure 1, give global distance – vector tables when

(i) Each node knows only the distance to its immediate neighbours.

(ii)Each node has reported the information it had in the preceding step to its immediate neighbors

(iii) Step (ii) happens a second time. (Dec 2017)



Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 696

10. **Explain details about Transition from IPv4 to IPv6.**
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 603
11. **Explain working of Protocol Independent Multicast (PIM) in detail.**
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 692
12. **Explain in detail about the access method and frame format used in Ethernet and Token ring.APR/MAY 2015**
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 397

13. Explain the functioning of wireless LAN in detail.NOV/DEC 2017

Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 454

14. Explain the functions of Wi-Fi and Bluetooth in detail. Nov/Dec 17

Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 436

15. Explain the Datagram forwarding in IP. Nov/Dec 17

Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 1097

UNIT III TRANSPORT AND APPLICATION LAYERS

Transport Layer Protocols – UDP and TCP Connection and State Transition Diagram - Congestion Control and Avoidance(DEC bit, RED)- QoS - Application Layer Paradigms – Client – Server Programming – Domain Name

PART-A

1. **What** are the services provided by Transport layer protocol. (May 2018)

ansport layer protocol provides

- Connection oriented services
- Reliable service by using Error Control and Flow Control.
- Multiplexing: Transport layer performs multiplexing/demultiplexing function. Multiple applications employ same transport protocol, but use different port number. According to lower layer n/w protocol, it does upward multiplex or downward multiplexing.

2. **Mention** the various adaptive retransmission policy of TCP.

- Simple average
- Exponential / weighted average
- Exponential RTT backoff
- Jacobson's Algorithm

3. **Define** congestion. (Nov 2011)

Congestion in a network occurs if user sends data into the network at a rate greater than that allowed by network resources. Any given node has a few I/O ports attached to it. There are two buffers at each port. One to accept arriving packets and another one to hold packets that are waiting to depart. If packets arrive too fast to the node than to process them or faster than packets can be cleared from the outgoing buffers, then there will be no empty buffer.

4. **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.

Source Port Address 16 bits	Destination Port Address 16 bits
Total Length 16 bits	Checksum 16 bits

- Source port address: Address of the application program that has created the message.
- Destination port address: Address of the application program that will receive the message.
- Total Length: It defines the total length of the user datagram in bytes.
- Checksum: It is a 16 bit field used in error correction.

5. **What** is the main difference between TCP & UDP? (Nov 2014,Nov 2016)

TCP	UDP
It provides Connection oriented service	Provides connectionless service.
Connection Establishment delay will be there	No connection establishment delay
Provides reliable service	Provides unreliable, but fast service
It is used by FTP, SMTP	It is used by DNS, SNMP, audio, video and multimedia applications.

6. **What** are the advantages of using UDP over TCP? (Nov 2010)

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.

7. What is TCP? (Nov 2011)

Transmission Control Protocol provides Connection oriented and reliable services. TCP guarantees the reliable, in order delivery of a stream of bytes. It is a full-duplex protocol, meaning that each TCP connection supports a pair of byte streams, one flowing in each direction. It is used by FTP, SMTP. The different phases in TCP state machine are Connection Establishment, Data transfer and Connection Release. TCP services to provide reliable communication are Error control, Flow control, Connection control and Congestion control.

8. **Name** the policies that can prevent (avoid) congestion.

DEC (Digital Equipment Corporation) bit, Random Early Detection (RED) and Source based congestion avoidance. The congestion may be avoided by two bits:

BECN - Backward Explicit Congestion Notification, FECN - Forward Explicit Congestion Notification.

9. List out various congestion control techniques.

Various congestion control techniques are AIMD (Additive Increase Multiplicative Decrease), Slow start Fast retransmit/Recovery.

10. What are the two categories of QoS attributes? (May 2015)

User Oriented and Network Oriented.

User related attributes are 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).

11. **Define** congestion control. (May 2018)

Congestion control is the process of preventing the source from sending data that will end up getting dropped by a router because its queue is full.

12. What is meant by slow start in TCP congestion? (May 2016)

TCP Slow Start is part of the ***congestion control*** algorithms to help control the amount of data flowing through to a network. It 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.

13. What is UDP?

It stands for User Datagram Protocol. It is part of the TCP/IP suite of protocols used for data transferring. UDP is a known as a "stateless" protocol, meaning it doesn't acknowledge that the packets being sent, have been received.

14. List the different phases used in TCP Connection. (May 2016)

Three phases used in TCP Connection are 1. Connection establishment 2. Data transfer 3. Connection termination

15. Compare flow control versus congestion control. (Nov 2015, Dec 17)

ngestion Control	**ow Control**
Congestion control means preventing the sourc from sending data that will end up getting droppe by a router because its queue is full.	Flow control means preventing the source from sending data that the receiver will end u dropping because it runs out of buffer space.
congestion control is concerned with how hosts and networks interact	It is an end to an end issue
This is more complicated, because packets from ferent sources travelling different paths can nverge on the same queue.	This is fairly easy with a sliding window protocol
chniques ● AIMD (Additive Increase Multiplicative Decrease) ● Slow start ● Fast retransmit/Recovery.	chniques ● Stop and wait ● Sliding window

16. How do fast retransmit mechanism of TCP works. (May 2017)

In TCP/IP, fast retransmit and recovery (FRR) is a congestion control algorithm that makes it possible to quickly recover lost data packets. With FRR, if a receiver receives a data segment that is out of order, it immediately sends a duplicate acknowledgement to the sender. If the sender receives three duplicate acknowledgements, it assumes that the data segment indicated by the acknowledgements is lost and immediately retransmits the lost segment.

17. **Suppose** TCP operates over 10-Gbps link. Assuming TCP could utilize the full bandwidth continuously, how long would it take the sequence numbers to wrap around completely? Is the sequence number space adequate? (NOV 2018)

The minimum packet size is 40 bytes.

2^32 packets * 320 bits per packet = 1.4 * 10^12 bits

1.4 * 10^12 bits / 1 * 10^10 bits per second = 1.4 * 10^2 seconds About 2.3 minutes.

18.**Define** QoS. (May 2012, Nov 2014, May 2015, Nov 2015 ,NOV 2018)

The quality of service defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute each service class is associated with a set of attributes. The attributes are- Bandwidth, Latency or Delay, Jitter, Packet loss ratio.

19.**What** is DNS? (May 2018)

Domain Name System converts domain names into IP addresses so browsers can load Internet resources. It is mainly used for a memorable way of identifying hosts because IP numbers uniquely identify hosts on the Internet but are difficult to remember.. A DNS Resolver is responsible for making requests of the local DNS server on behalf of clients

20.**What** is WWW and SMTP? (Nov 2010,May 2014, May 2015)

World Wide Web is an internet application that allows user to view pages and move from one web page to another. 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. SMTP provides mail exchange between users on the same or different computers.

21. What **is PGP? (Nov 2010, May 2012,May 2014)**

Pretty Good Privacy (PGP) is used to provide security for electronic mail. It provides authentication, confidentiality, data integrity, and non repudiation. It is a program using public key encryption popularly used with email.

22. **Present** the information contained in a DNS resource record.(May 2017)

Resource Records define data types in the Domain Name System (DNS).Resource Records identified by RFC 1035 are stored in binary format internally for use by DNSsoftware. But resource records are sent across a network in text format while they perform zone transfers.

23.What is the use of MIME Extension?(Nov 2014)

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.

24.What is POP3?(Nov 2016)

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server.

25.What is IMAP?

Internet Message Access Protocol (IMAP) is a standard protocol for accessing e-mail from your local server. IMAP is a client/server protocol in which e-mail is received and held for you by your Internet server. IMAP can be thought of as a remote file server. POP3 can be thought of as a "store-and-forward" service.

26.Mention the different levels in domain name space. (May 2012,16)

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.
- Country domain: Uses two characters to identify a country as the last suffix.
- Inverse domain: Finds the domain name given the IP address.

27.State the usage of conditional get in HTTP.(May 2017)

A conditional GET is an HTTP GET request that may return an HTTP 304 response. An HTTP 304 response indicates that the resource has not been modified since the previous GET, and so the resource is not returned to the client in such a response.

28. Write short notes on Email.

E-mail (electronic mail) is the exchange of computer-stored messages by telecommunication. Email messages are usually encoded in ASCII text. The architecture of the email system consists of two kinds of subsystems: the user agents, which allow people to read and send email, and the message transfer agents, which move the messages from the source to the destination.

29.Consider an HTTP client that wants to retrieve a Web document at a given URL. The IP address of the HTTP server is initially unknown. What transport and application layer protocols are needed in this scenario? (NOV 2018)

Application layer protocol: DNS and HTTP

ansport layer protocol : UDP for DNS and TCP for HTTP

30. Write the use of Hyper Text Transfer Protocol (HTTP). (Dec2017, May 2018))

The browser **uses HTTP**, which is carried over TCP/IP to communicate to the server and retrieve Web content for

the user. **HTTP** is a widely used **protocol** and has been rapidly adopted over the Internet because of its simplicity. It is a stateless and connectionless **protocol**.

.

31. State few disadvantages of wireless LAN s?(N/D 19)

i. This communication **is** very prone to interference and noise.

ii. It has limited coverage area.

iii. Communication **is** not very secure and unauthorised access **is** common.

32. Distinguish between virtual circuit and datagram type of routing ?(N/D 19)

A virtual circuit network uses a fixed path for a particular session, after which it breaks the connection and another path has to be set up for the next the next session. A Datagram based network is a true packet switched network. Packets reach in order to the destination as data follows the same path.

33. What is the two major mechanisms defined to help transition from IPv4 to IPv6?(A/M 19)

Ans: **Tunneling and Dual stack**

34. Make a routing table for the Router RI using the configuration given in the figure below. **?(A/M 19)**

Ans: Routers examine the destination IP address of a received packet and make routing decisions accordingly. When a router receives a packet that needs to be forwarded to a host on another network, it examines its destination IP address and looks for the routing information stored in the routing table.

35. What are the benefits of Open Shortest Path First(OSPF) Protocol? ?(A/M-18)

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.Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information.

36. What is multicast routing? ?(A/M-18)

- To support multicasting, routers *additionally* build multicast forwarding tables.
- Multicast forwarding table is a tree structure, known as *multicast distribution trees*.
- Internet multicast is implemented on physical networks that support broadcasting.
- Major multicast routing protocols are:

Distance-Vector Multicast Routing Protocol (DVMRP)
Protocol Independent Multicast Sparse Mode (PIM-SM)
Interdomain Multicast (MSDP)
Bidirectional Trees (BIDR-PIM)

37. List the two factors that affect the performance of a network switch.(N/D -18)

Factors that affect the performance of a network switch are- Bandwidth. Throughput. Latency, Jitter and Error rate

38. **Check whether the following IPv6 address notations are correct? (N/D -18)**

a)::0F53:6382:AB00:67DB:BB27:7332 - Incorrect

b)7803:42F2:::88EC:D4BA:B75D:11CD – Incorrect

39. Differentiate between forwarding table and routing table.(N/D-17)

A routing table uses a packet's destination IP address to determine which IP address should next receive the packet, that is, the "next hop" IP address.

A forwarding table uses the "next hop" IP address to determine which interface should deliver the packet to that next hop, and which layer 2 address (e.g., MAC address) should receive the packet on multipoint interfaces like Ethernet or Wi-Fi.

40. What is Border Gateway Protocol (BGP)? (N/D-17)

Border Gateway Protocol (BGP) is a routing protocol used to transfer data and information between different host gateways, the Internet or autonomous systems. BGP is a Path Vector Protocol (PVP), which maintains paths to different hosts, networks and gateway routers and determines the routing decision based on that. It does not use Interior Gateway Protocol (IGP) metrics for routing decisions, but only decides the route based on path, network policies and rule sets. Sometimes, BGP is described as a reach ability protocol rather than a routing protocol.

41. How do routers differentiate the incoming unicast, multicast and broadcast IP packets?(A/M- 17)

unicast addresses – represent a single LAN interface. A unicast frame will be sent to a specific device, not to a group of devices on the LAN.

multicast addresses – represent a group of devices in a LAN. A frame sent to a multicast address will be forwarded to a group of devices on the LAN.

broadcast addresses – represent all device on the LAN. Frames sent to a broadcast address will be delivered to all devices on the LAN.

42. Why is IPV4 to IPV6 transition required?(A/M-17)

Auto Configuration - Auto Configuration is now built in and helps make IP addressing more managable. With IPv4, we relied on DHCP or manually configurating IP addresses.

Direct Addressing - With Direct Addressing, the primary use of NAT (Network Area Translation) now becomes obsolete with IPv6. So, Direct Addressing is now possible.

Mobility - Mobility is better integrated into IPv6 than it is with IPv4. It makes it easier for users to roam to different networks and keep their same IP address.

Improved Integrated Security (IPSec) - IPSec is now integrated into IPv6, while with IPv4 it was more an add-on.

43. Define VCI. (N/D-16)

An Incoming **virtual circuit identifier (VCI)** uniquely identifies the connection at this switch and that will be carried inside the header of the packets that belong to this connection. It is a potentially different **outgoing VCI** that will be used for outgoing packets. The combination of incoming interface and incoming VCI uniquely identifies the virtual connection. VCI assigned by n/w admin is an unused value on that interface and VCIs are unique on a link and not on entire n/w. Also incoming and outgoing VCIs need not be same.

44. What is fragmentation and reassembly? (N/D-16)

Fragmentation—In IPv6, source host uses a path MTU discovery technique to find smallest MTU on the path and fragments the packet accordingly

Auto configuration—Auto or stateless configuration of IP addresses to hosts using interface id and address prefix for that subnet i.e., plug and play.

45. Write the types of connecting devices in internetworking?(A/M-16)

Backbone Network is a means of connecting 2 LAN's. It provides a transmission channel for packets from being transmitted from one LAN to the other. The individual LAN's are connected to the Backbone Network by using some types of devices such as Hubs, Repeaters, Switches, Bridges, Routers and Gateways.

46. Identify the class of the following ipv4 address (N/D-15)

110.34.56.45

212.208.63.23

110.34.56.45: This IP address belongs to Class A.

212.208.63.23: This IP address belongs to Class C

47. How does a router differ from a bridge? (A/M-15) (N/D-15)

A bridge is a product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or Token Ring). You can envision a bridge as being a device that decides whether a message from you to someone else is going to the local area network in your building or to someone on the local area network in the building across the street.

A router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each point-of-presence on the Internet. A router is often included as part of a network switch.

48. What are the metrics used by routing protocols? (A/M-15)

Metrics are used to determine whether one route should be chosen over another.

Router metrics can contain any number of values that help the router determine the best route among multiple routes to a destination. A router metric typically based on information like path length, bandwidth, load, hop count, path cost, delay, Maximum Transmission Unit (MTU), reliability and communications cost.

49. Define routing. (Nov/Dec 2012)

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.

50. Write on the packet cost referred in distance vector and link state routing. (Apr/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.

51. **Distinguish between forwarding and routing table.**

- Forwarding table contains mapping between network number and outgoing interface as well as physical address of the next hop.
- Routing table contains mapping between network number and logical address of next hop. It is built by routing algorithm.

Prefix/Length	Next Hop
18/8	171.69.245.10

Routing Table Example

Prefix/Length	Interface	MAC Address
18/8	if0	8:0:2b:e4:b:1:2

Forwarding Table Example

52. Define autonomous system or domain.

- A domain or autonomous system is an internetwork in which all routers are under a single administrative control (eg. University campus, Service provider network).
- Routing within a domain is known as intra-domain routing whereas routing between domains is known as inter-domain routing.
- Distance vector routing (RIP) and Link state routing (OSPF) are intra-domain routing, whereas Path vector (BGP) is inter domain routing.

53. Explain distance vector routing (or) routing information protocol (or) bellman-ford algorithm

- Each node *knows* the distance (cost) to each of its directly connected neighbors.
- Nodes construct a *vector* (Destination, Cost, NextHop) and distributes it to neighbors.

- Nodes compute routing table of *minimum* distance to every other node via NextHop using information obtained from its neighbors.

54. Define a switch.

Switches are hardware or software device capable of creating temporary connections between more devices which are not directly connected. It is a multi input/output port device. It transfers data coming from one input port to one or more output ports. This function is called as forwarding. Reliability, performance, security, and geography are the reason for using bridges in LAN.

55. What is the function of a router? (Nov/Dec 2010)

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 as the physical, data link and network layer of the OSI model. A router is termed as an intelligent device. Therefore, its capabilities are much more than those of a repeater or a bridge. A router is useful for interconnecting two or more heterogeneous networks that differ in their physical characteristics such as frame size, transmission rates, topologies, addressing etc. A router has to determine the best possible transmission path among several available paths. Destination, Cost and Next Hop are the important fields in a routing table.

PART-B

1. What is meant by QoS in networking? State the techniques to improve QoS. **(May 2012)**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 786
2. Why does TCP uses adaptive retransmission and describe its mechanism**.(Nov/Dec 2013)**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 723
3. Write Short notes on i) DNS ii) WWW iii) HTTP iv) E-Mail
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 812
4. With TCPs slow start and AIMD for congestion control, show how the window size will vary for transmission where every 5^{th} packet is lost. Assume an advertised window size of 50 MSS. (**May 2017)**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 820
5. Draw a TCP state transition diagram for connection management. (7) (**Dec2017)**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 759
6. **Brief about approaches used for TCP congestion control. (6)**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 765
7. **Discuss the working of E Mail in detail** (May 2015,May 2018)
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 824
8. **Discuss about MIME, IMAP and POP3.** (Nov 2010)
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 836
9. **Describe how SMTP protocol is used in E-mail applications.**
   Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 834
10. **Explain HTTP with an example.** (May 2016)
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 861
11. **Explain in detail about SNMP messages** (Nov 2016,DEC 17)
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 877
12. **Illustrate the role of POP3 in Electronic mail applications**
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 838
13. **Briefly explain the Domain Name Service protocol with an example** (DEC17/NOV 2018)
    Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 797
14. **Explain in detail about Address Resolution protocol and subnetting? NOV/DEC 2012.**

Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 613

15. **Describe the methods that are used to calculate the shortest path between two routers? A/M 17**

Refer : Behrouz.A.Forouzan, Data Communication and Networking Page no: 668

U

NIT IV NETWORK SECURITY

PAR

OSI Security Architecture – Attacks – Security Services and Mechanisms – Encryption –

PART-A

1. What is Security attack, Security mechanism and Security service?

Security attack: Any action that compromises the security of information owned by an organization.
Security mechanism: A mechanism that is designed to detect, present or recover from a security attack.
Security service: A service that enhances the security of the data processing systems and the information transfer of an organization.

2. Define confidentiality.

Confidentiality ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. This type of access includes printing, displaying, and other forms of disclosure.

3. Define integrity.

Integrity ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing, deleting, creating and delaying or replaying of transmitted messages.

4. Define Authentication, Nonrepudiation, Availability and Access control.

Authentication: Ensures that the origin of a message is correctly identified, with an assurance that the identity is not false.
Nonrepudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.
Availability: Requires that computer system assets be available to authorized parties when needed.
Access control: Requires that access to information resource may be controlled by or for the target system.

5. List 4 general categories of attack.

Interruption, Interception, Modification, Fabrication

List the components involved in network security (i.e. Model for network security)

Message, Two principals (Source and Destination), Trusted third party Opponent

6. List the 4 basic tasks in designing a particular security service.

Design an algorithm for performing the security-related Transformation

Generate the secret information to be used with the algorithm

Develop methods for the distribution and sharing of secret information

Specify a protocol to be used by the two principals.

7. List the five main components of a conventional encryption system.

Plaintext, Encryption algorithm, Ciphertext, Decryption algorithm

Define Plaintext, Ciphertext

Plaintext: Refers to the original message that is created and sent into encryption method. **Ciphertext:** It is the text that is now scrambled and ready to send. It may look like a random stream of data, and is unreadable.

8. How cryptographic systems are generally classified?

Cryptographic systems are generally classified along 3 independent dimensions.

The type of operations used for transforming plaintext into ciphertext (permutation/substitution)

The number of keys used (single key/different key)

The way in which the plaintext is processed (Block cipher/Stream cipher)

9. Differentiate block cipher and stream cipher.

Block cipher: A block cipher processes the input one block of elements at a time, producing an output block for each input block.

Stream cipher: A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along

10. What is steganography?

Steganography is the practice of concealing a file, message, image or video within another file, message, image or video. i.e. It is hiding a secret message within an ordinary message and the extraction of it at its destination.

11. Compare steganography and cryptography.

- The meaning of steganography is covered or hidden writing while cryptography signifies secret writing.
- Steganography is an attempt to achieve secure and undictable communication. Cryptography intends to make the message readable for only the target recipient and not by others.
- In steganography, the main structure of the message is not changed whereas cryptography imposes a change on the secret message before transferring it over the network.
- The steganography can be employed on text, and in video and image while cryptography is implemented only on the text file.

12. What is symmetric key encryption?

Symmetric key encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.

13. List the 5 main components of a symmetric encryption system.

Plaintext, Encryption algorithm, Secret key, Ciphertext, Decryption algorithm

14.* Give the 5 modes of operations of block cipher. (*Dec 2020)

Electronic codebook (ECB), Cipher block chaining (CBC), Cipher feedback (CFB), Output feedback (OFB), Counter (CTR)

15. Define confusion and diffusion

Confusion refers to making the relationship between the key and the cipher text as complex and involved as possible

Diffusion refers to the property that redundancy in the statistics of the plaintext is dissipated in the statistics of plaintext.

16. List the 4 different stages of AES.

Substitute bytes, Shift rows, Mix column, Add round key

17. Why random numbers are use in network security?

Random numbers used to generate keys

- Symmetric keys
- RSA: Prime numbers
- Diffie-Hellman secret values Random numbers used for nonce
- Sometimes a sequence is okay
- But sometimes nonce must be random Random numbers also used in simulations.

18. What is public key cryptography?

Public key cryptography (or asymmetric cryptography) is an encryption scheme that uses two mathematically related, but not identical keys – a public key and a private key. Each key performs a unique function. The public key is used to encrypt and the private key is used to decrypt.

19. List the 6 ingredients of public key encryption.

- ✓ Plaintext
- ✓ Encryption algorithm
- ✓ Public key
- ✓ Private key
- ✓ Cipher text

Decryption algorithm

20. Perform encryption for the plaintext M=88 using the RSA algorithm. P=17, q=11 and public component e=7

i. p=17, q=11
ii. Calculate n=p*q = 17*11 =187
iii. Calculate □(*n*) = (p-1)(q-1) = 16*10=160
iv. Select e=7
v. Determine d such that de □ 1(mod 60). The correct value of d is 23

Public key (7,187) and private key (23,187) Encryption: 88^7 mod 187 = 11

21. Perform encryption and decryption using the RSA algorithm for the following. P=7, q=11, e=17 and M=8

i. p=7, q=11
ii. Calculate n=p*q = 7*11 =77
iii. Calculate □(*n*) = (p-1)(q-1) = 6*10=60
iv. Select e=17
v. Determine d such that de □ 1(mod 60). The correct value of d is 53

Public key (17,77) and private key (53,77)

Encryption: 8^{17} mod 77 = 56

Decryption: 56^{53} mod 77 = 8

22. List the 5 possible approaches to attacking the RSA algorithm

✓ Brute force
✓ Mathematical attacks
✓ Timing attacks
✓ Hardware fault-based attack

Chosen ciphertext attacks

23. Show how SHA is more secure than MD5

□ It produces a largest digest (160-bit compared to 128 bits, so a brute force attack would be more difficult to carry out)
□ No known collisions have been formed for SHA

Never version have been introduced in SHA (SHA-256, SHA-384, SHA-512) that are much more secure than the original.

24. What is digital signature?

A digital signature is an authentication technique that also includes measures to counter repudiation by either source or destination

25. List the types of functions that may be used to produce an authenticator.

✓ **Message encryption:** The ciphertext of the entire message serves as its authenticator.
✓ **Message Authentication Code(MAC):** A public function of the message and a secret key that produces a fixed length value that serves as the authenticator.
✓ **Hash function:** A public function that maps a message of any length into fixed-length hash value, which serves as the authenticator.

26. What is hash(function) in cryptography?

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

27. What is the role of compression function in hash function?

The compression function is a function that transforms two fixed length inputs into a fixed length output. The transformation is one-way, meaning that it is difficult given a particular output to compute inputs which compress to that output. One-way compression function are not related to conventional data compression algorithm, which

instead can be inverted exactly or approximately to the original data.

28. Specify the various types of authentication protocol

An authentication protocol is a type of computer communication protocol or cryptographic protocol specifically designed for transfer of authentication data between two entities. Different types are

- ✓ Password Authentication Protocol (PAP)
- ✓ Challenge Handshake Authentication Protocol (CHAP)
- ✓ Extensible Authentication Protocol (EAP)
- ✓ Remote Authentication Dial-In User Service (RADIUS)

Kerberos (Protocols)

29. What is digital signature?

A digital signature is an authentication mechanism that allows the sender to attach an electronic code with the message in order to ensure its authenticity and integrity. This electronic code acts as the signature of the sender and, hence is named digital signature. Digital signature uses the public-key cryptographic technique. The sender uses his private key and a signing algorithm creates a digital signature, and the signed document can be made public. The receiver uses the public key of the sender and a verifying algorithm to verify the digital signature.

30. Distinguish between TCP and UDP ?(N/D 19)

TCP is a connection-oriented protocol and UDP is a connection-less protocol. TCP establishes a connection between a sender and receiver before data can be sent. UDP does not establish a connection before sending data.

31. Mention various techniques used in improve Quality of service (Qos)?(N/D 19)

QoS or Quality of Service in **networking** is the process of managing **network** resources to reduce packet loss as well as lower **network** jitter and latency. **QoS** technology can manage resources by assigning the various types of **network** data different priority levels

32. How does UDP address flow control mechanism?(A/M 19)

Ans: A typical session involves sending packets from a source IP address and port to a destination IP address and port. TCP and UDP packet headers contain source and destination port address information. These packets flow between the applications at either end of the connection. Therefore, they are often called "flows."

33. State the purpose of service model.(A/M 19)

Ans: Service design may function as a way to inform changes to an existing service or create a new service entirely. The purpose of service design methodologies is to establish best practices for designing services according to both the needs of customers and the competencies and capabilities of service providers

34. What are the services provided by Transport layer protocol?(A/M-18)

- ➢ Guaranteed and in-order delivery of the message.
- ➢ Supports multiple application processes on each host.
- ➢ Supports synchronization between the sender and the receiver.
- ➢ Allows receiver to apply flow control to the sender.
- ➢ Transport layer protocols are UDP, TCP and RTP.

35. Define congestion control. (A/M-18)

- ➢ Congestion occurs if load (number of packets sent by sources) is greater than capacity of the network

/ link (number of packets that can be handled).

- When load exceeds capacity, queues become full and routers have to discard some packets. Hence throughput declines sharply.
- TCP provides both congestion control and avoidance mechanisms.

36. Suppose TCP operates over 10-Gbps link. Assuming TCP could utilize the full bandwidth continuously, how long would it take the sequence numbers to wrap around completely? Is the sequence number space adequate?(N/D 18)

The minimum packet size is 40 bytes.

2^32 packets * 320 bits per packet = 1.4 * 10^12 bits

1.4 * 10^12 bits / 1 * 10^10 bits per second = 1.4 * 10^2 seconds About 2.3 minutes.

37. Define QoS.? (N/D 18)

The quality of service defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute each service class is associated with a set of attributes.The attributes are-Bandwidth, Latency or Delay, Jitter, Packet loss ratio

38. Compare flow control versus congestion control. .(N/D-17)

Congestion Control	**Flow Control**
Congestion control means preventing the source from sending data that will end up getting dropped by a router because its queue is full.	Flow control means preventing the source from sending data that the receiver will end up dropping because it runs out of buffer space.
This is more complicated, because packets from different sources travelling different paths can converge on the same queue.	This is fairly easy with a sliding window protocol

39. What are the approaches used to provide a range of quality of service (QoS) ? (N/D-17)

The techniques to improve QOS are

- Scheduling
- Traffic shaping
- Resource reservation
- Admission control

Fine grained approaches-which provide QOS to individual applications or flows.

Integrated services- a QOS architecture developed in the IETE and often associated with RSVP.

40. List the advantages of connection oriented services over connectionless services.(A/M-17)

Connection-oriented Requires a session connection (analogous to a phone call) be established before any data can be sent. This method is often called a "reliable" network service. It can guarantee that data will arrive in the same order.

Connectionless : Does not require a session connection between sender and receiver. The sender simply starts sending packets (called datagrams) to the destination. This service does not have the reliability of the connection-oriented method.

41. How do fast retransmit mechanism of TCP works? (A/M-17)

In TCP/IP, fast retransmit and recovery (FRR) is a congestion control algorithm that makes it possible to quickly recover lost data packets. Without FRR, the TCP uses a timer that requires a retransmission timeout if a packet is lost. No new or duplicate packets can be sent during the timeout period. With FRR, if a receiver receives a data segment that is out of order, it immediately sends a duplicate acknowledgement to the sender. If the sender receives three duplicate acknowledgements, it assumes that the data segment indicated by the acknowledgements is lost and immediately retransmits the lost segment.

42. Give the comparison of unicast, multicast and broadcast routing. (N/D-16)

Unicast addresses – represent a single LAN interface. A unicast frame will be sent to a specific device, not to a group of devices on the LAN.

Multicast addresses – represent a group of devices in a LAN. A frame sent to a multicast address will be forwarded to a group of devices on the LAN.

Broadcast addresses – represent all device on the LAN. Frames sent to a broadcast address will be delivered to all devices on the LAN.

43. Differentiate between TCP and UDP (N/D-16)

UDP (Connection-less)	TCP (Connection-oriented)
Datagram model (connection-less)	Byte-stream service (connection-oriented)
Unreliable delivery	Reliable delivery using acknowledgement
No flow control	Supports flow control
No congestion control	Built-in congestion control mechanism
Light overhead	Heavy overhead
Data is collected in order of receipt	Segments are ordered using sequence number

44. What do you mean by slow start in TCP congestion? .(A/M-16)

It is a congestion control technique. The additive increase mechanism is the right approach to use when the source is operating close to the available capacity of the network, but it takes too long to ramp up a connection when it is starting from scratch.

45. List the difference phases used in TCP connection.(A/M-16)

- Client performs an *active* connection to establish connection with a *passive* open server, prior to data communication
- Finally connection is terminated after data transmission

46. what is the difference between congestion control and flow control?(N/D-15)

Congestion Control	Flow Control
Congestion control means preventing the source from sending data that will end up getting dropped by a router because its queue is full.	Flow control means preventing the source from sending data that the receiver will end up dropping because it runs out of buffer space.
This is more complicated, because packets from different sources travelling different paths can converge on the same queue.	This is fairly easy with a sliding window protocol

47. What do you mean by QOS? (N/D-15)

The quality of service defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute each service class is associated with a set of attributes.

48. List some of the Quality of Service parameters of transport layer.(A/M-15)

User Oriented and Network Oriented. User related attributes are 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).

49. How does transport layer perform duplication control? .(A/M-15)

To detect and discard duplicates, the receiver maintains a sliding window starting at the lowest payload number not yet received (which is zero when the connection is first established) and covering the next 2^16 payloads

50. Distinguish between network and transport layer

Network layer	Transport layer
Responsible for *host*-to-*host* delivery	Responsible for *process*-to-*process* delivery
Host address is required for delivery	Host IP, port number is required for delivery
Flow control is not done	Flow control is end-to-end
Multicasting capability is not inbuilt	Support for multicasting is embedded

51. List the features desired of a transport layer protocols.

- Guaranteed and in-order delivery of the message.
- Supports multiple application processes on each host.
- Supports synchronization between the sender and the receiver.
- Allows receiver to apply flow control to the sender.
- Transport layer protocols are UDP, TCP and RTP.

52. Give any two Transport layer service.

Multiplexing: Transport layer performs multiplexing/demultiplexing 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.

53. Define process and port number?

- Processes are programs that run on hosts. It could be either *server* or *client*.
- Each process is identified by an abstract locator known as port and is assigned a unique 16-bit *port number* on that host.
- Server processes operate at *well-known ports* (0–1024), assigned by IANA.
- Client processes are assigned *ephemeral ports* (49152–65535) by operating system.

54. Write short notes on simple demultiplexer (or) User Datagram Protocol (or) UDP .

- User Datagram Protocol (UDP) is a *connectionless, unreliable* transport protocol.
- Adds *process-to-process* communication to best-effort service provided by IP.
- Simple *demultiplexer* allows multiple processes on each host to communicate.
- *Does not provide* flow control / reliable / ordered delivery.
- It is *suitable* for a process that requires simple request-response communication with little concern for error control.

55. Explain about UDP Header

- UDP packet header has 8-bytes
- SrcPort and DstPort—Source and destination port number.
- Length—total length of the user datagram, i.e., header plus data.
- Checksum—computed over UDP header, data and *pseudo header*. Pseudo header consists of IP fields (Protocol, SourceAddr, DestinationAddr) and UDP Length field.

PART-B&C

1. Explain OSI security architecture model with neat diagram
   Refer : William Stallings, Cryptography and Network security Page no: 26
2. Describe the various security mechanism.
   Refer : William Stallings, Cryptography and Network security Page no: 32
3. Explain the network security model and its important parameters with a neat block Diagram.
   Refer : William Stallings, Cryptography and Network security Page no: 41
4. Write note on different types of security attacks and services in detail**.**

Discuss examples from real life, where the following security objectives are needed :

i) Confidentiality.

ii) Integrity.

iii) Non-repudiation.

Refer : William Stallings, Cryptography and Network security Page no: 37

5. Suggest suitable security mechanisms to achieve them.
   Refer : William Stallings, Cryptography and Network security Page no: 41
6. Explain AES algorithm with all its round functions in detail.
   Refer : William Stallings, Cryptography and Network security Page no: 179
7. What do you mean by AES? Diagrammatically illustrate the structure of AES.
   Refer : William Stallings, Cryptography and Network security Page no: 174
8. Describe the steps in AES encryption process with example.
   Refer : William Stallings, Cryptography and Network security Page no: 197
9. Describe in detail the key generation in AES algorithm and its expansion format
10. Explain RSA algorithm, perform encryption and decryption to the system with p=7, q=11, e=17, M=8
    Refer : William Stallings, Cryptography and Network security Page no:433
11. Describe RSA algorithm & Perform encryption and decryption using RSA algorithm for the following: p=7, q=11, e=7, M=9
    Refer : William Stallings, Cryptography and Network security Page no: 438
12. Explain the working of RSA and chose an application of your choice for RSA and explain w encryption and decryption is carried out?
    Refer : William Stallings, Cryptography and Network security Page no: 430
13. In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M.
    Refer : William Stallings, Cryptography and Network security Page no: 399
14. List out the advantages of MD5 and SHA algorithms.
    Refer : William Stallings, Cryptography and Network security Page no:438
15. Explain the concepts of digital signature algorithm with key generation and verification in detail.
    Refer : William Stallings, Cryptography and Network security Page no: 421
16. Explain detail about Hash functions.
    Refer : William Stallings, Cryptography and Network security Page no: 339

U

NIT V HARDWARE SECURITY

Introduction to hardware security, Hardware Trojans, Side – Channel Attacks – Physical Attacks and Countermeasures – Design for Security. Introduction to Block chain

PART-A

1. **What do you mean by hardware security?**

Hardware security is **vulnerability protection that comes in the form of a physical device rather than software that's installed on the hardware of a computer system**. Hardware security can pertain to a device used to scan a system or monitor network traffic. Common examples include hardware firewalls and proxy servers.

2. **Why is hardware security important?**

Hardware security **protects physical devices from threats that allow unauthorized access to enterprise systems**. Hardware security is defined as the protection of physical devices from threats that would facilitate unauthorized access to enterprise systems.

3. **What are the 3 types of security?**

There are three primary areas or classifications of security controls. These include **management security, operational security, and physical security controls**

4. **What are all Hardware Vulnerabilities**

Physical Attacks (e.g. side channel attacks; microarchitectural vuln.) ● Trojan Horses (implemented at different design levels) ● IP Piracy (cloning of IP) ● IC Piracy & Counterfeiting (cloning, overproduction) ● Backdoors (modifications leaking secret) ● Tampering (e.g. FPGA bitstream modifications) ● Reverse Engineering

5. **What is Hardware Trojan?**

A malicious addition or modification to the existing circuit elements

6. **What hardware Trojans can do?**

○ Change the functionality ○ Reduce the reliability ○ Leak valuable information

7. **What is hardware Trojan detection?**

Hardware Trojans (HTs) are identified as **an emerging threat for the integrity of Integrated Circuits (ICs) and their applications**. Attackers attempt to maliciously manipulate the functionality of ICs by inserting HTs, potentially causing disastrous effects (Denial of Service, sensitive information leakage, etc.).

8. **What is meant by side-channel attack?**

Share to Facebook Share to Twitter. Definition(s): **An attack enabled by leakage of information from a physical cryptosystem**. Characteristics that could be exploited in a side-channel attack include timing, power consumption, and electromagnetic and acoustic emissions.

9. **Is Trojan a serious virus?**

The effects of Trojans can be highly dangerous. Like viruses, they can destroy files or information on hard disks. They can also capture and resend confidential data to an external address or open communication ports, allowing an intruder to control the infected computer remotely.

10. **What is side-channel attack on RSA?**

Side channel attacks **exploit information about timing, power consumption, electromagnetic emanations or even sound to recover secret information about a cryptosystem** . Timing attacks exploit the timing variations in cryptographic operations.

11. **What are hardware based attacks?**

Hardware based attacks **require the use of Rogue Devices which go under the radar of existing security solutions by operating on the Physical Layer**. Spoofed Peripherals impersonate legitimate HIDs and, due to a lack of Physical Layer visibility, are recognized as the legitimate device that they imitate.

12. **What are 3 types of attacks?**

The different types of cyber-attacks are **malware attack, password attack, phishing attack, and SQL injection attack**.

13. **What is the most common type of attacks?**

Malware. Phishing, Man-in-the-middle attack (MITM), Distributed Denial-of-Service (DDoS) Attack, SQL Injection, Zero-day Exploit, DNS Tunnelling., Business Email Compromise

14. **What are the three 3 basic network security measures?**

This includes within a corporate or home network and outside of those networks such as across the internet or on a service provider's network, Secure Socket Layer (SSL)/Transport Layer Security (TLS), Secure Shell (SSH), Internet Protocol Security (IPsec)

15. **How do you design a secure network?**

Physical security.
Get into VLANS with subnets and QoS.
Add more and better firewalls.

Use the DMZ.
Design for hierarchy.
Add port security.

16. What is design for security?

Security by design is an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as continuous testing, authentication safeguards and adherence to best programming practices.

17. What are secure network design principles?

We recommend that your network security design be grounded in the strategic principles of **compartmentalization, the weakest link, vulnerability testing, and layering**

18. What are the 4 goals of a secure network?

Network security entails protecting the usability, reliability, integrity, and safety of network and data. Effective network security defeats a variety of threats from entering or spreading on a network. The primary goal of network security are **Confidentiality, Integrity, and Availability**.

19. What is the network design?

Network design is **the practice of planning and designing a communications network**. Network design starts with identifying business and technical requirements and continues until just before the network implementation stage

20. What is meant by blockchain technology?

Blockchain is **a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system**. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain

21. What is the main purpose of blockchain technology?

The purpose of the blockchain is **to share information amongst all parties that access it via an application**. Access to this ledger in terms of reading and writing may be unrestricted ('permissionless'), or restricted ('permissioned').

22. What is an example of blockchain?

Bitcoin and Ethereum are popular examples of blockchains. Everyone is allowed to connect to the blockchain and transact on them

23. What are the 3 technologies that form blockchain?

Blockchain is a combination of three leading technologies: **Cryptographic keys**. A peer-to-peer network containing a shared ledger. A means of computing, to store the transactions and records of the network

24. Which tool is used for blockchain?

Solidity is, undoubtedly, one of the most popular languages used by Blockchain Developers. Influenced by C++, Python, and JavaScript, it was designed to target the Ethereum Virtual Machine (EVM). Solidity is statically typed, supports inheritance, libraries, and complex user-defined types.

25. What are the disadvantages of blockchain?

One of the main disadvantages of blockchain technology is the **immutability of data**. It benefits financial and supplies chain systems. Immutability can only exist if network nodes are distributed. A blockchain network is vulnerable if one entity owns at least half the nodes.

26. What are physical attacks?

An actual and intentional striking of another person against his or her will, or the intentional causing of bodily harm to an individual.

27. What are the basic types of attacks?

- Common Types of Cybersecurity Attacks.
- Phishing Attacks: A Deep Dive with Prevention Tips.
- SQL Injection Attacks (SQLi)
- Cross-Site Scripting (XSS) Explained and Preventing XSS Attacks.
- Man-in-the-Middle (MITM) Attacks.
- Malware Attacks: Examined and Best Practices.
- Denial-of-Service Attacks.

28. What is active attacks example?

Examples of active attacks include man-in- the middle (MitM), impersonation, and session hijacking. An attack on the authentication protocol where the attacker transmits data to the claimant, Credential Service Provider (CSP), verifier, or Relying Party (RP)

29. What are the different types of attacks in cryptography?

- Brute force attack.
- Ciphertext-only attack.
- Chosen plaintext attack.
- Chosen ciphertext attack.
- Known plaintext attack.

30. What the mail transfer protocol used in the internet ?(N/D 19)

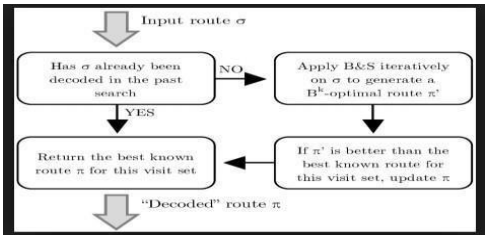
The Simple Mail Transfer Protocol (SMTP) is a communication protocol for electronic mail

transmission. As an Internet standard, SMTP was first defined in 1982 by RFC 821, and updated in 2008 by RFC 5321 to Extended SMTP additions, which is the protocol variety in widespread use today.

31. State the operations of the packet filter firewall ?(N/D 19)

A packet-filtering firewall examines each packet that crosses the firewall and tests the packet according to a set of rules that you set up. Packet filters work by inspecting the source and destination IP and port addresses contained in each Transmission Control Protocol/Internet Protocol (TCP/IP) packet.

32. Draw a diagram that illustrate tunneling strategy.(A/M 19)



33. What is the function of mail readers?

- Mail readers or Message Access Agent (MAA) allows user to *retrieve* messages in the mailbox from a remote host, so that user can perform actions such as reply, forward, etc.
- Two major access protocols are:
  - Post Office Protocol (POP3)
  - Internet Message Access Protocol (IMAP4)

34. Give the functions of an user agent.

User agent (UA) is software (eg. Microsoft Outlook, Netscape) that facilitates: ○

Compose—create message by providing template with built-in editor.

- *Read*—read mail and provide sender, subject, flag (read, new) information. ○

Reply—allows user to reply (send message) back to sender

- *Forward*— facilitates forwarding message to a third party.
- *Mailboxes*—two mailboxes for each user namely *inbox* and *outbox.*

35. What is hypertext?

- Hypertext is a text that contains *embedded* URL known as links.
- When hypertext is clicked, browser opens a new connection, retrieves file from the server and displays the file.

36. State the usage of conditional get in HTTP. Apr/May 17

The HTTP Protocol defines a caching mechanism, in which the proxy web-servers can cache pages, files, images etc. Since caching is in place, There is a method which the servers are asked to return the document, either the "cached" or "live" document.

This request of asking the server for a document considering a specific parameter is called a

Conditional GET Request

37. What is WWW? (Nov/Dec 2010,May/June 2014))

World Wide Web is an internet application that allows user to view pages and move from one web page to another. It helps to store and share data across varied distances.

38. What is a Web browser?

Web browser is a software program that interprets and displays the contents of HTML webpages.

39. What do you mean by TELNET?

TELNET is used to connect remote computers and issue commands on those computers.

40. Write down the three types of WWW documents.

The documents in the WWW can be grouped into three broad categories: static, dynamic

and active.

- *Static:* Fixed-content documents that are created and stored in a server.
- *Dynamic*: Created by web server whenever a browser requests the document.
- *Active:* A program to be run at the client side

.

41. Define Name Resolution.

To improve reliability, some of the name servers can be located outside the zone. The process of looking up a name and finding an address is called name resolution.

.

42. What is meant by SOAP

- SOAP provides a simple messaging framework whose core functionality is concerned with providing extensibility.
- SOAP is used to define transport protocols with features required to support a particular application protocol.
- A SOAP feature specification includes:
  - URI that identifies the feature
  - State information required for implementation
  - Information to be relayed to the next node
  - Life cycle and relationships of the messages exchanged

43. What is meant by RE presentational State Transfer (REST)

- REST web service architecture is based on re-applying the model underlying the WWW architecture. It treats individual web services as WWW resources, accessed via HTTP.
- REST uses HTTP methods such as GET and POST to provide interface for web services.
- In REST model, *complexity* is shifted from protocol to the payload.

Payload is a representation of the abstract state of a resource. For example, GET returns a representation of current state of the resource.

44. Define proxy server.

- *Proxy server* copies responses sent by the server to recent requests.
- Client's request is intercepted by proxy and responds if it has a cache of the document, or else forwards request to the server.

45. What is a web service? List its types.

- Web services are architectures that offer remotely accessible services for client applications to form network applications, such as business-to-business (B2B) and enterprise application integration (EAI).
- For example, application at *Amazon.com* tracks shipping of a book order by interacting with application from *Fedex.com*

46. List and explain web service architectures in detail.

- Two web services architectures are
  - WSDL / SOAP (*custom application protocols*)
  - REST (*generic application protocol*)

47. What is Generic Domains?

Generic domain define registered hosts according to their generic behaviour. Each node in the tree defines a domain, which is an index to the domain name space database

Eg. com – Commercial organizations
edu - Educational institutions
gov - Government institutions

48. What are the parts of a browser?

The parts of a browser are

- A controller

- A client program
- Interpreter

49. List the types of resource records stored in a name server.

- Resource record is a *5-tuple* with fields <Name, Value, Type, Class, TTL>
- Type —indicates what kind of record it is. Commonly used types are:
  - NS — Value field contains address of a name server
  - MX — Value field contains a mail server.
  - A — Value field contains an IP address
  - CNAME— Value field contains canonical name of a host

50. Explain how SNMP is used to manage nodes on the network (or) network management.

- Simple Network Management Protocol (SNMP) is an application layer protocol that monitors and manages routers, distributed over a network.
- SNMP uses the concept of *manager* and *agent*.
  - Manager is a host that runs SNMP *client* program (GUI)
    Agent is a router that runs SNMP *server* program.
- SNMP uses services of UDP on two well-known ports: 161 (agent) and 162 (manager).
- SNMP is supported by two protocols:
  Structure of Management Information (SMI) Management Information Base (MIB).

PART-B&C

1. Explain in details about Hardware Security.
2. Explain in details about Side Channel Attacks
3. What are the countermeasures in physical attacks?
4. Discuss in details about design for security
5. Explain in details about Block chain technology
6. What are the physical attacks explain in detail
7. Explain in detail about Hardware threat.
8. Explain detail about Hardware Vulnerabilities.
9. Explain in detail about Trojan Taxonomy.
10. How Block chain works.
11. Discuss in details about Bit coin.
12. How does a side channel attacks works.
13. Explain the type of encryption/decryption method. Conventional Methods?
14. Brief the importance of Single Network Management.
15. Explain the role of a DNS on a computer Network.