Computer Networks

CORE COURSE VI

COMPUTER NETWORKS

Objective:

To understand the Design and Organization of Computer Networks

Unit I

Overview and Physical Layer: Introduction: Data Communications - Networks - Network Types, Network Models: TCP/IP Protocol Suite- The OSI Model, Bandwidth utilization : Multiplexing- Spread Spectrum, Transmission Media: Guided Media-Unguided Media, Switching: Circuit Switched Network-Packet Switching-Structure of a switch

Unit II

Data Link Layer: Error Deduction and Correction : Introduction- Cyclic codes-Forward error correction, Data link Control: Data link layer protocols- Media Access Control: Random Access- Controlled Access, Wireless Networks: IEEE 802.11- Bluetooth-Cellular Telephone- Satellite network- Connection devices,

Unit III

Network Layer Services : Packet Switching- Network layer performance- IPV4 Addresses- Internet Protocol-Routing Algorithms - IPV6 Addressing

Unit IV

Transport Layer : Transport Layer Protocols- User Datagram Protocol - TCP:TCP Services TCP features - Windows in TCP - Flow Control - Error Control- TCP Congestion Control - TCP timers

Unit V

Application Layers : Client Server Programming - Word Wide Web & HTTP - FTP - Email - DNS

Text Book:

1. Data Communications and Networking, Behrouz A Forouzan, Tata McGraw Hill, Fifth Edison, 2013.

Reference Book:

1. Data Communications and Networks, Achyut Godbole and Atul Kahate, McGraw Hill Education, 2011.

*****

UNIT-1 – Overview and Physical Layer

1. **What is Computer Networks?**

A **computer network** is a set of **computers** connected together for the purpose of sharing resources. The most common resource shared today is connection to the **Internet**.
Other shared resources can include a printer or a file server. The **Internet** itself can be considered a **computer network**.

2. **Define Data communication.**

- It is the process of using computing and **communication** technologies to **transfer data** from one place to another, and vice versa.
- It enables the movement of electronic or digital **data** between two or more nodes, regardless of geographical location, technological medium or **data** contents.

3. **What are the fundamentals of Data communications?**

- Data communications system depends on four fundamental characteristics:
- **Delivery, accuracy, timeliness, and jitter**.
- Received by the intended device or user and only by that device or user.
- Altered in transmission and left uncorrected are unusable.

4. **List out the components of Data Communication.**

Components or Elements of a Data Communication:

- Message.
- Sender.
- Receiver.
- Medium (Communication Channel)
- Encoder & Decoder.

5. Mention the different Types of Networks.

Types of Networks in Use Today

- Personal Area Network (PAN) ...
- Local Area Network (LAN) ...
- Wireless Local Area Network (WLAN) ...
- Campus Area Network (CAN) ...
- Metropolitan Area Network (MAN) ...
- Wide Area Network (WAN) ...
- Storage-Area Network (SAN) ...
- System-Area Network (also known as SAN)

6. What is the different form of data representation?

Types of data representation

- Decimal number system.
- Binary number system.
- Octal number system.
- Hexadecimal number system.

7. List out the three types of data flow.

The three types of data flows are

- Simplex,-One way communication E.g.: radio and television broadcasts
- Half-duplex – data flows in both directions but only one direction at a time on the data communication line. For example, a walkie-talkie
- Full duplex- both parties can communicate with each other simultaneously. An example of a full-duplex device is a telephone

8. What are the types of topology?

There are five types of topology in computer networks:

- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology
- Hybrid Topology

9. Define Multipoint.

Computer network having more than two terminals connected by a single communications channel

10.What is circuit switching network?

- It a type of network where the communications between end devices (nodes) must be set up before they can communicate.
- Once set up, the "**circuit**" is dedicated to the two nodes it connects for the duration of that connection. An **example** of a **circuit-switched** network is an analog telephone network.

11. What is Internet?

- The **internet** is a globally connected network system that uses TCP/IP to transmit data via various types of media.
- The **internet** is a network of global exchanges – including private, public, business, academic and government networks – connected by guided, wireless and fiber-optic technologies.

12. List out the layers in TCP/IP.

The TCP/IP model consists of five layers:

- The application layer, transport layer, network layer, data link layer and physical layer.

13. What are the layers in OSI reference model?

Functions of the OSI Layers

- Physical Layer.
- Data-Link Layer.
- Network Layer.
- Transport Layer.
- Session Layer.
- Presentation Layer.
- Application Layer.

14. What do you mean by encapsulation in networking?

- Encapsulation is the process of taking data from one protocol and translating it into another protocol, so the data can continue across a network.
- For example, a TCP/IP packet contained within an ATM frame is a form of encapsulation

15. Define Decaptulation in networks.

- Decaptulation is the process of opening up encapsulated data that are usually sent in the form of packets over a communication network.
- It can be literally defined as the process of opening a capsule, which, in this case, refers to encapsulated or wrapped-up data.

16. What is Multiplexing?

- **Multiplexing** (sometimes contracted to muxing) is a method by which multiple analog or digital signals are combined into one signal over a shared medium.

- The aim is to share a scarce resource. ... The **multiplexed** signal is transmitted over a communication channel such as a cable.

17. Define Demultiplexing.

- **Demultiplexing** (Demuxing) is a term relative to multiplexing. It is the reverse of the multiplexing process.
- **Demultiplexing** is a process reconverting a signal containing multiple analog or digital signal streams back into the original separate and unrelated signals.

18. Expand:-HTTP, TELNET, SMTP, SNMP.

- HTTP:- Hypertext Transfer Protocol.
- TELNET:-Telecommunication Networks
- SMTP:-Simple Main Transfer Protocol
- SNMP:- Simple Network Management Protocol.

19. What are the categories of Multiplexing?

- There are mainly two **types of multiplexers**, namely analog and digital.
- They are further divided into Frequency Division **Multiplexing** (FDM), Wavelength Division **Multiplexing** (WDM), and Time Division **Multiplexing** (TDM).

20. What is FDM?

- Frequency Division Multiplexing (FDM) is a networking technique in which multiple data signals are combined for simultaneous transmission via a shared communication medium.
- FDM uses a carrier signal at a discrete frequency for each data stream and then combines many modulated signals.

21. Define TDM.

Time-division multiplexing (**TDM**) is a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line so that each signal appears on the line only a fraction of time in an alternating pattern.

22. Define WDM.

- Wavelength division multiplexing (**WDM**) is a technology or technique modulating numerous data streams,
- i.e. optical carrier signals of varying wavelengths (colors) of laser light, onto a single optical fiber.
- **WDM** enables bi-directional communication as well as multiplication of signal capacity.

23. What is Spread Spectrum?

- **Spread spectrum** is a technique used for transmitting radio or telecommunications signals.
- The term refers to the practice of spreading the transmitted signal to occupy the frequency **spectrum** available for transmission.

24. List out the techniques of Spread Spectrum.

- There are four techniques of spread spectrum namely
- Direct sequence spread spectrum (DSSS),
- Frequency hopping spread spectrum (FHSS),
- Chirp spread spectrum (CSSS) and time
- Hopping spread spectrum (THSS).

UNIT-2 – DataLink Layer

1. List out the types of error.

Single Bit Error, Burst error

2. Define error detection.

- Error detection refers to the techniques used to detect noise or other impairments introduced into data while it is transmitted from source to destination.
- Error detection ensures reliable delivery of data across vulnerable networks.

3. What is Hamming Distance?

- Hamming distance is the number of bit positions in which the two bits are different.
- The Hamming distance between two strings, a and b is denoted as d(a,b).
- It is used for error detection or error correction when data is transmitted over computer networks.

4. Define CRC.

- A cyclic redundancy check (CRC) is an error-detecting code commonly used in digital networks
- and storage devices to detect accidental changes to raw data.
- Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomial division of their contents.

5. What is checksum?

- A value used to ensure data are stored or transmitted without error.
- It is created by calculating the binary values in a block of data using some algorithm and storing the results with the data.

6. List out the protocols in Data link Layer.

- Simple,
- Stop -and -Wait,
- Go-Back-N,and
- Selective-Repeat

7. What are the types of Random Access protocol?

- ALOHA,
- CSMA,
- CSMA/CD,
- CSMA/CA

8. Expand:-RTS, CTS, NAV, CSMA

- RTS:-Request to sent.
- CTS:-Clear To Send.
- NAV:-Network Allocation Vector.
- CSMA:-Carrier Sense Multiple Access.

9. What is Bluetooth?

- Bluetooth is a wireless short-range communications technology standard found in millions of products we use every day
- including headsets, smart phones, laptops and portable speakers.
- A Bluetooth device works by using radio waves instead of wires or cables to connect with your cell phone, smart phone or computer.

10. List out the types of network in Blue tooth.

Piconet and Seatter

11. Define MSC.

A mobile switching center (MSC) is the centerpiece of a network switching subsystem (NSS). The MSC is mostly associated with communications switching functions, such as call set-up, release, and routing.

12. What is generation in cellular Telephone?

- The first generation (1G) mobile wireless communication network was analog used for voice calls only.
- The second generation (2G) is a digital technology and supports text messaging.
- The third generation (3G) mobile technology provided higher data transmission rate, increased capacity and provide multimedia support.
- 4G is being developed to accommodate the QoS and rate requirements set by forthcoming applications like wireless broadband access,
- Multimedia Messaging Service (MMS),
- video chat, mobile TV, HDTV content,
- Digital Video Broadcasting (DVB), minimal services like voice and data, and other services that utilize bandwidth

13. Define Satellite network.

- Satellite Internet is the ability to transmit and receive data from a relatively small satellite dish on Earth and
- communicate with an orbiting geostationary satellite 22,300 miles above Earth's equator

14. What are the categories of satellite?

- GEO-Geostationary Earth Orbit
- LEO-Low Earth Orbit
- MEO-Medium Earth Orbit

15. Define HUB.

A hub is the most basic networking device that connects multiple computers or other network devices together

16. Define router.

- A router is a device that forwards data packets along networks.
- A router is connected to at least two networks.
- Commonly two LANs or WANs or a LAN and its ISP's network.
- Routers are located at gateways, the places where two or more networks connect.

17. What is GPS?

- The **GPS** (Global Positioning System) is a "constellation" of approximately 30 well-spaced satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location.
- The location accuracy is anywhere from 100 to 10 meters for most equipment.

18. Define orbit and List out its types

- An orbit is a regular, repeating path that an object in space takes around another one.
- An object in an orbit is called a satellite.
- A satellite can be natural, like the moon, or human
- Types: **Equatorial-orbit satellite, Inclined-orbit satellite, Polar-orbit satellite**

19. Define Token passing.

- On a local area network, token passing is a channel access method where a signal called a token is passed between nodes to authorize that node to communicate.
- In contrast to polling access methods, there is no pre-defined "master" node.

20. **Expand:-FSM, GPS, L2CAP, GSM**

FSM:-Finite State Machine
GPS:-Global Positing System
L2CAP:-Logical Link Control and Adaptation Protocol
GSM: - Global System for Mobile Communication

UNIT-3 – Network Layer

1. Define packetizing in Network layer.

- Packetizing is a process of dividing long messages into smaller ones.
- Definition of packetizing in term of network layer, upper layer, data link layer.
- While receiver, receives those packets from its data-link layer, decapsulates the packet, and pass the data (packets which is received) to the upper-layer protocol.

2. What is mean by Routing?

- **Routing** is the process of moving packets across a network from one host to another.
- It is usually performed by dedicated devices called **routers**.
- Packets are the fundamental unit of information transport in all modern computer networks, and increasingly in other communications networks as well.

3. Define congestion control.

Congestion control is a network layer issue, and is thus concerned with what happens when there is more data in the **network** than can be sent with reasonable packet delays, no lost packets, etc. Flow **control** is a local, **congestion control** is global.

4. What do you mean by quality of service?

- Quality of service (QoS) refers to any technology that manages data traffic to reduce packet loss, latency and jitter on the network.
- **QoS** controls and manages network resources by setting priorities for specific types of data on the network.

5. Define packet switching.

- Packet switching is a method of grouping data that is transmitted over a digital network into packets.
- Packets are made of a header and a payload.
- Data in the header are used by networking hardware to direct the packet to its destination where the payload is extracted and used by application software

6. What is datagram?

- A **datagram** is a basic transfer unit associated with a packet-switched **network**.
- **Datagram** provides a connectionless communication service across a packet-switched **network**.
- The delivery, arrival time, and order of arrival of **datagram** need not be guaranteed by the **network**.

7. List out the types of delay in packet switched networks.

- In **packet** switched **networks**, there are four **types** of commonly identified **delays**.
- Processing, queuing, transmission and propagation **delays**.
- Processing and propagation **delays** are often considered negligible.
- Transmission **delay** is related to transmission rate of an interface.

8. What is throughput computer network?

- **Throughput** is a measure of how many units of information a system can process in a given amount of time.
- It is applied broadly to systems ranging from various aspects of **computer** and **network** systems to organizations.

9. Define ipv4.

- It is the fourth revision of the Internet Protocol and a widely used protocol in data communication over different kinds of networks.
- IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet.

10. What is class full address?

- A Class full **addressing**, the **address** space is divided into five **classes**:
- A, B, C, D, and E. Each of these **classes** has a valid range of IP **addresses**.
- **Classes** and E are reserved for multicast and experimental purposes respectively. The order of bits in the first octet determines the **classes** of IP **address**.

11. What is DHCP protocol in networking?

- A **DHCP Server** is a **network server** that automatically provides and assigns IP addresses, default gateways and other **network** parameters to client devices.
- It relies on the standard **protocol** known as Dynamic Host Configuration **Protocol** or **DHCP** to respond to broadcast queries by clients.

12. Describe network addressing resolution protocol.

Address Resolution Protocol, a **network** layer **protocol** used to convert an **IP address** into a physical **address** (called a DLC **address**), such as an Ethernet **address**. A host wishing to obtain a physical **address** broad casts an **ARP** request onto the TCP/**IP network**.

13. Define **network address translation**

- **NAT** translates the **IP addresses** of computers in a local **network** to a single **IP address**. This **address** is often used by the router that connects the computers to the Internet.

14. What is IP address with example?

An **IP address** is written in "dotted decimal" notation, which is 4 sets of numbers separated by period each set representing 8-bit number ranging from (0-255). An **example** of **IPv4 address** is 216.3.128.12, which is the **IP address** previously assigned to iplocation.net.

15. What is distance vector routing with example?

A **distance-vector routing** (DVR) protocol requires that a **router** inform its neighbours of topology changes periodically. Historically known as the old ARPANET **routing** algorithm (or known as Bellman-Ford algorithm). ... Distances, based on a chosen metric, are computed using information from the neighbours' **distance vectors**.

16.What is link state routing?

Link state routing is a complex **routing** technique in which each **router** shares information with other **routers** about the reachability of other networks and the metric to reach the other networks in order to determine the best path. **Routing** is the process of moving packets across a network from one host to another.

17. Define Ipv6.

An Internet Protocol Version 6 **address** (**IPv6 address**) is a numerical label that is used to identify a network interface of a computer or a network node participating in an **IPv6** computer network.

18. Describe the three address types of Ipv6.

The **three types of IPv6 addresses** are: unicast, anycast, and multicast.

19.Define payload.

- The **payload** is the part of transmitted data that is the actual intended message.
- Headers and metadata are sent only to enable **payload** delivery.
- In the context of a computer virus or worm, the **payload** is the portion of the malware which performs malicious action.

20. Desctibe encrypted security payload.

- It is a protocol within the IPSec for providing authentication, integrity and confidentially of network packets data/**payload** in IPv4 and IPv6 networks.
- ESP provides message/**payload** encryption and the authentication of a **payload** and its origin within the IPSec protocol suite.

UNIT-3 – Transport Layer

1. What is main function of transport layer?

- It responsible for end-to-end communication over a network.
- It provides logical communication between application processes running on different hosts within a layered architecture of protocols and other network components.

2. What is FSM in networking?

- It is a computation model that can be used to simulate sequential logic, or, in other words, to represent and control execution flow.
- Finite State Machines can be used to model problems in many fields, including mathematics, artificial intelligence, games or linguistics.

3. What is meant by stop and wait protocol?

- Stop-and-wait ARQ also referred to as alternating bit protocol, is a method in telecommunications to send information between two connected devices.
- It ensures that information is not lost due to dropped packets and that packets are received in the correct order.

4. Why sliding window protocol is better than stop and wait protocol?

- Only one frame is transmitted at a time in the **stop-and-wait protocol** while **sliding window** transmits more **than** one frame at a time.
- The efficiency of the **sliding window protocol** is more **than** the **stop-and-wait protocol** because it produces short propagation delay.

5. What is the purpose of piggybacking?

- **Piggybacking**, in a wireless communications context, is the unauthorized access of a wireless LAN.
- The usual **purpose of piggybacking** is simply to gain free network access rather than any malicious intent, but it can slow down data transfer for legitimate users of the network.

6. What is the difference between TCP and UDP?

- **TCP** (Transmission Control Protocol) is connection oriented, whereas **UDP** (User Datagram Protocol) is connection-less.
- **UDP** does not use acknowledgments at all, and is usually used for protocols where a few lost datagram do not matter.
- Because of acknowledgments, **TCP** is considered a reliable data transfer protocol.

7. What is UDP and how it works?

- **UDP** stands for User Datagram Protocol and is a connectionless network protocol.
- **UDP works** on top of the IP protocol. The data the sender wants to transmit is also append to the datagram.
- The datagram packet is sent and may or may not be delivered to the recipient, **UDP** does not care.

8. Write some advantage of UDP.

- Small packet sizes than TCP by **about** 60%
- **UDP** header 20 bytes.
- TCP header 80 bytes.
- Connectionless: No connection to create and maintain.
- You don't have to create connection first before sending out data.
- You have more control of when data is being sent out.

9. Write some disadvantage of UDP.

- Data corruption is a common occurrence on the Internet; **UDP** has a primitive form of error detection.
- No compensation for lost packets.
- Packets can arrive out of order.
- No congestion control.

10. Describe the segment in UDP.

- **UDP** is a connectionless and unreliable protocol.
- **UDP** does not do flow control, error control or retransmission of a bad **segment**. **UDP** transmits **segments** consisting of an 8-byte header.
- Its contains Source port, Destination port, **UDP** length and Checksum.

11. Define UDP checksum.

- It is the complement of a 16-bit one's complement sum calculated over an IP "pseudo-header" and the actual **UDP** data.
- The IP pseudo-header is the source address, destination address, protocol (padded with a zero byte) and **UDP** length.

12. Describe congestion window.

- It is a TCP state variable that limits the amount of data the TCP can send into the network before receiving an ACK.
- The Receiver **Window** (rwnd) is a variable that advertises the amount of data that the destination side.

13. Describe congestion detection.

- It is a mechanism that generally triggers **congestion** alleviation or control procedure.
- **Congestion** can be **detected** either at the sink node or at the intermediate sensor nodes.
- In either case, the source traffic rate is usually reduced in order to mitigate **congestion** problem from the network.

14. What is Timer in TCP?

- **TCP** Timers are used to avoid excessive delays during communication.
- **TCP** Timers are- Time Out **Timer**, Time Wait **Timer**, Keep Alive **Timer**, and Persistent **Timer**.
- Time out **timer** is used for retransmission.
- Time Wait **Timer** is used during connection termination.

15. Describe Round-Trip time.

- It is the length of **time** it takes for a signal to be sent plus the length of **time** it takes for an acknowledgement of that signal to be received.
- This **time** therefore consists of the propagation times between the two points of signal.

16. Define TCP service.

- The Transmission Control Protocol (**TCP**) is an important transport layer protocol providing a reliable data transfer **service** to support many applications running over the Internet such as the World Wide Web.
- It is therefore important to **define** the intent of **TCP**

17. What are persistence timers?

- It deal with a zero-window-size deadlock situation, TCP uses a **persistence timer**.
- When the sending TCP receives an acknowledgment with a window size of zero, it starts a **persistence timer**.
- When the **persistence timer** goes off, the sending TCP sends a special segment called a probe.

18. Describe Retransmission timer.

- **Retransmission Timer** – To **retransmit** lost segments, TCP uses **retransmission timeout** (RTO). When TCP sends a segment the **timer** starts and stops when the acknowledgment is received.
- If the **timer** expires **timeout** occurs and the segment is **retransmitted**.

19. How to measured RTT?

- **RTT** is typically **measured** using a ping — a command-line tool that bounces a request off a server and calculates the time taken to reach a user device.
- Actual **RTT** may be higher than that **measured** by the ping due to server throttling and network congestion.

20. Describe congestion policies.

- It is the **policy** in which retransmission of the packets are taken care.
- If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted.
- This transmission may increase the **congestion** in the network.

UNIT-3 – Network Layer

1. Define API.

- It is a set of routines, protocols, and tools for building software applications.
- Basically, an **API** specifies how software components should interact.
- Additionally, **APIs** are used when programming graphical user interface (GUI) components.

2. What is meant by socket interface?

- A **socket** is an endpoint of communication to which a name can be bound.
- A **socket** has a type and one associated process.
- The **interface** to network protocols needs to accommodate multiple communication protocols, such as TCP/IP, Xerox internet protocols (XNS), and UNIX family.

3. What is the difference between network layer and transport layer?

- Difference between Network Layer and Transport Layer.
- The basic **difference between network layer and transport layer** is that **transport layer protocol** provides logical communication **between** processes running on **different** hosts, whereas **network layer protocol** provides logical communication **between** hosts.

4. What is local socket addressing?

- **Local socket address**, consisting of the **local** IP **address** and (for TCP and UDP, but not IP) a port number. protocol:
- A transport protocol, e.g., TCP, UDP, raw IP.
- A **socket** that has been connected to another **socket**, e.g., during the establishment of a TCP connection, also has a remote **socket address**.

5. What is difference between port and socket?

- A **port** is a logical connection method two end points communicate with.
- **Ports** operate at the Transport layer of the OSI.
- **Sockets** are determined by an IP address and **port** number.
- For example, for a VPN client to connect the client would need to use the **socket** determined by the **port** number and IP of the local client.

6. What do you mean by Remote socket addressing?

- This **means** that (local or **remote**) endpoints with TCP port 53 and UDP port 53 **are** distinct **sockets**, while IP **does** not have ports.
- A **socket** that has been connected to another **socket**, e.g., during the establishment of a TCP connection, also has a**re mote socket address**.

7. Describe concurrent communication.

- **Concurrent** execution of code allows for **communication** between the parts of code that are executed **concurrently**.
- The **communication** can be done either through models using shared memory or by models using message passing.

8. What is WWW in computer networks?

- The Internet is a global system of interconnected **computer networks**.
- In contrast, the World Wide Web is a global collection of documents and other resources, linked by hyperlinks and URIs.

9. Describe web client and web server.

- The **client**-**server** characteristic **describes the relationship** of cooperating programs in an application.
- The **server** component provides a function or service to one or many **clients**, which initiate requests for such services. ... For example, a **web server** serves **web** pages and a file **server** serves computer files.

10. Define URL in computer network.

- A Uniform Resource Locator (**URL**), colloquially termed a web address, is a reference to a web resource that specifies its location on a **computer network** and a mechanism for retrieving it.
- A **URL** is a specific type of Uniform Resource Identifier (URI), although many people use the two terms interchangeably.

11. What is HTTP and why it is used?

- **HTTP** means Hyper Text Transfer Protocol.
- **HTTP** is the underlying protocol **used** by the World Wide Web and this protocol defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

12. What you mean by host?

- A **host** (also known as "network **host**") **is** a computer or other device that communicates with other **hosts** on a network.
- **Hosts** on a network include clients and servers -- that send or receive data, services or applications.

13. What is a port on a computer?

- When referring to a physical device, a hardware **port** or peripheral **port** is a hole or connection found on the front or back of a **computer**.
- **Ports** allow **computers** to access external devices such as printers.

14. How many types of ports are there?

- In Computers, communication **ports** can be divided into two **types** based on the **type** or protocol used for communication.
- They are Serial **Ports** and Parallel **Ports**.

15. What are FTP and its uses?

- **FTP** is an acronym for File Transfer Protocol.
- As the name suggests, **FTP** is used to transfer files between computers on a network.
- You can **use FTP** to exchange files between computer accounts, transfer files between an account and a desktop computer, or access online software archives.

16. Describe electronic mail.

- **Email** is information stored on a computer that is exchanged between two users over telecommunications.
- More plainly, **e**-**mail** is a message that may contain text, files, images, or other attachments sent through a network to a specified individual or group of individuals.

17. What are the features of electronic mail?

The main **features of email** is,

- Attachment: Ability to attach the files along the messages is one of most useful **features of email**.

- (2)Address book: It is also most important **features of email** that allows a user to storing the information.

18. What is SMTP and how it works?

- **SMTP** is part of the application layer of the TCP/IP protocol.
- Using a process called "store and forward," **SMTP** moves your email on and across networks.
- It **works** closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox.

19. Describe MIME.

- The **MIME** stands for Multi-Purpose Internet Mail Extensions.
- As the name indicates, it is an extension to the Internet email protocol that allows its users to exchange different kinds of data files over the Internet such as images, audio, and video.
- The **MIME** is required if text in character sets other than ASCII.

20. Define DNS.

- **DNS**. (Domain Name System) The Internet's system for converting alphabetic names into numeric IP addresses.
- For example, when a Web address (URL) is typed into a browser, **DNS** servers return the IP address of the Web server associated with that name.

Valluvar College of Science and Management,Karur.
Department of Computer Science
April-2020

Subject Name		Computer Networks	Subject Code	16SCCCA8
Class	III BCA	Prepared By	S.Anandan,S.Boobalathandayuthapani	

UNIT-1 – Overview and Physical Layer

5 Marks

1. Discuss about TCP/IP protocol structures.
2. Draw the layer of OSI reference model.
3. Define frequency division multiplexing
4. Disucss about time division multiplexing
5. What is code division multiplexing?
6. Discuss about twisted pair.
7. Define co-axial cable
8. What are the header and trailer and how they get added and removed?
9. Give benefit note on switching.
10. Explain protocol hierarchies with need diagram
11. Discuss NSF net and internet.

10 Marks

1. What is mean by transmission media? Explain guided media.
2. Draw the block diagram of OSI reference model.
3. What is switching? Explain circuit switching networks.
4. Briefly discuss about packet switching networks.
5. Explain the different kinds of networks.
6. What is multiplexing? Explain FDM.

UNIT-2 – DataLink Layer

5 Marks

1. Show the type of errors in data link layer with neat diagram.
2. Explain the CRC with example
3. Explain geosynchronous satellite with diagram
4. Detail discussion about the public switched telephone network. Explain.
5. Discuss about MEO satellite with diagram.
6. Discuss about LEO satellite with diagram.
7. Discuss about various connecting devices.

10 Marks

1. Explain the requirement for error control mechanism
2. Discuss the following (i).Wireless transmission. (II) Communication satellite.

3. Explain briefly the architecture of Bluetooth.
4. What is ALOGA? Explain Pure ALOGA.
5. Discuss about CSMA and its types.

UNIT-3 – Network Layer

5 Marks

1. List down the functionality of network layers
2. Write short notes on network address.
3. Explain simplex stop and wait protocol.
4. Explain error deduction code with example.
5. What are the internet organizations of network layer?
6. Explain any one of the elementary data link protocol in detail.
7. Briefly explain the sliding window protocol detail.

10 Marks

1. Give a detailed account on Ipv6.
2. Explain congestion control algorithm.
3. Explain any two error deduction and correction technique briefly.
4. Explain in detail about routing algorithms.
5. Explain the structure of IPV4 Structure.

UNIT-4 – Transport Layer

5 Marks

1. List down the features of UDP.
2. Show the function of transport layer.
3. Discuss about the future of TCP.
4. Explain about transport layer design issues.
5. What is TCP timer? Explain.

10 Marks

1. Describe error control and flow control.
2. Explain congestion control algorithm.

UNIT-5 – Application Layer

5 Marks

1. Discuss message format in E-Mail system.
2. Explain domain naming system.
3. Write a short note on DNS?
4. Discuss about architecture of WWW.
5. Explain HTTPS.

10 Marks

1. Explain types of Domain Naming System.
2. Explain the architecture of WWW.

Class : III - BCA

Subject : Computer Networks

Network - Layer performance:

Delay:

All of us expect instantaneous response from a network, but a packet, its source to its destination, encounters delays.

The delays in a network can be divided into four types:

1. Transmission delay
2. Propagation delay
3. Processing delay
4. Queuing delay.

Throughput:

Throughput at any point in a network is defined as the number of bits passing through the point in a second, which is actually the transmission range of data at that data

Packet Loss:

Another issue that severly affects the performance of communication is the number of packets lost during transmission.

Congestion Control:

Congestion Control is a mechanism for improving performance.

We can divide congestion control mechanisms into two board categories:

1. open-loop congestion control
2. closed-loop congestion control.

open-loop congestion control:

In open-loop congestion control, policies are applied to prevent congestion before it happens.

1. Retransmission policy
2. Window policy
3. Acknowledgement policy
4. Discarding policy
5. Admission policy

Closed - loop congestion control

Closed - loop congestion control mechanisms try to alleviate congestion after it happens.

1. Backpressure
2. Choke packet
3. Implicit signaling
4. Explicit signaling.

10.02.2020

IPV4 ADDRESSES:

The identifier used in the IP layer of the TCP/IP protocol suite to identify connection of each device to the Internet is called the Internet address or IP address.

Classful addressing:

The whole address space was divided into five classes. This scheme is referred to as classful addressing.

class	prefixes	First byte
A	n=8 bits	0 to 127
B	n=16 bits	128 to 191
C	n=24 bits	192 to 223
D	not applicable	224 to 239
E	not applicable	240 to

Address depletion:

The Internet was faced with the problem of the addresses being rapidly used up, resulting in no more addresses available for organizations.

Subnetting and supernetting:

Each subnet has a longer prefix length than the original network.

Advantage of classful addressing:

Given an address, we can easily find the class of the address and, since the prefix length for each class is fixed.

Classless addressing:

The short-term solution still uses IPv4 addresses, but it is called classless addressing.

In 1996, the Internet authorities announced a new architecture called classless addressing.

Prefix length : slash notation :

The notation is informally referred to as slash notation and formally as classless information routing or CIDR strategy.

Extracting information from an address :

1. The number of addresses in the block is found as $N = 2^{32-n}$

2. To find the first address, we keep the n leftmost bits and set the $(32-n)$ rightmost bits all to 0s.

3. To find last address, we keep the n leftmost bits and set the (32-n) rightmost bits all to 1s.

Dynamic Host configuration Protocol (DHCP):

DHCP has found such widespread use in the Internet that is it often called a plug and-play protocol.

A network manager can configure DHCP to assign permanent IP addresses to the host and routers.

Network Address Resolution (NAT):

A technology that can provide the mapping between the private and universal addresses, and at the same time support virtual private network.

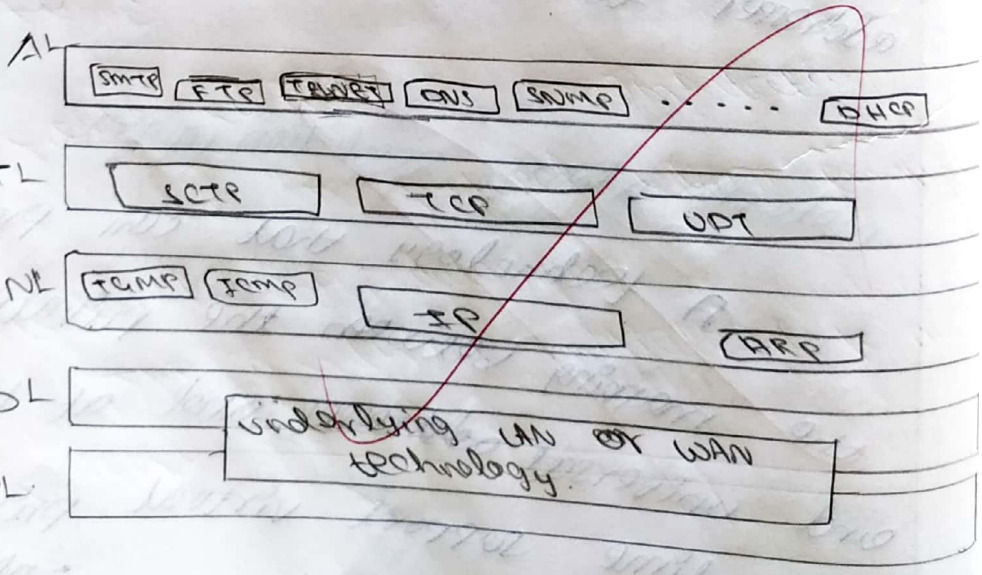
Address translation:

All of the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address.

Internet Protocol (IP):

The Internet Control message protocol version 4 (ICMP v4) helps to handle some errors that may occur in the network-layer delivery.

The Internet Group management Protocol (IGMP) used to help IPv4 in multicasting.



Datagram format:

packets used by the IP are called datagrams.

A datagram is a variable-length packet consisting of two parts: header and payload (data).

The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

Fields:

Version number

Header length

Service type

Total length

Identification, flags, and fragmentation offset.

Time-to-live

Protocol

Header checksum

source and destination addresses.

option

payload.

Fragmentation:

A datagram can travel through different networks. Each router decapsulates the IP datagram from the frame it receives, processes it and then encapsulates it in another frame.

Maximum transfer unit (MTU):

One of the features of each format is the maximum size of the payload that can be encapsulated. The total size of the datagram must be less than this maximum size.

Fields related to Fragmentation:

The IP protocol use a counter to label the datagrams.

The counter is initialized to a positive number.

The IP Protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by one.

Options:

The header of the IPv4 ~~number~~ is ~~100 x 8 = 800~~.

datagram is made of two parts:

1. A fixed part
2. A variable part.

They reserved for network testing and debugging.

Security of IPv4 Datagrams:

The IPv4 protocol, as well as the whole ~~Internet~~, was started when the internet users trusted each other.

No security was provided for the IPv4 protocol.

12-02-2020

packet sniffing:

An intruder may intercept an IP packet and make a copy of it.

packet modification:

The attacker intercepts the packet, changes its contents, and sends the new packet to the receiver.

IP spoofing:

An attacker can send an IP packet to a bank pretending that it is coming from one of the customers.

IPsec:

The IP packets today can be protected from the previously mentioned attacks using a protocol called IPsec (IP security).

four services:

1. Defining Algorithms and keys.
2. Packet Encryption
3. Data Integrity
4. Origin Authentication.

Routing Algorithms:

The general idea behind least-cost trees and the forwarding tables that can be made from them, now we concentrate on the routing algorithms.

Distance-Vector Routing:

In distance-vector routing, the first thing each node creates is its own least-cost tree with rudimentary information it has about its immediate neighbours.

Bellman - Ford Equation:

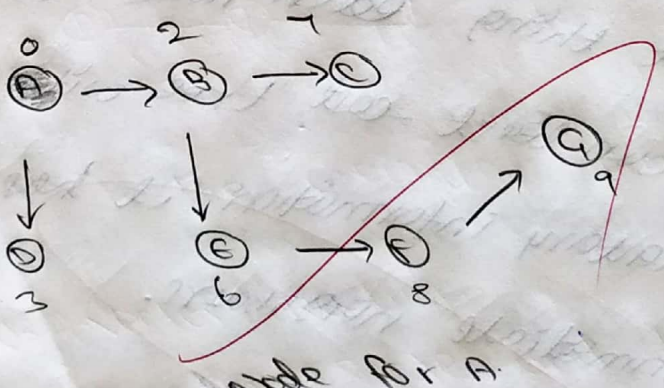
The heart of distance - vector routing is the famous Bellman-Ford equation.

$$D_{xy} = \min\{(C_{xa} + D_{ay}), (C_{xb} + D_{by}), (C_{xc} + D_{cy}), \ldots\}$$

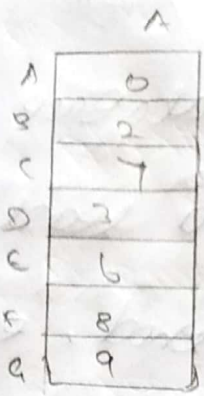
$$D_{xy} = \min\{D_{xy} + (C_{x2} + D_{2y})\}$$

Distance Vector:

The concept of a distance vector is the rationale for the name distance-vector routing.



Tree node for A.



Distance vector for node A.

Count to infinity:

A problem with distance-vector routing is that any decrease in cost propagates quickly, but any increase in cost will propagate slowly.

Two node loop:

Count to infinity is the two-node loop problem.

Link-State Routing:

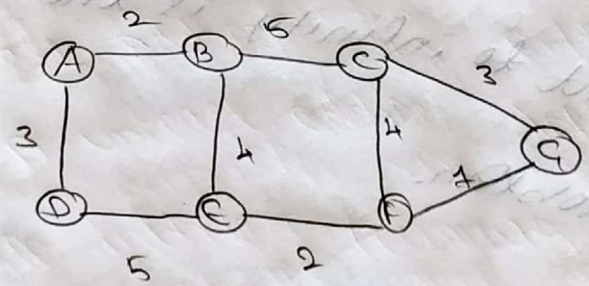
A routing algorithm that directly follows our discussion for creating least-cost trees and forwarding tables is link state (LS) routing.

D:

Link State DataBase (LSDB):

To create a least-cost tree with this method, each node needs to have a complete map of the network, which means it needs to know the state of each link.

The collection of states for all links is called the link state database (LSDB)



The weighted Graph:

path-vector Routing:

Both link state and distance-vector routing are based on the least-cost goal.

However, there are instances where this goal is not the priority.

Spanning trees:

In path-vector routing, the path from a source to all destinations is also determined by the best spanning tree.

Creation of Spanning Trees:

Path-vector routing, like distance-vector routing, is an synchronous and distributed routing algorithm.

The spanning trees are made, gradually and synchronously, by each node.

IPv6 addressing:

The main reason for migration from IPv4 to IPv6 is the small size of the address space in IPv4.

Representation:

A computer normally stores the address in binary, but it is clear that 128 bits cannot easily be handled by humans.

Address Space:

The address space of IPv6 contains 2^{128} addresses.

Three Address Types:

Unicast Address:

A unicast address defines a single interface (computer or router).

Anycast Address:

An anycast address defines a group of computers that all share single address.

Multicast Address: (1+4)

A multicast address also defines a group of computers.

Address Space Allocation:

Like the address space of IPv4, the address space of IPv6 divided into several blocks of varying size and each block is allocated for a special purpose.

Global Unicast Addresses:

The block in the address space that is used for unicast (one-to-one) communication between two hosts in the Internet is called the global unicast address block.

Autoconfiguration:

One of the interesting features of IPv6 addressing is the autoconfiguration of hosts.

The IPv6 PROTOCOL:

The change of the IPv6 address size requires the chan in the IPv4 packet format.

1. Better header format
2. New options
3. Allowance for extension
4. Support for resource allocation
5. Support for more security.

Packet format:

Each packet is composed of a base header followed by the payload.

Fields:

1. Version
2. Traffic class
3. Flow label
4. payload length
5. Next header
6. Hop limit
7. Source and destination addresses
8. payload.

Concept of flow and priority in IPv6:

The IP protocol was originally designed as a connectionless protocol. However, the tendency is to use the IP protocol as a connection-oriented protocol.

Fragmentation and Reassembly:

There are still fragmentation and reassembly of datagrams in the IPv6 protocol, but there is a major improvement in this respect.

Extension Header:

An IPv6 packet is made of a base header and some extension headers.

The length of the base header is fixed at 40 bytes.

Six types of headers:

1. Hop-by-hop
2. Destination
3. Source routing
4. Fragmentation
5. Authentication
6. ESP (Encrypted Security payload)

Comparison of options between IPv4 and IPv6:

The no-operation and end-of-option options in the IPv4 are replaced by Pad1 and PadN options in IPv6.

The record route option is not implemented in IPv6 because it was not used.

The timestamp option is not implemented because it was not used.

The source route option is called the source route extension header in IPv6.

The fragmentation field in the base header section of IPv4 have moved to the fragmentation extension header in IPv6.

The authentication extention header is new in IPv6.

The encrypted security payload extension header is new in IPv6.

Class : III - BCA

Subject : Computer Networks

17.2.2020

Unit - IV

Introduction to Transport Layer.

The transport layer is located between the application layer and the network layer.

It provides a process-to-process communication between two application layers, one at the localhost and the other at the remote host.

Transport layer services:

The transport layer is responsible for providing services to the application layer; it receives services from the network layer.

Process - to - process communication:

The first duty of a transport-layer protocol is to provide process-to-process communication.

A process is an application-layer entity (running program) that uses the services of the transport layer.

Addressing : Port Numbers:

Although there are a few ways to achieve process-to-process communication, the most common is through the client-server paradigm.

A process on the localhost, called a client, needs services from a process usually on the remote host, called a server.

The client program defines itself with a port number, called the ephemeral port number.

Ephemeral means "short-lived".

Transport Ranges:

Transport has divided the port numbers into three ranges:

1. Well-known ports
2. Registered ports
3. Dynamic ports

Socket Addresses:

The combination of an IP address and a port number is called a socket address.

Encapsulation and Decapsulation:

Encapsulation happens at the sender side.

Decapsulation happens at the receiver side.

Multiplexing and Demultiplexing:

Whenever an entity accepts items from more than one source, this is referred to as multiplexing (many to one); whenever an entity delivers items to more than one source, this is referred to as demultiplexing (one to many).

Flow control:

Whenever an entity produces items and another entity consumes them, there should be a balance between production and consumption rates.

Pushing or pulling:

Delivery of items from a producer to a consumer can occur in one of two ways:

1. Pushing
2. Pulling

If the sender delivers items whenever they are produced - without a prior request from the consumer - the delivery is referred to as pushing.

If the Producer delivers the items after the consumer has requested them, the delivery is referred to as pulling.

Flow control at Transport Layer:

In communication at the transport layer, we are dealing with four entities: Sender process, sender transport layer, receiver transport layer, and receiver process.

Buffer:

A buffer is a set of memory locations that can

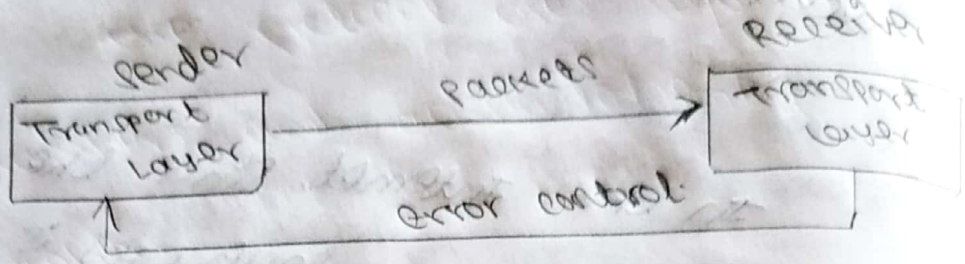
hold packets at the sender and receiver.

Error Control:

In the Internet, since the underlying network layer (IP) is unreliable, we need to make the transport layer reliable if the application requires reliability.

Error control at the transport layer is responsible for.

1. Detecting and discarding corrupted packets.
2. Keeping track of lost and discarded packets and resending them.
3. Recognizing duplicate packets and discarding them.
4. Buffering out-of-order packets until the missing packets arrive.



Sequence Numbers:

Error control requires that the sending transport layer knows which packet is to be resent and the receiving ~~bar~~ a duplicate, or which packet has arrived out of order.

Transport - Layer Protocols:

We can create a transport-layer protocol by combining a set of services described in the previous sections.

Simple Protocol:

Our first protocol is a simple connectionless protocol

20.02.2020

with neither flow nor error control.

FSMs:

The sender site should not send a packet until its application layer has a message to send.

Each FSM has only one state, the ready state.

Stop-and-wait Protocol:

A connection-oriented protocol called the Stop-and-wait protocol, which uses both flow and error control.

Both the sender and the receiver use a sliding window of size 1.

Sequence Numbers:

The protocol uses sequence numbers and acknowledgement number.

FSMs:

FSMs for the Stop-and-Wait protocol.

Sender:

1. Ready state
2. Blocking state.

Receiver:

The receiver is always in the ready state.

Efficiency:

The Stop-and-Wait Protocol is very inefficient if our channel is thick and long.

Pipelining:

In networking, and in other areas, a task is often begun before the previous task has ended. This is known as pipelining.

Go-Back-N Protocol (GBN):

To improve the efficiency of transmission, multiple packets must be in transition while the sender is waiting for acknowledgment.

Selective-Repeat Protocol:

This protocol is inefficient if the underlying network protocol loses a lot of packets.

Bidirectional Protocols: Piggybacking

A technique called piggybacking is used to improve the efficiency of the bidirectional protocols.

User Datagram Protocol:

The User Datagram Protocol is a connectionless, unreliable transport protocol.

It does not add anything to the services of IP except for providing process-to-process communication instead of host-to-host communication.

UDP is a very simple protocol using a minimum of overhead.

User Datagram:

UDP packets, called user datagrams, have a fixed-size header of 8 bytes made of four fields, each of 2 bytes (16 bits).

The 16 bits can define a total length of 0 to 65,535 bytes.

UDP services:

Earlier we discussed the general services provided by a transport-layer protocol.

1. Process-to-process communication.
2. Connectionless services.
3. Flow control.
4. Error control.
5. Checksum.
6. Congestion control.

UDP Applications:

Although UDP meets almost none of the criteria we mentioned earlier for a reliable transport-layer protocol, UDP is preferable for some applications.

Transmission Control Protocol:

Transmission Control Protocol (TCP) is a connection-oriented, reliable protocol.

TCP Services:

Process-to-Process communication

Stream delivery Service

Sending and Receiving Buffers

Segments

Full-duplex communication

Multiplexing and demultiplexing

connection-oriented Service.

TCP features:

Numbering system

Byte number

sequence number.

Acknowledgement number.

Segment:

A packet in TCP is called a segment.

1. Format
2. Source port address
3. Destination port address
4. Sequence number
5. Acknowledgement number
6. Header length
7. Control
8. Window size
9. Checksum
10. Urgent pointer
11. Option.

Encapsulation:

A TCP segment encapsulates the data received from the application layer.

Window in TCP:

- TCP uses two windows for each direction of data transfer, which means four windows for bidirectional communication.

1. Sent window
2. Receive window.

Flow control:

Flow control balances the rate a producer creates data with the rate a consumer can use the data.

- TCP separates flow control from error control.

1. opening and closing windows
2. Scenario
3. Shrinking of windows

4. Window Shutdown
5. Silly window syndrome
6. Syndrome created by the sender
7. Syndrome created by the receiver.

Error Control:

Error control includes mechanism for detecting and resending corrupted segments, resending lost segments, storing out of order segments until missing segments arrive, and detecting and discarding duplicated segments.

1. Checksum
2. Acknowledgement
3. Acknowledgement type.
   i) Cumulative Acknowledgement (ACK)
   ii) Selective Acknowledgement (SACK)

(ii) Generating Acknowledgement

4. Retransmission

5. out-of-order segments.

6. FSMs for Data Transfer in TCP

7. Sender-side FSM.

8. Receiver-side FSM.

Scenarios:

- Normal operation
- Lost segment.
- Fast retransmission
- Delayed segment
- Duplicate segment.

TCP congestion control.

Congestion window:

To control the number of segments to transmit. TCP uses

another variable called a, congestion window, cwnd.

Actual window = minimum(rwnd, cwnd).

congestion policies:

Slow start: Exponential increase

congestion avoidance: Additive increase

21/02/2020

24.02.2020

TCP Timers:

To perform their operations smoothly, most TCP implementations use at least four timers: Retransmission, persistence, keepalive and TIME-WAIT.

Round-Trip Time (RTT):

To calculate the retransmission time-out (RTO), we first need to calculate the round-trip time (RTT).

1. Measured RTT
2. Smoothed RTT
3. RTT deviation.

Retransmission Time-out:

The value of RTO is based on the smoothed round-trip time and its deviation.

most implementations use the following formula to calculate the RTO.

original → Initial value.

After any measurement → RTO = RTT$_s$ + 4 × RTT$_D$.

Karn's Algorithm:

Suppose that a segment is not acknowledged during the retransmission time-out period and is therefore retransmitted.

Karn's algorithm is simple. Do not consider the round-trip time of a retransmitted segment in the calculation of RTT$_s$.

Do not update the value of RTT$_s$ until you send a segment and receive an acknowledgment without the need for retransmission.

Exponential Backoff:

What is the value of RTO if a retransmission occurs? Most TCP implementation exponential backoff strategy. The value of RTO is doubled for each retransmission.

Persistence timer:

To deal with a zero-window-size advertisement, TCP needs another timer.

Keepalive timer:

A keepalive timer is used in some implementations to prevent a long idle connection between two TCPs.

Suppose that a client opens a TCP connection to a server,

transfers some data, and becomes silent. perhaps the client has crashed.

TIME-WAIT Timer:

The TIME-WAIT timer is used during connection termination.

The maximum segment lifetime (MSL) is the amount of time any segment can exist in a network before being discarded.

SCTP:

Stream control Transmission Protocol (SCTP) is a new transport-layer protocol designed to combine some features of UDP and TCP in an effort to create better protocol for multimedia communication.

Class : III - BCA

Subject : Computer Networks

Unit - V (1)

Client - Server Programming:

In a client - server paradigm communication at the application layer is between two running application programs called processes, a client and a server.

Application programming Interface:

A set of instructions of this kind is normally referred to as an application programming Interface (API).

Sockets:

Although a socket is supposed to behave like a terminal or a file, it is not a physical entity like them, it is an abstraction.

It is an object that is created and used by the application program.

Iterative communication using TCP.

TCP is a connection - oriented protocol. Before sending or receiving data, a connection need to be established between the client and the server.

02.03.2020

World wide web and HTTP:

www - World wide web.

World wide web.

The purpose of the web has gone beyond the simple retriving of linked documents. Today, the web is used to provide electronic shopping and gaming.

Web client (Browser)

A variety of vendors offer commercial browsers that interpret and display a web page, and all of them use nearly the same architecture.

Each browser usually consists of three parts.

1. Controller
2. Client protocols
3. Interpreters.

Uniform Resource Locator (URL):

A web page, as a file, needs to have a unique identifier to distinguish it from other web pages.

To define a web page, we need three identifiers:

1. Host
2. port
3. path.

Web documents:

The documents in the can be grouped into three board categories.

1. Static
2. Dynamic
3. Active.

Hyper Text Transfer Protocol (HTTP):

The Hyper Text Transfer Protocol (HTTP) is used to define how the client-server programs can be written to retrieve web pages from the web.

Response Message:

The first line in a response message is called the status line.

the first field defines the version of HTTP protocol.

Cookies:

The world wide web has originally designed as a stateless entity. A client sends a request; a server responds. Their relationship is over.

05.03.2020

FTP:

File Transfer Protocol (FTP) is the standard protocol provided by TCP/IP for copying a file from one host to another.

The client has three components:

1. User interface
2. Control process
3. Data transfer process.

The server has two
1. Control Proces
2. Data transfer Proces

Two Connections:

The two connections in FTP have different lifetimes.

1. Control Connection
2. Data Connection.

Electronic mail:

Electronic mail (or e-mail) allows users to exchange messages.

The nature of this application, however, is different from other applications discussed so far.

User Agent:

The first component of an electronic mail system is the user agent (UA).

It provides service to the user to make the process of sending and receiving a message easier.

There are two types of user agents:

1. command - driven.
2. GUI based.

POP3:

Post Office Protocol, version 3 (POP3) is simple but limited in functionality.

IMAP4:

Another mail access protocol is Internet mail Access Protocol version 4 (IMAP4).

MIME:

Multipurpose Internet mail extension (MIME) is a supplementary protocol that allows non-ASCII data to be sent through e-mail.

DOMAIN NAME SYSTEM (DNS):

The last client-server application program we discuss has been designed to help other application programs.

Since the Internet is so huge today, a central directory system cannot hold all the mapping.

Name Space:

A name space that maps each address to a unique name can be organized in two ways:

1. flat
2. Hierarchical.

DNS in the Internet:

DNS is a protocol that can be used in different platforms. In the Internet, the domain name space (tree) was originally divided into three sections:

1. Generic domains
2. Country domains
3. Inverse domains.

Resolution:

Mapping a name to an address is called name-address resolution.

DNS is designed as a client-server application. A host that needs to map an address to a name or a name to an address calls a DNS client called a resolver.