MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

CY

LECTURE HANDOUTS

L-1

II/III

Course Name with Code **: COMPUTER NETWORKS-19CYC05**

Course Faculty **: Dr. J.PREETHA**

Unit **: I- Data Communications** **Date of Lecture:**

Topic of Lecture: Introduction Data Communication

Introduction : (Maximum 5 sentences) :

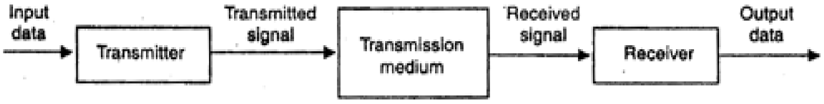
- Data Communication is defined as a process in which more than one computer transfers information, instructions to each other and for sharing resources.
- Or in other words, communication is a process or act in which we can send or receive data.
- A network of computers is defined as an interconnected collection of autonomous computers.
- Autonomous means no computer can start, stop or control another computer.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Basics of Network
- OSI Layer & TCP/IP Model
- Network Topologies

Detailed content of the Lecture:

- Data communication refers to the exchange of data between a source and a receiver via form of transmission media such as a wire cable.
- Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area.
- The meanings of source and receiver are very simple.
- The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver.
- Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the information at the source and receiver.
- Datum mean the facts information statistics or the like derived by calculation or experimentation.
- The facts and information so gathered are processed in accordance with defined systems of procedure.
- Data can exist in a variety of forms such as numbers, text, bits and bytes.
- The Figure is an illustration of a simple data communication system.



- A data communication system may collect data from remote locations through data transmission circuits, and then outputs processed results to remote locations.
- Figure provides a broader view of data communication networks.
- The different data communication techniques which are presently in widespread use evolved gradually either to improve the data communication techniques already existing or to replace the same with better options and features.

A Data Communication System using Remote Locations

- Then, there are data communication jargons to contend with such as baud rate, modems, routers, LAN, WAN, TCP/IP, ISDN, during the selection of communication systems.
- Hence, it becomes necessary to review and understand these terms and gradual development of data communication methods.

Video Content / Details of website for further learning (if any):
https://ecomputernotes.com/computernetworkingnotes/communication-networks/what-is-data-communication

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

CY

LECTURE HANDOUTS

L-2

II/III

Course Name with Code **: COMPUTER NETWORKS-19CYC05**

Course Faculty **: Dr. J.PREETHA**

Unit **: I- Data Communications** **Date of Lecture:**

Topic of Lecture: Data Communication
Introduction : (Maximum 5 sentences) : ● Data communication refers to the exchange of data between a source and a receiver via form of transmission media such as a wire cable. ● Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area.
Prerequisite knowledge for Complete understanding and learning of Topic: **(Max. Four important topics)** ● Basics of Network ● OSI Layer & TCP/IP Model ● Network Topologies

Detailed content of the Lecture:

Components of data communication system

A Communication system has following components:

1. **Message**: It is the information or data to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.

2. **Sender**: It is the device/computer that generates and sends that message.

3. **Receiver**: It is the device or computer that receives the message. The location of receiver computer is generally different from the sender computer. The distance between sender and receiver depends upon the types of network used in between.

4. **Medium**: It is the channel or physical path through which the message is carried from sender to the receiver. The medium can be wired like twisted pair wire, coaxial cable, fiber-optic cable or wireless like laser, radio waves, and microwaves.

5. **Protocol**: It is a set of rules that govern the communication between the devices. Both sender and receiver follow same protocols to communicate with each other.

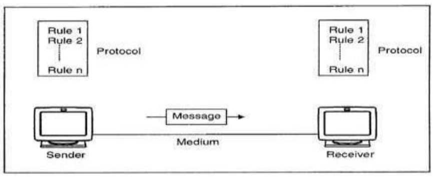
A protocol performs the following functions:

1. **Data sequencing**. It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.

2. **Data routing**. Data routing defines the most efficient path between the source and destination.

3. **Data formatting**. Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.

4. **Flow control**. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.



5. **Error control**. These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.

6. **Precedence and order of transmission**. These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.

7. **Connection establishment and termination**. These rules define how connections are established,

Video Content / Details of website for further learning (if any): https://ecomputernotes.com/computernetworkingnotes/communication-networks/what-is-data-communication
Important Books/Journals for further learning including the page nos.: Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L-3

CY

LECTURE HANDOUTS

II/III

Course Name with Code **: COMPUTER NETWORKS-19CYC05**

Course Faculty **: Dr. J.PREETHA**

Unit **: I- Data Communications** **Date of Lecture:**

Topic of Lecture: The OSI Model

Introduction : (Maximum 5 sentences) :

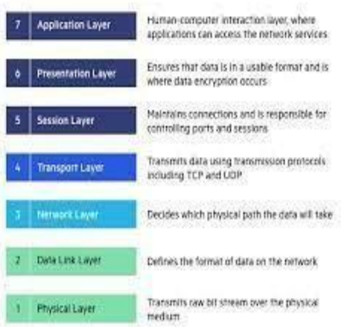
- The OSI Model (Open Systems Interconnection Model) is a conceptual framework used to describe the functions of a networking system.
- The OSI model characterizes computing functions into a universal set of rules and requirements in order to support interoperability between different products and software.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Basics of Network
- OSI Layer & TCP/IP Model
- Network Topologies

Detailed content of the Lecture:

- In the OSI reference model, the communications between a computing system are split into seven different abstraction layers:
  - Physical
  - Data Link
  - Network
  - Transport
  - Session
  - Presentation
  - Application.
- Created at a time when network computing was in its infancy, the OSI was published in 1984 by the International Organization for Standardization (ISO).
- Though it does not always map directly to specific systems, the OSI Model is still used today as a means to describe Network Architecture.



7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

The 7 Layers of the OSI Model

Physical Layer :

The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network from the physical layer of the sending device to the physical layer of the receiving device. It can include specifications such as voltages, pin layout, cabling, and radio frequencies. At the physical layer, one might find “physical” resources such as network hubs, cabling, repeaters, network adapters or modems.

Data Link Layer :

At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames. The data link layer also corrects errors that may have occurred at the physical layer. The data link layer encompasses two sub-layers of its own. The first, media access control (MAC), provides flow control and multiplexing for device transmissions over a network. The second, the logical link control (LLC), provides flow and error control over the physical medium as well as identifies line protocols

Network Layer :

The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame. The network layer finds the destination by using logical addresses, such as IP (internet protocol). At this layer, routers are a crucial component used to quite literally route information where it needs to go between networks.

Transport Layer :

The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. One of the most common examples of the transport layer is TCP or the Transmission Control Protocol.

Session Layer :

The session layer controls the conversations between different computers. A session or connection between machines is set up, managed, and termined at layer 5. Session layer services also include authentication and reconnections.

Presentation Layer :

The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts. Because of this, it at times also called the syntax layer. This layer can also handle the encryption and decryption required by the application layer.

Application Layer :

At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications such as a web browser or Office 365. The application layer identifies communication partners, resource availability, and synchronizes communication.

Video Content / Details of website for further learning (if any):
https://www.forcepoint.com/cyber-edu/osi-model#:~:text=The%20OSI%20Model%20(Open%20Systems,between%20different%20products%20and%20software.

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

CY

LECTURE HANDOUTS

L-4

Course Name with Code **: COMPUTER NETWORKS-19CYC05**

II/III

Course Faculty **: Dr. J.PREETHA**

Unit **: I- Data Communications** **Date of Lecture:**

Topic of Lecture: TCP/IP Protocol Suite

Introduction : (Maximum 5 sentences) :

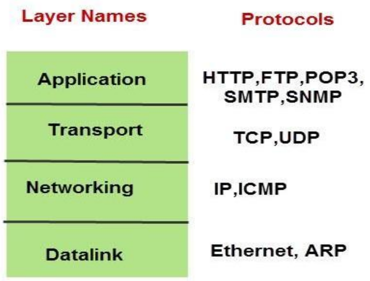
- The Internet protocol suite, commonly known as TCP/IP, is the set of communications protocols used in the Internet and similar computer networks.
- The current foundational protocols in the suite are the Transmission Control Protocol and the Internet Protocol.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Basics of Network
- OSI Layer & TCP/IP Model
- Network Topologies.

Detailed content of the Lecture:

- A protocol is a set of rules that govern how systems communicate.
- For networking they govern how data is transferred from one system to another.
- A protocol suite is a collection of protocols that are designed to work together.
- The TCP/IP protocol suite consists of many protocols that operate at one of 4 layers.
- The protocol suite is named after two of the most common protocols –
    - TCP (transmission Control Protocol) and
    - IP (internet Protocol).
- TCP/IP was designed to be independent of networking Hardware and should run across any connection media.
- The earliest use, and the most common use is over Ethernet networks.
- Ethernet is a 2 layer protocol/standard covering the physical and data link layer, shown in the diagram below.



TCP/IP Networking Model

Important Notes:

- HTTP (hypertext transfer protocol) - This is the workhorse of the Web.
- SMTP, POP3, IMap4 – These are email protocols
- TCP (Transmission control protocol) is a connection orientated protocol and is used to provides a reliable end to end connection.
- UDP (used datagram protocol) is connection less protocol and doesn’t guarantee delivery.

Applications will choose which transmission protocol to use based on their function.

- HTTP, POP3, IMAP4, SMTP and many more use TCP.
- UDP is used more in utility applications like DNS, RIP (routing information protocol), DHCP.
- IP (Internet Protocol) – This is the main networking protocol.
- There are two version of IP :
- ARP (address resolution Protocol) - Translates an IP address to a MAC or physical address.(IP4 networks).

- IPv4 and
- IPV6

Video Content / Details of website for further learning (if any):
http://www.steves-internet-guide.com/internet-protocol-suite-explained/

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L-5

CY

LECTURE HANDOUTS

II/III

Course Name with Code **: COMPUTER NETWORKS-19CYC05**

Course Faculty **: Dr. J.PREETHA**

Unit **: I- Data Communications** **Date of Lecture:**

Topic of Lecture: Addressing

Introduction : (Maximum 5 sentences) :

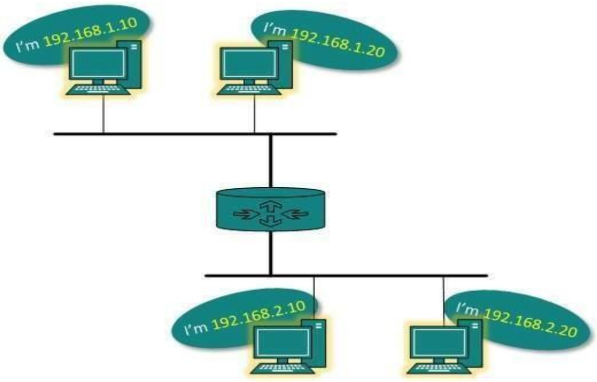
- A network address is any logical or physical address that uniquely distinguishes a network node or device over a computer or telecommunications network.
- It is a numeric/symbolic number or address that is assigned to any device that seeks access to or is part of a network.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Basics of Network
- OSI Layer & TCP/IP Model
- Network Topologies.

Detailed content of the Lecture:

- Layer 3 network addressing is one of the major tasks of Network Layer.
- Network Addresses are always logical i.e. these are software based addresses which can be changed by appropriate configurations.
- A network address always points to host / node / server or it can represent a whole network.
- Network address is always configured on network interface card and is generally mapped by system with the MAC address (hardware address or layer-2 address) of the machine for Layer-2 communication.
- There are different kinds of network addresses in existence:
    - IP
    - IPX
    - AppleTalk
- We are discussing IP here as it is the only one we use in practice these days.



- IP addressing provides mechanism to differentiate between hosts and network.
- Because IP addresses are assigned in hierarchical manner, a host always resides under a specific network.T
- he host which needs to communicate outside its subnet, needs to know destination network address, where the packet/data is to be sent.
- Hosts in different subnet need a mechanism to locate each other.
- This task can be done by DNS. DNS is a server which provides Layer-3 address of remote host mapped with its domain name or FQDN.
- When a host acquires the Layer-3 Address (IP Address) of the remote host, it forwards all its packet to its gateway.
- A gateway is a router equipped with all the information which leads to route packets to the destination host.
- Routers take help of routing tables, which has the following information:
    - Method to reach the network
- Routers upon receiving forwarding request, forwards packet to its next hop (adjacent router) towards the destination.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/data_communication_computer_network/network_addressing.htm

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

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

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

CY

LECTURE HANDOUTS

L-6

II/III

Course Name with Code **: COMPUTER NETWORKS-19CYC05**
Course Faculty **: Dr. J.PREETHA**

Unit **: I- Data Communications** **Date of Lecture:**

Topic of Lecture: Transmission Media

Introduction : (Maximum 5 sentences) :

- Transmission media is a communication channel that carries the information from the sender to the receiver.
- Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through LAN(Local Area Network).

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Basics of Network
- OSI Layer & TCP/IP Model
- Network Topologies.

Detailed content of the Lecture:

- Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through **LAN**(Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits in the form of electrical signals.
- In a fibre based network, the bits in the form of light pulses.
- In **OSI** (Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum.
- The characteristics and quality of data transmission are determined by the characteristics of medium and signal.
- Transmission media is of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., **Physical layer**.

Some factors need to be considered for designing the transmission media:

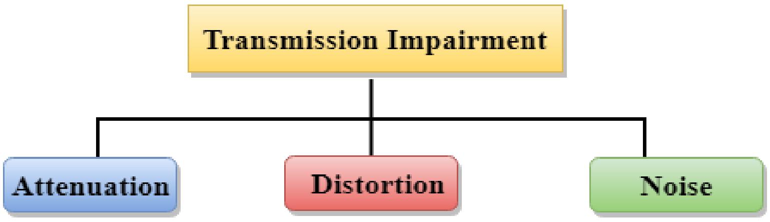
- **Bandwidth:** All the factors are remaining constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.

- **Transmission impairment:** When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will get destroyed due to transmission impairment.

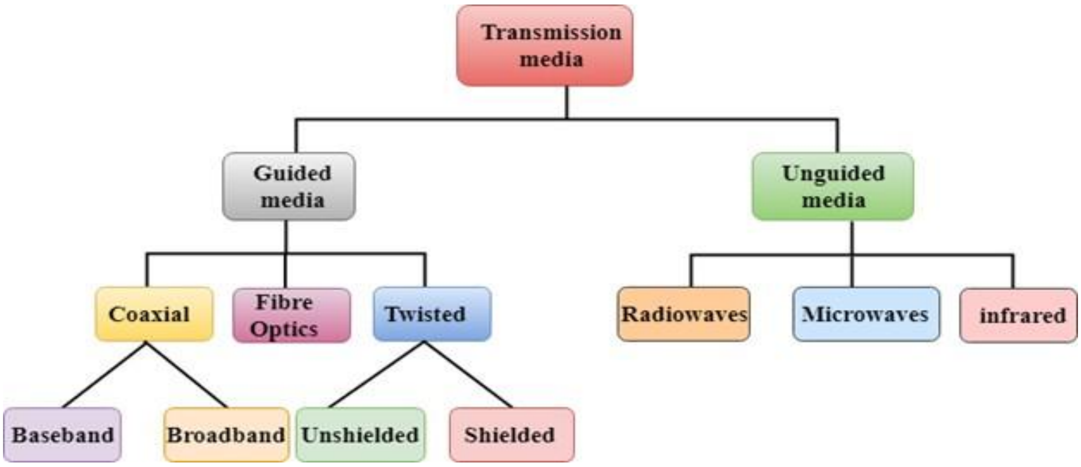
- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing the distance which causes the loss of energy.
- **Interference:** An interference is defined as the process of disrupting a signal when it travels over a communication medium on the addition of some unwanted signal.

- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its own propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is travelled over a transmission medium, some unwanted signal is added to it which creates the noise.

Causes of Transmission Impairment:



Classification Of Transmission Media:



- Guided Transmission Media
- UnGuided Transmission Media

Video Content / Details of website for further learning (if any):
https://www.javatpoint.com/transmission-media

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

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

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

CY

LECTURE HANDOUTS

L-7

II/III

Course Name with Code : COMPUTER NETWORKS-19CYC05

Course Faculty : Dr. J.PREETHA

Unit : I- Data Communications

Date of Lecture:

Topic of Lecture: Networking devices

Introduction : (Maximum 5 sentences) :

- Networking hardware, also known as network equipment or computer networking devices, are electronic devices which are required for communication and interaction between devices on a computer network.
- A "network" device is a component that makes up the network infrastructure such as modems, routers and switches.
- Specifically, they mediate data transmission in a computer network.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Basics of Network
- OSI Layer & TCP/IP Model
- Network Topologies.

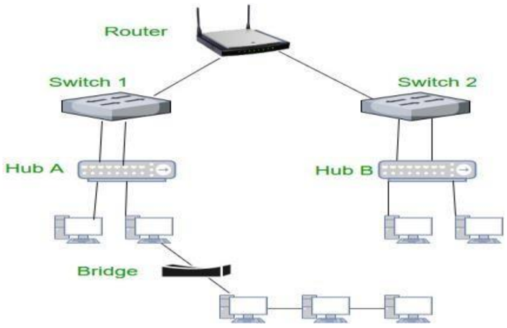
Detailed content of the Lecture:

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

2. Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub:-** These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub :-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
- **Intelligent Hub :-** It works like active hubs and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.



Gateway – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. Gateway is also called a protocol converter

Bridge – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device

Router – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks, and working as the bridge, it is capable of filtering local area network traffic.

NIC – NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and router or modem. NIC card is a layer 2 device which means that it works on both physical and data link layer of the network model.

Types of Bridges

Transparent Bridges:- These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.

- **Source Routing Bridges:-** In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network
- **Switch** – A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same
- **Routers** – A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

LECTURE HANDOUTS

CY

II/III

Course Name with Code : **COMPUTER NETWORKS-19CYC05**

Course Faculty : **Dr. J.PREETHA**

Unit : **I- Data Communications** **Date of Lecture:**

Topic of Lecture : Network Topologies

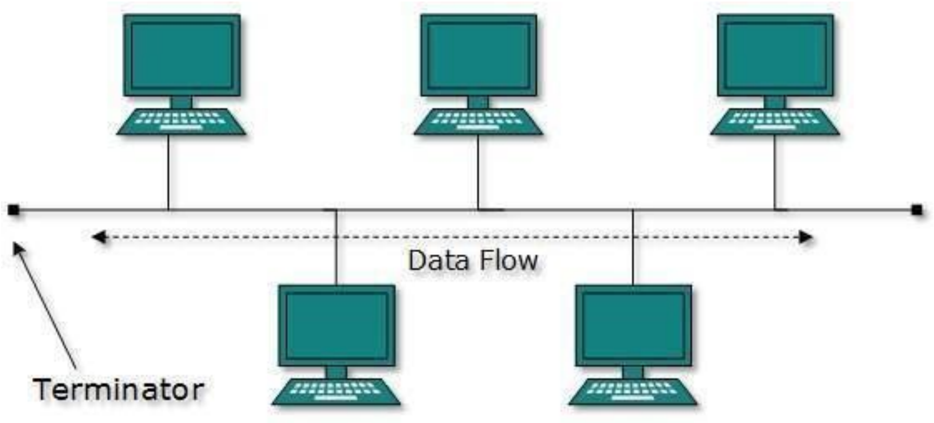
Introduction : (Maximum 5 sentences) :

- Network topology is the arrangement of the elements of a communication network.
- Network topology can be used to define or describe the arrangement of various types of telecommunication networks, including command and control radio networks, industrial fieldbusses and computer networks.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Basics of Network
- OSI Layer & TCP/IP Model
- Network Topologies.

Detailed content of the Lecture:



Bus Topology

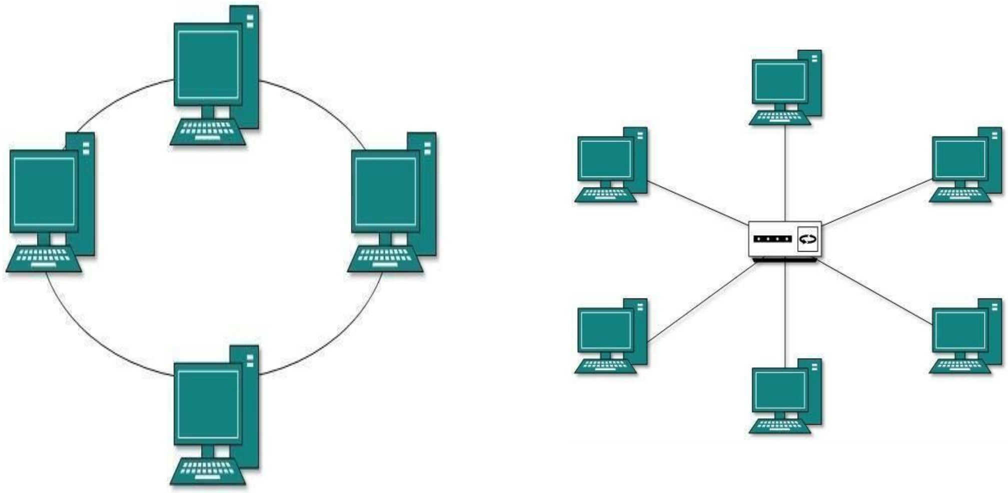
In case of Bus topology, all devices share single communication line or cable.Bus topology may have problem while multiple hosts sending data at the same time.

Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.

Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

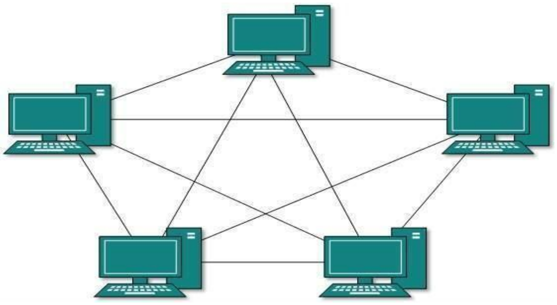
- Layer-1 device such as hub or repeater

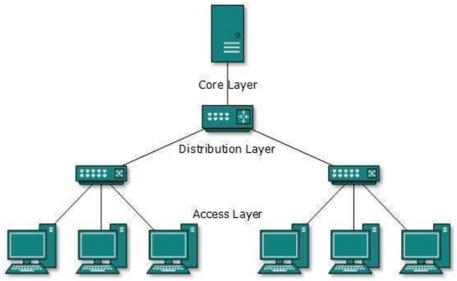


Ring Topology

- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway

As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts, takes place through only the hub.Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.





Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/data_communication_computer_network/computer_network_topologies.htm

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

L-9

LECTURE HANDOUTS

CY

II/III

Course Name with Code :**19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.Preetha**

Unit : **II-Data Link Layer** **Date of Lecture:**

Topic of Lecture: Encoding

Introduction : (Maximum 5 sentences) :

- Encoding is **the process of converting the data or a given sequence of cccharacters, symbols, alphabets etc**., into a specified format, for the secured transmission of data.
- Decoding is the reverse process of encoding which is to extract the information from the converted format.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

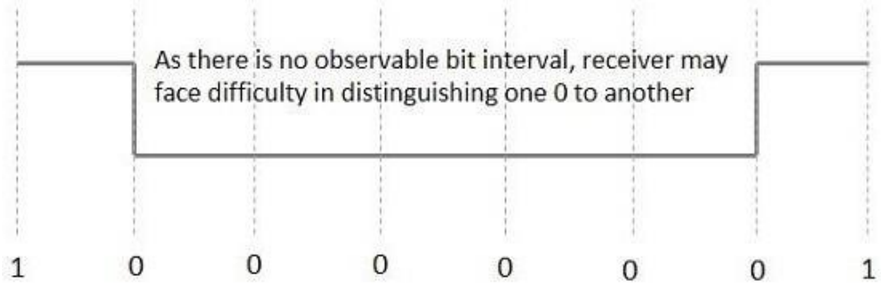
- OSI Layer
- Basics Of Networking

- **Detailed content of the Lecture:**

- Data Encoding
- Encoding is the process of using various patterns of voltage or current levels to represent **1s** and **0s** of the digital signals on the transmission link.
- The common types of line encoding are Unipolar, Polar, Bipolar, and Manchester.

- Encoding Techniques
- The data encoding technique is divided into the following types, depending upon the type of data conversion.
- **Analog data to Analog signals** − The modulation techniques such as Amplitude Modulation, Frequency Modulation and Phase Modulation of analog signals, fall under this category.
- **Analog data to Digital signals** − This process can be termed as digitization, which is done by Pulse Code Modulation PCM*PCM*. Hence, it is nothing but digital modulation. As we have already discussed, sampling and quantization are the important factors in this. Delta Modulation gives a better output than PCM.
- **Digital data to Analog signals** − The modulation techniques such as Amplitude Shift Keying ASK*ASK*, Frequency Shift Keying FSK*FSK*, Phase Shift Keying PSK*PSK*, etc., fall under this category. These will be discussed in subsequent chapters.
- Non Return to Zero NRZ*NRZ*
- NRZ Codes has **1** for High voltage level and **0** for Low voltage level. The main behavior of NRZ codes is that the voltage level remains constant during bit interval. The end or start of a bit will not be indicated and it will maintain the same voltage state, if the value of the previous bit and the value of the present bit are same.

- The following figure explains the concept of NRZ coding.


As there is no observable bit interval, receiver may face difficulty in distinguishing one 0 to another
1
0
0
0
0
0
0
1

NRZ Coding

-
- If the above example is considered, as there is a long sequence of constant voltage level and the clock synchronization may be lost due to the absence of bit interval, it becomes difficult for the receiver to differentiate between 0 and 1.

Video Content / Details of website for further learning (if any):
Data Encoding Techniques (tutorialspoint.com)

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

L-10

LECTURE HANDOUTS

CY

II/III

Course Name with Code :19CYC05 & COMPUTER NETWORKS

Course Faculty : Dr.J.Preetha

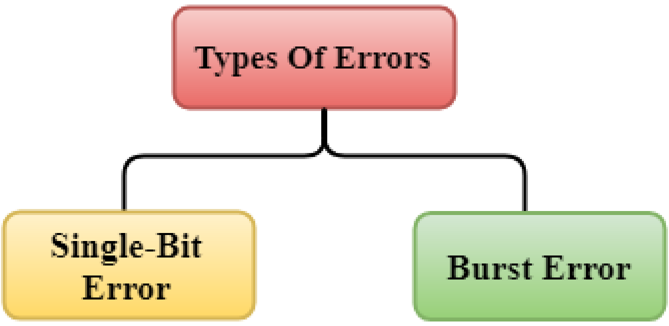
Unit : II- Data Link Layer **Date of Lecture:**

Topic of Lecture: Error Detection
Introduction : (Maximum 5 sentences) : • When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. • An Error is a situation when the message received at the receiver end is not identical to the message transmitted.
Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics) • OSI Layer • Basics Of Networking

Types Of Errors

Error Detection

- When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device.
- An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

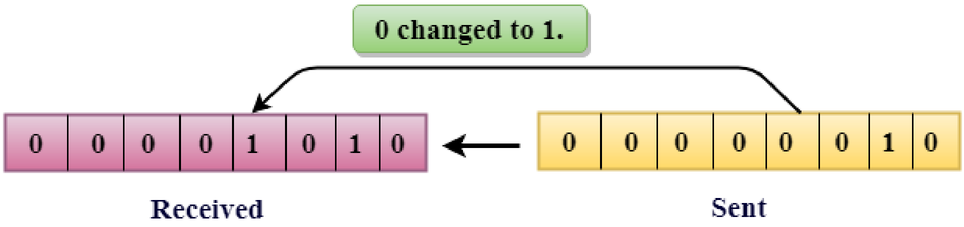


Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:

- The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



- In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.
- **Single-Bit Error** does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.
- Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

Video Content / Details of website for further learning (if any):
[Computer Network | Error Detection - javatpoint]()

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

L-11,12

LECTURE HANDOUTS

CY

II/III

Course Name with Code :19CYC05 & COMPUTER NETWORKS

Course Faculty : Dr.J.Preetha

Unit : II- Data Link Layer **Date of Lecture:**

Topic of Lecture: Error Detection

Introduction : (Maximum 5 sentences) :

- An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

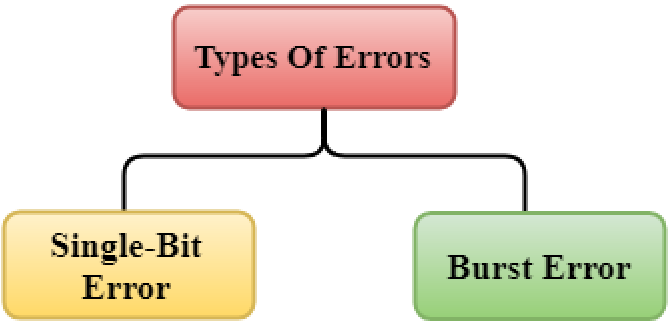
- OSI Layers
- Basic Networking

Detailed content of the Lecture:

Types Of Errors

Error Detection

- When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device.
- An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

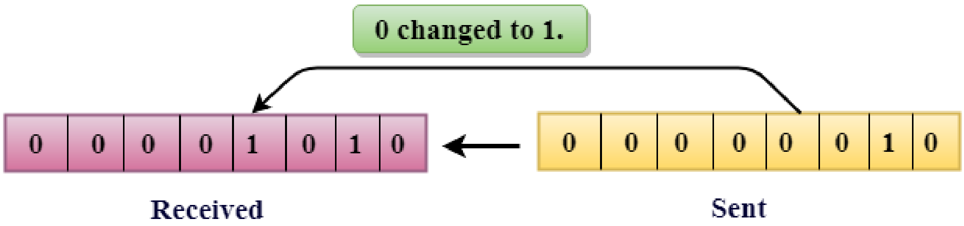


Errors can be classified into two categories:

- Single-Bit Error
- Burst Error

Single-Bit Error:

- The only one bit of a given data unit is changed from 1 to 0 or from 0 to 1.



- In the above figure, the message which is sent is corrupted as single-bit, i.e., 0 bit is changed to 1.
- **Single-Bit Error** does not appear more likely in Serial Data Transmission. For example, Sender sends the data at 10 Mbps, this means that the bit lasts only for 1 ?s and for a single-bit error to occurred, a noise must be more than 1 ?s.
- Single-Bit Error mainly occurs in Parallel Data Transmission. For example, if eight wires are used to send the eight bits of a byte, if one of the wire is noisy, then single-bit is corrupted per byte.

The two or more bits are changed from 0 to 1 or from 1 to 0 is known as Burst Error.

- As discussed in Chapter 1, bit errors are sometimes introduced into frames. This happens, for example, because of electrical interference or thermal noise.

- Although errors are rare, especially on optical links, some mechanism is needed to detect these errors so that corrective action can be taken.

- Otherwise, the end user is left wondering why the C program that successfully compiled just amoment ago now suddenly has a syntax error in it, when all that happened in the interim is thatit was copied across a network file system.

- There is a long history of techniques for dealing with bit errors in computer systems, dating back to at least the 1940s.

- Hamming and Reed-Solomon codes are two notable examples that were developed for use in punch card readers, when storing data on magnetic disks, and in early core memories. This section describes some of the error detection techniques most commonly used in networking.

- Detecting errors is only one part of the problem. The other part is correcting errors once detected. Two basic approaches can be taken when the recipient of a message detects an error. One is to notify the sender that the message was corrupted so that the sender can retransmit a copy of the message.

- If bit errors are rare, then in all probability the retransmitted copy will be error free. Alternatively, some types of error detection algorithms allow the recipient to reconstruct the correct message even after it has been corrupted; such algorithms rely on *error-correcting codes*, discussed below.

- One of the most common techniques for detecting transmission errors is a technique known as the *cyclic redundancy check* (CRC). It is used in nearly all the link-level protocols discussed in this chapter. This section outlines the basic CRC algorithm, but before discussing that approach, we first describe the simpler *checksum* scheme used by several Internet protocols.

- The basic idea behind any error detection scheme is to add redundant information to a frame that can be used to determine if errors have been introduced. In the extreme, we could

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=EMrY-8m8D1E

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

L-13

LECTURE HANDOUTS

CY

II/III

Course Name with Code :**19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.Preetha**

Unit : **II- Data Link Layer** **Date of Lecture:**

Topic of Lecture: Reliable Transmission

Introduction : (Maximum 5 sentences) :

- Reliable delivery is usually accomplished using a combination of two fundamental mechanisms—**acknowledgments and timeouts**.
- An acknowledgment (ACK for short) is a small control frame that a protocol sends back to its peer saying that it has received an earlier frame.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- OSI layer
- Basics Of Networking

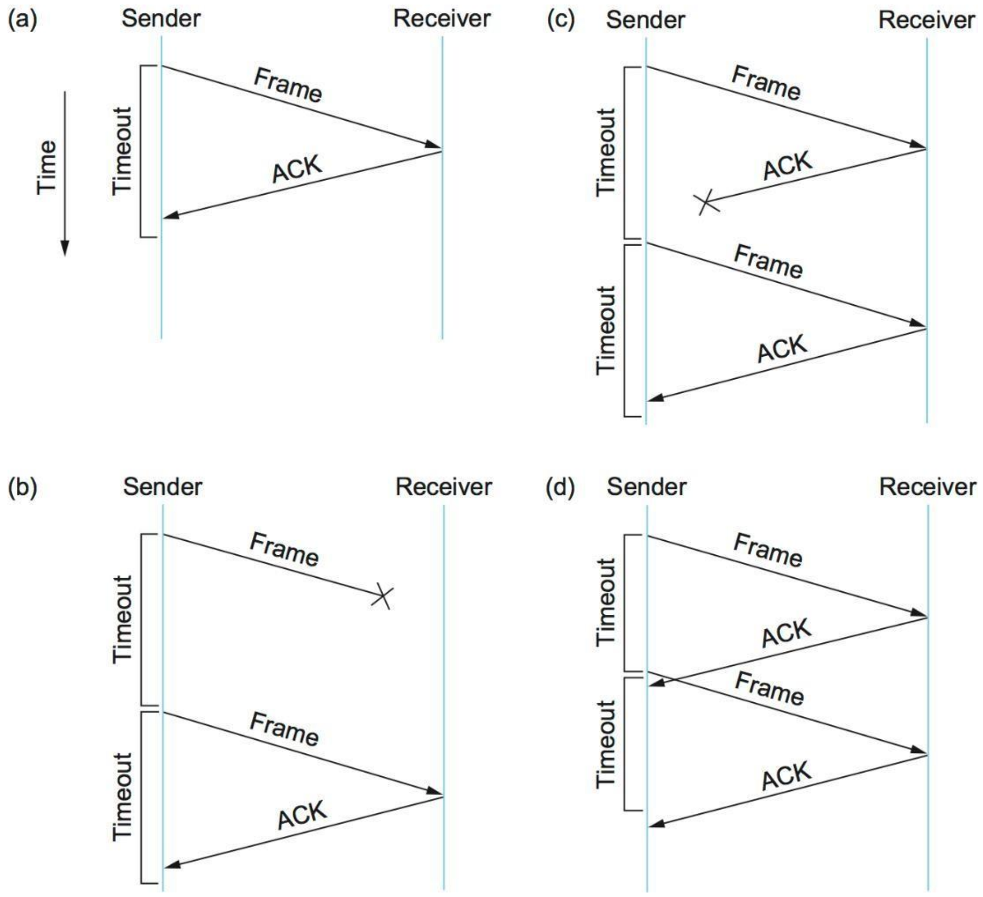
Detailed content of the Lecture:

Reliable Transmission

- Reliable delivery is usually accomplished using a combination of two fundamental mechanisms—**acknowledgments and timeouts**.
- An acknowledgment (ACK for short) is a small control frame that a protocol sends back to its peer saying that it has received an earlier frame.

Stop-and-Wait

- The simplest ARQ scheme is the *stop-and-wait* algorithm. The idea of stop-and-wait is straightforward:
- After transmitting one frame, the sender waits for an acknowledgment before transmitting the next frame.
- If the acknowledgment does not arrive after a certain period of time, the sender times out and retransmits the original frame.



Sliding Window

- Consider again the scenario in which the link has a delay × bandwidth product of 8 KB and frames are 1 KB in size. We would like the sender to be ready to transmit the ninth frame at pretty much the same moment that the ACK for the first frame arrives. The algorithm that allows us to do this is called *sliding window*, and an illustrative timeline is given in Figure 36.

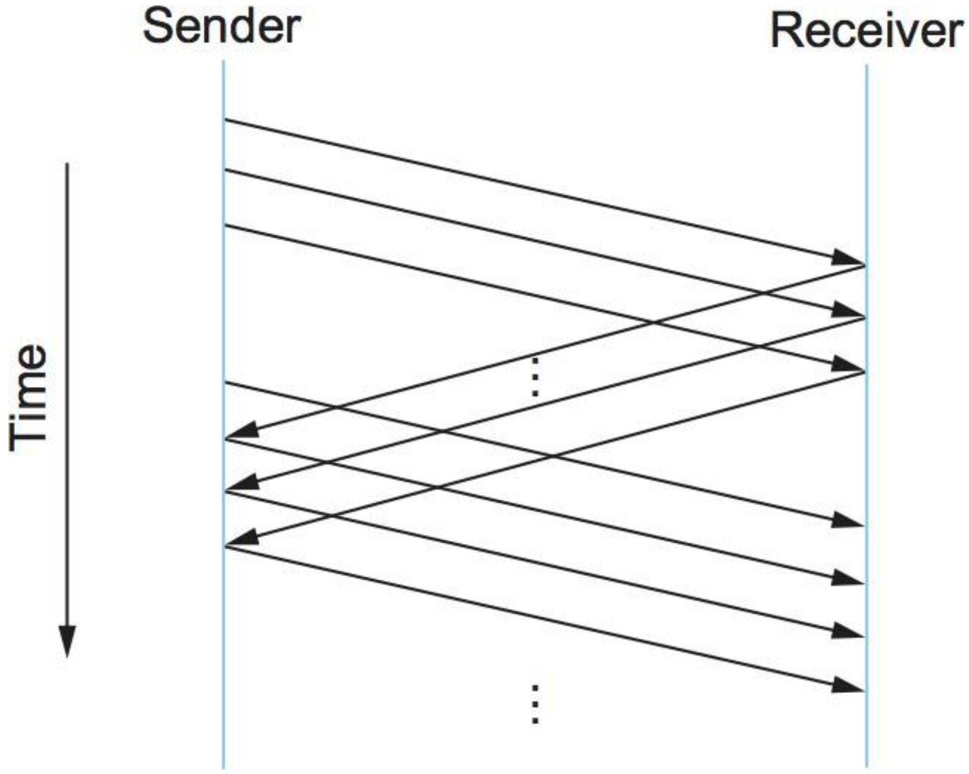


Figure 36. Timeline for the sliding window algorithm.

The Sliding Window Algorithm

- The sliding window algorithm works as follows. First, the sender assigns a *sequence number*, denoted

SeqNum, to each frame.

- For now, let's ignore the fact that SeqNum is implemented by a finite-size header field and instead assume that it can grow infinitely large.
- The sender maintains three variables: The *send window size*, denoted SWS, gives the upper bound on the number of outstanding (unacknowledged) frames that the sender can transmit;
- LAR denotes the sequence number of the *last acknowledgment received*; and LFS denotes the sequence number of the *last frame sent*.
- The sender also maintains the following invariant:
- LFS - LAR <= SWS

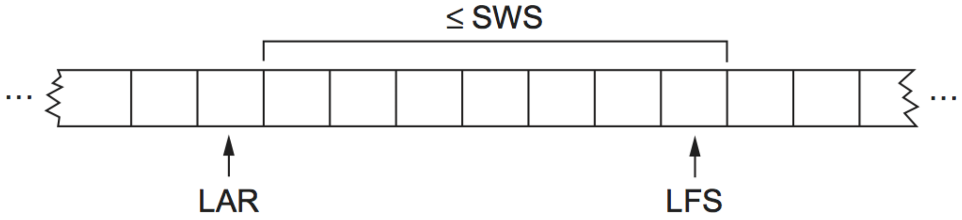
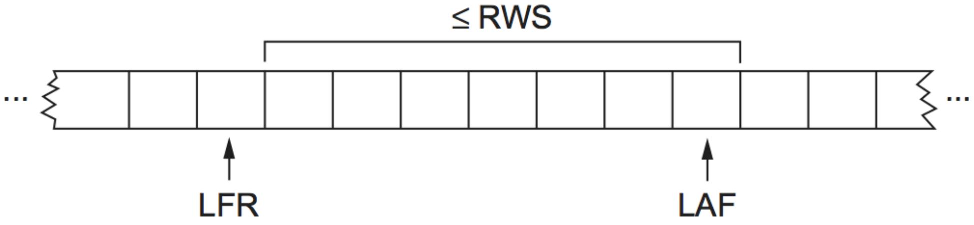


Figure 37. Sliding window on sender.

- When an acknowledgment arrives, the sender moves LAR to the right, thereby allowing the sender to transmit another frame.
- Also, the sender associates a timer with each frame it transmits, and it retransmits the frame should the timer expire before an ACK is received.
- Notice that the sender has to be willing to buffer up to SWS frames since it must be prepared to retransmit them until they are acknowledged.
- The receiver maintains the following three variables: The *receive window size*, denoted RWS, gives the upper bound on the number of out-of-order frames that the receiver is willing to accept; LAF denotes the sequence number of the *largest acceptable frame*; and LFR denotes the sequence number of the *last frame received*. The receiver also maintains the following invariant:
- LAF - LFR <= RWS

This situation is illustrated in



Video Content / Details of website for further learning (if any):
2.5 Reliable Transmission — Computer Networks: A Systems Approach Version 6.2-dev documentation

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

L-14

LECTURE HANDOUTS

CY

II/III

Course Name with Code :19CYC05 & COMPUTER NETWORKS

Course Faculty : Dr.J.Preetha

Unit : II- Data Link Layer Date of Lecture:

Topic of Lecture: Reliable Transmission

Introduction : (Maximum 5 sentences) :

- Reliable delivery is usually accomplished using a combination of two fundamental mechanisms—
acknowledgments and timeouts.
- An acknowledgment (ACK for short) is a small control frame that a protocol sends back to its peer saying that it has received an earlier frame.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- OSI layer
- Basics Of Networking

Detailed content of the Lecture:

- In computer networking, a **reliable** protocol is a communication protocol that notifies the sender whether or not the delivery of data to intended recipients was successful.
- Reliability is a synonym for **assurance**, which is the term used by the ITU and ATM Forum.
- Reliable protocols typically incur more overhead than unreliable protocols, and as a result, function more slowly and with less scalability. This often is not an issue for unicast protocols, but it may become a problem for reliable multicast protocols.
- Transmission Control Protocol (TCP), the main protocol used on the Internet, is a reliable unicast protocol. UDP is an unreliable protocol and is often used in computer games, streaming media or in other situations where speed is an issue and some data loss may be tolerated because of the transitory nature of the data.
- Often, a reliable unicast protocol is also connection oriented. For example, TCP is connection oriented, with the virtual-circuit ID consisting of source and destination IP addresses and port numbers.
- However, some unreliable protocols are connection oriented, such as Asynchronous Transfer Mode and Frame Relay.
- In addition, some connectionless protocols, such as IEEE 802.11, are reliable.
- In the context of distributed protocols, reliability properties specify the guarantees that the protocol provides with respect to the delivery of messages to the intended

recipient(s).

- An example of a reliability property for a unicast protocol is "at least once", i.e. at least one copy of the message is guaranteed to be delivered to the recipient.
- Reliability properties for multicast protocols can be expressed on a per-recipient basis (simple reliability properties), or they may relate the fact of delivery or the order of delivery among the different recipients (strong reliability properties).
- In the context of multicast protocols, strong reliability properties express the guarantees that the protocol provides with respect to the delivery of messages to different recipients.
- An example of a strong reliability property is *last copy recall*, meaning that as long as at least a single copy of a message remains available at any of the recipients, every other recipient that does not fail eventually also receives a copy.
- Strong reliability properties such as this one typically require that messages are retransmitted or forwarded among the recipients.
- An example of a reliability property stronger than *last copy recall* is atomicity. The property states that if at least a single copy of a message has been delivered to a recipient, all other recipients will eventually receive a copy of the message.
- In other words, each message is always delivered to either all or none of the recipients.
- One of the most complex strong reliability properties is virtual synchrony.
- Reliable messaging is the concept of message passing across an unreliable infrastructure whilst being able to make certain guarantees about the successful transmission of the messages.
- For example, that if the message is delivered, it is delivered at most once, or that all messages successfully delivered arrive in a particular order.
- Reliable delivery can be contrasted with best-effort delivery, where there is no guarantee that messages will be delivered quickly, in order, or at all.
- Transmission Control Protocol (TCP), the main protocol used on the Internet, is a reliable unicast protocol. UDP is an unreliable protocol and is often used in computer games, streaming media or in other situations where speed is an issue and some data loss may be tolerated because of the transitory nature of the data.
- Often, a reliable unicast protocol is also connection oriented. For example, TCP is connection oriented, with the virtual-circuit ID consisting of source and destination IP addresses and port numbers.
- However, some unreliable protocols are connection oriented, such as Asynchronous Transfer Mode and Frame Relay.
- If a network does not guarantee packet delivery, then it becomes the host's responsibility to provide reliability by detecting and retransmitting lost packets.
- Subsequent experience on the ARPANET indicated that the network itself could not reliably detect all packet delivery failures, and this pushed responsibility for error detection onto the sending host in any case.
- This led to the development of the end-to-end principle, which is one of the Internet's fundamental design principles.

Video Content / Details of website for further learning (if any): **https://book.systemsapproach.org/direct/reliable.html#:~:text=Reliable%20delivery%20is%20usually%20accomplished,has%20received%20an%20earlier%20frame.**
Important Books/Journals for further learning including the page nos.: Page No:

Course Faculty

Verified by HOD

L-15

LECTURE HANDOUTS

CY **II/III**

Course Name with Code :**19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.Preetha**

Unit : **II- Data Link Layer** **Date of Lecture:**

Topic of Lecture: MAC protocols

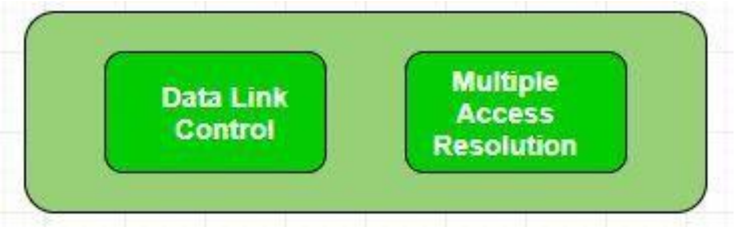
Introduction : (Maximum 5 sentences) :

- A media access control is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable.
- The essence of the MAC protocol is **to ensure non-collision and eases the transfer of data packets between two computer terminals**.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- OSI layer
- Basics Of Networking

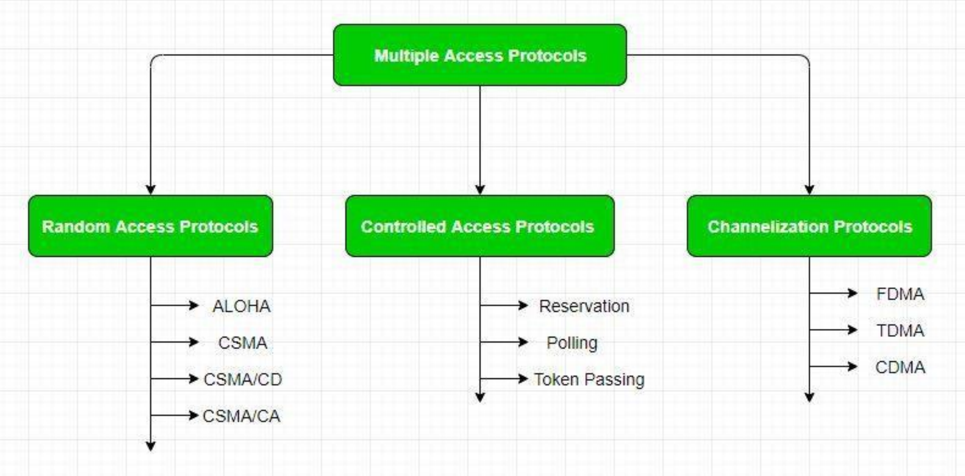
Detailed content of the Lecture:

- The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-
- Data Link Control
- 

-

- Data Link control –
  The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control.
- For Data link control refer to – Stop and Wait ARQ
- Multiple Access Control –
  If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access

protocols) to manage the students and make them answer one at a time.

- Thus, protocols are required for sharing data on non dedicated channels. Multiple access
- 

- Random Access Protocol: In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:
- There is no fixed time for sending data
- There is no fixed sequence of stations sending data
- The Random access protocols are further subdivided as:
- ALOHA – It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.
- CSMA – Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay.
- For example, if station A wants to send data, it will first sense the medium.If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.
- CSMA/CD – Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected. For more details refer – Efficiency of CSMA/CD
- CSMA/CA – Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.
- Controlled Access:
  In this, the data is sent by that station which is approved by all other stations. For further details refer – Controlled Access Protocols
- Channelization:
  In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.
- Frequency Division Multiple Access (FDMA) – The available bandwidth is divided into equal

bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.

- Time Division Multiple Access (TDMA) – In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.
  For more details refer – Circuit Switching
- Code Division Multiple Access (CDMA) – One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.

Video Content / Details of website for further learning (if any):
Multiple Access Protocols in Computer Network - GeeksforGeeks

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-16

CY

III/V

Course Name with Code :19CYC05 & COMPUTER NETWORKS

Course Faculty : Dr.J.Preetha

Unit : II- Data Link Layer **Date of Lecture:**

Topic of Lecture:MAC protocols

Introduction : (Maximum 5 sentences) :

- The MAC sublayer and the logical link control (LLC) sublayer together make up the data link layer
- Within the hierarchy of the OSI model and IEEE 802 standards, the MAC sublayer provides a control abstraction

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- OSI layer
- Basics Of Networking

Detailed content of the Lecture:

- In IEEE 802 LAN/MAN standards, the **medium access control** (**MAC**, also called **media access control**) sublayer is the layer that controls the hardware responsible for interaction with the wired, optical or wireless transmission medium.
- The MAC sublayer and the logical link control (LLC) sublayer together make up the data link layer. Within the data link layer, the LLC provides flow control and multiplexing for the logical link (i.e. EtherType, 802.1Q VLAN tag etc), while the MAC provides flow control and multiplexing for the transmission medium.
- These two sublayers together correspond to layer 2 of the OSI model. For compatibility reasons, LLC is optional for implementations of IEEE 802.3 (the frames are then "raw"), but compulsory for implementations of other IEEE 802 physical layer standards.
- Within the hierarchy of the OSI model and IEEE 802 standards, the MAC sublayer provides a control abstraction of the physical layer such that the complexities of physical link control are invisible to the LLC and upper layers of the network stack.
- Thus any LLC sublayer (and higher layers) may be used with any MAC. In turn, the medium access control block is formally connected to the PHY via a media-independent interface.
- Although the MAC block is today typically integrated with the PHY within the same device package, historically any MAC could be used with any PHY, independent of the transmission medium.
- When sending data to another device on the network, the MAC sublayer encapsulates higher-level frames into frames appropriate for the transmission medium (i.e. the MAC adds a syncword preamble and also padding if necessary), adds a frame check sequence to identify

transmission errors, and then forwards the data to the physical layer as soon as the appropriate channel access method permits it.

- For topologies with a collision domain (bus, ring, mesh, point-to-multipoint topologies), controlling when data is sent and when to wait is necessary to avoid collisions.
- Additionally, the MAC is also responsible for compensating for collisions by initiating retransmission if a jam signal is detected.
- When receiving data from the physical layer, the MAC block ensures data integrity by verifying the sender's frame check sequences, and strips off the sender's preamble and padding before passing the data up to the higher layers.
- The channel access control mechanisms provided by the MAC layer are also known as a multiple access method.
- This makes it possible for several stations connected to the same physical medium to share it. Examples of shared physical media are bus networks, ring networks, hub networks, wireless networks and half-duplex point-to-point links.
- The multiple access method may detect or avoid data packet collisions if a packet mode contention based channel access method is used, or reserve resources to establish a logical channel if a circuit-switched or channelization-based channel access method is used.
- The channel access control mechanism relies on a physical layer multiplex scheme.
- The most widespread multiple access method is the contention-based CSMA/CD used in Ethernet networks. This mechanism is only utilized within a network collision domain, for example an Ethernet bus network or a hub-based star topology network. An Ethernet network may be divided into several collision domains, interconnected by bridges and switches.
- A multiple access method is not required in a switched full-duplex network, such as today's switched Ethernet networks, but is often available in the equipment for compatibility reasons.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/classification-of-mac-protocols

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

L-17

LECTURE HANDOUTS

CY **II/III**

Course Name with Code :**19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.Preetha**

Unit : **II- Data Link Layer** **Date of Lecture:**

Topic of Lecture:CSMA/CD

Introduction : (Maximum 5 sentences) :

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a **network protocol for carrier transmission** that operates in the Medium Access Control (MAC) layer.
- On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

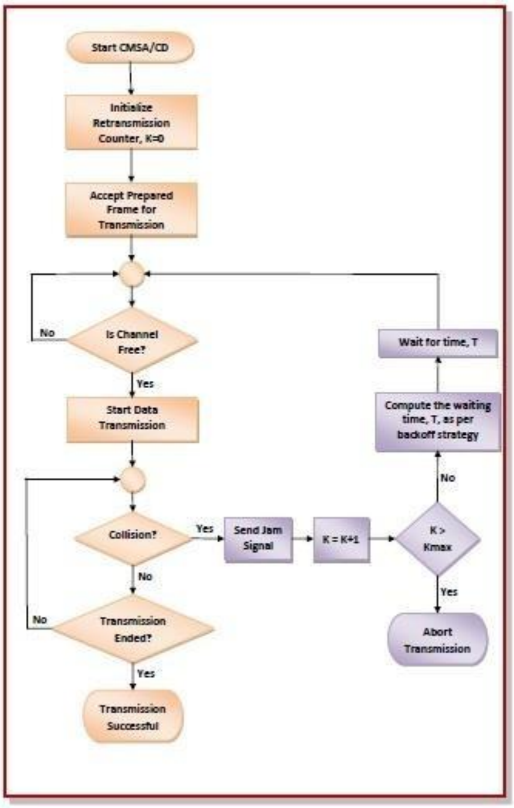
- OSI layer
- Basics Of Networking

Detailed content of the Lecture:

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer.
- It senses or listens whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free.
- The collision detection technology detects collisions by sensing transmissions from other stations.
- On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

- **Algorithms**
- The algorithm of CSMA/CD is:
- When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- If the channel is busy, the station waits until the channel becomes idle.
- If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
- If a collision is detected, the station starts the collision resolution algorithm.
- The station resets the retransmission counters and completes frame transmission.
- The algorithm of Collision Resolution is:
- The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.

- The station increments the retransmission counter.
- If the maximum number of retransmission attempts is reached, then the station aborts transmission.
- Otherwise, the station waits for a backoff period which is generally a function of the number of collisions and restart main algorithm.
- The following flowchart summarizes the algorithms:



- Though this algorithm detects collisions, it does not reduce the number of collisions.
- It is not appropriate for large networks performance degrades exponentially when more stations are added.

Video Content / Details of website for further learning (if any):
CSMA with Collision Detection (CSMA/CD) (tutorialspoint.com)

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

L-18

LECTURE HANDOUTS

CY

II/III

Course Name with Code :19CYC05 & COMPUTER NETWORKS

Course Faculty : Dr.J.Preetha

Unit : II- Data Link Layer **Date of Lecture:**

Topic of Lecture: CSMA/CA

Introduction : (Maximum 5 sentences) :

- Collision avoidance is used to improve the performance of the CSMA method by attempting to divide the collision domain.

Prerequisite knowledge for Complete understanding and learning of Topic:(Max. Four important topics)

- OSI layer
- Basics Of Networking

Detailed content of the Lecture

- Collision avoidance is used to improve the performance of the CSMA method by attempting to divide collision domain.
- Carrier Sense: prior to transmitting, a node first listens to the shared medium (such as listening for wireless transmitting or not.
- Note that the hidden node problem means another node may be transmitting which goes undetected at this node
- Collision Avoidance: if another node was heard, we wait for a period of time (usually random) for the nocommunications channel.
- Request to Send/Clear to Send (RTS/CTS) may optionally be used at this point to mediate access to the s
- This goes some way to alleviating the problem of hidden nodes because, for instance, in a wireless network time.
- However, wireless 802.11 implementations do not typically implement RTS/CTS for all transmissions; tpackets (the overhead of RTS, CTS and transmission is too great for small data transfers).
- Transmission: if the medium was identified as being clear or the node received a CTS to explicitly indicates
- Unlike CSMA/CD, it is very challenging for a wireless node to listen at the same time as it transmits (its
- Continuing the wireless example, the node awaits receipt of an acknowledgement packet from the Accesscorrectly.
- If such acknowledgement does not arrive in a timely manner, it assumes the packet collided with

some of exponential back off prior to attempting to re-transmit.

- Although CSMA/CA has been used in a variety of wired communication systems, it is particularly benefit stations being able to see the Access Point, but not each other.
- This is due to differences in transmit power, and receive sensitivity, as well as distance, and location with
- This will cause a station to not be able to 'hear' another station's broadcast. This is the so-calle 'hidden n standards can enjoy the benefits of collision avoidance (RTS / CTS handshake, also Poin coordination fu
- By default they use a Carrier sensing mechanism called 'exponential back off', or (Distribute coordination another station's broadcast before sending. CA, or PCF relies upon the AP (or th 'receiver' for Ad hoc negiven period of time after requesting it (Request to Send / Clear to Send).
- CSMA-CA requires a determination of whether a channel is 'idle', even when incompatible standard

Video Content / Details of website for further learning (if any):
https://book.systemsapproach.org/direct/reliable.html#:~:text=Reliable%20delivery%20is%20usually%

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L - 19

LECTURE HANDOUTS

CY **II/III**

Course Name with Code : 19CYC05 & COMPUTER NETWORKS

Course Teacher : Dr.J.Preetha

Unit : III – Network Layer **Date of Lecture:**

Topic of Lecture: circuit switching

Introduction:

- Circuit switching is a connection-oriented network switching technique. Here, a dedicated route is established between the source and the destination and the entire message is transferred through it.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Switching techniques
- Basics of MAC Addresses
- ARP and RARP

Detailed content of the Lecture:

Types of Switching Techniques

The different types of switching techniques

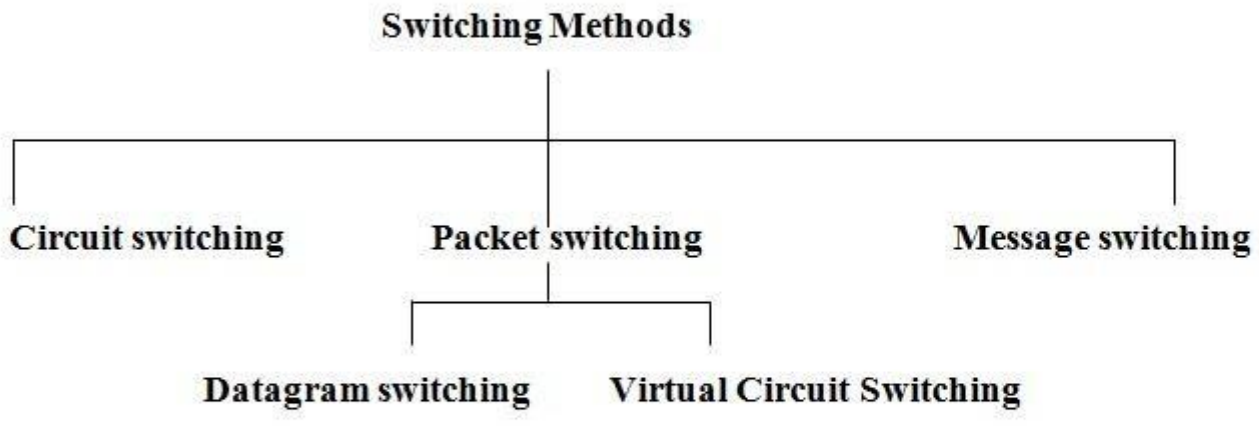


Fig- Types of switching methods

Phases of Circuit Switch Connection

Circuit Switching is a dedicated connection path between the sending and receiving devices. The dedicated route is a connected series of connections between the switching nodes.

A traditional mobile network, where a dedicated route is established between the caller and the called party for the span of a mobile call, is termed as circuit switching.

Circuit Establishment

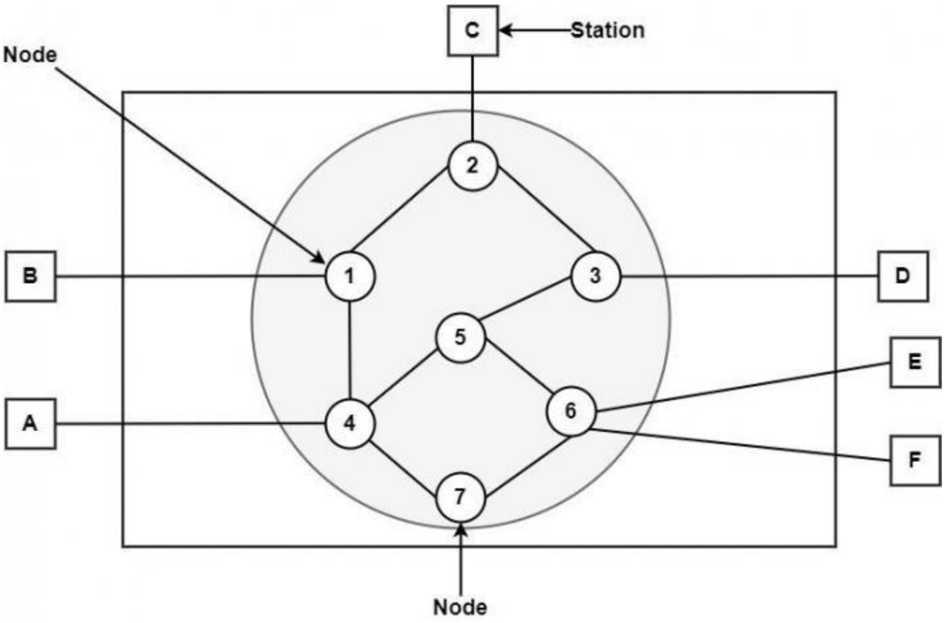
A circuit switching network is necessary to establish an end-to-end link before any signal is transmitted. For example, if the communication is between A and D, then the path from A to node 4 to node 5 to node 3 and D must be established first.

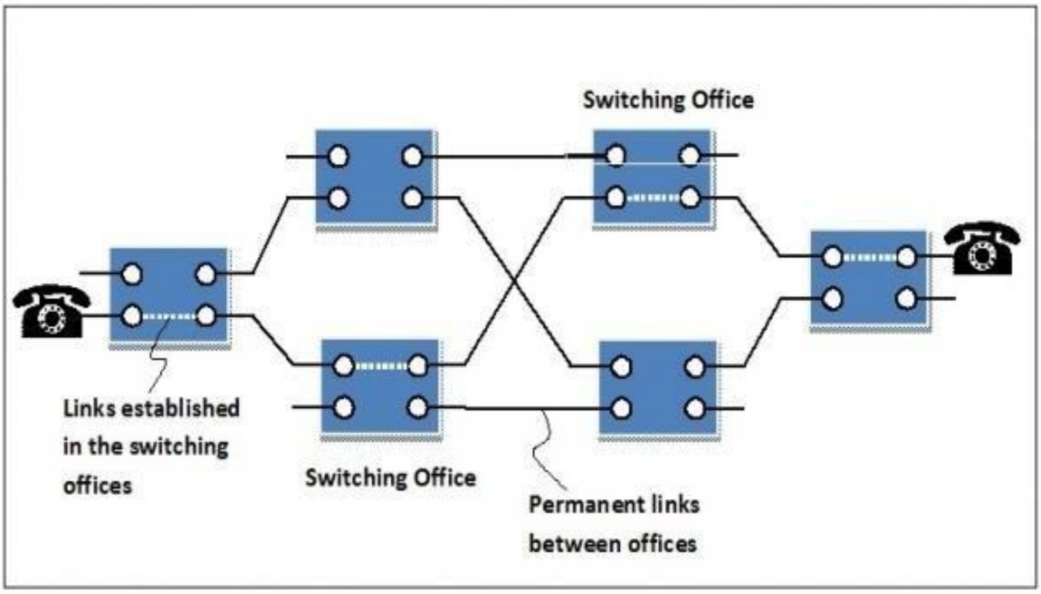
Data Transfer

Once a circuit is established between the two stations, it is exclusively used by the two parties. The information can be transferred from A to D through the network. The data can be analog or digital, relying on the features of the network.

Circuit Disconnect

After the transfer of complete data, the connection is terminated either by the sender or receiver.




Switching Office
Links established in the switching offices
Switching Office
Permanent links between offices

- **Circuit Establishment** : In this phase, a dedicated circuit is established from the source to the destination through a number of intermediate switching centres. The sender and receiver transmits communication signals to request and acknowledge establishment of circuits.
- **Data Transfer** : Once the circuit has been established, data and voice are transferred from the source to the destination. The dedicated connection remains as long as the end parties communicate.
- **Circuit Disconnection** : When data transfer is complete, the connection is relinquished. The disconnection is initiated by any one of the user. Disconnection involves removal of all

intermediate links from the sender to the receiver.

Advantages

The advantages of circuit switching are as follows −

- During the circuit is settled, data is communicated with no delay.
- The approach is feasible for high infinite communication, because a dedicated endless communication route is settled.
- The approach is easy and does not require specific facilities.

Disadvantages

The disadvantages of circuit switching are as follows

- The time needed to settle a physical connection between the two stations is considerable.
- The network resources are not adequately utilised, because the physical connection is a dedicated one.
- It is an uneconomical method.

Video Content / Details of website for further learning (if any):
https://en.wikipedia.org/wiki/Circuit_switching

Important Books/Journals for further learning including the page nos.:

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

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

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L - 20

LECTURE HANDOUTS

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Teacher : **Dr.J.Preetha**

Unit : **III – Network Layer** **Date of Lecture:**

Topic of Lecture: packet switching

Introduction:

- Packet switching is a connectionless network switching technique. Here, the message is divided and grouped into a number of units called packets that are individually routed from the source to the destination. There is no need to establish a dedicated circuit for communication.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Logical Addressing
- Physical Addressing
- Basics of MAC Addresses

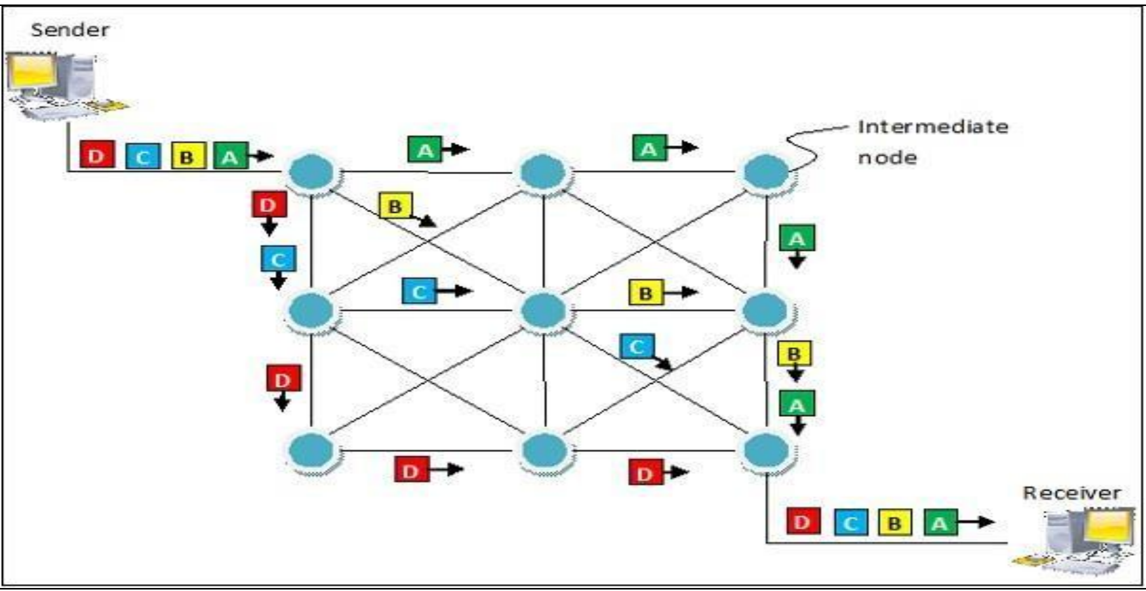
Detailed content of the Lecture:

Process:

Each packet in a packet switching technique has two parts: a header and a payload. The header contains the addressing information of the packet and is used by the intermediate routers to direct it towards its destination. The payload carries the actual data.

A packet is transmitted as soon as it is available in a node, based upon its header information. The packets of a message are not routed via the same path. So, the packets in the message arrive in the destination out of order. It is the responsibility of the destination to reorder the packets in order to retrieve the original message.

In telecommunications, store − and − forward packet switching is a technique where the data packets are stored in each intermediate node, before they are forwarded to the next node. The intermediate node checks whether the packet is error−free before transmitting, thus ensuring integrity of the data packets. In general, the network layer operates in an environment that uses store and forward packet switching.



Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/difference-between-arp-and-rarp/
https://www.geeksforgeeks.org/arp-reverse-arprarp-inverse-arp-inarp-proxy-arp-and-gratuitous-arp/

Important Books/Journals for further learning including the page nos.:
William Stallings, “Data and Computer Communications”, Pearson Education, 2013.Page No: 612

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

L - 21

LECTURE HANDOUTS

CY **II/IV**

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Teacher : **Dr.J.Preetha**

Unit : **III – Network Layer** **Date of Lecture:**

Topic of Lecture: Bridges and LAN Switches: Spanning Tree algorithm

Introduction:

- A bridge is **a network device that connects multiple LANs (local area networks) together to form a larger LAN**. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Logical Addressing
- Physical Addressing
- Basics of MAC Addresses

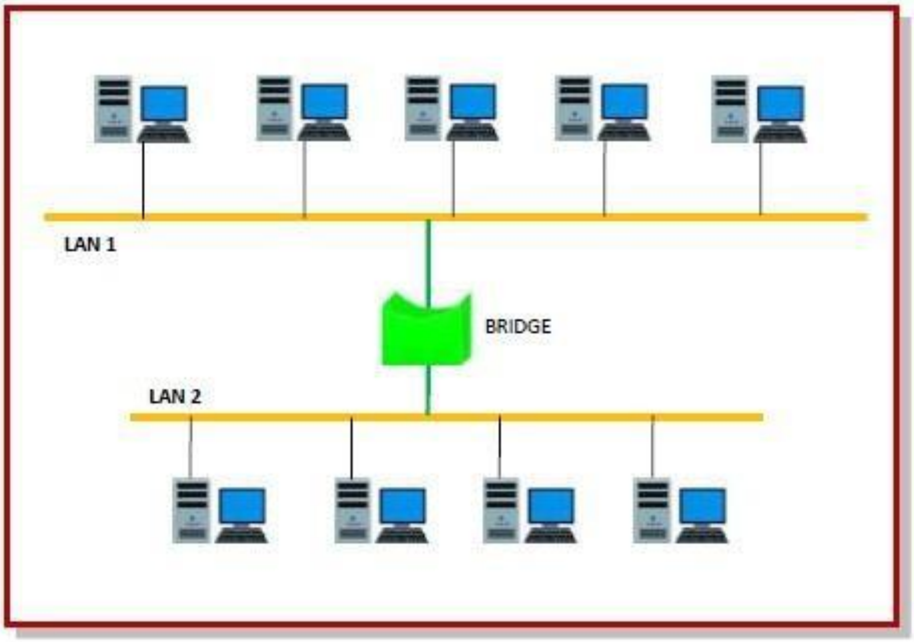
Detailed content of the Lecture:

Process:

Uses of Bridge

- Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them.
- By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
- Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.
    - If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it.
    - If the frame has a destination MAC address in a connected network, it will forward the frame toward it.
- By deciding whether to forward or discard a frame, it prevents a single faulty node from bringing down the entire network.
- In cases where the destination MAC address is not available, bridges can broadcast data frames to each node. To discover new segments, they maintain the MAC address table.
- In order to provide full functional support, bridges ideally need to be transparent. No major hardware, software or architectural changes should be required for their installation.
- Bridges can switch any kind of packets, be it IP packets or AppleTalk packets, from the network layer above. This is because bridges do not examine the payload field of the data frame that arrives, but simply looks at the MAC address for switching.
- Bridges also connect virtual LANs (VLANs) to make a larger VLAN.

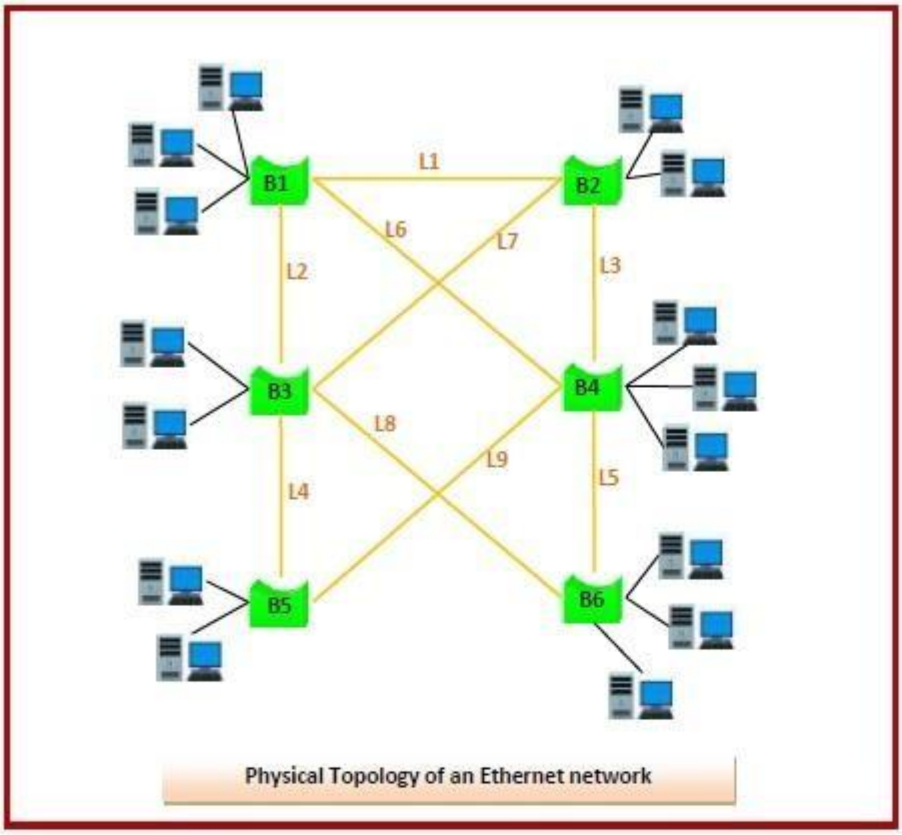
- A wireless bridge is used to connect wireless networks or networks having a wireless segment.



Spanning tree bridges.

To construct a spanning tree, the bridges broadcast their configuration routes. Then they execute a distributed algorithm for finding out the minimal spanning tree in the network, i.e. the spanning tree with minimal cost. The links not included in this tree are disabled but not removed.

In case a particular active link fails, the algorithm is executed again to find the minimal spanning tree without the failed link. The communication continues through the newly formed spanning tree. When a failed link is restored, the algorithm is re-run including the newly restored link.



Let us consider a physical topology, as shown in the diagram, for an Ethernet network that comprises of six interconnected bridges. The bridges are named {B1, B2, B3, B4, B5, B6} and several nodes are connected to each bridge. The links between two bridges are named {L1, L2, L3, L4, L5, L6, L7, L8, L9}, where L1 connects B1 and B2, L2 connects B1 and B3 and so on. It is assumed that all links are of uniform costs.

From the diagram we can see that there are multiple paths from a bridge to any other bridge in the network, forming several bridge loops that makes the topology susceptible to broadcast storms.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/spanning-tree-protocol

Important Books/Journals for further learning including the page nos.:

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L - 22

LECTURE HANDOUTS

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Teacher : **Dr.J.Preetha**

Unit : **III – Network Layer** **Date of Lecture:**

Topic of Lecture: Internetworking IPv4 Addresses

Introduction:

- An IP address is used globally to refer to the logical address in the network layer of the TCP/IP protocol.
- The Internet addresses are 32 bits in length; this gives us a maximum of $\mathbf{2^{32}}$ addresses.
- These addresses are referred to as IPv4 (IP version 4) addresses or popularly as IP addresses.

Prerequisite knowledge for Complete understanding and learning of Topic:

- TCP/ IP Internet Suite
- Network layer responsibilities
- Number system- Basics

Detailed content of the Lecture:

Logical Addressing:

- A logical Address is also called as IP Address is a 32- bit address assigned to each system in a network
- This works in Layer-3 of OSI Model
- This would be generally the IP Address

IPv4 Addresses

- The identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address.
- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.
- The IP address is the address of the connection, not the host or the router.

Address Space

- A protocol like IPv4 that defines addresses has an address space.
- An address space is the total number of addresses used by the protocol.
- If a protocol uses b bits to define an address, the address space is 2 b because each bit can have two different values (0 or 1).
- IPv4 uses 32-bit addresses, which means that the address space is 2 32 or 4,294,967,296 (more than four billion).
- If there were no restrictions, more than 4 billion devices could be connected to the Internet.

IPv4 supports three different types of addressing modes:

Unicast Addressing Mode

- In this mode, data is sent only to one destined host.
- The Destination Address field contains 32- bit IP address of the destination host.
- Here the client sends data to the targeted server.

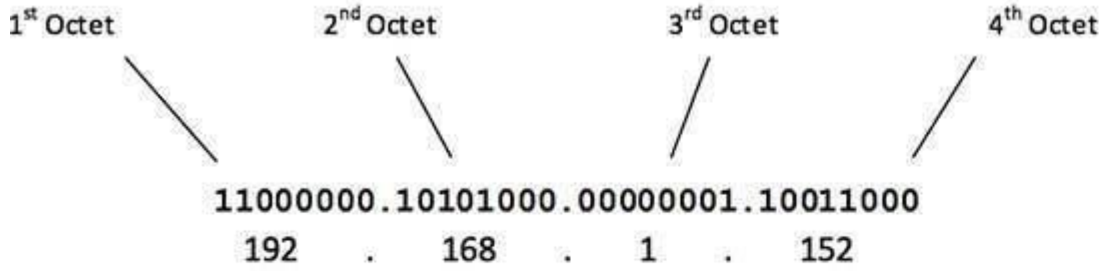
Broadcast Addressing Mode

- In this mode, the packet is addressed to all the hosts in a network segment.
- The Destination Address field contains a special broadcast address, i.e. **255.255.255.255**.
- When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the Servers.

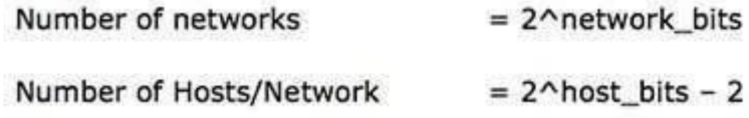
Multicast Addressing Mode

- This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host nor all the hosts on the segment.
- In this packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address:



The number of networks and the number of hosts per class can be derived by this formula,


Number of networks = 2^network_bits

Number of Hosts/Network = 2^host_bits – 2

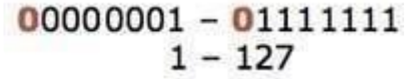
When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Classful Addressing

- When the Internet started, an IPv4 address was designed with a fixed-length prefix, but to accommodate both small and large networks, three fixed-length prefixes were designed instead of one (n = 8, n = 16, and n = 24).
- The whole address space was divided into five classes (class A, B, C, D, and E).
- This scheme is referred to as classful addressing.

Class A Address

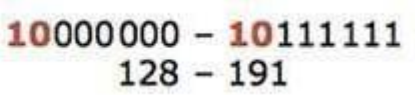
- The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.


00000001 – 01111111
1 – 127

- Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.
- The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).
- Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address

- An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

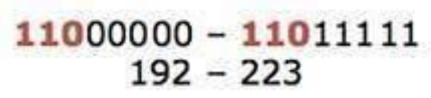


10000000 - 10111111
128 - 191

- Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.
- Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.
- Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Class C Address

- The first octet of Class C IP address has its first 3 bits set to 110, that is −

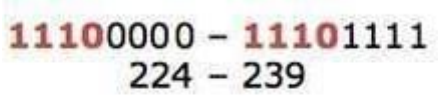


11000000 - 11011111
192 - 223

- Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.
- Class C gives 2097152 (2^{21}) Network addresses and 254 (2^{8}-2) Host addresses.
- Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

Class D Address

- Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of



11100000 - 11101111
224 - 239

- Class D has IP address range from 224.0.0.0 to 239.255.255.255.
- Class D is reserved for Multicasting.
- In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

- This IP Class is reserved for experimental purposes only for R&D or Study.
- IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254.
- Like Class D, this class too is not equipped with any subnet mask.

Slash Notation

- Slash notation is a compact way to show or write an IPv4 subnet mask.
- When you use slash notation, you write the IP address, a forward slash (/), and the subnet mask number. To find the subnet mask number: Convert the decimal representation of the subnet mask to a binary representation.

Video Content / Details of website for further learning (if any):

https://www.youtube.com/watch?v=crrdZx6u6MQ
https://www.youtube.com/watch?v=U7-h2hyM1Dc

Important Books/Journals for further learning including the page nos.:

William Stallings, “Data and Computer Communications”, Pearson Education, 2013.Page No: 549

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L-23

LECTURE HANDOUTS

CY **II/III**

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Teacher : **Dr.J.Preetha**

Unit : **III – Network Layer** **Date of Lecture:**

Topic of Lecture: Subnetting

Introduction:

- **Subnetting** is a process of dividing a single large **network** in multiple smaller **networks**.
- In computer networking, Subnetting is used to divide a large IP network in smaller IP networks known as subnets.

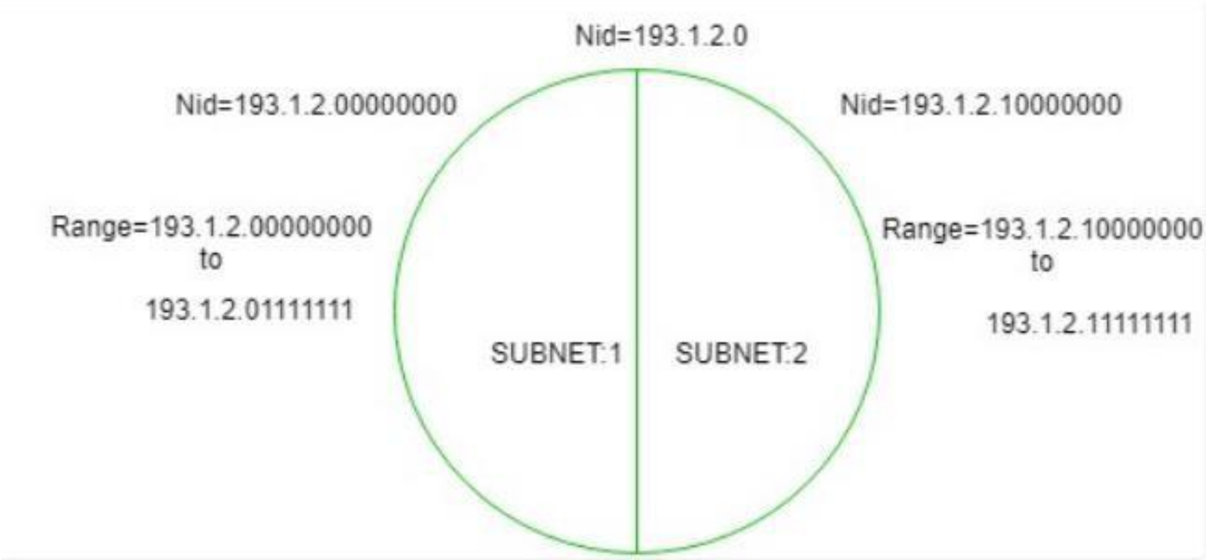
Prerequisite knowledge for Complete understanding and learning of Topic:

- IP Addressing concepts
- Network layer functionalities
- Number system- Basics

Detailed content of the Lecture:

Subnetting

- **Subnetting** is a process of dividing a single large **network** in multiple smaller **networks**.
- In computer networking, Subnetting is used to divide a large IP network in smaller IP networks known as subnets.
- When a bigger network is divided into smaller networks, in order to maintain security, then that is known as Subnetting. so, maintenance is easier for smaller networks.
- So to divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



- In the above diagram, there are two Subnets.

For Subnet-1:

- The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part.
  Thus, the range of subnet-1:

  193.1.2.0 to 193.1.2.127

For Subnet-2:

- The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1's in the host ID part i.e, 193.1.2.11111111).
  Thus, the range of subnet-2:

  193.1.2.128 to 193.1.2.255

1. To divide a network into four (2^2) parts you need to choose two bits from host id part for each subnet i.e, (00, 01, 10, 11).
2. To divide a network into eight (2^3) parts you need to choose three bits from host id part for each subnet i.e, (000, 001, 010, 011, 100, 101, 110, 111) and so on.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/introduction-to-subnetting/
http://ecomputernotes.com/computernetworkingnotes/naming-and-addressing/what-is-subnetting

Important Books/Journals for further learning including the page nos.:
William Stallings, "Data and Computer Communications", Pearson Education, 2013.Page No: 552

Course Teacher

Verified by HOD

L-24

LECTURE HANDOUTS

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Teacher : **Dr.J.Preetha**

Unit : **III – Network Layer** **Date of Lecture:**

Topic of Lecture: CIDR

Introduction:

- A default class A, B and C network provides 16777214, 65534, 254 hosts respectively
- Classless inter-domain routing (**CIDR**) is a set of Internet protocol (IP) standards that is used to create unique identifiers for networks and individual devices.

Prerequisite knowledge for Complete understanding and learning of Topic:

- IP Addressing concepts
- Network layer functionalities
- Number system- Basics

Detailed content of the Lecture:

CIDR

- Classless Inter Domain Routing
- If a network grows to more than 255 hosts, it may want a Class B address.
- One possible way of avoiding is to handle many Class C routing addresses -- but then, for this one network, each router has to maintain multiple routing entries.
- CIDR is an attempt to balance the desire to minimize the number of routes that a router needs to know versus the need to hand out addresses efficiently.
- CIDR enables aggregation of routes , thereby a single entry is used to reach multiple networks.

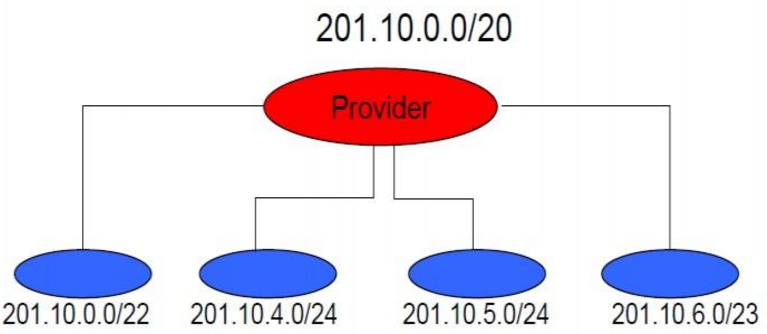
Subnets vs CIDR

- The concept is similar but:
  - In a subnet, a single address is shared among multiple physical networks.
  - With CIDR, we collapse multiple network addresses into a longer network address that is typically assigned to an AS (the single AS would have a network number or prefix that reflects the block of addresses).
- Thus, when we want to route to “any” of the networks or even subnets within the AS, we route to the AS.

Route Aggregation

- Specifying simply the prefix associated with an AS (as opposed to stating the subnet number explicitly) is called route aggregation.
- When sending route advertisements (we will see how), it suffices to simply advertise “common prefixes”.
- Note that for this, careful planning would be needed.

CIDR Address Assignment



Example

- Consider an autonomous system (AS) with 16 class C networks. Instead of handling providing 16 addresses at random, a block of contiguous class C address is given.
- For example, from 192.4.16 to 192.4.31 A bitwise analysis shows that 20 MSBs (11000000 00000100 0001) are the same for that block, i.e., a 20-bit network id.
- This 20-bit network number can support hosts that range between class B and C (mid-sized blocks)

Restrictions

1. The addresses in a block must be contiguous, one after another.
2. The number of addresses in a block must be a power of 2.
3. The first address must be evenly divisible by the number of addresses.

Notation

- The term classless in CIDR implies that a network number may be of any length, not fixed as in classful addressing.
- It is represented of the form x.y.z.t/n where x.y.z.t is any address in the block and n can take values in the range 0–32.
- The first address in the block can be found by setting 32 - n right-most bits in the binary notation of the address to 0s. The last address in the block can be found by setting 32 - n right-most bits in the binary notation of the address to 1s.
- The number of addresses in the block can be found by computing 232 - n
- The first address in a block is used as the network address that represents the organization to the rest of the world.
- The following figure shows aggregation of routes to two corporations connected to a provider using BGP protocol.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/classless-inter-domain-routing-cidr/

Important Books/Journals for further learning including the page nos.:
William Stallings, "Data and Computer Communications", Pearson Education, 2013.Page No: 552

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

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

Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L-25

LECTURE HANDOUTS

CY **II/III**

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Teacher : **Dr.J.Preetha**

Unit : **III – Network Layer** **Date of Lecture:**

Topic of Lecture: IPV6 Addresses

Introduction:

- An IPv6 address consists of 16 bytes (octets); it is 128 bits long. An IPv6 address is 128 bits long. IP v6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IP v4 exhaustion.
- IP v6 is 128-bits address having an address space of 2^128, which is way bigger than IPv4.

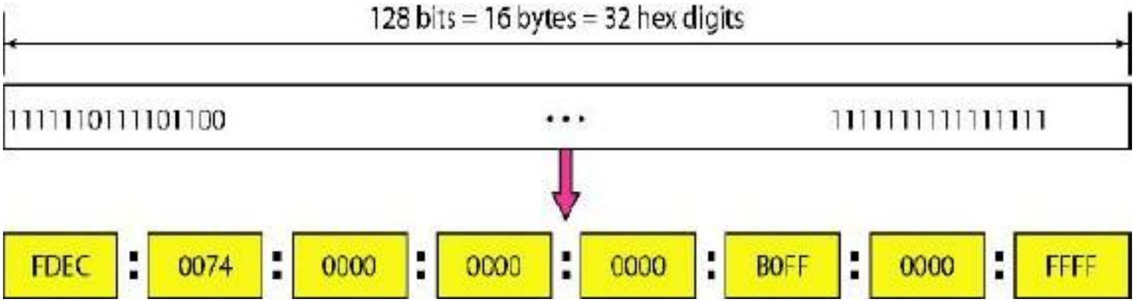
Prerequisite knowledge for Complete understanding and learning of Topic:

- Information and commands exchanged across adjacent layers
- Primitives (functions to be performed)
  - Send -Request transmission of data unit
  - Deliver -Notify user of arrival of data unit
  - Parameters – Used to pass data and control info

Detailed content of the Lecture:

Hexadecimal Colon Notation :

- To make addresses more readable, IPv6 specifies hexadecimal colon notation. In this notation, 128 bits is divided into eight sections, each 2 bytes in length.
- Two bytes in hexadecimal notation requires four hexadecimal digits. Therefore, the address consists of 32 hexadecimal digits, with every four digits separated by a colon.



Abbreviation

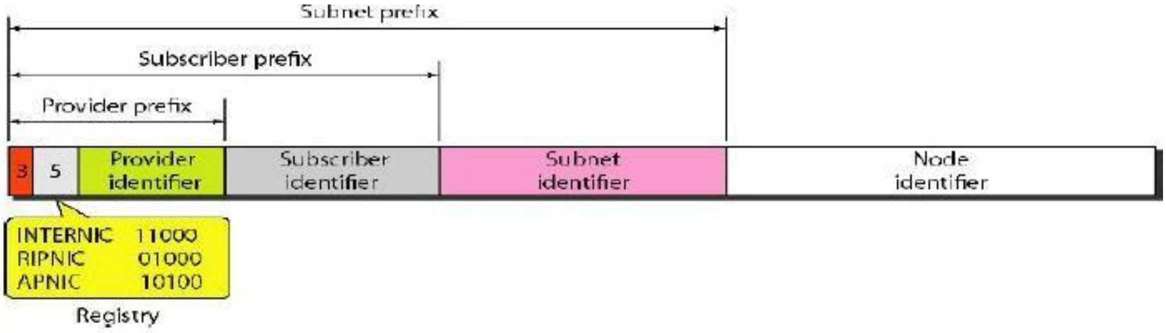
- Although the IP address, even in hexadecimal format, is very long, many of the digits are zeros. In this case, we can abbreviate the address. The leading zeros of a section (four digits between two colons) can be omitted. Only the leading zeros can be dropped, not the trailing zeros.
- Using this form of abbreviation, 0074 can be written as 74, 000F as F, and 0000 as 0.

Address Space

- IPv6 has a much larger address space; 2128 addresses are available. The designers of IPv6 divided the address into several categories. A few leftmost bits, called the type prefix, in each address define its category. The type prefix is variable in length, but it is designed such that no code is identical to the first part of any other code. In this way, there is no ambiguity; when an address is given, the type prefix can easily be determined.

Unicast Addresses

- A **unicast address** defines a single computer. The packet sent to a unicast address must be delivered to that specific computer. IPv6 defines two types of unicast addresses: geographically based and provider-based. We discuss the second type here; the first type is left for future definition. The provider-based address is generally used by a normal host as a unicast address.



Multicast Addresses

- Multicast addresses are used to define a group of hosts instead of just one. A packet sent to a multicast address must be delivered to each member of the group.

All cast Addresses

- IPv6 also defines anycast addresses. An anycast address, like a multicast address, also defines a group of nodes. However, a packet destined for an anycast address is delivered to only one of the members of the anycast group, the nearest one (the one with the shortest route).

Reserved Addresses

- Another category in the address space is the reserved address. These addresses start with eight Os (type prefix is 00000000). A few subcategories are defined in this categor. An unspecified address is used when a host does not know its own address and sends an inquiry to find its address. A loopback address is used by a host to test itself without going into the network. A compatible address is used during the transition from IPv4 to IPv6.

Local Addresses

- These addresses are used when an organization wants to use IPv6 protocol without being connected to the global Internet. In other words, they provide addressing for private networks. Nobody outside the organization can send a message to the nodes using these addresses. Two types of addresses are defined for this purpose.

Video Content / Details of website for further learning (if any):
https://www.youtube.com/watch?v=HCTl3UJ9FlE

Important Books/Journals for further learning including the page nos.:
William Stallings, “Data and Computer Communications”, Pearson Education, 2013.Page No: 566

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

L-26

LECTURE HANDOUTS

CY **II/III**

Course Name with Code : 19CYC05 & COMPUTER NETWORKS

Course Teacher : Dr.J.Preetha

Unit : III – Network Layer **Date of Lecture:**

Topic of Lecture: Routing Technics Distance Vector(Rip)

Introduction:

- Internetworking is the process or technique of connecting different networks by using intermediary devices such as routers or gateway devices.
- The interconnected computer networks or Internetworking use the Internet Protocol. Two architectural models are commonly used to describe the protocols and methods used in internetworking.
- The standard reference model for internetworking is Open Systems Interconnection (OSI).

Prerequisite knowledge for Complete understanding and learning of Topic:

- Client and Server Communication
- Routing
- Network Configuration

Detailed content of the Lecture:

Internetworking:

- Internetworking is combined of 2 words, inter and networking which implies an association between totally different nodes or segments. This connection area unit is established through intercessor devices akin to routers or gateway.
- The first term for associate degree internetwork was catenet. This interconnection is often among or between public, private, commercial, industrial, or governmental networks.
- Thus, associate degree internetwork could be an assortment of individual networks, connected by intermediate networking devices, that functions as one giant network. Internetworking refers to the trade, products, and procedures that meet the challenge of making and administering internetworks.
- To enable communication, every individual network node or phase is designed with similar protocol or communication logic, that is Transfer Control Protocol (TCP) or Internet Protocol (IP). Once a network communicates with another network having constant communication procedures, it’s called Internetworking.
- Internetworking was designed to resolve the matter of delivering a packet of information through many links.
- There a minute difference between extending the network and Internetworking. Merely exploitation of either a switch or a hub to attach 2 local area networks is an extension of LAN whereas connecting them via the router is associate degree example of Internetworking.
- Internetworking is enforced in Layer three (Network Layer) of OSI-ISO model. The foremost notable example of internetworking is that the Internet.

There are chiefly 3 unit of Internetworking:

1. Extranet
2. Intranet
3. Internet

Internetwork Addressing:

- Internetwork addresses establish devices severally or as members of a bunch. Addressing schemes differ based on the protocol family and therefore the OSI layer.

- Three kinds of internetwork addresses area unit ordinarily used: data-link layer addresses, Media Access control (MAC) addresses, and network-layer addresses.

1. **Data Link Layer addresses:** A data-link layer address unambiguously identifies every physical network association of a network device. Data-link addresses typically area unit cited as physical or hardware addresses. Data-link addresses sometimes exist among a flat address area and have a pre- established and usually fastened relationship to a selected device. End systems usually have just one physical network association, and therefore have just one data-link address. Routers and different internetworking devices usually have multiple physical network connections and so eventually have multiple data-link addresses.
2. **MAC Addresses:** Media Access management (MAC) addresses encompass a set of data-link layer addresses. MAC addresses establish network entities in LANs that implement the IEEE MAC addresses of the data-link layer. MAC addresses different area unit distinctively for every local area network interface. MAC addresses are forty-eight bits long and are expressed in form of twelve hexadecimal digits. The primary half dozen hexadecimal digits, that are usually administered by the IEEE, establish the manufacturer or merchant and therefore comprise the Organizational Unique Identifier (OUI). The last half dozen positional notation digits comprise the interface serial variety or another price administered by the particular merchant. MAC addresses typically area unit referred to as burned-in addresses (BIAs) as a result of burned into read-only memory(ROM) and are traced into random-access memory (RAM) once the interface card initializes.
3. **Network-Layer Addresses:** Network addresses sometimes exist among a gradable address area and typically area unit referred to as virtual or logical addresses. the connection between a network address and a tool is logical and unfixed, it usually relies either on physical network characteristics or on groupings that don’t have any physical basis. finish systems need one network-layer address for every network-layer protocol they support. Routers and different Internetworking devices need one network-layer address per physical network association for every network-layer protocol supported.

Video Content / Details of website for further learning (if any):

https://www.geeksforgeeks.org/introduction-of-internetworking/

Important Books/Journals for further learning including the page nos.:

William Stallings, “Data and Computer Communications”, Pearson Education, 2013.Page No: 582

Course Teacher

Verified by HOD

L-27

LECTURE HANDOUTS

CY **II/III**

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Teacher : **Dr.J.Preetha**

Unit : **III – Network Layer** **Date of Lecture:**

Topic of Lecture: Link state (OSPF)

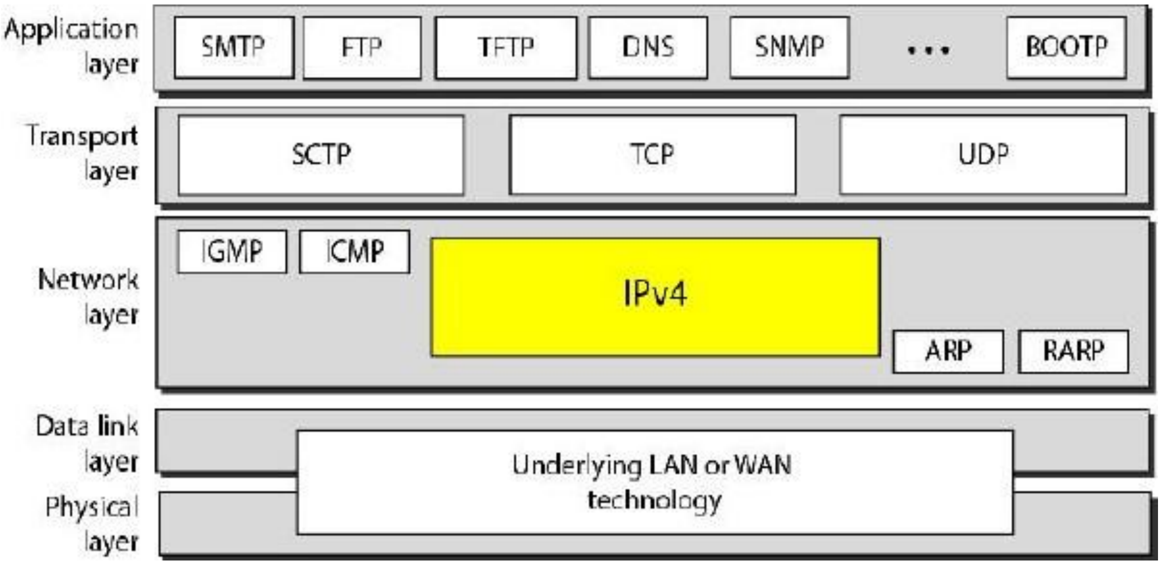
Introduction:

- The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols.
- IPv4 is an unreliable and connectionless datagram protocol-a best-effort delivery service.
- The term best-effort means that IPv4 provides no error control or flow control (except for error detection on the header). IPv4 assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

Prerequisite knowledge for Complete understanding and learning of Topic:

- IP Addressing
- Basics of MAC Addresses

Detailed content of the Lecture:

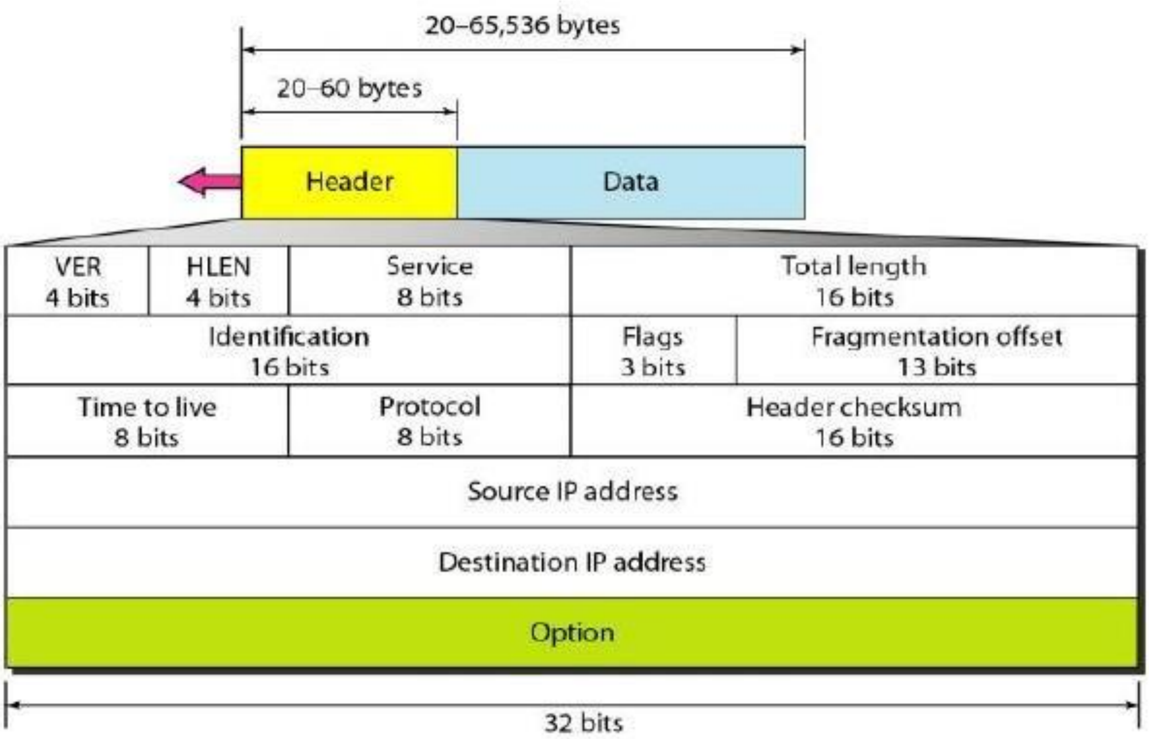


Datagram

- Packets in the IPv4 layer are called datagrams. A datagram is a variable-length packet consisting of two parts: header and data. The header is 20 to 60 bytes in length and contains information essential to routing and delivery. It is customary in TCP/IP to show the header in 4-byte sections.

Version (VER):

- This 4-bit field defines the version of the IPv4 protocol. Currently the version is 4. However, version 6 (or IPv6) may totally replace version 4 in the future. This field tells the IPv4 software running in the processing machine that the datagram has the format of version 4. All fields must be interpreted as specified in the fourth version of the protocol.



Header length (HLEN):

- This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes). When there are no options, the header length is 20 bytes, and the value of this field is 5 (5 x 4 = 20). When the option field is at its maximum size, the value of this field is 15 (15 x 4 = 60).

Services:

- IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.

1. Service Type

- In this interpretation, the first 3 bits are called precedence bits. The next 4 bits are called type of service (TOS) bits, and the last bit is not used.
- **Precedence** is a 3-bit subfield ranging from 0 (000 in binary) to 7 (111 in binary). The precedence defines the priority of the datagram in issues such as congestion.
- **TOS bits** are a 4-bit subfield with each bit having a special meaning. Although a bit can be either 0 or 1, one and only one of the bits can have the value of 1 in each datagram.

2. Differentiated Services

- In this interpretation, the first 6 bits make up the code point subfield, and the last 2 bits are not used. The code point subfield can be used in two different ways.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/ipv4/ipv4_quick_guide.htm

Important Books/Journals for further learning including the page nos.:
William Stallings, “Data and Computer Communications”, Pearson Education, 2013.Page No: 546

Course Teacher

Verified by HOD

L-28

LECTURE HANDOUTS

CY

II/III

Course Name with Code	:	**19CYC05 & COMPUTER NETWORKS**
Course Teacher	:	**Dr.J.Preetha**
Unit	:	**III – Network Layer** **Date of Lecture:**

Topic of Lecture: Inter-domain Routing (BGP)

Introduction:

- With the number of IPv4 addresses almost completely depleted, the implementation of IPv6 has become a priority for many organizations.
- However, it is not all that feasible to just switch everything over to IPv6 without some type of transition.

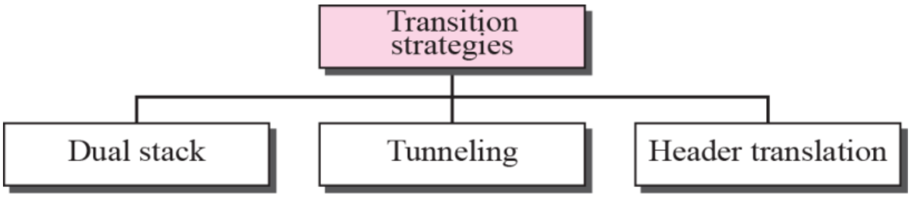
Prerequisite knowledge for Complete understanding and learning of Topic:

- IP Addressing concepts (IPv4 & IPv6)
- Router
- Networking

Detailed content of the Lecture:

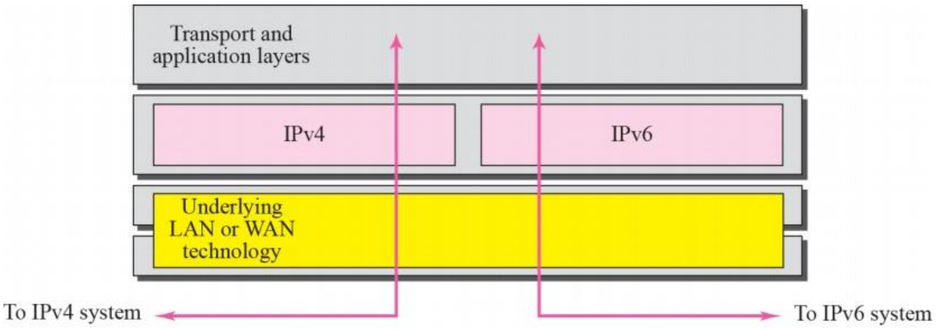
Transition from IPv4 to IPv6

- The transition must be smooth to prevent any problems between IPv4 and IPv6 systems.
- When we want to send a request from an IPv4 address to an IPv6 address but it isn’t possible because IPv4 and IPv6 transition is not compatible.



Dual stack

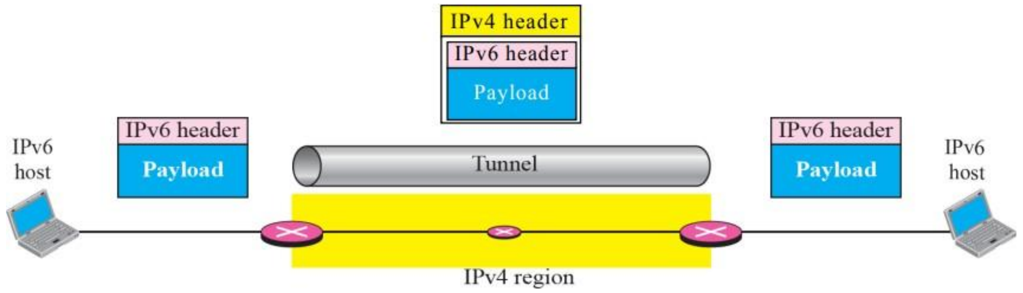
- In dual stack, a router’s interface is attached with IPv4 and IPv6 addresses configured is used in order to transition from IPv4 to IPv6.


Transport and application layers
IPv4
IPv6
Underlying LAN or WAN technology
To IPv4 system
To IPv6 system

- In this above diagram, A given server with both IPv4 and IPv6 address configured can communicate with all hosts of IPv4 and IPv6 via dual stack router (DSR).
- The dual stack router (DSR) gives the path for all the hosts to communicate with server without changing their IP addresses.

Tunneling

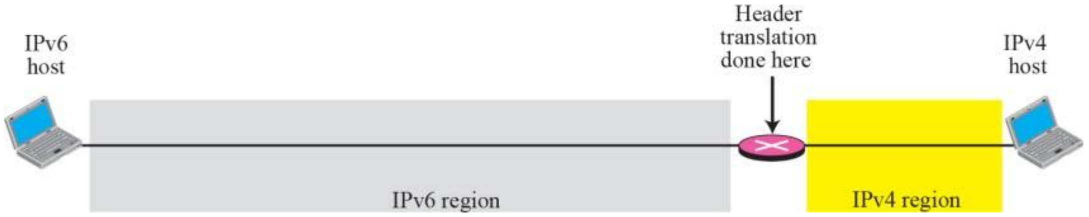
- Tunneling is used as a medium to communicate the transit network with the different ip versions.



- In this above diagram, the different IP versions such as IPv4 and IPv6 are present.
- The IPv4 networks can communicate with the transit or intermediate network on IPv6 with the help of Tunnel.
- It also possible that the IPv6 network can also communicate with IPv4 networks with the help of Tunnel.

Header translation strategy

- A translation method provides a way to translate IPv6 to IPv4 traffic and vice versa.
- When using translation, the traffic is not encapsulated but is converted to the destination type (be that IPv4 or IPv6).



NAT Protocol Translation:

- By the help of NAT Protocol Translation technique, the IPv4 and IPv6 networks can also communicate with each other which do not understand the address of different IP version.
- Generally, an IP version doesn't understand the address of different IP version, for the solution of this problem we use NAT-PT device which remove the header of first (sender) IP version address and add the second (receiver) IP version address so that the Receiver IP version address understand that the request is send by the same IP version, and its vice-versa is also possible.

Video Content / Details of website for further learning (if any):

https://www.petri.com/ipv6-transition

https://www.geeksforgeeks.org/transition-from-ipv4-to-ipv6-address/

Important Books/Journals for further learning including the page nos.:

William Stallings, “Data and Computer Communications”, Pearson Education, 2013.Page No: 603

Course Teacher

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

DESIGNING YOUR FUTURE
Estd. 2000

IQAC

LECTURE HANDOUTS

L-29

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **IV - Transport Layer** **Date of Lecture:**

Topic of Lecture: UDP

Introduction : (Maximum 5 sentences) :

- The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite.
- It involves minimum amount of communication mechanism.
- UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

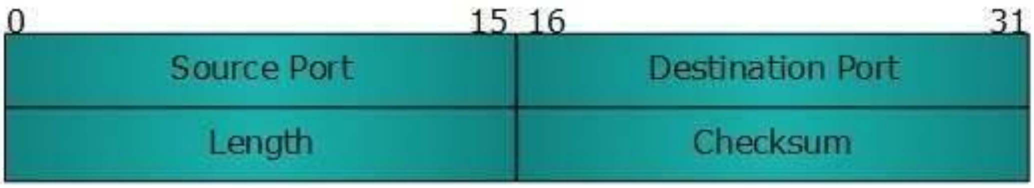
- Domain Name System (DNS),
- Simple Network Management Protocol (SNMP),
- Routing Information Protocol (RIP)
- Dynamic Host Configuration Protocol (DHCP).

Detailed content of the Lecture:

- UDP is used when acknowledgement of data does not hold any significance.
- UDP is good protocol for data flowing in one direction.
- UDP is simple and suitable for query based communications.
- UDP is not connection oriented.
- UDP does not provide congestion control mechanism.
- UDP does not guarantee ordered delivery of data.
- UDP is stateless.
- UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.

UDP Header

UDP header is as simple as its function.



0 15	16 31
Source Port	Destination Port
Length	Checksum

UDP header contains four main parameters:

- **Source Port** - This 16 bits information is used to identify the source port of the packet.
- **Destination Port** - This 16 bits information, is used identify application level service on destination machine.
- **Length** - Length field specifies the entire length of UDP packet (including header). It is 16-bits field and minimum value is 8-byte, i.e. the size of UDP header itself.
- **Checksum** - This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional so when checksum field does not contain any value it is made 0 and all its bits are set to zero.

UDP application

Here are few applications where UDP is used to transmit data:

- Domain Name Services
- Simple Network Management Protocol
- Trivial File Transfer Protocol
- Routing Information Protocol
- Kerberos

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/user-datagram-protocol-udp/

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-30

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **IV - Transport Layer** **Date of Lecture:**

Topic of Lecture: TCP

Introduction : (Maximum 5 sentences) :

- TCP stands for Transmission Control Protocol.
- It is a transport layer protocol that facilitates the transmission of packets from source to destination.
- It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

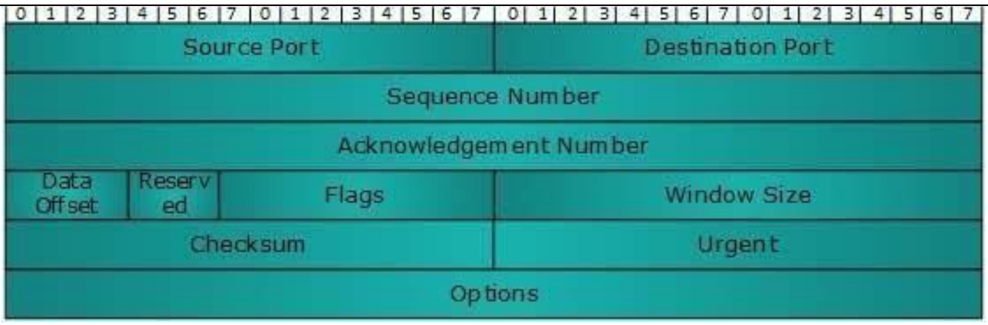
- Domain Name System (DNS),
- Simple Network Management Protocol (SNMP),
- Routing Information Protocol (RIP)

Detailed content of the Lecture:

- TCP is reliable protocol. That is, the receiver always sends either positive or negative acknowledgement about the data packet to the sender, so that the sender always has bright clue about whether the data packet is reached the destination or it needs to resend it.
- TCP ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented. TCP requires that connection between two remote points be established before sending actual data.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control and quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex server, i.e. it can perform roles of both receiver and sender.

Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.



- **Source Port (16-bits)** - It identifies source port of the application process on the sending device.
- **Destination Port (16-bits)** - It identifies destination port of the application process on the receiving device.
- **Sequence Number (32-bits)** - Sequence number of data bytes of a segment in a session.
- **Acknowledgement Number (32-bits)** - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- **Data Offset (4-bits)** - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- **Reserved (3-bits)** - Reserved for future use and all are set zero by default.
- **Flags (1-bit each)**
  - **NS** - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
  - **CWR** - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
  - **ECE** -It has two meanings:
    - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
    - If SYN bit is set to 1, ECE means that the device is ECT capable.
  - **URG** - It indicates that Urgent Pointer field has significant data and should be processed.
  - **ACK** - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
  - **PSH** - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
  - **RST** - Reset flag has the following features:
    - It is used to refuse an incoming connection.
    - It is used to reject a segment.
    - It is used to restart a connection.
  - **SYN** - This flag is used to set up a connection between hosts.
  - **FIN** - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.
- **Windows Size** - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.

- **Checksum** - This field contains the checksum of Header, Data and Pseudo Headers.
- **Urgent Pointer** - It points to the urgent data byte if URG flag is set to 1.
- **Options** - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

Video Content / Details of website for further learning (if any):

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-31

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **IV - Transport Layer** **Date of Lecture:**

Topic of Lecture: Congestion Control

Introduction : (Maximum 5 sentences) :

- Congestion Control is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.
- Congestive-Avoidance Algorithms (CAA) are implemented at the TCP layer as the mechanism to avoid congestive collapse in a network.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- Domain Name System (DNS),
- Simple Network Management Protocol (SNMP),
- Routing Information Protocol (RIP)

Detailed content of the Lecture:

- Congestion causes choking of the communication medium.
- When too many packets are displayed in a method of the subnet, the subnet's performance degrades.
- Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.

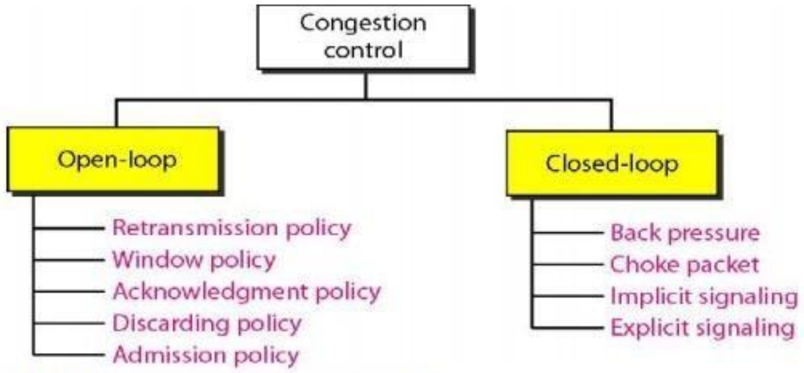


Figure 4. 27 Congestion control categories

1. Open-Loop Congestion Control

In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination.

a. Retransmission Policy

Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion.

b. Window Policy

The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control. In the Go-Back-N window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver.

c. Acknowledgment Policy

The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.

d. Discarding Policy

A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.

e. Admission Policy

An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks.

2. Closed-Loop Congestion Control

Closed-loop congestion control mechanisms try to alleviate congestion after it happens. Several mechanisms have been used by different protocols.

a. Backpressure

The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes.

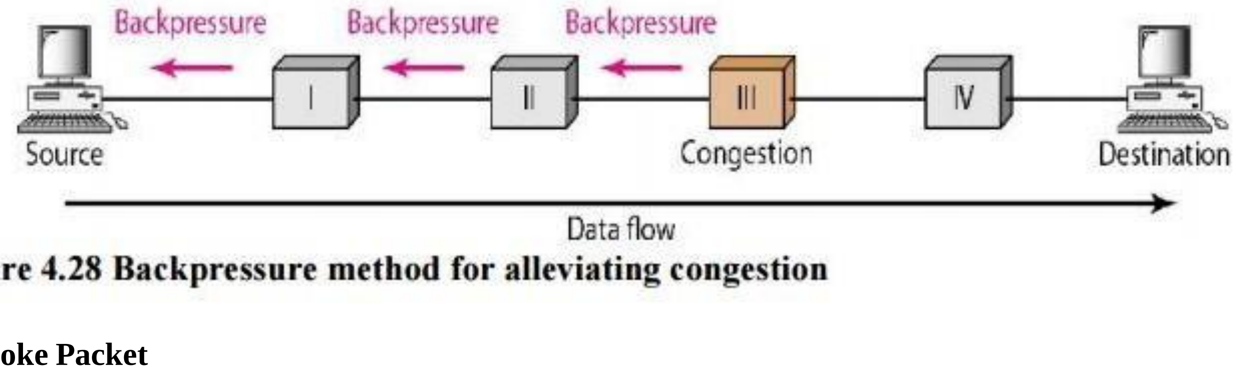


Figure 4.28 Backpressure method for alleviating congestion

b. Choke Packet

A choke packet is a packet sent by a node to the source to inform it of congestion.

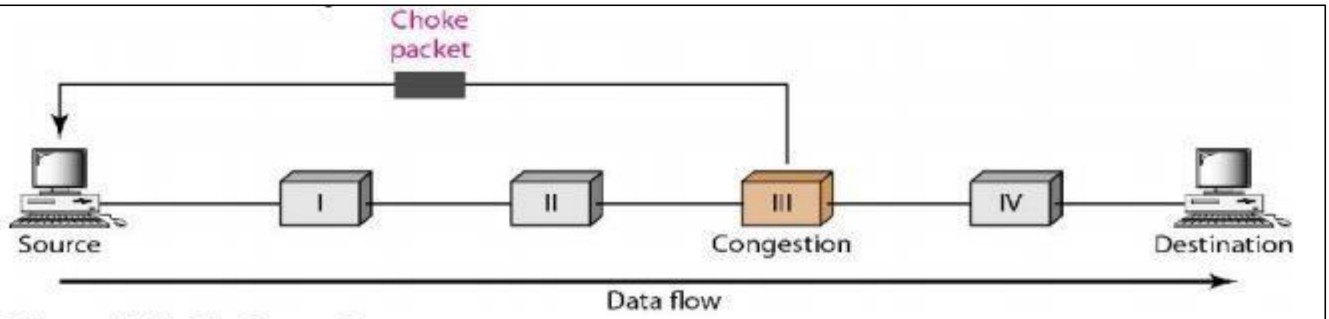


Figure 4.29 Choke packet

c. Implicit Signaling

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms.

d. Explicit Signaling

The node that experiences congestion can explicitly send a signal to the source or destination.

i. Backward Signaling

A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.

ii. Forward Signaling

A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.

Video Content / Details of website for further learning (if any):
https://www.brainkart.com/article/Congestion-Control--Open-Loop-and-Closed-Loop_13488/

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-32

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **IV - Transport Layer** **Date of Lecture:**

Topic of Lecture: Resource Allocation

Introduction : (Maximum 5 sentences) :

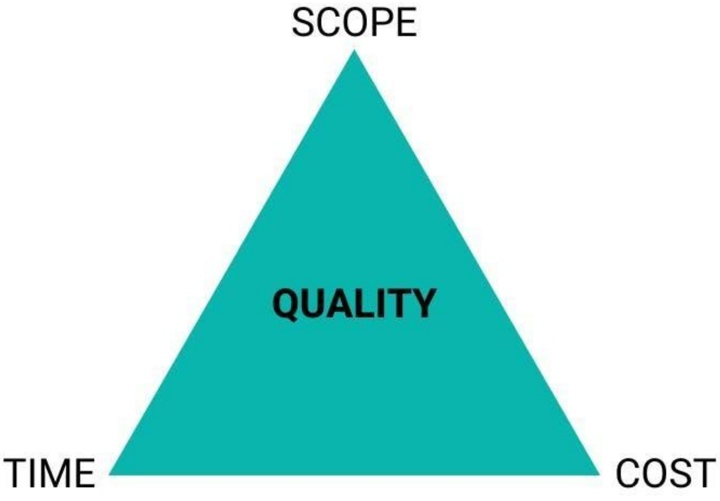
- Resource allocation is the process by which a computing system aims to meet the hardware requirements of an application run by it.
- Computing, networking and energy resources must be optimized taking into account hardware, performance and environmental restrictions.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Domain Name System (DNS),
- Simple Network Management Protocol (SNMP),
- Routing Information Protocol (RIP)

Detailed content of the Lecture:

- Resource allocation is an important feature in a heterogeneous network meant to ensure its high efficiency as well as its maintenance as a cost-benefit network.
- Proper resource allocation improves the performances of both the associated system and the network, and also helps in avoiding the different kinds of transient bottlenecks involved in the network.



- Project Management Triangle, it’s a diagram showing how scope, cost, and time affect quality.
- The triangle is a metaphor for how a project manager should look at their resources.
- They need to allocate resources to ensure fairness and quality, while also considering factors of planning like project limitations and budget constraints.
- Let’s put that into practice and say someone on your team booked time off midway through a project.
- It's the project manager's responsibility to figure out how it’ll impact deliverables.
- The person’s absence should be visible on the project schedule so you can reassign the tasks and prevent delays.

Video Content / Details of website for further learning (if any):
https://www.float.com/resources/guide-to-resource-allocation/

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-33

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **IV - Transport Layer** **Date of Lecture:**

Topic of Lecture: TCP Congestion Control

Introduction : (Maximum 5 sentences) :

- TCP controls congestion by means of Window mechanism.
- TCP sets a window size telling the other end how much data segment to send.
- TCP may use three algorithms for congestion control

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Simple Network Management Protocol (SNMP),
- Routing Information Protocol (RIP)

Detailed content of the Lecture:

- Additive increase, Multiplicative Decrease
- Slow Start
- Timeout React

Timer Management

TCP uses different types of timer to control and management various tasks:

Keep-alive timer:

- This timer is used to check the integrity and validity of a connection.
- When keep-alive time expires, the host sends a probe to check if the connection still exists.

Retransmission timer:

- This timer maintains stateful session of data sent.
- If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.

Persist timer:

- TCP session can be paused by either host by sending Window Size 0.
- To resume the session a host needs to send Window Size with some larger value.
- If this segment never reaches the other end, both ends may wait for each other for infinite time.

- When the Persist timer expires, the host re-sends its window size to let the other end know.
- Persist Timer helps avoid deadlocks in communication.

Timed-Wait:

- After releasing a connection, either of the hosts waits for a Timed-Wait time to terminate the connection completely.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/data_communication_computer_network/ transmission_control_protocol.htm

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-34

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **IV - Transport Layer** **Date of Lecture:**

Topic of Lecture: Congestion Avoidance Mechanisms

Introduction : (Maximum 5 sentences) :

- A congestion avoidance scheme allows a network to operate in the region of low delay and high throughput.
- Such schemes prevent a network from entering the congested state.
- Congestion avoidance is a prevention mechanism while congestion control is a recovery mechanism.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Simple Network Management Protocol (SNMP),
- Routing Information Protocol (RIP)

Detailed content of the Lecture:

- Congestion is said to occur in the network when the resource demands exceed the capacity and packets are lost due to too much queuing in the network.
- During congestion, the network throughput may drop to zero and the path delay may become very high. A congestion control scheme helps the network to recover from the congestion state.
- A congestion avoidance scheme allows a network to operate in the region of low delay and high throughput.
- Such schemes prevent a network from entering the congested state.
- Congestion avoidance is a prevention mechanism while congestion control is a recovery mechanism.
- We compare the concept of congestion avoidance with that of flow control and congestion control.

- A number of possible alternative for congestion avoidance have been identified. From these a few were selected for study.
- The criteria for selection and goals for these schemes have been described. In particular, we wanted the scheme to be globally efficient, fair, dynamic, convergent, robust, distributed, configuration independent, etc.
- These goals and the test cases used to verify whether a particular scheme has met the goals have been described.
- We model the network and the user policies for congestion avoidance as a feedback control system.
- The key components of a generic congestion avoidance scheme are: congestion detection, congestion feedback, feedback selector, signal filter, decision function, and increase/decrease algorithms.

Video Content / Details of website for further learning (if any):

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-35

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **IV - Transport Layer** **Date of Lecture:**

Topic of Lecture: Quality of Services, Integrated Services,congestion avoidance

Introduction : (Maximum 5 sentences) :

- Quality of Services: Quality of Service (QOS) determines a network's capability to support predictable service over various technologies, containing frame relay, Asynchronous Transfer Mode (ATM), Ethernet, SONET IP-routed networks.
- The networks can use any or all of these frameworks.
- In computer networking, integrated services or Integrated Services is an architecture that specifies the elements to guarantee quality of service (QoS) on networks.
- Integrated Services can for example be used to allow video and sound to reach the receiver without interruption.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Simple Network Management Protocol (SNMP),
- Routing Information Protocol (RIP)

Detailed content of the Lecture:

- The QOS is primarily used to control resources like bandwidth, equipment, wide-area facilities etc.
- It can get more efficient use of network resources, provide tailored services, provide coexistence of mission-critical applications, etc.

QOS Concepts

The QOS concepts are explained below

Congestion Management

- The burst feature of data traffic sometimes bounds to increase traffic more than a connection speed.
- QoS allows a router to put packets into different queues.
- Service specific queues more often depend on priority than buffer traffic in an individual queue and let the first packet by the first packet out.

Queue Management

- The queues in a buffer can fill and overflow.

- A packet would be dropped if a queue is complete, and the router cannot prevent it from being dropped if it is a high priority packet.
- This is referred to as tail drop.

Link Efficiency

- The low-speed links are bottlenecks for lower packets.
- The serialization delay caused by the high packets forces the lower packets to wait longer.
- The serialization delay is the time created to put a packet on the connection.

Elimination of overhead bits

- It can also increase efficiency by removing too many overhead bits.

Traffic shaping and policing

- Shaping can prevent the overflow problem in buffers by limiting the full bandwidth potential of the applications packets.
- Sometimes, many network topologies with a high bandwidth link connected with a low-bandwidth link in remote sites can overflow low bandwidth connections.

Integrated Services

- Integrated services is an architecture that specifies the elements to guarantee quality of service (QoS) on networks.
- Integrated services can for example be used to allow video and sound to reach the receiver without interruption.
- Integrated services specifies a fine-grained QoS system, which is often contrasted with DiffServ's coarse-grained control system.
- Under Integrated services every router in the system implements integrated services, and every application that requires some kind of QoS guarantee has to make an individual reservation.

Video Content / Details of website for further learning (if any):
Integrated services - Wikipedia,

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE

(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

Estd. 2000

LECTURE HANDOUTS

L-36

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **IV - Transport Layer** **Date of Lecture:**

Topic of Lecture: Differentiated Services

Introduction : (Maximum 5 sentences) :

- Differentiated services is a computer networking architecture that specifies a simple and scalable mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks.

- Differentiated services can, for example, be used to provide low-latency to critical network traffic such as voice or streaming media while providing simple best-effort service to non-critical services such as web traffic or file transfers.

Prerequisite knowledge for Complete understanding and learning of Topic: (Max. Four important topics)

- Simple Network Management Protocol (SNMP),
- Routing Information Protocol (RIP)

Detailed content of the Lecture:

- Differentiated Services is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence.

- Example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic.

- Differentiated Services is the most advanced method for managing traffic in terms of what is called Class of Service (CoS).

- Type of Service (ToS), Differentiated Services avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet.

- An analogy is made to travel services, in which a person can choose among different modes of travel - train, bus, airplane - degree of comfort, the number of stops on the route, standby status, the time of day or period of year for the trip, and so forth. For a given set of packet travel rules, a packet is given one of 64 possible forwarding behaviors - known as per hop behaviors (PHBs).

- A six-bit field, known as the Differentiated Services Code Point (DSCP), in the Internet Protocol (IP) header specifies the per hop behavior for a given flow of packets.

- Differentiated Services and the Class of Service approach provide a way to control traffic that is both more flexible and more scalability than the Quality of Service approach.

Video Content / Details of website for further learning (if any):

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-37

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **IV - Transport Layer** **Date of Lecture:**

Topic of Lecture: Network Traffic Analysis

Introduction : (Maximum 5 sentences) :

- Network traffic analysis (NTA) is a method of monitoring network availability and activity to identify anomalies, including security and operational issues.
- Common use cases for NTA include: Collecting a real-time and historical record of what's happening on your network.
- Detecting malware such as ransom ware activity.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- Simple Network Management Protocol (SNMP),
- Routing Information Protocol (RIP)

Detailed content of the Lecture:

- Network traffic monitoring and analysis techniques allow the traffic at particular points on a network to be recorded, displayed in useful form and analyzed
- Traffic can be monitored
- At the network boundary
- On specific segments
- At particular interfaces
- The rapid growth of Internet Traffic has emerged as a major issue due to the rapid development of various network applications and Internet services.
- One of the challenges facing Internet Service Providers (ISPs) is to optimize the performance of their networks in the face of continuously increasing amounts of IP traffic while guaranteeing some specific Quality of Services (QoS).
- Therefore it is necessary for ISPs to study the traffic patterns and user behaviors in different localities, to estimate the application usage trends, and thereby to come up with solutions that can effectively, efficiently, and economically support their user’s traffic.

- The data about the amount of traffic was measured using a real-time traffic-monitoring tool from Packet Logic.
- Traffic from the monitored network to various destinations was captured and classified into 5 ring-wise locality levels in accordance with the Parameters such as traffic patterns and user behavior at different geographic localities were studied in this project

Video Content / Details of website for further learning (if any):

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

LECTURE HANDOUTS **L-38**

CY **II/III**

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **V- Application Layer** **Date of Lecture:**

Topic of Lecture: Domain Name System

Introduction : (Maximum 5 sentences) :

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

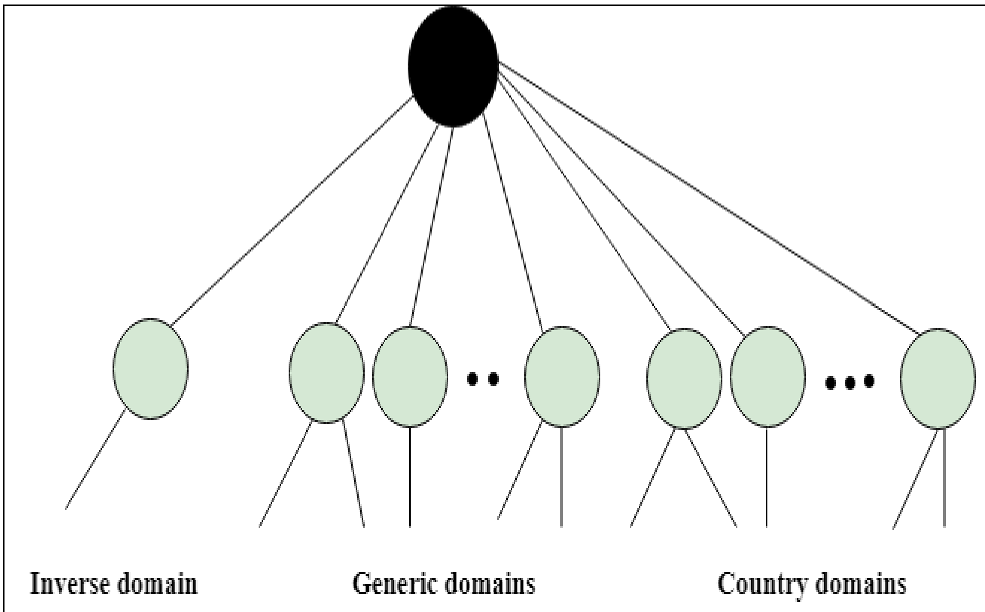
- HTTP
- FTP
- DNS
- SMTP

Detailed content of the Lecture:

An application layer protocol defines how the application processes running on different systems; pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

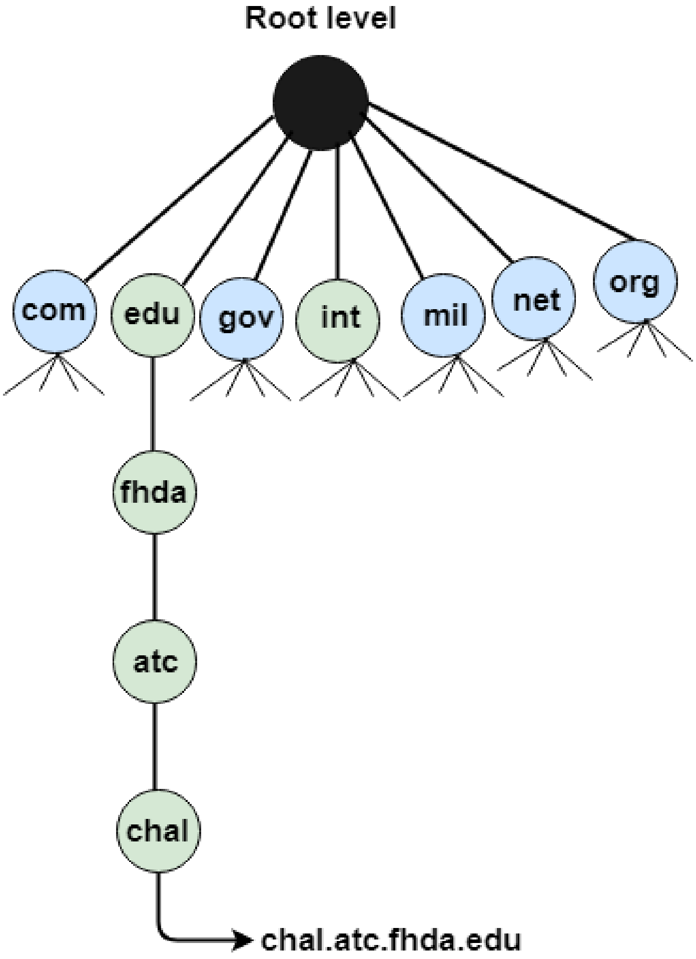
DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.



Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Label	Description
aero	Airlines and aerospace companies
biz	Businesses or firms
com	Commercial Organizations
coop	Cooperative business Organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International Organizations
mil	Military groups
museum	Museum & other nonprofit organizations
name	Personal names
net	Network Support centers
org	Nonprofit Organizations
pro	Professional individual Organizations



Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Working of DNS

- DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
- Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
- DNS implements a distributed database to store the name of all the hosts available on the internet.
- If a client like a web browser sends a request containing a hostname, then a piece of software such as **DNS resolver** sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server. If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

Video Content / Details of website for further learning (if any):
DNS - Domain Name System - javatpoint

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)

(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

LECTURE HANDOUTS

L-39

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **V- Application Layer** **Date of Lecture:**

Topic of Lecture: Electronic Mail –SMTP

Introduction : (Maximum 5 sentences) :

- SMTP stands **for Simple Mail Transfer Protocol**. SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.
- It is a program used for sending messages to other computer users based on e-mail addresses.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

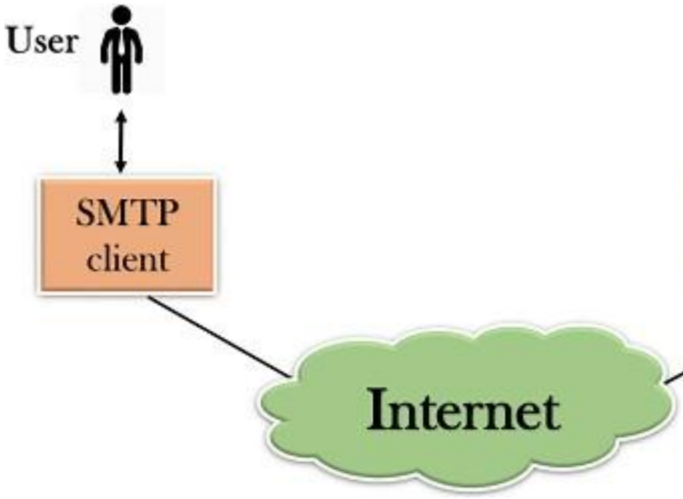
- HTTP
- FTP
- DNS
- SMTP

Detailed content of the Lecture:

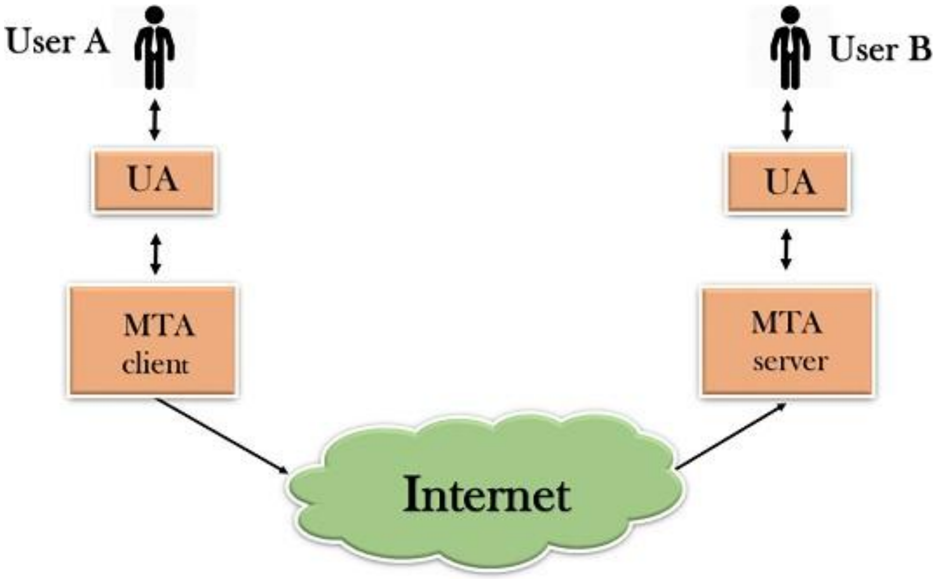
SMTP

- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called **Simple Mail Transfer Protocol**.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
  - It can send a single message to one or more recipients.
  - Sending message can include text, voice, video or graphics.
  - It can also send the messages on networks outside the internet.
- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. They also have a way of handling the errors such as incorrect email address. For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.

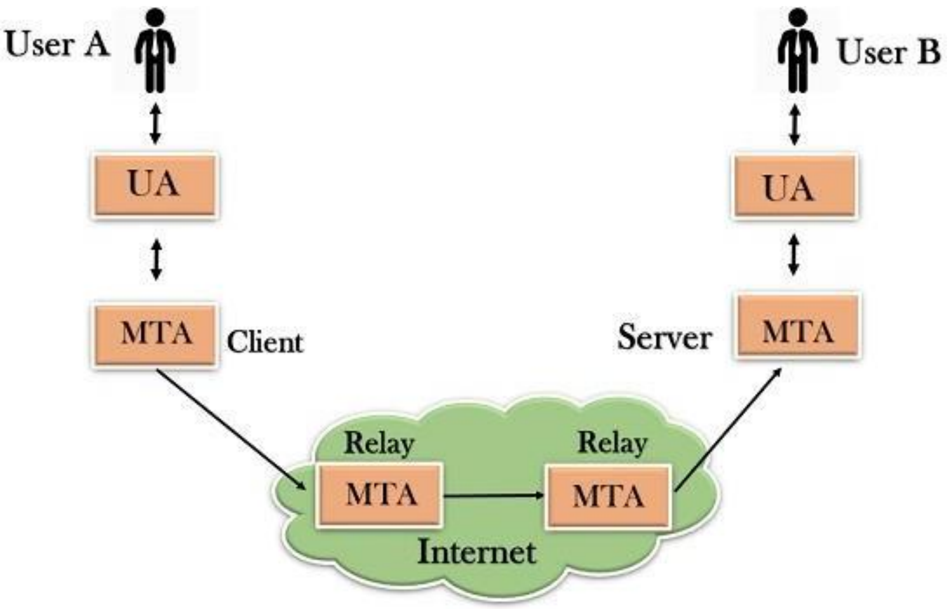
Components of SMTP



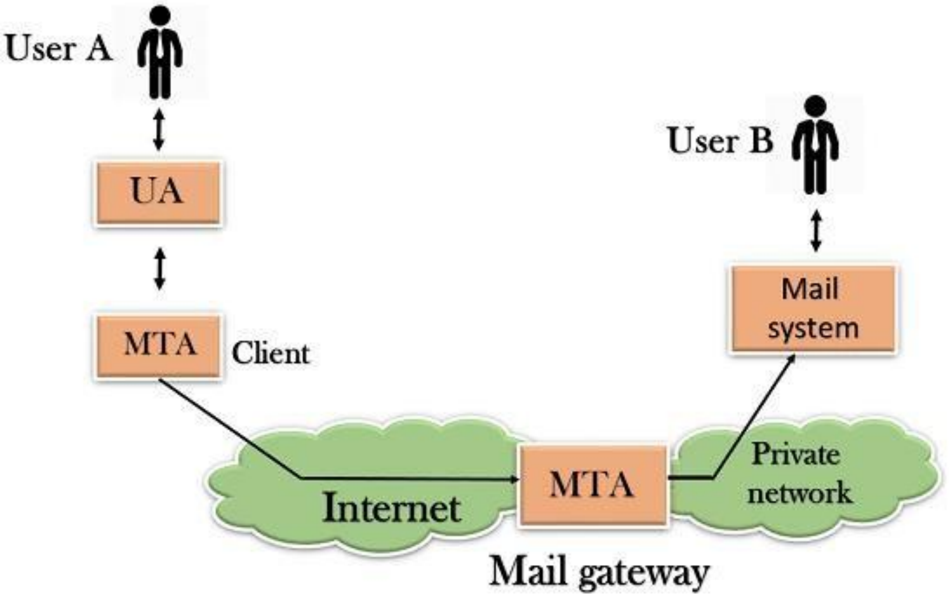
- First, we will break the SMTP client and SMTP server into two components such as user agent (UA) and mail transfer agent (MTA). The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope. The mail transfer agent (MTA) transfers this mail across the internet.



- SMTP allows a more complex system by adding a relaying system. Instead of just having one MTA at sending side and one at receiving side, more MTAs can be added, acting either as a client or server to relay the email.



- The relaying system without TCP/IP protocol can also be used to send the emails to users, and this is achieved by the use of the mail gateway. The mail gateway is a relay MTA that can be used to receive an email.



Working of SMTP

1. **Composition of Mail:** A user sends an e-mail by composing an electronic mail message using a Mail User Agent (MUA). Mail User Agent is a program which is used to send and receive mail. The message contains two parts: body and header. The body is the main part of the message while the header includes information such as the sender and recipient address. The header also includes descriptive information such as the subject of the message. In this case, the message body is like a letter and header is like an envelope that contains the recipient's address.
2. **Submission of Mail:** After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.
3. **Delivery of Mail:** E-mail addresses contain two parts: username of the recipient and domain name. For example, vivek@gmail.com, where "vivek" is the username of the recipient and "gmail.com" is the domain name.

If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA). To relay the email, the MTA will find the target domain. It checks the MX record from Domain Name System to obtain the target domain. The MX record contains the domain name and IP address of the recipient's domain. Once the record is located, MTA connects to the exchange server to relay the message.

4. **Receipt and Processing of Mail:** Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.
5. **Access and Retrieval of Mail:** The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.

Video Content / Details of website for further learning (if any):
SMTP - Simple Mail Transfer Protocol - javatpoint

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-40

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **V- Application Layer** **Date of Lecture:**

Topic of Lecture: Electronic Mail-MIME

Introduction : (Maximum 5 sentences) :

- MIME represents **Multi-Purpose Internet Mail Extensions**. It is a development to the Internet email protocol that enables its users to exchange several kinds of data files over the Internet, including images, audio, and video.
- The MIME is required if the text in character sets other than the American Standard Code for Information Interchange (ASCII).

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- HTTP
- FTP
- DNS
- SMTP

Detailed content of the Lecture:
MIME :

- MIME represents **Multi-Purpose Internet Mail Extensions**. It is a development to the Internet email protocol that enables its users to exchange several kinds of data files over the Internet, including images, audio, and video.
- The MIME is required if the text in character sets other than the American Standard Code for Information Interchange (ASCII). Virtually, all human-written Internet email and a fairly large proportion of automated email is transmitted via Simple Mail Transfer Protocol (SMTP) in MIME format.
- MIME was designed mainly for SMTP, but the content types defined by MIME standards are important also in communication protocols outside of email, such as Hypertext Transfer Protocol (HTTP).

MIME Header

There are five header fields represented in MIME which are as follows −

- **MIME-version** − It denotes the MIME version being used. The current version is 1.1. It is defined as MIME-version: 1.1.

- **Content-type** − It defines the type and subtype of the data in the body of the message. The content type and content subtype are divided by a slash. This field defines how the object in the body is to be executed. The default value is plaintext in US ASCII.

The content-type field is represented as follows −
Context-type: <type/subtype; parameters>

- **Content-transfer encoding** − It defines how the object inside the body has been encoded to US ASCII to create it acceptable for mail transfer. Thus, it determines the method used to encode the message into 0s and 1s for transport.

The content transfer encoding field is represented as follows −
Content-transfer-encoding : <type>

- **Content-Description** − This field tells what the message is. It is the form of ASCII recipient will know whether it is worth decoding and reading the message.
- **Content-ID** − This field identifies the contents. Its format is the same as the format of the standard Message-Id header.

Video Content / Details of website for further learning (if any):
What is MIME in the Computer Network? (tutorialspoint.com)

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-41

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **V- Application Layer** **Date of Lecture:**

Topic of Lecture: Electronic Mail-IMAP

Introduction : (Maximum 5 sentences) :

- Internet Message Access Protocol (IMAP) is a protocol for accessing email or bulletin board messages from a (possibly shared) mail server or service.

- IMAP allows a client e-mail program to access remote message stores as if they were local.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

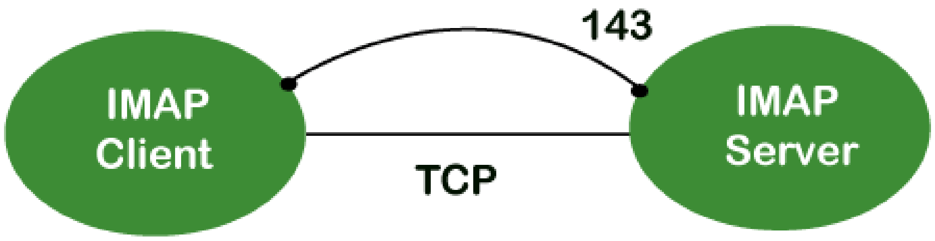
- HTTP
- FTP
- DNS
- SMTP

Detailed content of the Lecture:

IMAP Protocol

IMAP stands for **Internet Message Access Protocol**. It is an application layer protocol which is used to receive the emails from the mail server. It is the most commonly used protocols like POP3 for retrieving the emails.

It also follows the client/server model. On one side, we have an IMAP client, which is a process running on a computer. On the other side, we have an IMAP server, which is also a process running on another computer. Both computers are connected through a network.



The IMAP protocol resides on the TCP/IP transport layer which means that it implicitly uses the reliability of the protocol. Once the TCP connection is established between the IMAP client and IMAP server, the IMAP server listens to the port 143 by default, but this port number can also be changed.

By default, there are two ports used by IMAP:

- Port 143: It is a non-encrypted IMAP port.
- Port 993: This port is used when IMAP client wants to connect through IMAP securely.

Why should we use IMAP instead of POP3 protocol?

POP3 is becoming the most popular protocol for accessing the TCP/IP mailboxes. It implements the offline mail access model, which means that the mails are retrieved from the mail server on the local machine, and then deleted from the mail server. Nowadays, millions of users use the POP3 protocol to access the incoming mails. Due to the offline mail access model, it cannot be used as much. The online model we would prefer in the ideal world. In the online model, we need to be connected to the internet always. The biggest problem with the offline access using POP3 is that the mails are permanently removed from the server, so multiple computers cannot access the mails. The solution to this problem is to store the mails at the remote server rather than on the local server. The POP3 also faces another issue, i.e., data security and safety. The solution to this problem is to use the disconnected access model, which provides the benefits of both online and offline access. In the disconnected access model, the user can retrieve the mail for local use as in the POP3 protocol, and the user does not need to be connected to the internet continuously. However, the changes made to the mailboxes are synchronized between the client and the server. The mail remains on the server so different applications in the future can access it. When developers recognized these benefits, they made some attempts to implement the disconnected access model. This is implemented by using the POP3 commands that provide the option to leave the mails on the server. This works, but only to a limited extent, for example, keeping track of which messages are new or old become an issue when both are retrieved and left on the server. So, the POP3 lacks some features which are required for the proper disconnected access model.

In the mid-1980s, the development began at Stanford University on a new protocol that would provide a more capable way of accessing the user mailboxes. The result was the development of the interactive mail access protocol, which was later renamed as **Internet Message Access Protocol**.

IMAP History and Standards

The first version of IMAP was formally documented as an internet standard was IMAP version 2, and in RFC 1064, and was published in July 1988. It was updated in RFC 1176, August 1990, retaining the same version. So they created a new document of version 3 known as IMAP3. In RFC 1203, which was published in February 1991. However, IMAP3 was never accepted by the market place, so people kept using IMAP2. The extension to the protocol was later created called IMAPbis, which added support for Multipurpose Internet Mail Extensions (MIME) to IMAP. This was a very important development due to the usefulness of MIME. Despite this, IMAPbis was never published as an RFC. This may be due to the problems associated with the IMAP3. In December 1994, IMAP version 4, i.e., IMAP4 was published in two RFCs, i.e., RFC 1730 describing the main protocol and RFC 1731 describing the authentication mechanism for IMAP 4. IMAP 4 is the current version of IMAP, which is widely used today. It continues to be refined, and its latest version is actually known as IMAP4rev1 and is defined in RFC 2060. It is most recently updated in RFC 3501.

IMAP Features

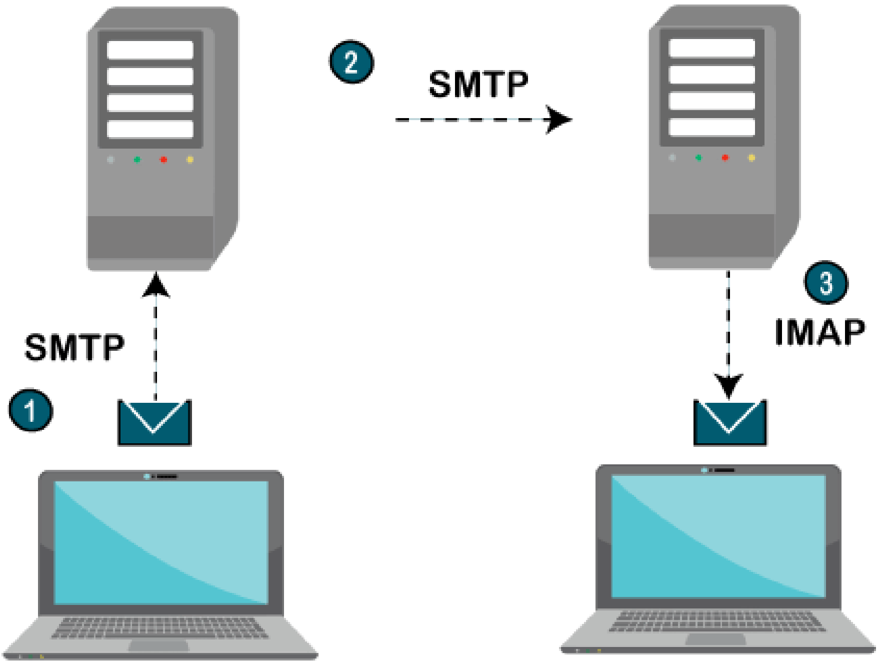
IMAP was designed for a specific purpose that provides a more flexible way of how the user accesses the mailbox. It can operate in any of the three modes, i.e., online, offline, and disconnected mode. Out of these, offline and disconnected modes are of interest to most users of the protocol.

The following are the features of an IMAP protocol:

- Access and retrieve mail from remote server: The user can access the mail from the remote server while retaining the mails in the remote server.
- Set message flags: The message flag is set so that the user can keep track of which message he has already seen.
- Manage multiple mailboxes: The user can manage multiple mailboxes and transfer messages from one mailbox to another. The user can organize them into various categories for those who are working on various projects.
- Determine information prior to downloading: It decides whether to retrieve or not before downloading the mail from the mail server.

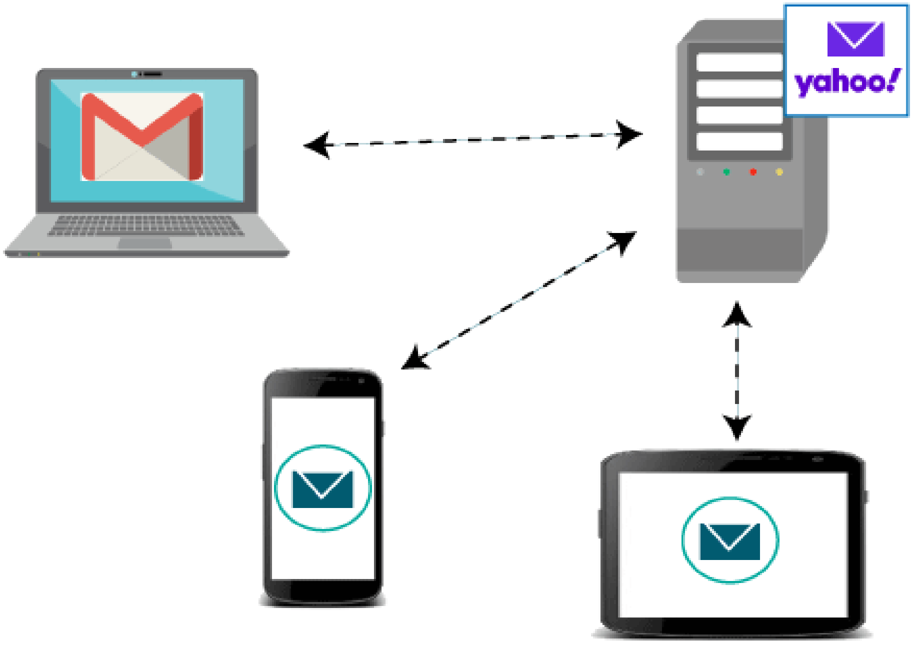
- Downloads a portion of a message: It allows you to download the portion of a message, such as one body part from the mime-multi part. This can be useful when there are large multimedia files in a short-text element of a message.
- Organize mails on the server: In case of POP3, the user is not allowed to manage the mails on the server. On the other hand, the users can organize the mails on the server according to their requirements like they can create, delete or rename the mailbox on the server.
- Search: Users can search for the contents of the emails.
- Check email-header: Users can also check the email-header prior to downloading.
- Create hierarchy: Users can also create the folders to organize the mails in a hierarchy.

IMAP General Operation



6. The IMAP is a client-server protocol like POP3 and most other TCP/IP application protocols. The IMAP4 protocol functions only when the IMAP4 must reside on the server where the user mailboxes are located. In c the POP3 does not necessarily require the same physical server that provides the SMTP services. Therefore, in the case of the IMAP protocol, the mailbox must be accessible to both SMTP for incoming mails and IMAP for retrieval and modifications.
7. The IMAP uses the Transmission Control Protocol (TCP) for communication to ensure the delivery of data and also received in the order.
8. The IMAP4 listens on a well-known port, i.e., port number 143, for an incoming connection request from the IMAP4 client.

Let's understand the IMAP protocol through a simple example.



The IMAP protocol synchronizes all the devices with the main server. Let's suppose we have three devices desktop, mobile, and laptop as shown in the above figure. If all these devices are accessing the same mailbox, then it will be synchronized with all the devices.

Video Content / Details of website for further learning (if any):
IMAP Protocol | Internet Message Access Protocol - javatpoint

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L-42

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **V- Application Layer** **Date of Lecture:**

Topic of Lecture: File Transfer (FTP)

Introduction : (Maximum 5 sentences) :

- The term file transfer protocol (FTP) refers to a process that involves the transfer of files between devices over a network. ...
- File transfer protocol allows individuals and businesses to share electronic files with others without having to be in the same space.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- HTTP
- FTP
- DNS
- SMTP

Detailed content of the Lecture:

FTP

- FTP stands for File transfer protocol.
- FTP is a standard internet protocol provided by TCP/IP used for transmitting the files from one host to another.
- It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet.
- It is also used for downloading the files to computer from other servers.

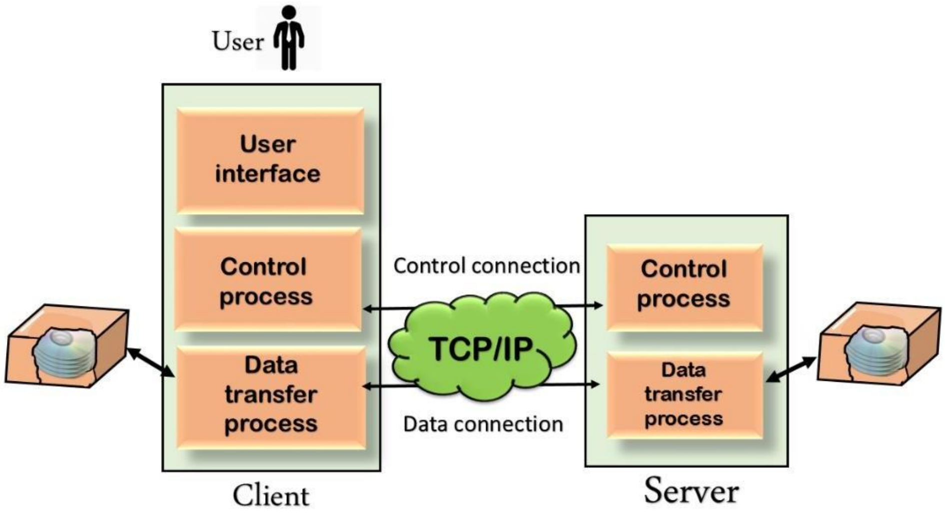
Objectives of FTP

- It provides the sharing of files.
- It is used to encourage the use of remote computers.
- It transfers the data more reliably and efficiently.

Why FTP?

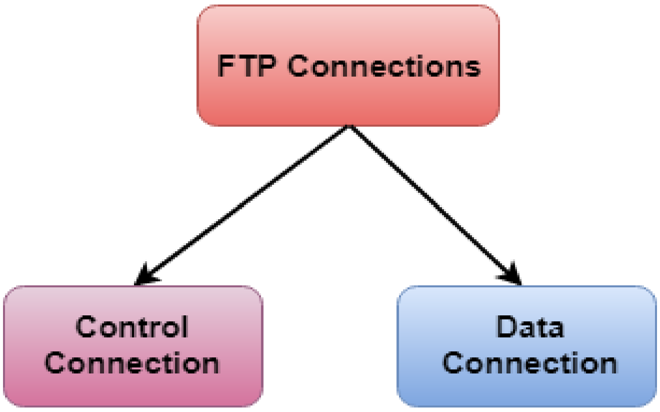
Although transferring files from one system to another is very simple and straightforward, but sometimes it can cause problems. For example, two systems may have different file conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. FTP protocol overcomes these problems by establishing two connections between hosts. One connection is used for data transfer, and another connection is used for the control connection.

Mechanism of FTP



The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

There are two types of connections in FTP:



- **Control Connection:** The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- **Data Connection:** The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

FTP Clients

- FTP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet.
- It allows a user to connect to a remote host and upload or download the files.
- It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection.

- The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

Advantages of FTP:

- **Speed:** One of the biggest advantages of FTP is speed. The FTP is one of the fastest way to transfer the files from one computer to another computer.
- **Efficient:** It is more efficient as we do not need to complete all the operations to get the entire file.
- **Security:** To access the FTP server, we need to login with the username and password. Therefore, we can say that FTP is more secure.
- **Back & forth movement:** FTP allows us to transfer the files back and forth. Suppose you are a manager of the company, you send some information to all the employees, and they all send information back on the same server.

Disadvantages of FTP:

- The standard requirement of the industry is that all the FTP transmissions should be encrypted. However, not all the FTP providers are equal and not all the providers offer encryption. So, we will have to look out for the FTP providers that provides encryption.
- FTP serves two operations, i.e., to send and receive large files on a network. However, the size limit of the file is 2GB that can be sent. It also doesn't allow you to run simultaneous transfers to multiple receivers.
- Passwords and file contents are sent in clear text that allows unwanted eavesdropping. So, it is quite possible that attackers can carry out the brute force attack by trying to guess the FTP password.
- It is not compatible with every system.

Video Content / Details of website for further learning (if any):

FTP - File Transfer Protocol - javatpoint

Important Books/Journals for further learning including the page nos.:

Page No:

Course Faculty

Verified by HOD

MUTHAYAMMAL ENGINEERING COLLEGE
(An Autonomous Institution)
(Approved by AICTE, New Delhi, Accredited by NAAC & Affiliated to Anna University)
Rasipuram - 637 408, Namakkal Dist., Tamil Nadu

DESIGNING YOUR FUTURE
Estd. 2000

IQAC

LECTURE HANDOUTS

L-42

CY

II/III

Course Name with Code : **19CYC05 & COMPUTER NETWORKS**

Course Faculty : **Dr.J.PREETHA**

Unit : **V- Application Layer** **Date of Lecture:**

Topic of Lecture: WWW (HTTP)

Introduction : (Maximum 5 sentences) :

- The **World Wide Web** abbreviated as WWW and commonly known as the web.
- The WWW was initiated by CERN (European library for Nuclear Research) in 1989.

Prerequisite knowledge for Complete understanding and learning of Topic:
(Max. Four important topics)

- HTTP
- FTP
- DNS
- SMTP

Detailed content of the Lecture:

World Wide Web (WWW)

- Difficulty Level : Medium
- Last Updated : 22 Sep, 2021

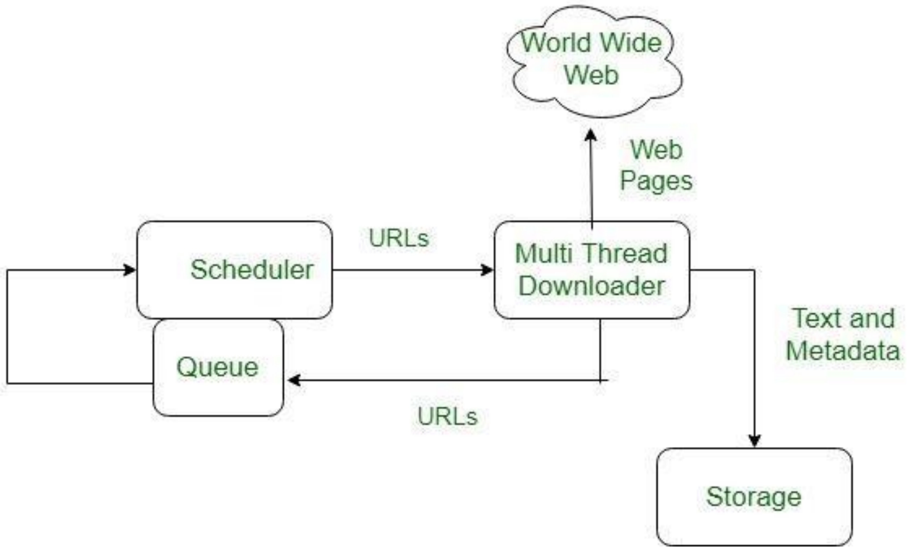
The **World Wide Web** abbreviated as WWW and commonly known as the web. The WWW was initiated by CERN (European library for Nuclear Research) in 1989.

History:

It is a project created, by Timothy Berner's Lee in 1989, for researchers to work together effectively at CERN. is an organization, named World Wide Web Consortium (W3C), which was developed for further development in the web. This organization is directed by Tim Berner's Lee, aka the father of the web.

System Architecture:

From the user's point of view, the web consists of a vast, worldwide connection of documents or web pages. Each page may contain links to other pages anywhere in the world. The pages can be retrieved and viewed by using browsers of which internet explorer, Netscape Navigator, Google, Chrome, etc are the popular ones.



Here the browser displaying a web page on the client machine when the user clicks on a line of text that is linked to a page on abd.com, the browser follows the hyperlink by sending a message to abd.com server asking for the page.

Working of WWW:

The World Wide Web is based on several different technologies: Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).
A Web browser is used to access webpages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interface provided by Web browsers.
Cross-Platform

- Distributed
- Open Standards and Open Source
- Uses Web Browsers to provide a single interface for many services
- Dynamic, Interactive and Evolving.
- “Web 2.0”

Components of Web: There are 3 components of web:

9. **Uniform Resource Locator (URL):** serves as system for resources on web.
10. **Hypertext Transfer Protocol (HTTP):** specifies communication of browser and server.
11. **Hyper Text Markup Language (HTML):** defines structure, organization and content of webpage.

Video Content / Details of website for further learning (if any):
World Wide Web (WWW) - GeeksforGeeks

Important Books/Journals for further learning including the page nos.:
Page No:

Course Faculty

Verified by HOD