LECTURE HANDOUTS

L 01

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **I - Network Fundamentals**

Date of Lecture: 22.02.2021

Topic of Lecture: Introduction to Networks

Introduction :

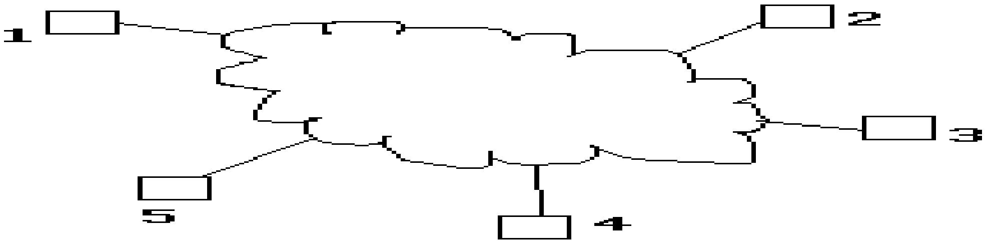
- A Network: A group of devices that can communicate with each other over links.
- Each device is called a host.
- Each host has a unique address.
- Network is a connection between two or more devices.
- Which is connected by a communication links.

Prerequisite knowledge for Complete understanding and learning of Topic:

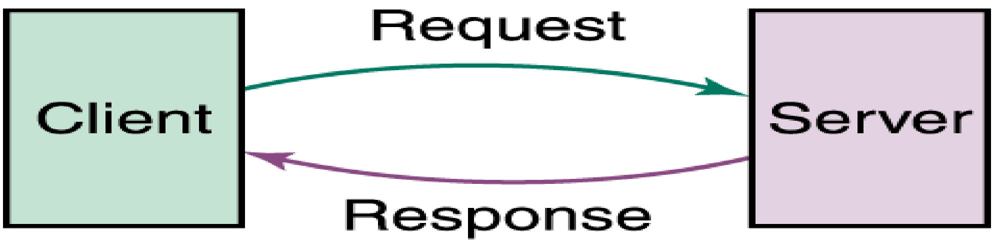
- Computer
- Telecommunication
- Data
- Information
- Internet

Detailed content of the Lecture:

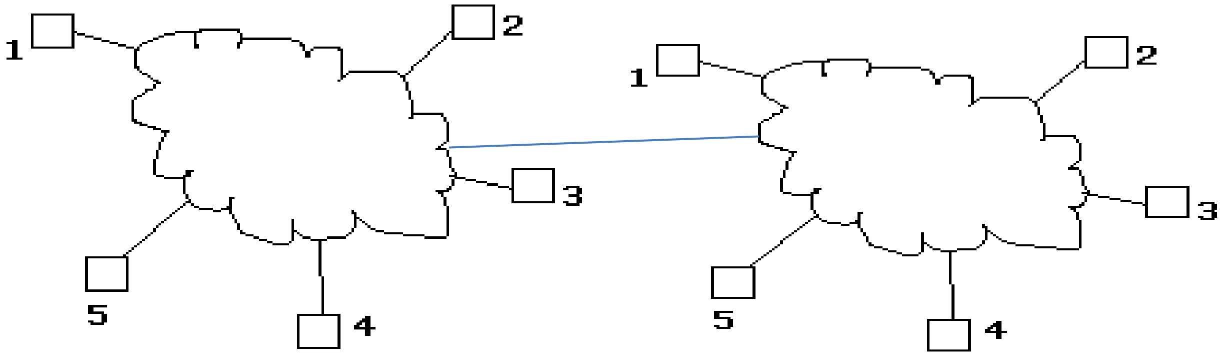
Network is a connection between two or more devices.Which is connected by a communication links.
A node can be computer, printer or any other devices which is capable of sending and receiving information at each other.



Example:



An internet: A network of networks or connection between two or more Networks is also known as internet. each host has an address of the form n/h where n is the network number and h is the number of the host on network n.



Uses of Networks :

It is Used for

- Business Application
- Home Application
- Mobile Users
- E-Mail

Point - to - Point Connection : It Provides a dedicated links between two devices.
For example, a wired system that connects two computers together can be thought of a point-to-point link.
Multi - Point Connection : It is a link between two or more devices. It is also known as Multi-Point configuration. The networks having multipoint configuration are called Broadcast Networks.

1) Client - Which gives the Request.

2) Server - Which gives the Response.

3) Modems - It Indicates Modulator / Demodulator.

4) Router - Which identifies the Path between Client & Server.

5) Channels - Which overcomes the Traffic problems.

Video Content / Details of website for further learning (if any):
https://cs.lmu.edu/~ray/notes/netsandinets

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

Book: Data Communication and Networking - Forouzan, Fifth Edition, TMH 2012 **(Page No : 4 - 7)**

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

LECTURE HANDOUTS

L 02

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **I - Network Fundamentals**

Date of Lecture: 23.02.2021

Topic of Lecture: Categories of Networks

Introduction :

- Networks are divided into two main categories:
- Local area networks (LANs) and Wide area networks (WANs).
- These two types of networks have different characteristics and different functionalities.
- The Internet is a collection of LANs and WANs held together by internetworking devices.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Client
- Server
- Telecommunication
- Data
- Information

Detailed content of the Lecture:

Categories of Networks:

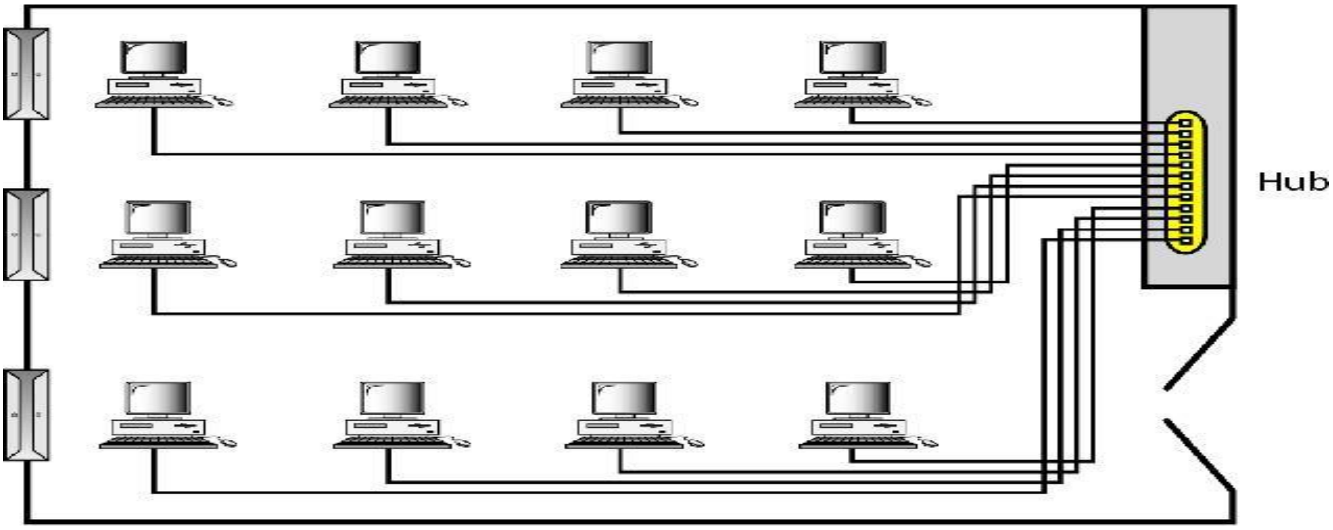
- Networks are generally referring to two primary categories: local-area networks and wide-area networks. A LAN normally covers an area less than 2 Meters. A WAN can be worldwide.
- Networks of a size in between are normally referred to as metropolitan area networks and span tens of miles.

a. Local Area Network:

- A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus.

Depending on the needs of an organization and thetype of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals.

Currently, LAN size is limited to a few kilometers.



b. Wide Area Network

A wide area network (WAN) provides long-distance transmission of data, image, audio and video information over large geographic areas that may comprise a country, a continent or even the whole world.

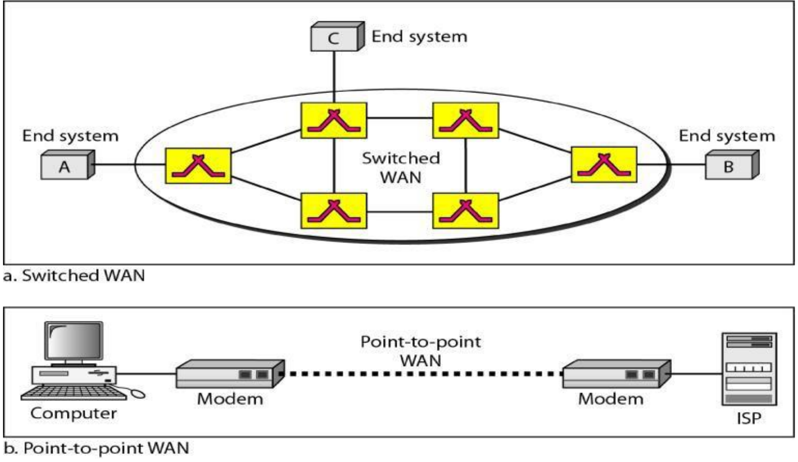
A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet.

We normally refer to thefirst as a switched WAN and to the second as a point-to-point WAN

c. Metropolitan Area Networks:

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city.

It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or partof city.



a. Switched WAN

b. Point-to-point WAN

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

Important Books/Journals for further learning including the page nos.:
Book: Data Communication and Networking - Forouzan, Fifth Edition, TMH 2012 **(Page No : 30 -33)**

Course Faculty

Verified by HOD

L 03

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **I - Network Fundamentals**

Date of Lecture: 24.02.2021

Topic of Lecture: Communication Model

Introduction :

- ➢ Networks are divided into two main categories:
- ➢ Local area networks (LANs) and Wide area networks (WANs).
- ➢ These two types of networks have different characteristics and different functionalities.
- ➢ The Internet is a collection of LANs and WANs held together by internetworking devices

Prerequisite knowledge for Complete understanding and learning of Topic:

- ➢ Computer
- ➢ Telecommunication
- ➢ Data
- ➢ Information
- ➢ Internet

Detailed content of the Lecture:

Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

Characteristics:

- The effectiveness of a data communications system depends on four fundamentalcharacteristics:

Delivery:

- The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

Accuracy:

- The system must deliver data accurately.

Timeliness:

- The system must deliver data in a timely manner. In the case of video and audio, timely delivery means delivering the data as they are produced. In the same order, that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

Jitter:

- Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packet.

Components:

A data communication system has five components.

a. **Message**:

The message is the information to be communicated. Popular forms of information include text, numbers, pictures audio and video.

b. **Sender**:

The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

c. Receiver:

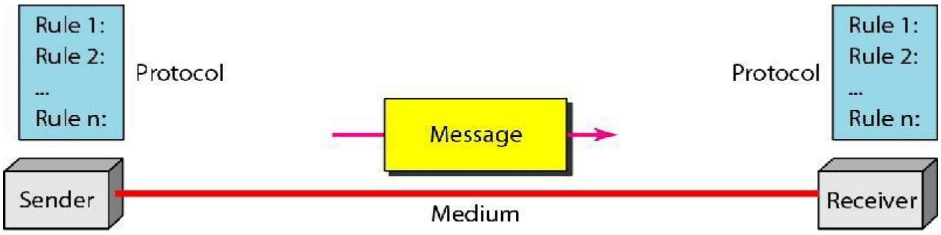
The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television and so on.

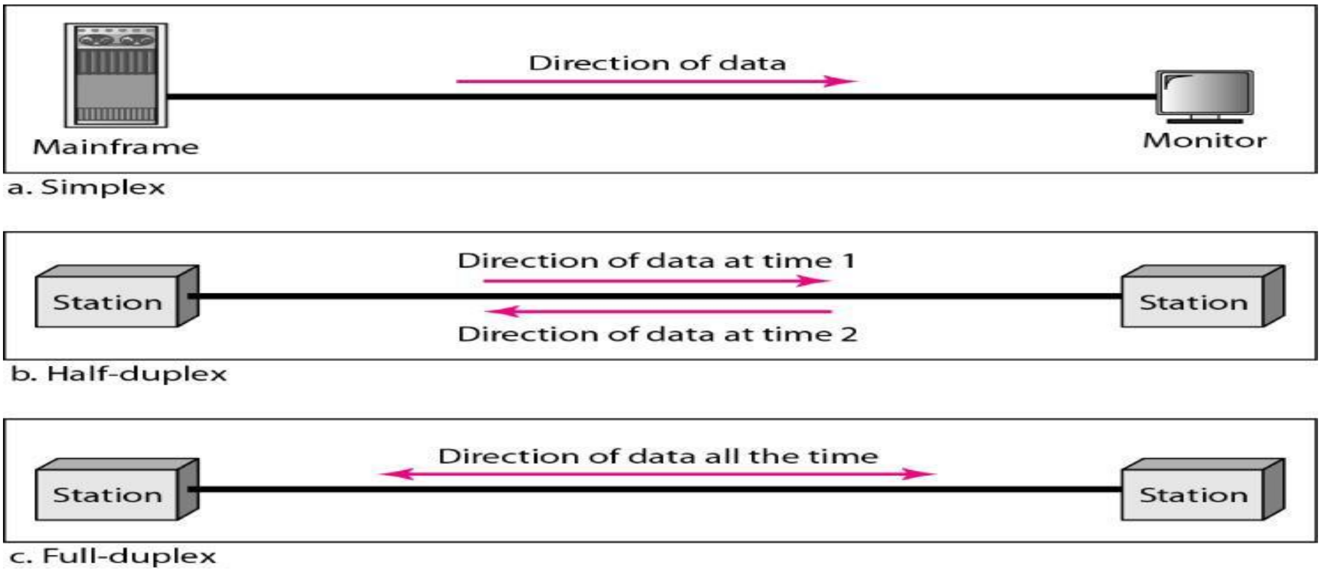
d. Transmission medium:

The transmission medium is the physical path by which a message travels from sender to receiver. Ex. Twisted pair wire, coaxial cable, fiber optic cable and radio waves.

e. Protocol:

A protocol is the set of rules that governs data communications. It represents an agreement between the communicating devices.




Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex

b. Half-duplex

c. Full-duplex

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

https://www.tutorialspoint.com/data_communication_computer_network/index.htm

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

Book: Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012 **(Page No : 2 - 4)**

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 04

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **I - Network Fundamentals**

Date of Lecture: 25.02.2021

Topic of Lecture: Data Transmission Concepts and Terminology

Introduction :

- It refers to the direction of information flow between two devices.
- Transmission media may be classified as guided or unguided.
- Communication is in the form of electromagnetic waves.
- The waves are guided along a physical path; examples of guided media are twisted pair, coaxial cable, and optical fiber.
- Data Transmission occurs between Sender and Receiver over some Transmission Medium.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Medium
- Data communication
- Message
- Information
- Network

Detailed content of the Lecture:

Data Transmission are the exchange of data between two devices via some form of transmission medium such as a wire cable.

Characteristics:

- The effectiveness of a data communications system depends on four fundamentalcharacteristics:

Delivery:

- The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

Accuracy:

- The system must deliver data accurately.

Timeliness:

- The system must deliver data in a timely manner. In the case of video and audio, timely delivery means delivering the data as they are produced. In the same order, that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

Jitter:

- Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packet.

Transmission Media may be classified into Two Types :

i) Guided Media [Wired Technology]
ii) Unguided Media [Wireless Technology]

i) Guided Media (Wired Network)

In Guided Media Signals are Passed in a " same physical path"

Example:

i) Twisted pair Cable
ii) Coaxial Cable
iii) Fiber Optic Cable

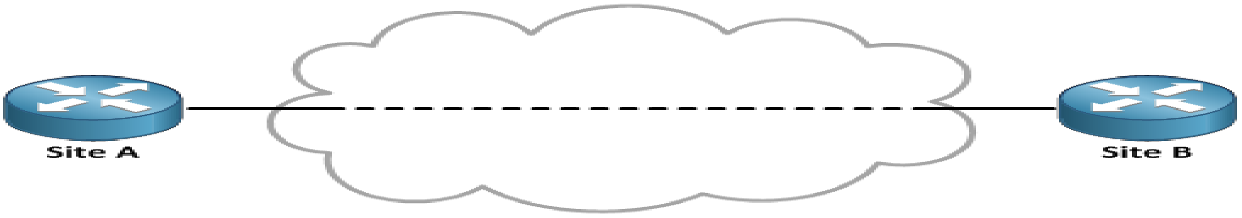
ii) Unguided Media (Wireless Network)

In Unguided Media Signals are Passed in the form of " Electromagnetic Waves"

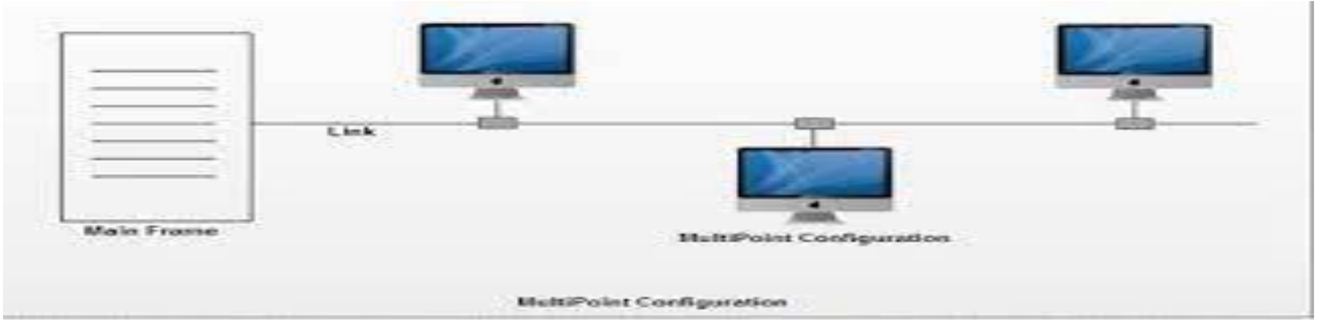
Example :

i) Mobile phones
ii) Satellite microwave
iii) Infrared

Point - to - Point Connection : It Provides a dedicated links between two devices.
For example, a wired system that connects two computers together can be thought of a point-to-point link.



Multi - Point Connection : It is a link between two or more devices. It is also known as Multi-Point configuration. The networks having multipoint configuration are called Broadcast Networks.



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

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

Book: Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012 **(Page No : 21 - 22)**

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 05

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **I - Network Fundamentals**

Date of Lecture: 26.02.2021

Topic of Lecture: Protocol Architecture

Introduction :

- It is a layered structure ofH/W and S/W that supports exchange of data b/w systems
- It supports distributed applications(E-Mail, File Transfer)
- Each layer of protocol architecture provides some set of rules
- it is model for understanding and designing a network architecture that is flexible, robust and interoperable.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Data Transmission
- Transmission Mode
- Internet
- Transmission Media

Detailed content of the Lecture:

There are 2 widely used protocol architecture

- **TCP/IP Architecture**
- **OSI Model**

Protocol is a set of rules that govern data communication

It represents what is communicated, when it is communicated and how it is communicated.

There are 3 key elements

- **Syntax**
- **Semantics**
- **Timing**

Syntax : It represents structure, Format of data the order in which it is presented

Data may contain:

First 8 bit -> Sender Address

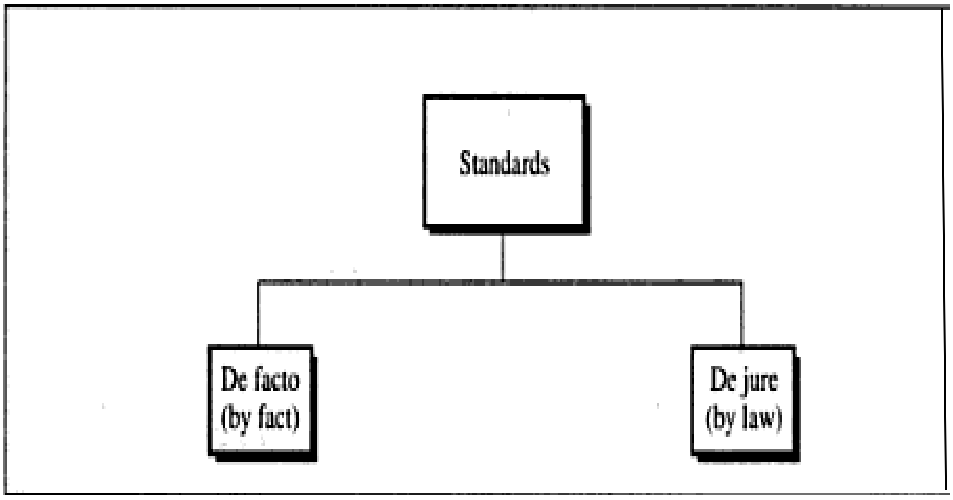
Second 8 bit -> Receiver Address

Remaining bits-> message stream

Semantics : It refers the meaning of each section of bit
Timing : It refers when data sent and how fast it is sent (Says Characteristics)

Ex:100Mbps

Protocol Standards :
It provides model for the development of product regardless of   individual manufacturer
It falls in 2 categories



- **De Facto standard**

Not officially adopted but used widespread
It has 2 categories
Proprietary->Wholly owned by company
Non-Proprietary->Group or communiy developed for public

- **De Jure Standard**

A Standard Legislated by an officially recognized body

Standard Organizations:

- **International Standard Organization**
- **ANSI**
- **IEEE**

Video Content / Details of website for further learning (if any):
https://webstor.srmist.edu.in/web_assets/srm_mainsite/files/files/Protocols%20and%20Architecture.pdf

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

Book: Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012 **(Page No : 7 - 9)**

Course Faculty

Verified by HOD

LECTURE HANDOUTS

MCA **I / II**

Course Name with Code	**: Data Communication And Networks / 19CAB09**
Course Faculty	**: Mr. S.Nithyananth**
Unit	**: I - Network Fundamentals**

Date of Lecture: 01.03.2021

Topic of Lecture: OSI Model

Introduction :

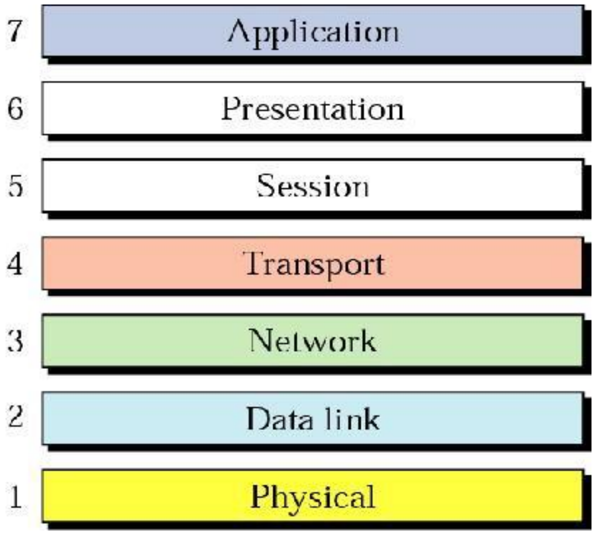
- Computer networks are created by different entities. Standards are needed so that these heterogeneous networks can communicate with one another. The two best-known standards are the OSI model and the Internet model.
- The OSI (Open Systems Interconnection) model defines a seven-layer network.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Computer
- Network Models
- Network Communication
- Topology
- Internet

Detailed content of the Lecture:

Layers in the OSI Model:



Physical Layer

- The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium.

Data Link Layer

- The data link layer transforms the physical layer, a raw transmission facility, to a reliable link.
- **The data link layer is responsible for moving frames from one hop (node) to the next.**

Network Layer:

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Transport layer:

- The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host.
- The transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source to-destination level.
- **The transport layer is responsible for the delivery of a message from one process toanother.**

Session Layer:

The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.

The session layer is responsible for dialog control and synchronization.

Presentation Layer:

- The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.
- **The presentation layer is responsible for translation, compression, and encryption.**

Application Layer:

- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.
- **The application layer is responsible for providing services to the user.**

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

https://www.tutorialspoint.com/data_communication_computer_network/ physical_layer_introduction.htm

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

Book: Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012 **(Page No : 43 - 55)**

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

MCA **I / II**

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **I - Network Fundamentals**

Date of Lecture: 02.03.2021

Topic of Lecture: TCP/IP

Introduction :

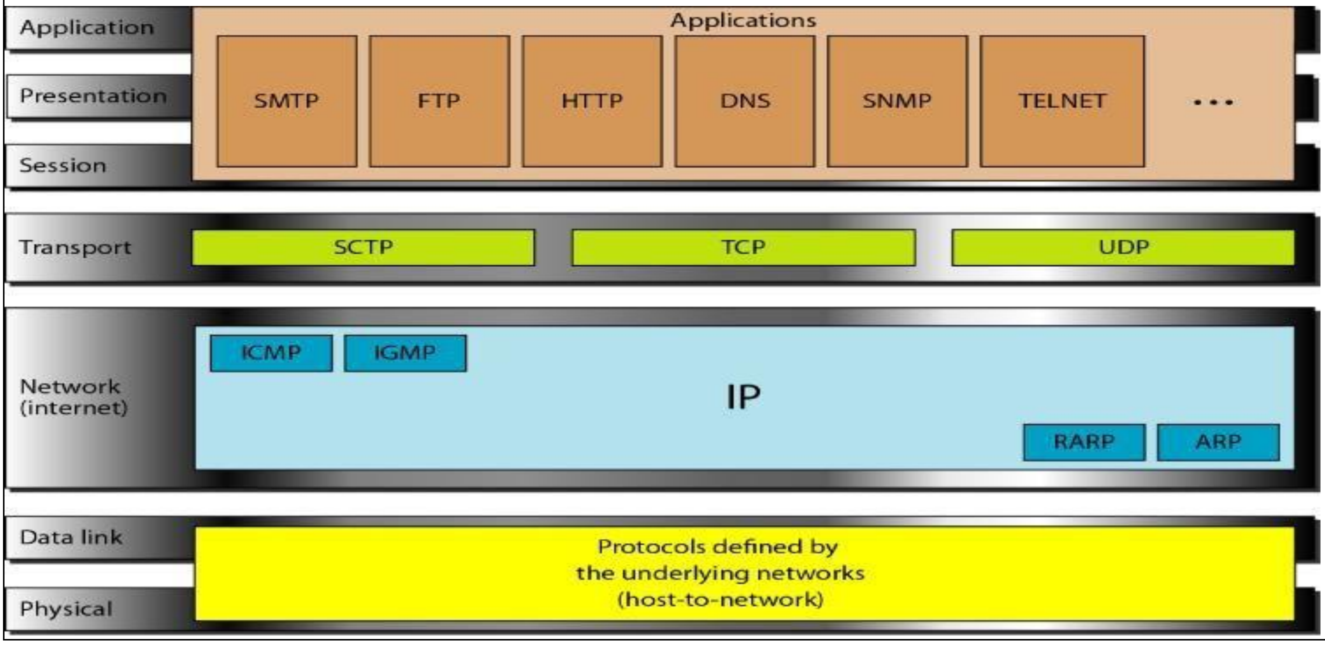
- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Computer
- Network Models
- Network Communication
- Topology
- OSI Model

Detailed content of the Lecture:

TCP/IP PROTOCOL



The TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces,
Inter-networking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer

Physical and Data Link Layers:

- At the physical and data link layers, TCP/IP does not define any specific protocol.
- It supports all the standard and proprietary protocols. A network in a TCP/IP internetwork can be alocal-area network or a wide-area network.

Network Layer:

- At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP, in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

Transport Layer:

- Traditionally the transport layer was represented in TCP/IP by two protocols:
- TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process. A new transport layer protocol, SCTP, hasbeen devised to meet the needs of some newer applications.

a. User Datagram Protocol

- The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

b. Transmission Control Protocol

- The Transmission Control Protocol (TCP) provides full transport-layer services to applications.
- TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

c. Stream Control Transmission Protocol

- The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.

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

https://www.javatpoint.com/computer-network-tcp-ip-model

Important Books/Journals for further learning including the page nos.:
Book: Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 56 - 57)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 08

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **I - Network Fundamentals**

Date of Lecture: 03.03.2021

Topic of Lecture: LAN Topology

Introduction :

- Protocols refer to the rules; a standard is a protocol that has been adopted by vendors and manufacturers. Network models serve to organize, unify, and control the hardware and software components of data communications and networking.

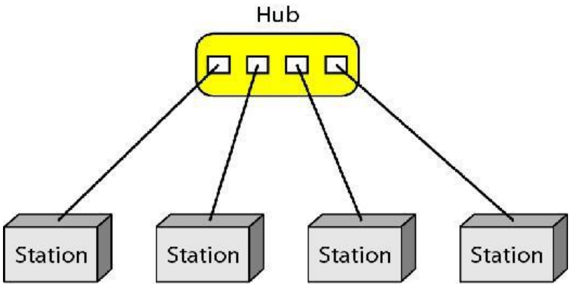
Prerequisite knowledge for Complete understanding and learning of Topic:

- Computer
- Telecommunication
- Data Communication
- Message
- Internet

Detailed content of the Lecture:

Physical Topology:

- The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
- There are four basic topologies possible: mesh, star, bus, and ring



Mesh Topology

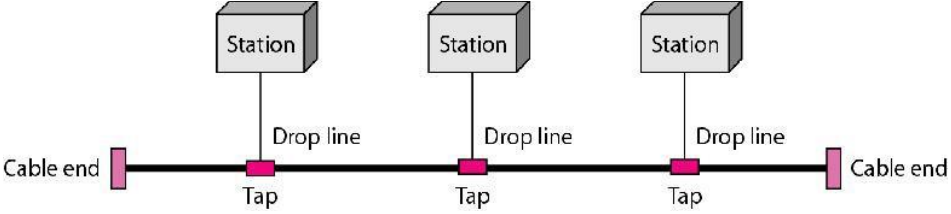
- In a mesh topology, every device has a dedicated point-to-point link to every other device. A fully connected mesh network with n nodes has n(n -1) /2 physical channels.
- To accommodate that many links, every device on the network must have n – 1 input/output(I/O) ports to be connected to the other n – 1 stations.

Star Topology:

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub.
- The devices are not directly linked to one another. Unlike a mesh topology, A star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

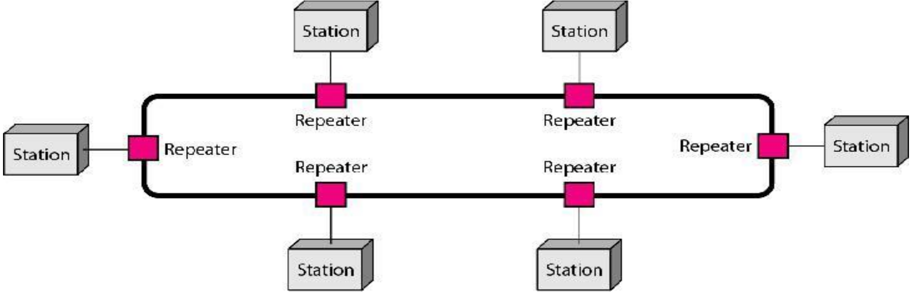
Bus Topology:

- A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network (see Figure 1.7). Nodes are connected to the bus cable by drop lines andtaps.

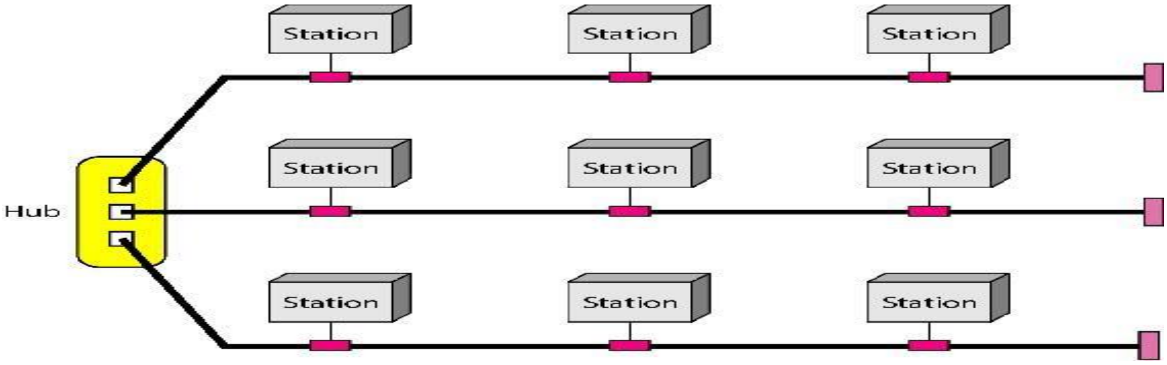


Ring Topology:

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater.



Hybrid Topology: A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology



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.:

Book: Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012 **(Page No : 22 - 28)**

Course Faculty

Verified by HOD

L 09

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **I - Network Fundamentals**

Date of Lecture: 04.03.2021

Topic of Lecture: Transmission Media

Introduction :

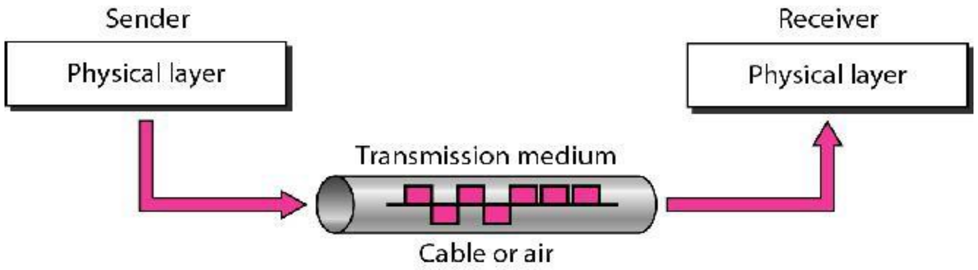
- Transmission media are actually located below the physical layer and are directly controlled by the physical layer.
- A transmission medium can be broadly defined as anything that can carry information from a source to a destination.

Prerequisite knowledge for Complete understanding and learning of Topic:

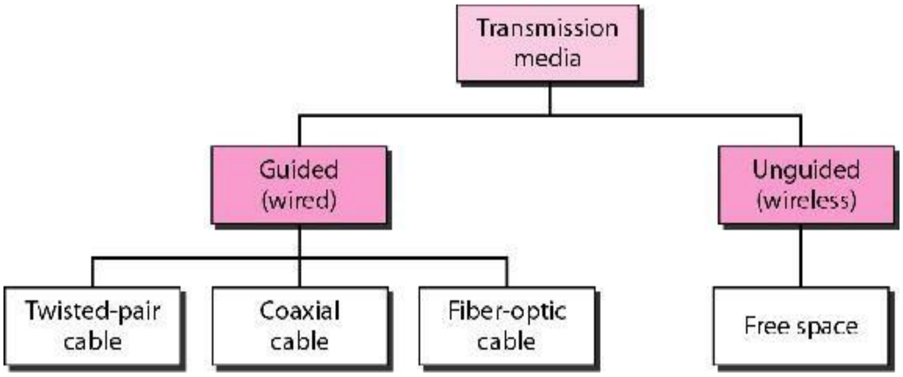
- Computer
- Network Models
- Network Communication
- Physical Medium

Detailed content of the Lecture:

Transmission media:



- In telecommunications, transmission media can be divided into two broad categories:
- guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-opticcable. Unguided medium is free space.

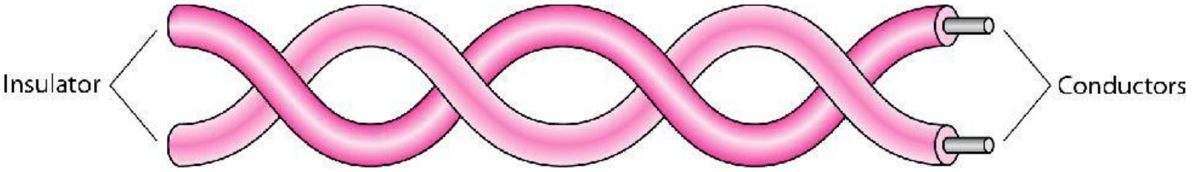


Guided media:

- Guided media, which are those that provide a conduit from one device to another, include twisted-paircable, coaxial cable, and fiber-optic cable.
- A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

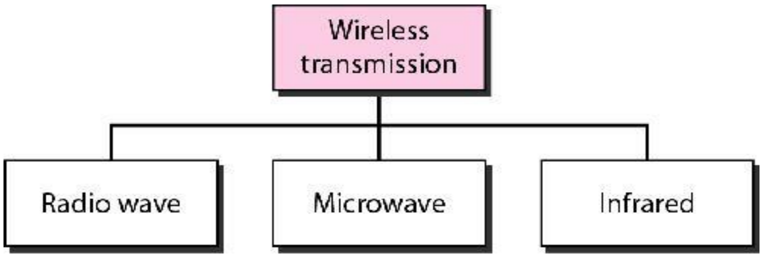
Twisted-Pair Cable

- A twisted pair consists of two conductors (normally copper), each with its own plastic insulation,twisted together.
- One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference.



Unguided media:

Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation



Radio Waves:

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves; waves ranging in frequencies between 1 and 300 GHz are called microwaves. Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions.

Microwaves

Electromagnetic waves having frequencies between I and 300 GHz are called Microwaves. Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowlyfocused.

Infrared:

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls.

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

https://www.javatpoint.com/transmission-media
https://www.javatpoint.com/unguided-transmission-media

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

Book: Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012 **(Page No : 188-206**

Course Faculty

Verified by HOD

L 10

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **II - Data Link Layer**

Date of Lecture: 05.03.2021

Topic of Lecture: Data link control

Introduction :

- The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as data link control.
- low control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.

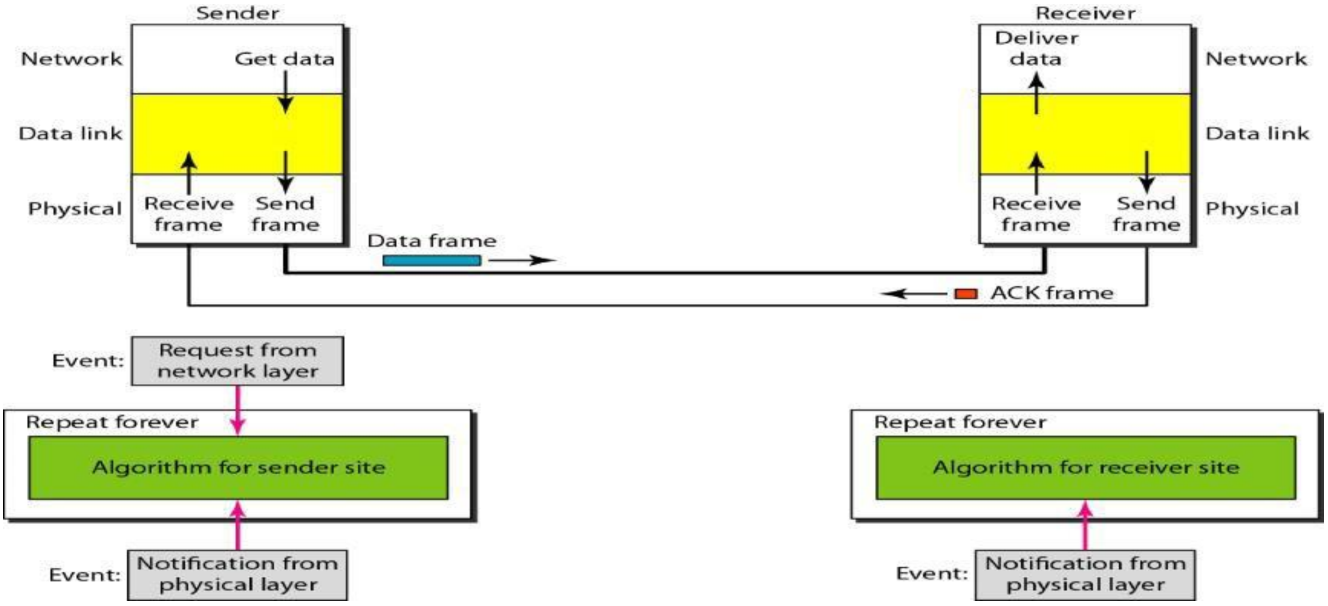
Prerequisite knowledge for Complete understanding and learning of Topic:

- Physical Layer
- Data Link layer
- Framing
- Simple Protocols

Detailed content of the Lecture:

Stop-and-Wait Protocol

- If data frames arrive at the receiver site faster than they can be processed, the frames must be storeduntil their use.
- In Stop-and-Wait Protocol the sender sends one frame, stops until it receives confirmation from thereceiver (okay to go ahead), and then sends the next frame.

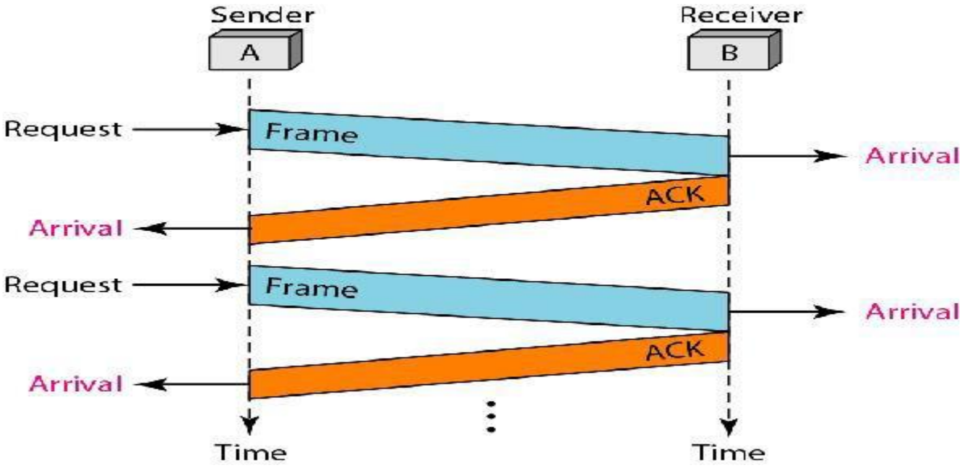


Design

- Comparing this figure with Figure 2.6, we can see the traffic on the forward channel (from sender to receiver) and the reverse channel.
- At any time, there is either one data frame on the forward channel or one ACK frame on the reverse channel. We therefore need a half-duplex link.

Example

- It shows an example of communication using this protocol. It is still very simple. The sender sends one frame and waits for feedback from the receiver.
- When the ACK arrives, the sender sends the next frame. Note that sending two frames in the protocol involves the sender in four events and the receiver in two events.



Sliding Window

In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

High-level Data Link Control

a. Normal Response Mode

In normal response mode (NRM), the station configuration is unbalanced. We have one primary station and multiple secondary stations. A primary station can send commands; a secondary station can only respond. The NRM is used for both point-to-point and multiple-point links.

b. Asynchronous Balanced Mode

In asynchronous balanced mode (ABM), the configuration is balanced. The link is point-to- point, and each station can function as a primary and a secondary (acting as peers). This is the common mode today.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/error-detection-in-computer-networks/

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 301 - 304)

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

L 11

LECTURE HANDOUTS

MCA **I / II**

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **II - Data Link Layer**

Date of Lecture: 06.03.2021

Topic of Lecture: Error Detection,VRC, LRC, CRC & Checksum

Introduction :

- Error detection is the detection of errors caused by noise or other impairments during transmission from the transmitter to the receiver. Error correction is the detection of errors and reconstruction of the original, error-free data.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Data Link layer
- Data Link Control
- Framing
- Sliding Window Protocols

Detailed content of the Lecture:

Framing

- source to the destination. The physical layer provides bit synchronization to ensure that the sender andreceiver use the same bit duration and timing.

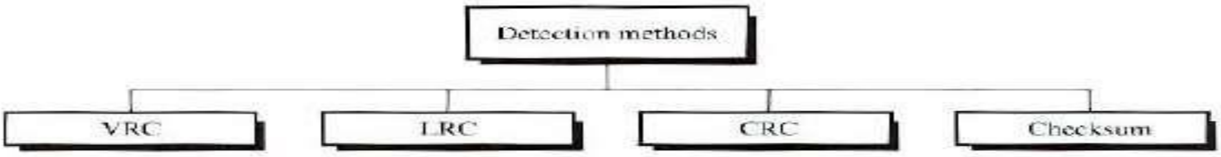
Fixed size Framing:

- Frames can be of fixed or variable size. In fixed-size framing, there is no need for defining the boundariesof the frames; the size itself can be used as a delimiter.

Variable-Size Framing

- In variable-size framing, we need a way to define the end of the frame and the beginning of the next. Historically, two approaches were used for this purpose: a character-oriented approach and a bit-orientedapproach.

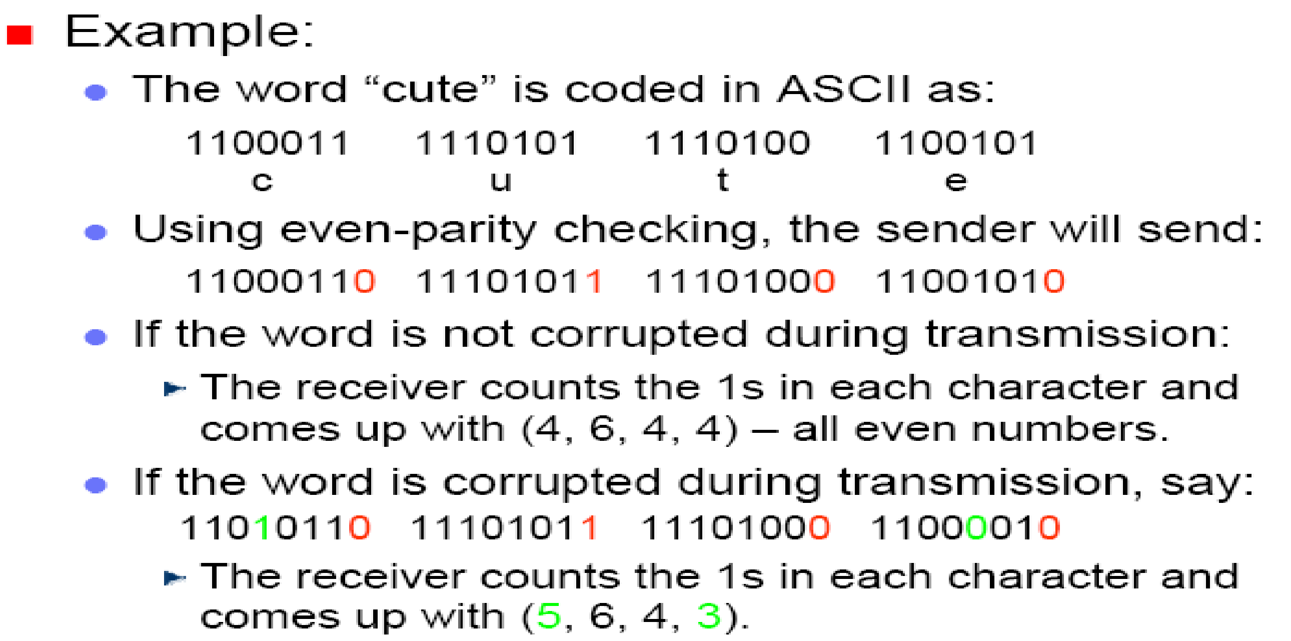
■ Four types of redundancy checks:



- VRC: vertical redundancy check or parity check
- LRC: longitudinal redundancy check
- CRC: cyclic redundancy check
- VRC, LRC, CRC used by data link layers.
- Checksum used by higher-layer protocols.

a. Character-Oriented Protocols

- In a character-oriented protocol, data to be carried are 8-bit characters from a coding system such as ASCII. The header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection or error correction redundant bits, are also multiples of 8 bits.



- Example:
  - The word “cute” is coded in ASCII as:

1100011	1110101	1110100	1100101
c	u	t	e

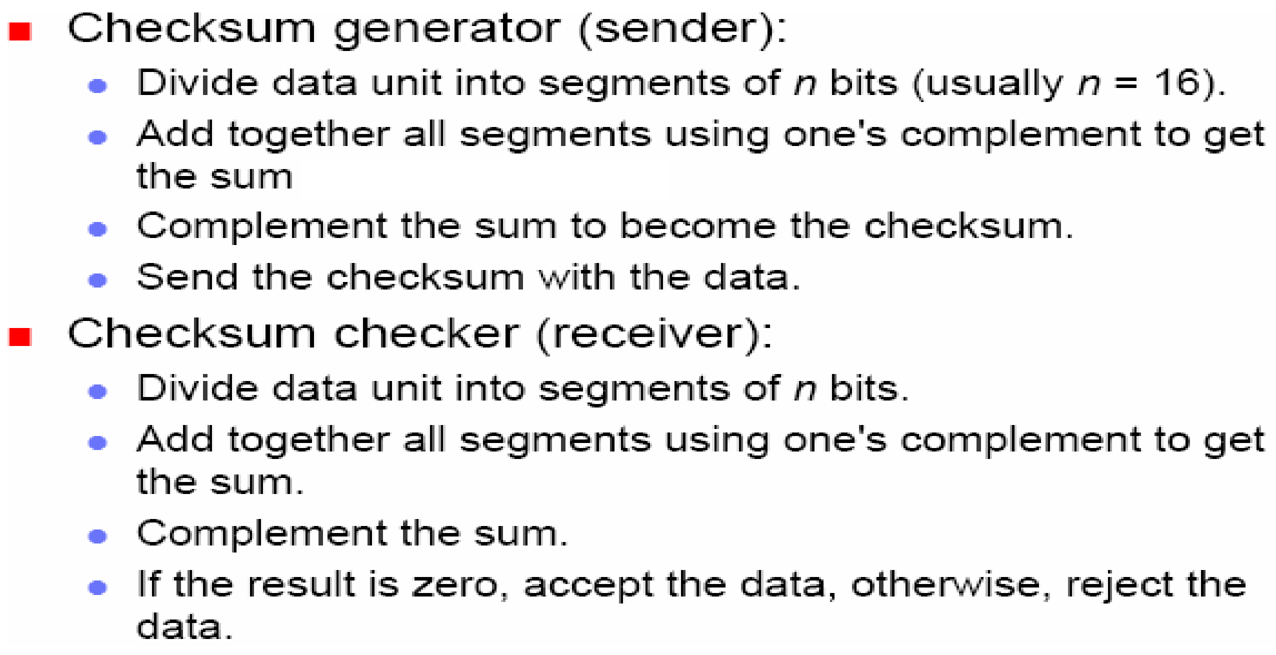
  - Using even-parity checking, the sender will send:

    11000110 11101011 11101000 11001010

  - If the word is not corrupted during transmission:
    - The receiver counts the 1s in each character and comes up with (4, 6, 4, 4) – all even numbers.
  - If the word is corrupted during transmission, say:

    11010110 11101011 11101000 11000010

    - The receiver counts the 1s in each character and comes up with (5, 6, 4, 3).



- Checksum generator (sender):
  - Divide data unit into segments of *n* bits (usually *n* = 16).
  - Add together all segments using one's complement to get the sum
  - Complement the sum to become the checksum.
  - Send the checksum with the data.
- Checksum checker (receiver):
  - Divide data unit into segments of *n* bits.
  - Add together all segments using one's complement to get the sum.
  - Complement the sum.
  - If the result is zero, accept the data, otherwise, reject the data.

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

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 273 - 284)

Course Faculty

Verified by HOD

L 12

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **II - Data Link Layer**

Date of Lecture: 08.03.2021

Topic of Lecture: Error Correction & Hamming Codes

Introduction :

- Error correction is the process of detecting errors in transmitted messages and reconstructing the original error-free data.
- Error correction ensures that corrected and error-free messages are obtained at the receiver side.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Error Detection
- Data Link layer
- Framing
- Protocol

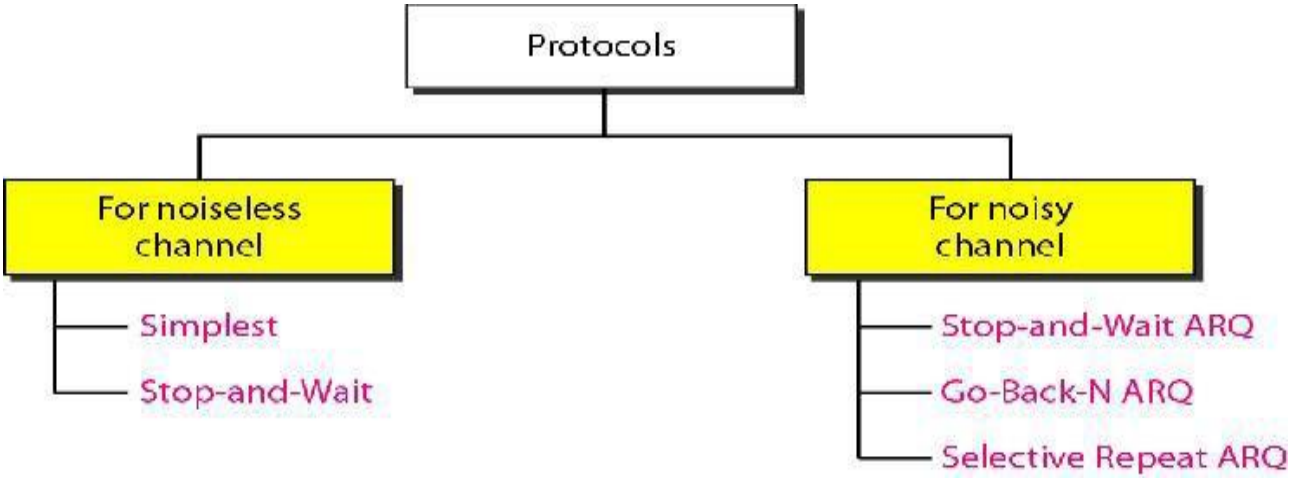
s

Detailed content of the Lecture:

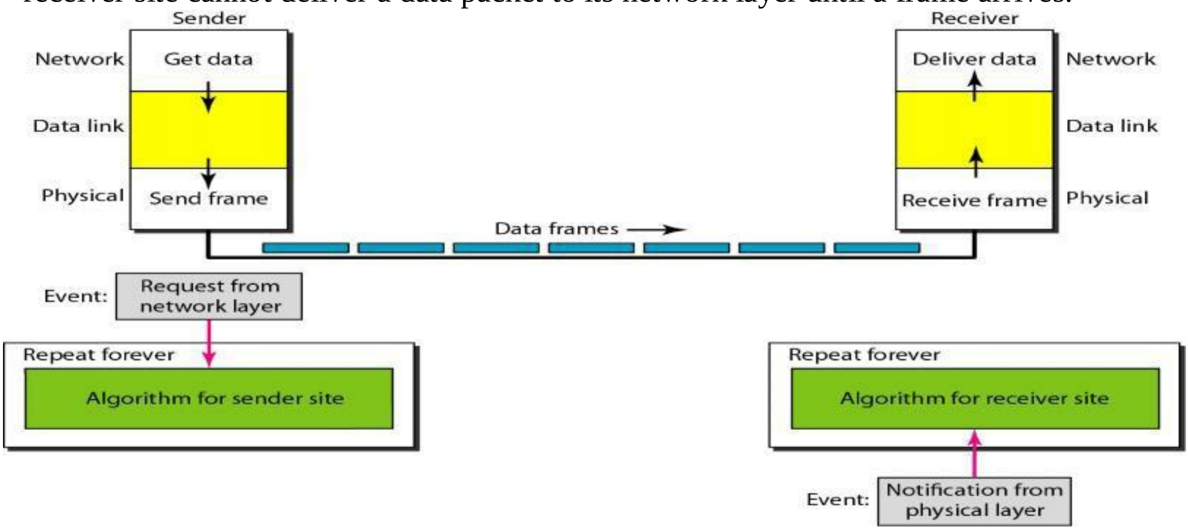
Error Control

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender.

- The most important responsibilities of the data link layer are flow control and error control.Collectively, these functions are known as data link control.
- low control refers to a set of procedures used to restrict the amount of data that the sender can sendbefore waiting for acknowledgment.



- The sender site cannot send a frame until its network layer has a data packet to send. The receiver site cannot deliver a data packet to its network layer until a frame arrives.



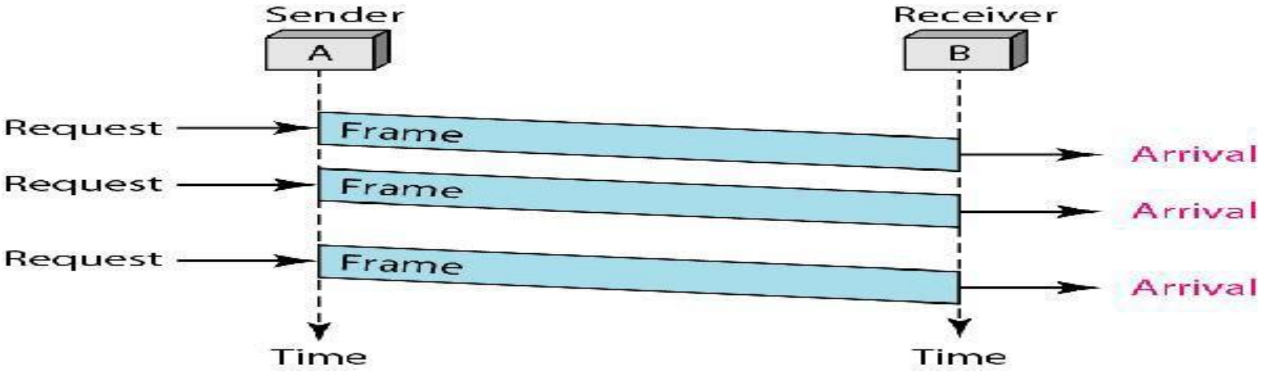
- If the protocol is implemented as a procedure, we need to introduce the idea of events in the protocol. The procedure at the sender site is constantly running; there is no action until there is a request from the network layer. The procedure at the receiver site is also constantly running, but there is no action until notification from the physical layer arrives

Example :

- It is very simple. The sender sends a sequence of frames without even thinking about the receiver. To send three frames, three events occur at the sender site and three events at the receiver site. Note that the data frames are shown by tilted boxes; the height of the box defines the transmission time difference between the first bit and the last bit in the frame.

Hamming Codes-Error correction :

- Hamming codes, like polynomial codes, are appended to the transmitted message.
- Hamming codes, unlike polynomial codes, contain the information necessary to locate a single bit error.



Video Content / Details of website for further learning (if any):
hhttps://www.geeksforgeeks.org/error-detection-in-computer-networks/

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 287 - 291)

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

L 13

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **II - Data Link Layer**

Date of Lecture: 09.03.2021

Topic of Lecture: MAC

Introduction :

- It resolves the contention of shared media
- It contains all information to move information from one place to another
- It contains the physical address of next station to route packet.
- MAC protocol are specific to LAN

Prerequisite knowledge for Complete understanding and learning of Topic:

- Data Link layer
- Noiseless Channel
- Noisy Channel
- HDLC

Detailed content of the Lecture:

ALOHA

It was designed for a radio (wireless) LAN, but it can be used on any shared medium.

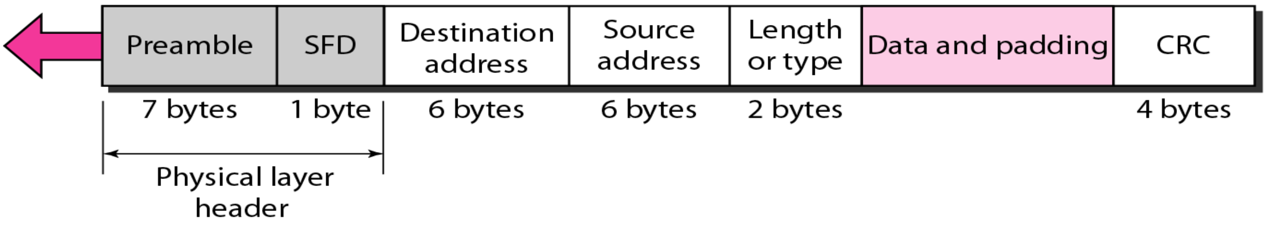
It is obvious that there are potential collisions in this arrangement. The medium is shared between the stations. When a station sends data, another station may attempt to do so at the same time. The data from the two stations collide and become garbled.

Pure ALOHA

The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send. However, since there is only one channel to share, there is the possibility of collision between frames from different stations.

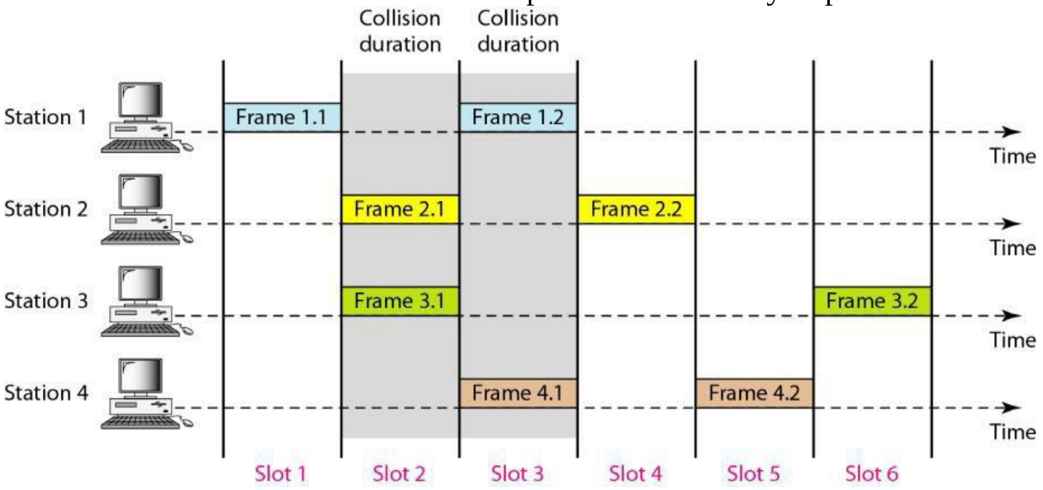
Preamble: 56 bits of alternating 1s and 0s.

SFD: Start frame delimiter, flag (10101011)



Slotted ALOHA

Pure ALOHA has a vulnerable time of 2 x Tfr . This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished. Slotted ALOHA was invented to improve the efficiency of pure ALOHA.



Carrier Sense Multiple Access (CSMA)

To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending.

The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it. In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision. In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

In a wired network, the received signal has almost the same energy as the sent signal because either the length of the cable is short or there are repeaters that amplify the energy between the sender and the receiver. This means that in a collision, the detected energy almost doubles. However, in a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy.invented for this network.Collisions are avoided through the use of CSMA/CA's three strategies: the inter frame space, thecontention window, and acknowledgments.

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

https://www.tutorialspoint.com/medium-access-control-sublayer-mac-sublayer

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012

(Page No : 373 - 374)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 14

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **II - Data Link Layer**

Date of Lecture: 10.03.2021

Topic of Lecture: Ethernet

Introduction :

- The LAN market has seen several technologies such as Ethernet, Token Ring, Token Bus, FDDI and ATM LAN. Ethernet has gone through a four-generation evolution during the last few decades, the main concept has remained. Ethernet has changed to meet the market needs and to make use of the newtechnologies.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Data Link layer
- HDLC
- PPP
- Media Access Control Layer

Detailed content of the Lecture:

Standard Ethernet

The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC).Since then, it has gone through four generations:

a. Standard Ethernet (l0 Mbps), b. Fast Ethernet (100 Mbps),
c. Gigabit Ethernet (l Gbps) d. Ten-Gigabit Ethernet (l0 Gbps)

Changes In the Standard

- The 10-Mbps Standard Ethernet has gone through several changes before moving to the higher data rates. These changes actually opened the road to the evolution of the Ethernet to become compatible with otherhigh-data-rate LANs.

Bridged Ethernet

- The first step in the Ethernet evolution was the division of a LAN by bridges. Bridges have two effectson an Ethernet LAN: They raise the bandwidth and they separate collision domains.

Raising the Bandwidth

- In an unbridled Ethernet network, the total capacity (10 Mbps) is shared among all stations with a frame to send; the stations share the bandwidth of the network.
- If only one station has frames to send, it benefits from the total capacity (10 Mbps). But if more than one station needs to use the network, the capacity is shared. For example, if two stations have a lot of frames to send, they probably alternate in usage. When one station is sending, the other one refrains from sending.

Switched Ethernet

- The idea of a bridged LAN can be extended to a switched LAN.
- Instead of having two to four networks. The bandwidth is shared only between the station and the switch (5 Mbps each). In addition, the collision domain is divided into *N* domains.
- A layer 2 switch is an *N-port* bridge with additional sophistication that allows faster handling of the packets. Evolution from a bridged Ethernet to a switched Ethernet was a big step that opened the way to an even faster Ethernet.

Full-Duplex Ethernet

- One of the limitations of 10Base5 and l0Base2 is that communication is half-duplex, a station can either send or receive, but may not do both at the same time.
- The next step in the evolution was to move from switched Ethernet to full-duplex switched Ethernet. The full-duplex mode increases thecapacity of each domain from 10 to 20 Mbps.

Fast Ethernet

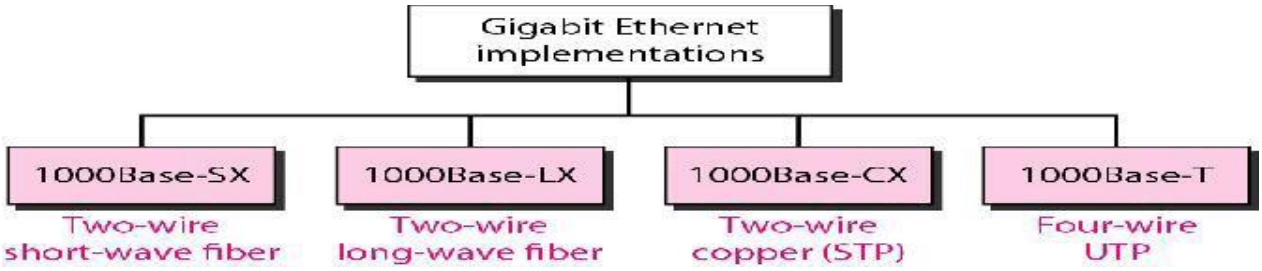
- Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel. IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward- compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps. The goals of Fast Ethernet canbe summarized as follows:

1. Upgrade the data rate to 100 Mbps.
2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bit address.
4. Keep the same frame format.
5. Keep the same minimum and maximum frame lengths.

Gigabit Ethernet

- The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z. The goals of the Gigabit Ethernet design can besummarized as follows:

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. To support auto negotiation as defined in Fast Ethernet.



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

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 372 - 376)

Course Faculty

Verified by HOD

L 15

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **II - Data Link Layer**

Date of Lecture: 11.03.2021

Topic of Lecture: Token ring & Token Bus

Introduction :

- Token Ring allows each station to sent one frame. .
- The access control mechanism used by Ethernet is inefficient sometimes because of collision.
- Token Bus combines the feature of token ring and Ethernet.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Ethernet
- Standard Ethernet
- Framing
- Fast Ethernet

Detailed content of the Lecture:

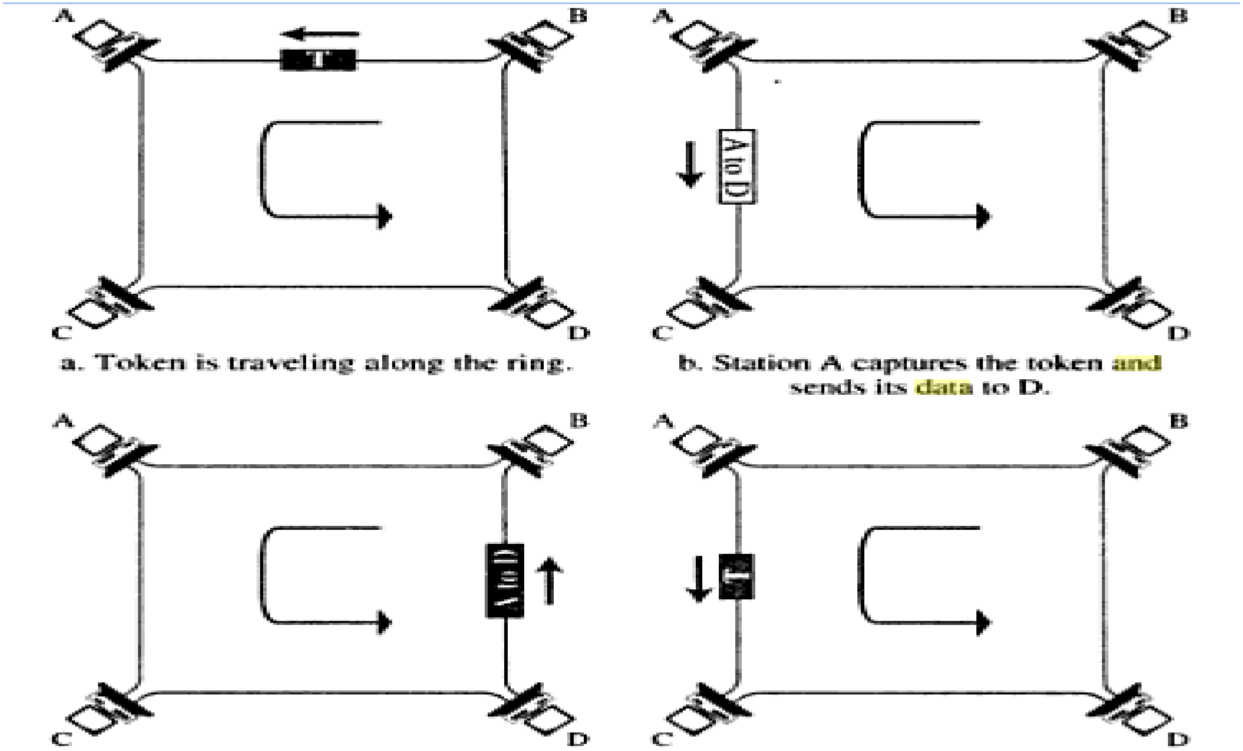
Token Ring :

- The access control mechanism used by Ethernet is inefficient sometimes because of collision.
- It solves the collision problem by passing token.
- Initially a station waits for token, if a token is free the station may send a data frame.
- This frame proceeds around the ring ,being regenerated by each station .Each station examines the destination address finds the frame is addressed to another station and relays it to its neighbor.
- The intended recipient recognizes its own address and copies the message and set the address bit
- The token finally reach the sender and it recognizes that the data is delivered through address bit
- Token is passed from NIC to NIC.
- local area network protocol standardized by ANSI.
- 100-Mbps token passing.
- Dual-ring LAN.
- A high-speed backbone technology.
- High bandwidth.
- Optical fiber transmission.
- Allows up to 1000 stations.

Token Bus :

- It combines the feature of token ring and Ethernet.

Token Ring :



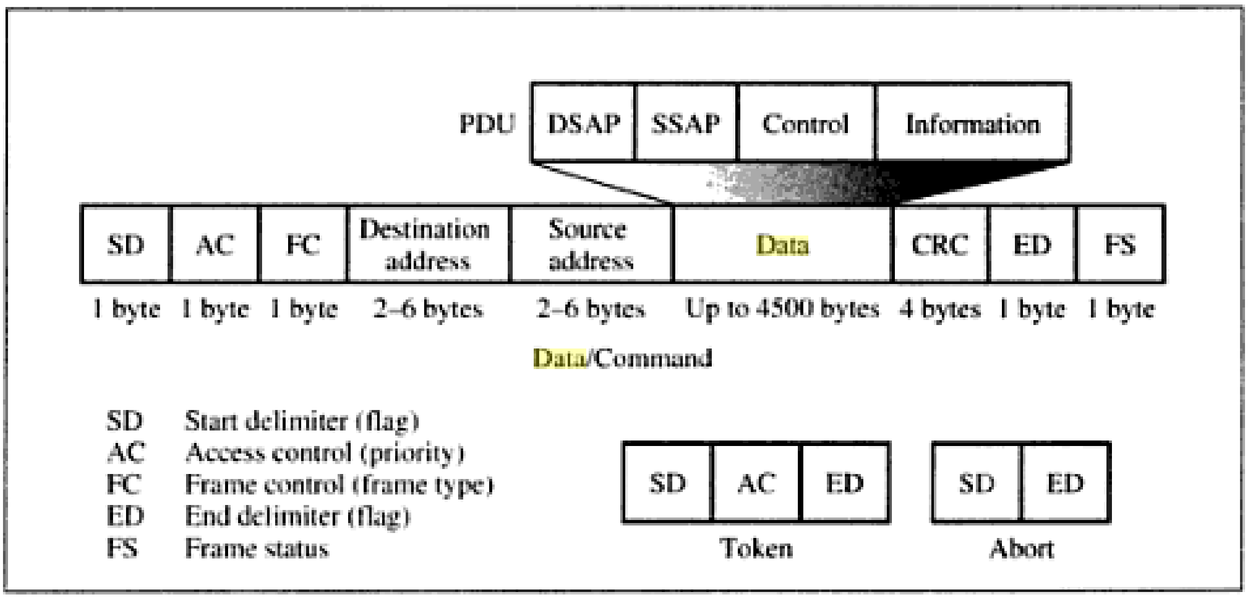
a. Token is traveling along the ring.

b. Station A captures the token and sends its data to D.

c. Station D copies the frame and sends the data back to the ring.

d. Station A receives the frame and releases the token.

Figure 12.22 *Token Ring frame*



PDU	DSAP	SSAP	Control	Information

SD	AC	FC	Destination address	Source address	Data	CRC	ED	FS
1 byte	1 byte	1 byte	2–6 bytes	2–6 bytes	Up to 4500 bytes	4 bytes	1 byte	1 byte

Data/Command

SD	Start delimiter (flag)
AC	Access control (priority)
FC	Frame control (frame type)
ED	End delimiter (flag)
FS	Frame status

SD	AC	ED

Token

SD	ED

Abort

Video Content / Details of website for further learning (if any):
https://www.ibm.com/docs/en/i/7.3?topic=standards-token-ring-networks

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 385 - 392)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 16

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **II - Data Link Layer**

Date of Lecture: 12.03.2021

Topic of Lecture: Wireless LAN

Introduction :

- LANs provide connectivity for interconnecting computing resources at the local levels of an organization.
- Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Data Link layer
- HDLC
- Media Access Control Layer
- Ethernet
- Token Ring

Detailed content of the Lecture:

Wireless LANs provide :

- Flexibility
- Portability
- Mobility
- Ease of Installation

Wireless LAN Applications :

- Medical Professionals
- Education
- Temporary Situations
- Airlines
- Security Staff
- Emergency Centers

IEEE 802.11

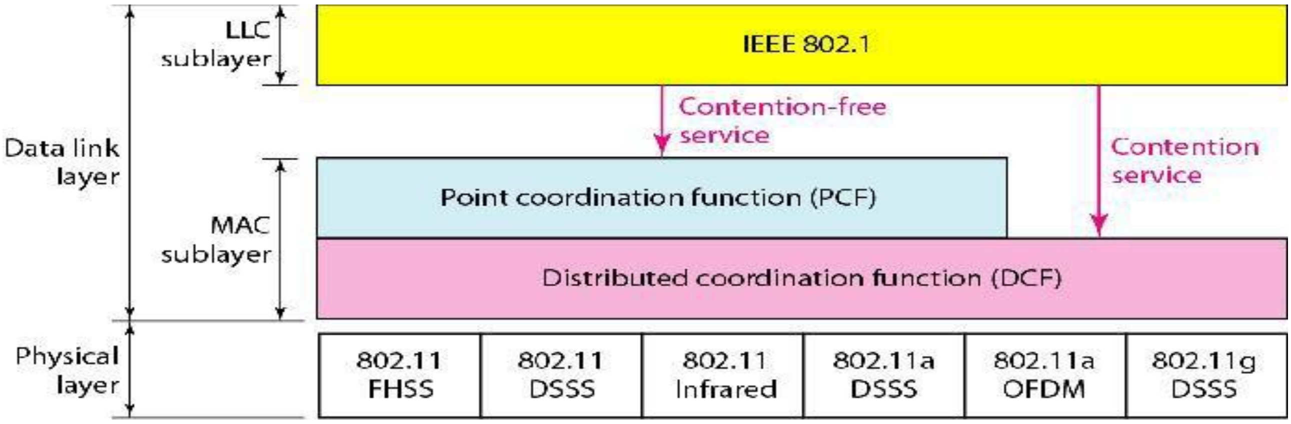
IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical anddata link layers.

Architecture: The standard defines two kinds of services: the basic service set (BSS) and the extendedservice set (ESS).

Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, knownas the access point (AP).

The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.



Benefits of 802.11 Standard :

- Appliance Interoperability
- Fast Product Development
- Stable Future Migration
- Price Reductions
- The 802.11 standard takes into account the following significant differences between wireless and wired LANs:
- Power Management
- Security
- Bandwidth

IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN:

- No-transition
- A station is either stationary (not moving) or moving only inside a BSS
- BSS- Transition station can move from one BSS to another, but the movement is confined inside one ESS.and ESS- transition mobility.A station can move from one ESS to another.

Video Content / Details of website for further learning (if any):
https://www.coursera.org/lecture/iot-wireless-cloud-computing/4-3-wi-fi-standards-part-1-QmD20

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 393 - 395)

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

L 17

LECTURE HANDOUTS

MCA **I / II**

Course Name with Code : Data Communication And Networks / 19CAB09

Course Faculty : Mr. S.Nithyananth

Unit : II - Data Link Layer

Date of Lecture: 13.03.2021

Topic of Lecture: Bluetooth

Introduction :

- Bluetooth is a wireless LAN technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, coffee makers, and so on.
- A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously; the devices, sometimes called gadgets, find each other and make a network called a piconet.

Prerequisite knowledge for Complete understanding and learning of Topic:

- HDLC
- Media Access Control Layer
- Ethernet
- Token Ring
- Wireless LAN

Detailed content of the Lecture:

- Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard. The standard defines a wireless personal-area network (PAN) operable in an area the size of a room or ahall.

Architecture

- Bluetooth defines two types of networks: piconet and scatternet.

Piconets

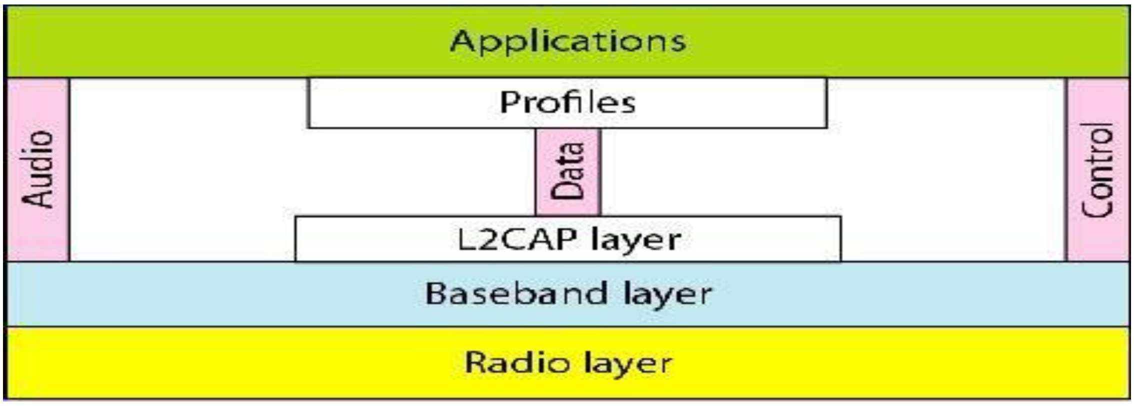
- A Bluetooth network is called a piconet, or a small net. A piconet can have up to eight stations, one of which is called the primary, the rest are called secondaries.
- All the secondary stations synchronize their clocks and hopping sequence with the primary. Note that a piconet can have only one primary station.
- The communication between the primary and the secondary can be one-to-one or one-to-many.

Scatternet

- Piconets can be combined to form what is called a scatternet.
- A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet (as a secondary) and, acting as a primary, deliver them to secondaries in the second piconet. A station can be a member of two piconets.

Radio Layer

- The radio layer is roughly equivalent to the physical layer of the Internet model. Bluetooth devices are low-power and have a range of 10 m.



Base band Layer :

- The base band layer is roughly equivalent to the MAC sublayer in LANs. The access method is TDMA.The primary and secondary communicate with each other using time slots.
- The length of a time slot is exactly the same as the dwell time, 625 µs. This means that during the time that one frequency is used, a sender sends a frame to a secondary, or a secondary sends a frame to the primary. Note that the communication is only between the primary and a secondary; secondaries cannot communicate directlywith one another.
- Synchronous connection-oriented (SCO)
- Latency is important than integrity.
- Transmission using slots.
- No retransmission.
- Asynchronous connectionless link (ACL)
- Integrity is important than latency.
- Does like multiple-slave communication.
- L2CAP (Logical Link Control and Adaptation Protocol)
- Equivalent to LLC sublayer in LANs.
- Used for data exchange on ACL Link. SCO channels do not use L2CAP.
- Frame format has 16-bit length [Size of data coming from upper layer in bytes], channel ID, data and control.

Video Content / Details of website for further learning (if any):
https://www.coursera.org/lecture/iot-wireless-cloud-computing/4-3-wi-fi-standards-part-1-QmD20

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

Book: Behrouz A. Foruzan, ‘Data communication & Networking’ – **(Page No : 434 - 438)**

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

L 18

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **II - Data Link Layer**

Date of Lecture: 15.03.2021

Topic of Lecture: Bridges

Introduction :

- A bridge is a structure built to span a physical obstacle without blocking the way underneath. It is constructed for the purpose of providing passage over.
- Divide a large network into smaller segment.
- It filters the traffic . It contains logic(Bridge table) that allows them to keep the traffic for each segment separate.

Prerequisite knowledge for Complete understanding and learning of Topic:

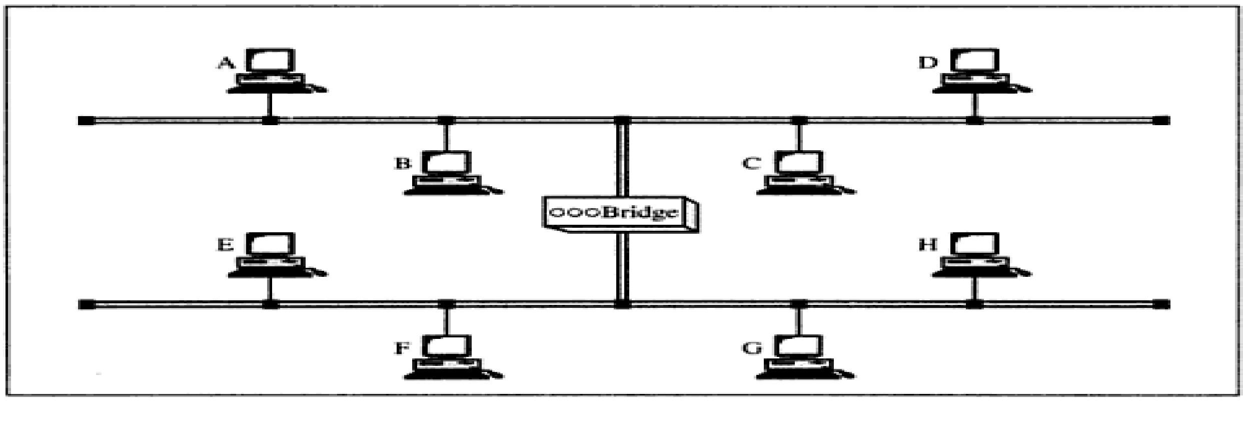
- Repeater
- Router
- Wireless LAN
- Framing
- Routing Protocols

Detailed content of the Lecture:

- Bridges are normally installed redundantly,that is two LANS may be connected by more than one bridge.in this cases they may create a loop.So packet may go round and round,It can be avoided by algorithms like Spannig tree algorithm and Source routing.
- A remote bridge takes the frame before it leaves the first LAN and encapsulates the WAN headers and trailers.
- When the packet arrives at the destination remote bridge, that bridge removes the WAN headers and trailers leaving the original frame.

Architecture :

Figure 21.7 *A bridge*



Types of Bridges :

1. **Simple Bridge**
2. **Multiport Bridge**
3. **Transparent Bridge**
4. **Remote Bridge**

Simple Bridge

- It is a less expensive type of bridge
- It links 2 segments (LANS) and lists the address of all the stations in table included in each of them.
- Here address must be entered manually.
- The table is modified when stations are added and removed.

Multiport Bridge

- It is used to connect more than two LANS.
- The bridge has 3 tables.Here address must be entered manually

Transparent Bridge

- A transparent or learning bridge builds its table of station on its own (automatically).
- The table is empty when it is installed, it builds its table when it encounters the packet for transmission. It uses the source address for building table.
- It identifies the changes and update the table when system moved from one station to another.

Remote Bridge

- A remote bridge is capable of passing a data frame from one local area network to another when the two LANs are separated by a long distance and there is a wide area network connecting the two LANs.
- A remote bridge takes the frame before it leaves the first LAN and encapsulates the WAN headers and trailers.
- When the packet arrives at the destination remote bridge, that bridge removes the WAN headers and trailers leaving the original frame.

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

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 616 - 620)

Course Faculty

Verified by HOD

L 19

LECTURE HANDOUTS

MCA **I / II**

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **III - Network Layer**

Date of Lecture: 16.03.2021

Topic of Lecture: Network layer & Switching concepts

Introduction :

- ➢ The Network layer is responsible for the source-to-destination delivery of a packet possible across multiple networks.
- ➢ It converts Frames into packets.
- ➢ Switches are needed to connect multiple devices for making one-one communication.

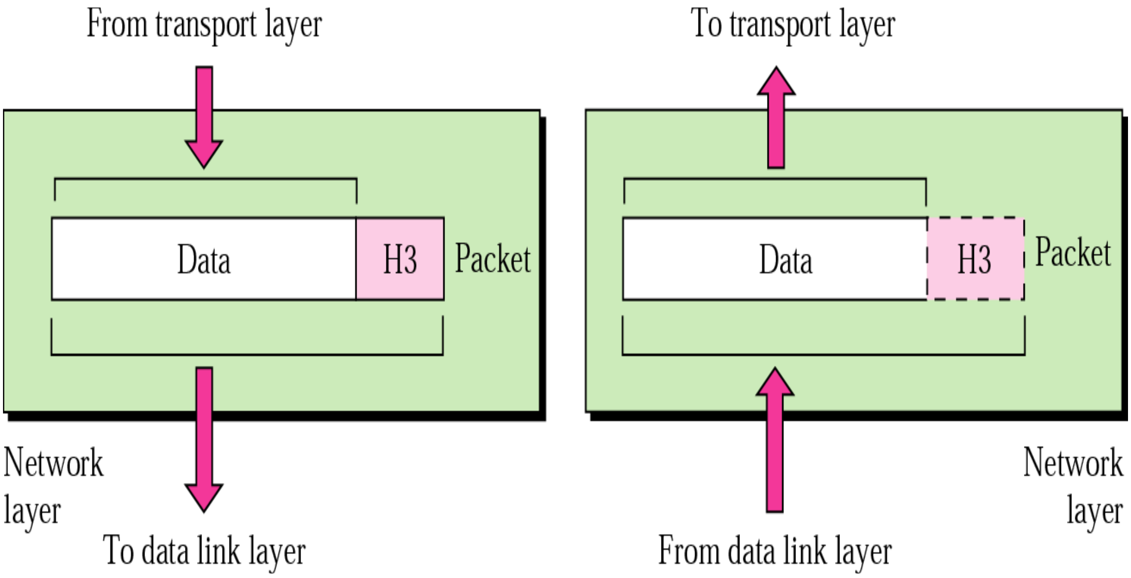
Prerequisite knowledge for Complete understanding and learning of Topic:

- Physical Layer
- Data Link layer
- Gateway
- Protocol Standards

Detailed content of the Lecture:

Network Layer Functions:

- Logical addressing-Physical addressing (May change) handle.
- Addressing problem locally.
- If packet pass the network boundary, we need another addressing called logical addressing (Never change).
- Routing - Route the packet to final destination.



Switching :

- Switches are hardware or software devices used for temporary connection b/w 2 or more devices linked to the switch in network but not to each another Switches are needed to connect multiple devices for making one-one communication.

1. **Source-to-Destination delivery of a packet**
2. **Logical addressing**
3. **Routing**
4. **Inter networking**

TYPES:

- **Circuit Switching**
- **Packet Switching**
- **Message Switching**

Figure 14.1 *Switched network*

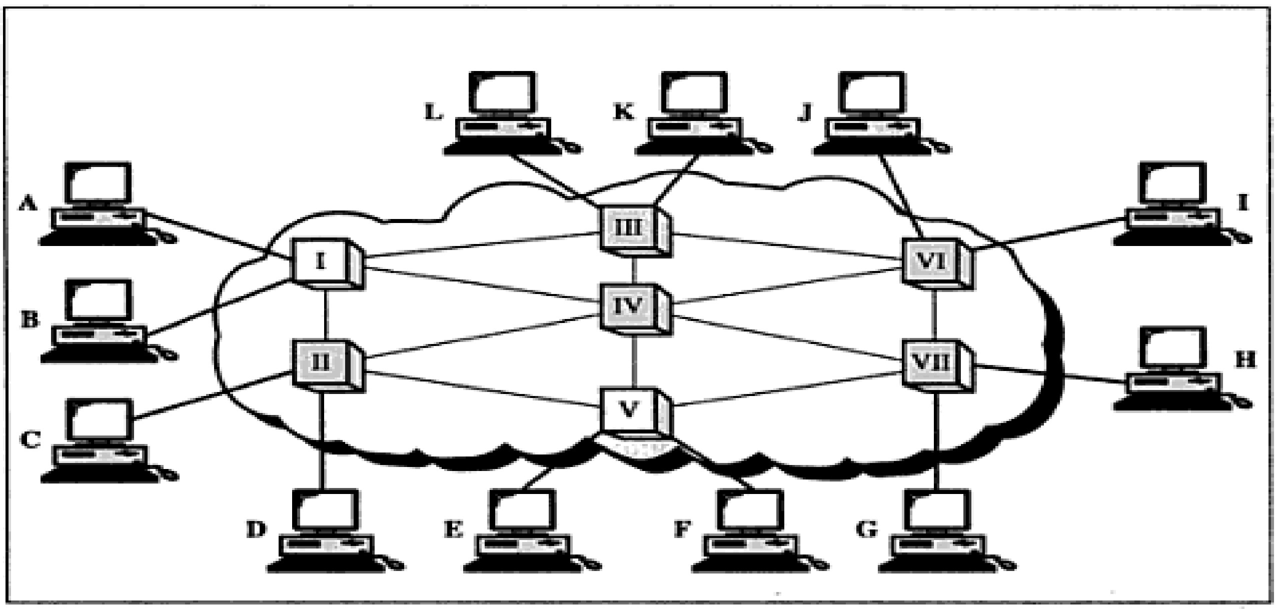
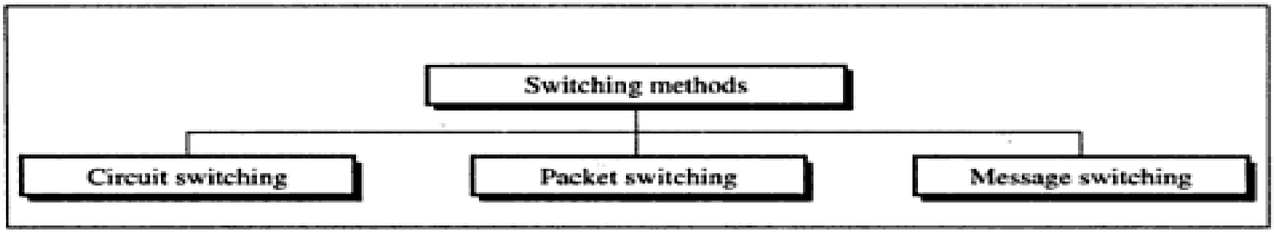


Figure 14.2 *Switching methods*



Video Content / Details of website for further learning (if any):
https://www.cloudflare.com/en-in/learning/network-layer/what-is-the-network-layer/

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 49 - 50)

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

L 20

LECTURE HANDOUTS

MCA **I / II**

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **III - Network Layer**

Date of Lecture: 17.03.2021

Topic of Lecture: Circuit Switching

Introduction :

- Switching involves sending data along routes so that it can be sent from the sender to the receiver.
- Circuit switching is a switching technique in which data travels along a dedicated communication path between a source and a destination.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Data Link layer
- Network Layer
- Switched Network
- Protocols

Detailed content of the Lecture:

Circuit Switching :

- If packet pass the network boundary, we need another addressing called logical addressing (Never change).
- Routing - Route the packet to final destination.
- It creates direct physical connection b/w two devices such as phone or computers.
- Any computer can be connected to any other using Levers.
- N-by-N folded switches can connect n lines in full duplex mode.

Two Types :

1. **Space division**
2. **Time division**

1. Space Division Switch :

Path in the circuit are separated from each other.

It is used both in analog and digital communication.

2 Types :

- **Crossbar switch**
- **Multistage switch**

It connects n inputs to m outputs using cross points

Limitation:

More cross points needed(1000 I/P - 1000 O/P requires 1000000 cross points)

Figure 14.3 *Circuit-switched network*

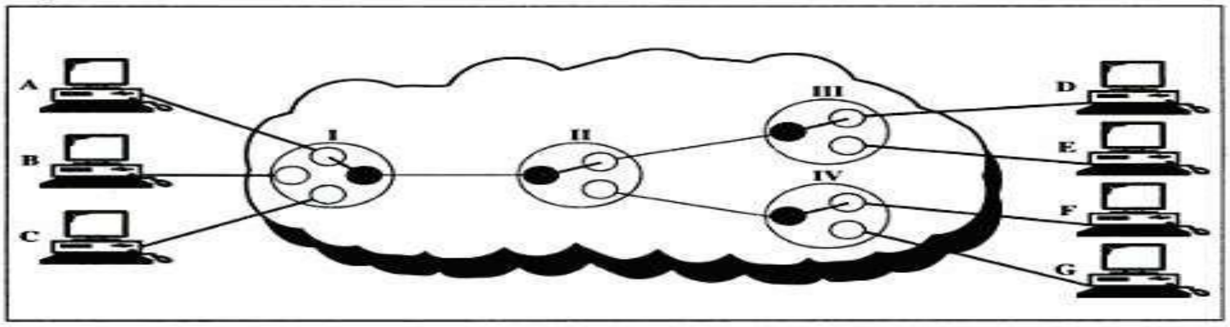
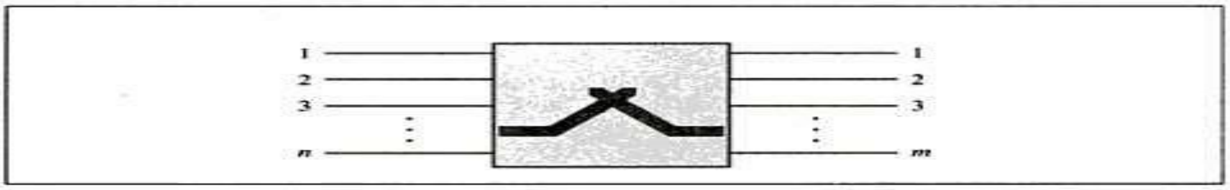


Figure 14.4 *A circuit switch*



Multistage Switch :

- Devices are linked to switches ,that are in turn linked to another switches(Hierarchy of switches)

Blocking:

- The reduction in a number of cross points causes a phenomena called Blocking.
- During heavy traffic one input cannot be connected to output because no path available.

2. Time Division Switches :

It uses time division multiplexing 2 methods:

- **Time slot interchange**
- **TDM bus**

Time slot interchange:

It changes the ordering of the slot based on the desired connection

It uses RAM to store time slot

Ex:

1->3 2->4 3->1 4->2

A B C D -> C D A B

TDM Bus- Time Division Multiplexing :

- Here each input and output lines are connected to high speed bus
- Each bus is closed during one of the four time slots

Limitations of Circuit Switching :

It is specially designed for voice communication(telephone). Not suitable for data communication. Once a circuit is established, it remains for duration of the session. It creates dialed(temporary)and leased(Permanent).

Less data rate because of point to point connection.

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.:

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012

(Page No : 432 - 439)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 21

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **III - Network Layer**

Date of Lecture: 18.03.2021

Topic of Lecture: Packet Switching

Introduction :

- Packet switching is better for data transmission.
- Data are transmitted through unit of variable length blocks called packets.
- Longer transmission are divided into multiple packets.
- Packet length is decided by network.

Prerequisite knowledge for Complete understanding and learning of Topic:

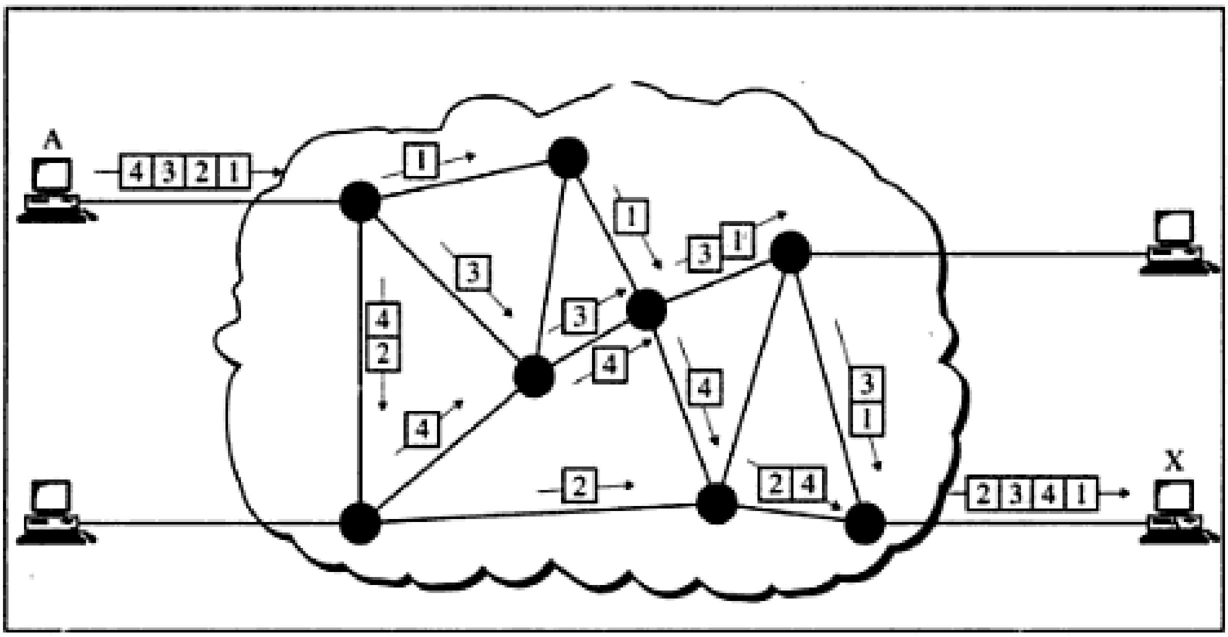
- Physical Layer
- Data Link layer
- Gateway
- Packet Addressing

Detailed content of the Lecture:

Datagram Approach :

- In this approach a message is divided into multiple packets.
- All packets choose various routes and reaches the destination.
- Ordering of packets in destination is done by transport layer.

Figure 14.17 *Datagram approach*



Virtual Circuit approach :
It uses single route to send all packets of the message
Two formats:

- **Switched virtual circuit**
- **Permanent virtual circuit**

Switched virtual circuit

- Connection is temporary
- Dial-up lines

During Transmission a connection is established-all packets are sent – proper ACK- Connection is terminated.

- Switches are hardware or software devices used for temporary connection b/w 2 or more devices linked to the switch in network but not to each another Switches are needed to connect multiple devices for making one-one communication.

Permanent virtual circuit

- Connection is permanent.
- Circuit is dedicated for two users, No one else can use the line when communication takes place.It always gets the same route.
- Leased lines.

During Transmission.No connection establishment or termination.
Message Switching

- It uses a mechanism called store and forward.
- A message is received and stored until a appropriate route is free, then sends along.
- Message switching- uses secondary storage(Disk).
- Packet switching – uses primary storage(RAM).

The routers decide which route is best among many routes in a particular transmission.
Routers are like stations on the network.

- The IP address is obtained from DNS (host) or from its routing table (router).
- The physical address of the receiver is needed to pass through the physical network.
- The address resolution protocol (ARP) enables to know the physical address of a node when the logical address is known.
- ARP enable each host on a network to build up a table of mappings between IP addresses and link-level addresses ARP takes advantage of the broadcast support rendered link-level networks, such as Ethernet and token ring.

Video Content / Details of website for further learning (if any):
https://avinetworks.com/glossary/packet-switching/

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 441 - 444)

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

L 22

LECTURE HANDOUTS

MCA **I / II**

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **III - Network Layer**

Date of Lecture: 19.03.2021

Topic of Lecture: IP Addressing

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.

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.

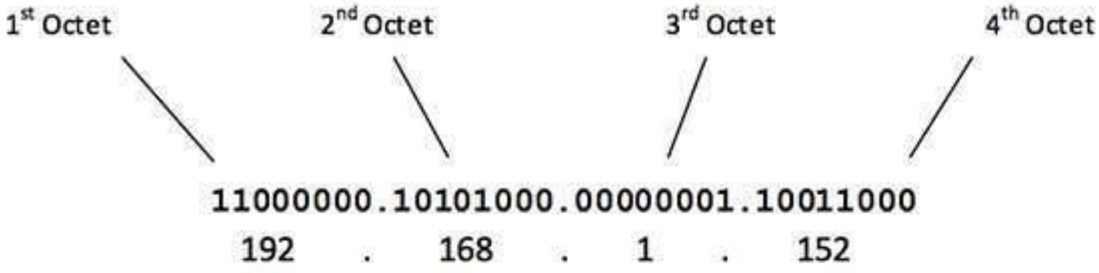
Broadcast Addressing Mode

- 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.

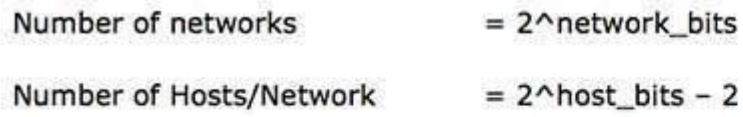
Multicast Addressing Mode

- 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

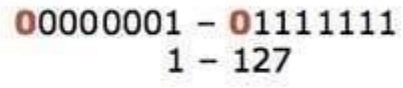
When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

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

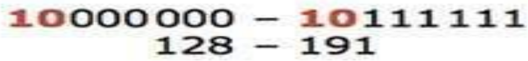
- The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.


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).
- ClassA 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

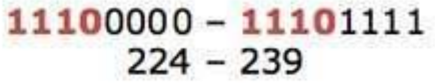
- Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.
- Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.
- Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Class C Address

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

CIDR or Classless Inter Domain Routing

- A larger address space was needed as a long-term solution.
- The larger address space, however, requires that the length of IP addresses also be increased, which means the format of the IP packets needs to be changed.

Slash Notation

- Slash notation is a compact way to show or write an IPv4 subnet mask.

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.:
Book : Data and Computer Communications -William Stallings, Pearson Education, 2013
(Page No : 549 - 551)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 23

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **III - Network Layer**

Date of Lecture: 20.03.2021

Topic of Lecture: IPV4

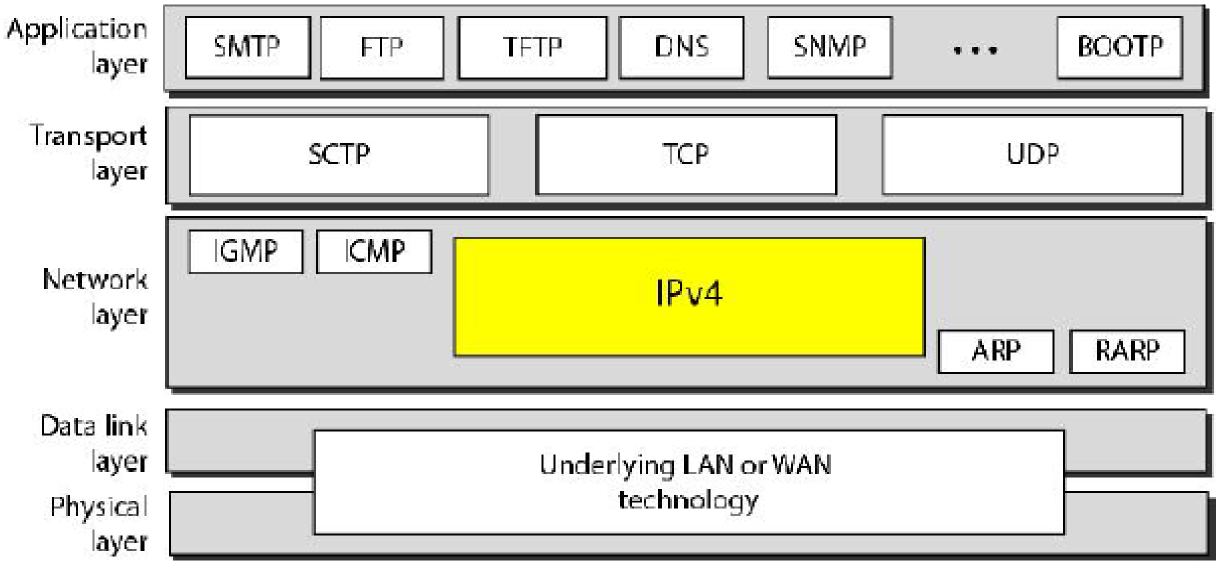
Introduction :

- 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:



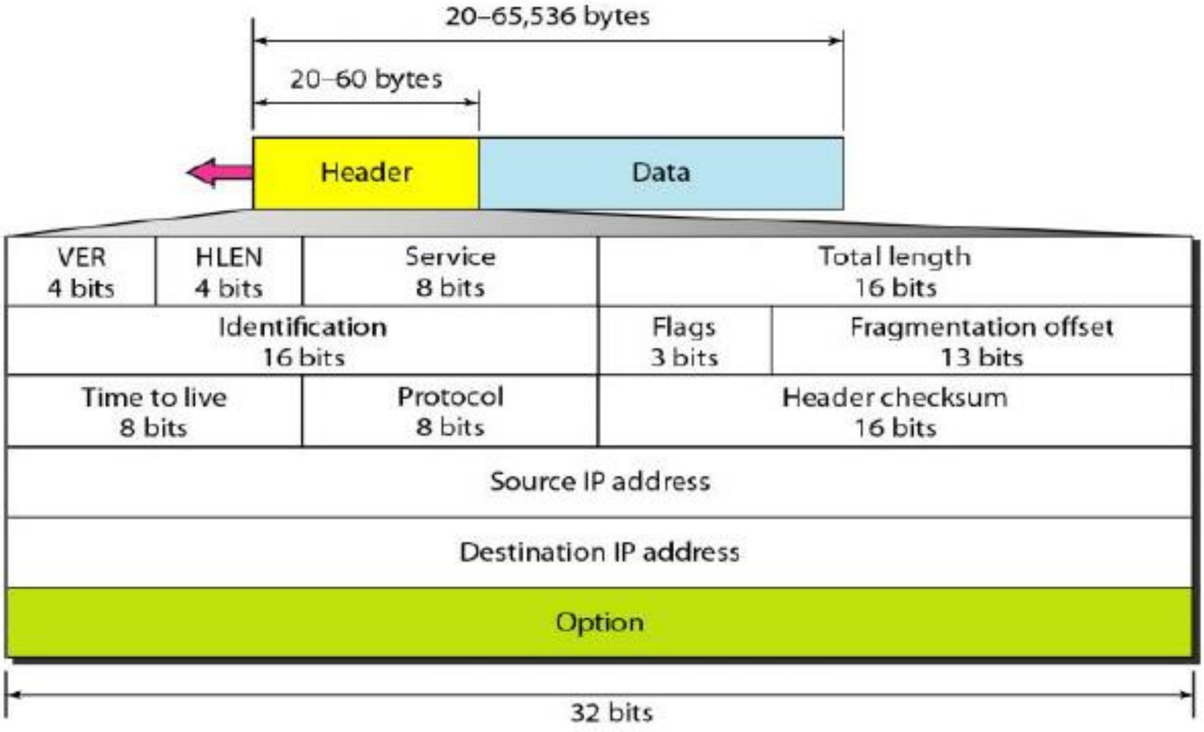
Datagram

- 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).

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 sub field ranging from 0 (000 in binary) to 7 (111 in binary).
- **TOS bits** are a 4-bit sub field with each bit having a special meaning.

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.:
Book : Data and Computer Communications -William Stallings, Pearson Education, 2013
(Page No : 546 - 548)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 24

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **III - Network Layer**

Date of Lecture: 22.03.2021

Topic of Lecture: IPV6

Introduction :

- An IPv6 address consists of 16 bytes (octets); it is 128 bits long. An IPv6 address is 128 bits long. IPv6 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.

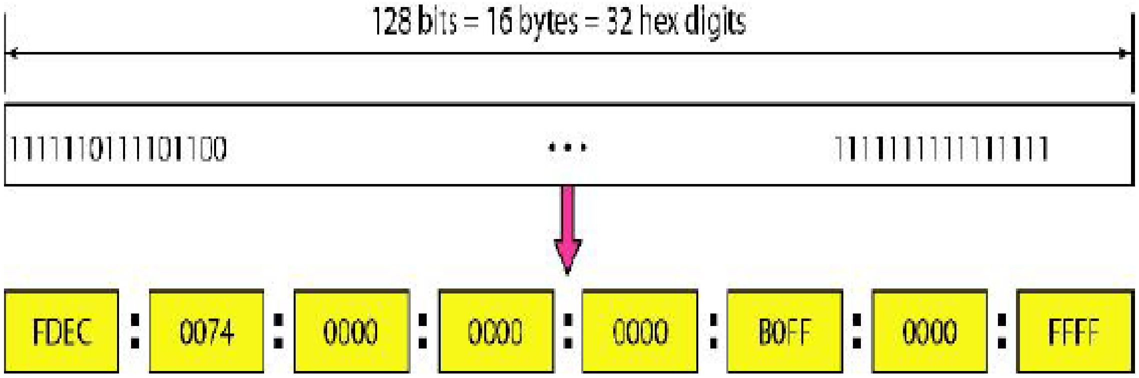
Prerequisite knowledge for Complete understanding and learning of Topic:

- IP Addressing
- 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

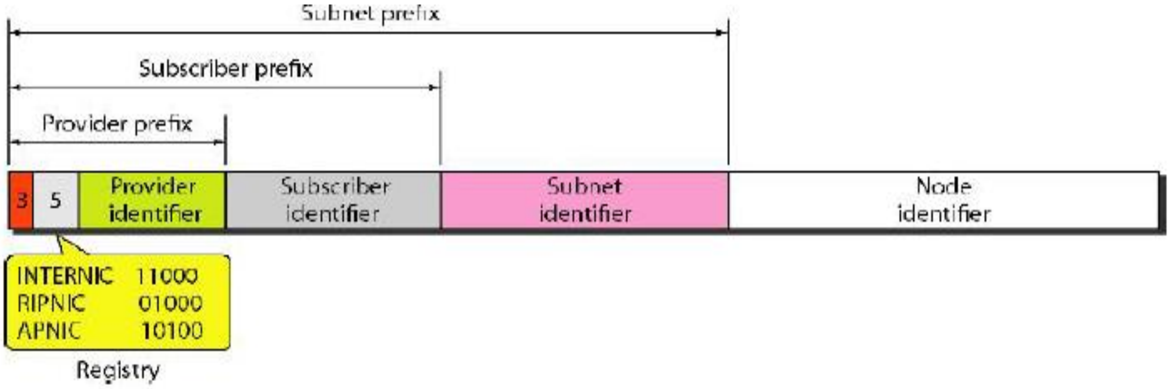
- Although the IP address, even in hexadecimal format, is very long, many of the digits are zeros. In this case, we can abbreviate the address. The leading zeros of a section (four digits between two colons) can be omitted. Only the leading zeros can be dropped, not the trailing zeros.
- Using this form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

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.:
Book : Data and Computer Communications -William Stallings, Pearson Education, 2013
(Page No : 566 - 569)

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

L 25

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **III - Network Layer**

Date of Lecture: 23.03.2021

Topic of Lecture: Routing Protocols

Introduction :

- An internet is made of a combination of physical networks connected by internetworking devices such as routers or Routing Protocols.
- A routing protocol specifies how routers communicate with each other to distribute information that enables them to select routes between nodes on a computer network.

Prerequisite knowledge for Complete understanding and learning of Topic:

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

Detailed content of the Lecture:

ARP:

- Address Resolution Protocol
- A host or a router to send a IP datagram, needs to know both the logical and physical address of the receiver. The IP address is obtained from DNS (host) or from its routing table (router).
- The physical address of the receiver is needed to pass through the physical network.
- The address resolution protocol (ARP) enables to know the physical address of a node when the logical address is known.
- ARP enable each host on a network to build up a table of mappings between IP addresses and link-level addresses.

Packet Format

<table>
<tr><td>0</td><td>8</td><td>16</td><td>31</td></tr>
<tr><td colspan="2">Hardware Type</td><td colspan="2">Protocol Type</td></tr>
<tr><td>Hardware length</td><td>Protocol length</td><td colspan="2">Operation</td></tr>
<tr><td colspan="4">Sender hardware address</td></tr>
<tr><td colspan="4">Sender protocol address</td></tr>
<tr><td colspan="4">Target hardware address</td></tr>
<tr><td colspan="4">Target Protocol address</td></tr>
</table>

Hardware type - defines the type of the network on which ARP is running. Each LAN has been assigned an integer based on its type. Ethernet has value 1.

Protocol type- specifies the protocol value. ARP can be used with any higher-level protocol. For IPv4 the value is 0x0800. Hardware length specifies length of the physical address in bytes. For Ethernet, the value is 6.

Protocol length- specifies length of the logical address in bytes. For IPv4 protocol, the value is 4. **Operation**-defines the type of packet. It is either ARP request (1) or ARP reply (2). Sender hardware address a variable-length field contains physical address of the sender.

Sender protocol address- a variable-length field contains logical address of the sender.

Target hardware address-a variable-length field contains physical address of the target.

Target protocol address- a variable-length field contains logical address of the target.

Address Translation

- The host checks its ARP table with the logical address. If an entry exists, then the corresponding physical address is used to construct a datagram. Otherwise, it finds physical address using ARP as follows:

1. An ARP request packet is created with value for operation field as 1.

2. The target physical address field is unknown and is filled with 0s (broadcast).

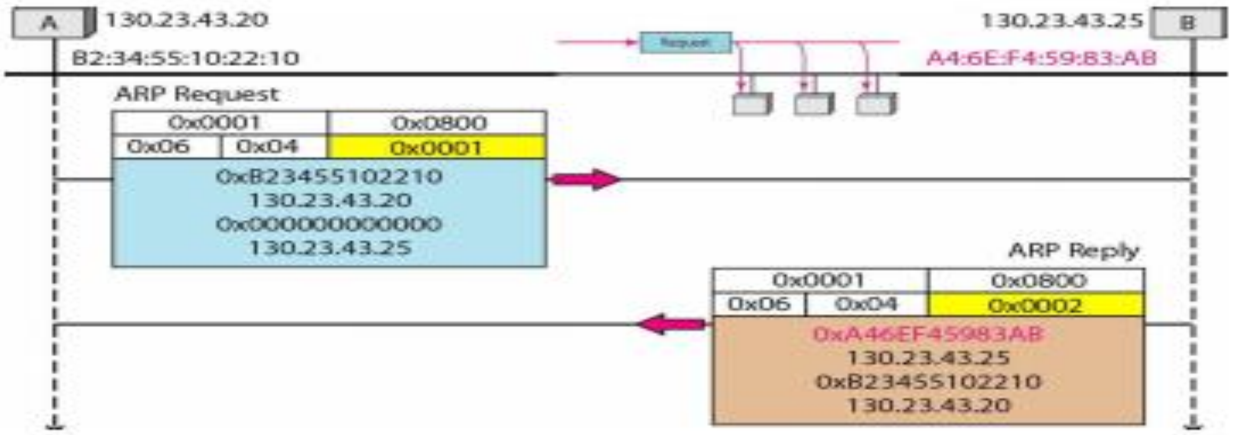
3. The ARP request is encapsulated in a IP packet and broadcasted on the physical network.

4. Every host or router receives it. All nodes except the target discard the packet.

5. The target node constructs an ARP reply packet with value of 2 for operation.

6. The ARP reply is unicast, sent back to the sender.

7. The sender receives the reply message and stores the target logical-physical address pair in its ARP table for sending future packets.



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

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 622 - 624)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 26

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **III - Network Layer**

Date of Lecture: 24.03.2021

Topic of Lecture: Distance Vector Routing

Introduction :

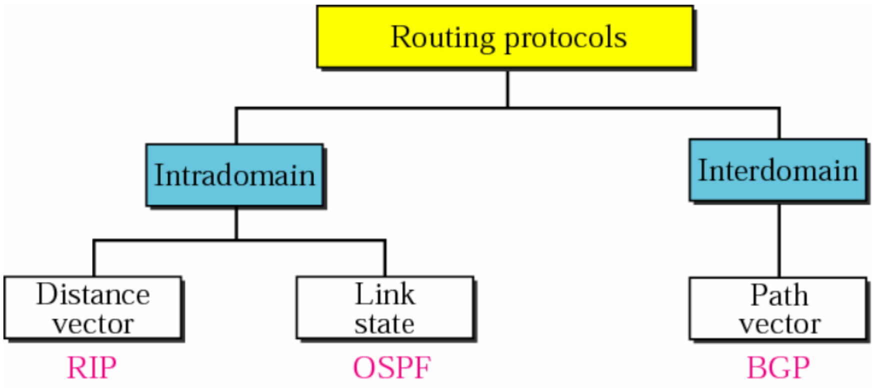
- Routing protocols are used to discover available routes within a network and find the least costly route to target router.
- The information from the routing discovery is used to build routing tables for the connected routers, each router then uses its routing table when making routing decisions.

Prerequisite knowledge for Complete understanding and learning of Topic:

- TCP/ IP Protocol
- Transport layer responsibilities
- Communication between Sender and Receiver using Routers.

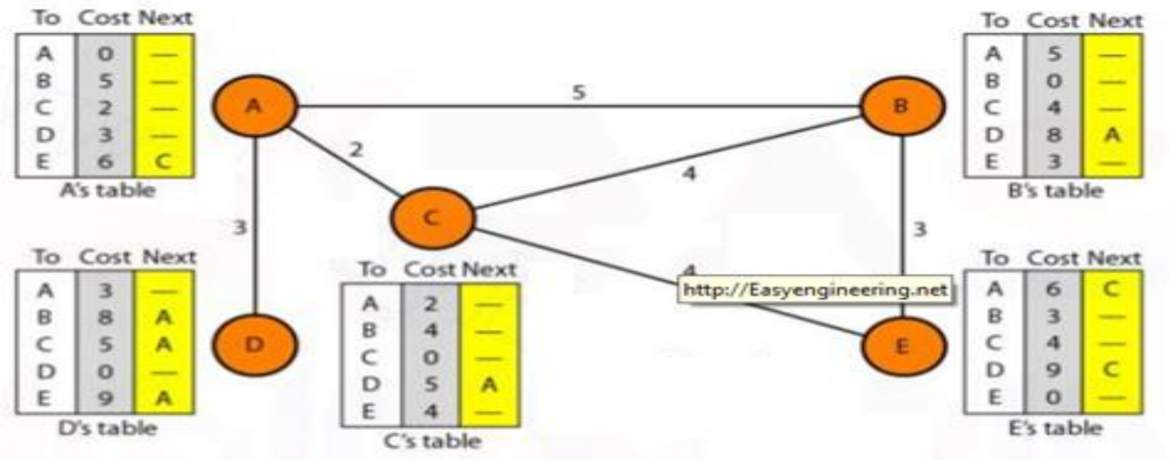
Detailed content of the Lecture:

Classification of Routing Protocols



Distance Vector Routing Protocol

- Adaptive algorithm – Exchange of info only with neighbours
- Data to be available in each router – Routing table: per destination
- Distance
- Outgoing line – Distance to all neighbours
- In distance vector routing, the least-cost route between any two nodes is the route with minimum distance.
- In this protocol, each node maintains a vector (table) of minimum distances to every node.



To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

A's table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	8	A
E	3	—

B's table

To	Cost	Next
A	3	—
B	8	A
C	5	A
D	0	—
E	9	A

D's table

To	Cost	Next
A	2	—
B	4	—
C	0	—
D	5	A
E	4	—

C's table

To	Cost	Next
A	6	C
B	3	—
C	4	—
D	9	C
E	0	—

E's table

Distance vector routing tables

Algorithm

- At each step within a router:
- Get routing tables from neighbours
- Compute distance to neighbours

Initialization

- Each node can know only the distance between itself and its immediate neighbors, those directly connected to it.
- The distance for any entry that is not a neighbour is marked as infinite (unreachable).

Sharing

- Each node shares its routing table with its immediate neighbours periodically and when there is a change.
- Eg. Node A does not know about node E, but node C does. So if node C shares its routing table with A, node A can also know how to reach node E.
- On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to reach node D.A node shares only the first two columns of its routing table to any neighbour.

Updating

1. The receiving node needs to add the cost between itself and the sending node to each value in the second column.

2. The receiving node needs to add the name of the sending node to each row as the third column.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/routing-information-protocol-rip/
https://searchnetworking.techtarget.com/definition/Routing-Information-Protocol

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 628 - 630)

Course Faculty

Verified by HOD

L 27

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **III - Network Layer**

Date of Lecture: 25.03.2021

Topic of Lecture: Link State Routing

Introduction :

- Link state routing is the second family of routing protocols.
- While distance vector routers use a distributed algorithm to compute their routing tables, link-state routing uses link-state routers to exchange messages that allow each router to learn the entire network topology.
- Based on this learned topology, each router is then able to compute its routing table by using a shortest path computation.

Prerequisite knowledge for Complete understanding and learning of Topic:

- TCP/ IP Protocol
- Transport layer responsibilities
- Communication between Sender and Receiver using Routers.
- Dijkstra algorithm

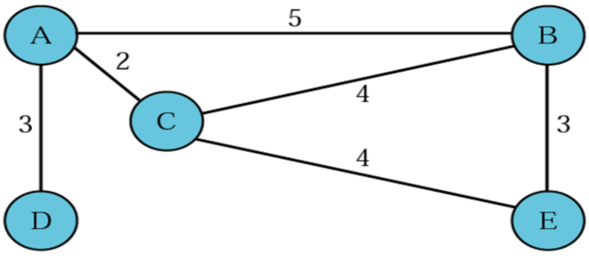
Detailed content of the Lecture:

Link State Routing

Each router must

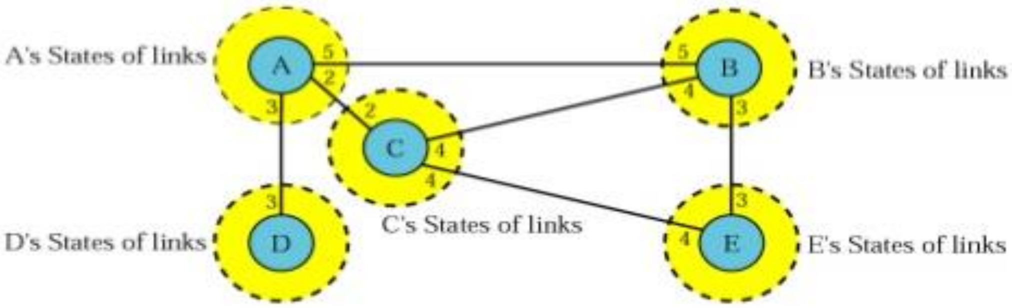
– Discover its **neighbours** and **learn** their network addresses
– Measure the delay or **cost** to each of its neighbours
– Construct a **packet** with these distances
– Send this packet to **all** other routers
– Compute the **shortest path** to every other router

- In link state routing, if each node in the domain has the entire topology of the domain such as the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down). Node can use Dijkstra's algorithm to build a routing table.



Link state knowledge

- Each router knows (maintains) its states of its links.
- Each router floods this info (via a Link State Packet) to other routers periodically (when there is a change in the topology, or every 60 to 120 minutes).



- Each router takes in this data and, using Dijkstra's algorithm, creates the shortest path tree and corresponding routing table.
- Node A knows that it is connected to node B with metric 5, to node C with metric 2, and to node D with metric 3.
- Node C knows that it is connected to node A with metric 2, to node B with metric 4, and to node E with metric 4.
- Node D knows that it is connected only to node A with metric 3. And so on.
- Although there is an overlap in the knowledge.
- The overlap guarantees the creation of a common topology-a picture of the whole domain for each node.

Usage:

- IS-IS protocol
- Designed for DECnet, adopted by ISO
- In use also in Internet
- Supports multiple network layer protocols
  - OSPF protocol used in Internet

Common features:

- Self-stabilizing method of flooding link state updates
- Concept of a designated router on a LAN
- Method of computing and supporting path splitting and multiple metrics.

Video Content / Details of website for further learning (if any):
https://www.geeksforgeeks.org/unicast-routing-link-state-routing/
https://www.javatpoint.com/link-state-routing-algorithm

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 633 - 637)

Course Faculty

Verified by HOD

L 28

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **IV - Transport Layer**

Date of Lecture: 26.03.2021

Topic of Lecture: Introduction to Transport layer

Introduction :

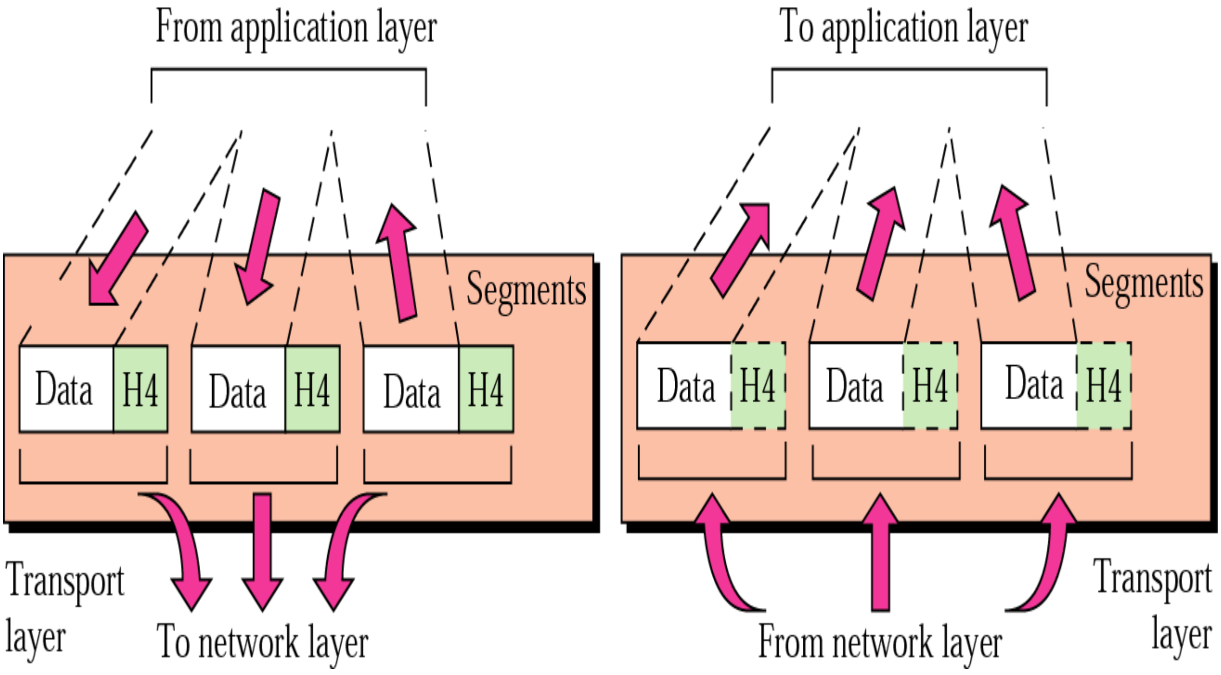
- The Transport layer is responsible for process-to-process or end-end delivery of the entire message.
- The transport layer ensures that the whole message arrives intact and overseeing both Error control and flow control at the process-to-process level.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Network Layer
- TCP/ IP Protocol
- Transport layer responsibilities
- Routing Protocols

Detailed content of the Lecture:

Architecture :



Functions of Transport layer :

Service point addressing:

- Computer often run several processes (running programs) at the same time. Process-to-process delivery means delivery from a specific process on one computer to a specific process on the other.
- The transport layer header include a type of address called port address.
- The network layer gets each packet to the correct computer;
- The transport layer gets the entire message to the correct process on that computer.

Segmentation and reassembly:

- A message is divided into transmittable segments, each having a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arrival at the destination.

Connection control:

- The transport layer can be either connectionless or connection-oriented.
- A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
- A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets.
- After all the data are transferred, the connection is terminated.

Flow control:

- The transport layer performs a flow control end to end. The data link layer performs flow control across a single link.

Error control:

- The transport layer performs error control end to end. The data link layer performs control across a single link.

Congestion control :

- It concerns controlling traffic entry into a telecommunication networks so as to avoid congestive collapse by attempting to avoid over subscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets. It should not be confused with flow control, which prevents the sender from overwhelming the receiver.

Video Content / Details of website for further learning (if any):
https://www.techopedia.com/definition/9760/transport-layer

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 649 - 651)

Course Faculty

Verified by HOD

L 29

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **IV - Transport Layer**

Date of Lecture: 27.03.2021

Topic of Lecture: Transport layer Services

Introduction :

- The Transport layer is responsible for process-to-process or end-end delivery of the entire message.
- The transport layer ensures that the whole message arrives intact and overseeing both Error control and flow control at the process-to-process level.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Transport layer
- TCP/ IP Protocol
- Transport layer responsibilities
- Transport layer Functions

Detailed content of the Lecture:

Transport layer Services

1. Address Mapping

It means mapping of transport address onto the network address. Whenever a session entity requests to send a transport service data unit (TSDU) to another session entity, it sends its transport service access point address as its identification.

The transport entity then determines the network service access point (NSAP) address. This is known as address mapping.

2. Assignment of Network Connection

The transport entity assigns a network connection for carrying the transport protocol data units (TPDUs).

The transport entity establishes this assigned network connection.

In some of the transport protocols, recovery from network disconnection is allowed. In such protocols, whenever a disconnection occurs, the transport entity reassigns the transport of TPDUs to a different network connection.

3. Multiplexing of Transport Connections

There are various TSDUs (multiplexed) identified by the receiving transport entity using the transport connection endpoint identifier (TCEPI), attached to each TSDU by the sending transport entity.

4. Splitting of Transport Connection

When the service quality offered by the network service is less than the required quality of service or when greater resilience is required against network connection failures, then splitting is done by the transport entity.

Splitting means TPDUs belonging to one transport connection may be sent over different network connections.

5. Establishment of Transport Connection

The transport layer establishes the transport connection by sending a request. For establishing a link, it uses the T-CONNECT service primitives.

The transport entity provides the quality of service, requirement, and collect addresses services.

6. Data Transfer

The transport layer provides the data transfer of two types, such as the regular data transfer and expedited data transfer. In normal data transfer, the user can request to transfer user data with any integral number of octets.

7. Segmentation and Concatenation of TPDUs

The transport entity divides the transport service data unit into several transport protocol data units, each with a separate header containing a PCI (Protocol Control Identifier). This function is known as segments.

8. Flow Control

The transport entity uses a modified form of sliding window protocol for flow control. This flow control is required because the transport layer may experience back pressure from the network layer.

9. Error Recovery

The errors at this level can be introduced due to TPDU errors, protocol errors or signal failure conditions of network connections, i.e., reset or release of network connections. Such errors occurring at layer 3 are reported to the transport layer.

The TPDU errors can be in the form of lost TPDU, duplicated TPDU, re-ordering of sequence, or content errors.

10. Sequence Numbering

Each TPDU is given a sequence number by a transport entity that is seven bits long in the normal operations mode.

This sequence numbering is done to provide flow control and error recovery. In the case of extended mode, the sequence number can be 31 bits long.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/what-are-the-services-provided-by-the-transport-layer

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 652 - 655)

Course Faculty

Verified by HOD

L 30

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **IV - Transport Layer**

Date of Lecture: 29.03.2021

Topic of Lecture: Connection Establishment

Introduction :

- To establish a connection, TCP uses a **three-way handshake protocol**. Before a client can connect to a target server, the server must first bind to a port for connection establishment; this is called a passive open. Once the passive open is established, a client may initiate an active open.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Transport layer
- Flow Control
- Error Detection
- Error Control

Detailed content of the Lecture:

Connection Establishment

A connection is typically used for client-server interaction. A server advertizes a particular server at a well-known address and clients establish connections to that socket to avail of the offered service. Thus the connection establishment procedure is asymmetric.

A server creates a socket, binds it to a ``well-known'' port number associated with the service, and then passively ``listens'' on the socket for requests to be served. It is possible for any unrelated process to rendezvous with the server. A client requests services from a server by initiating a ``connection'' to the server's socket. The client uses the connect system call to initiate a connection.

For example, the following call establishes a connection to a socket whose address is specified using the variable ``sname''.

```
struct sockaddr_in sname;

int s;      /* socket descriptor returned by system call socket */
     sname.sin_family = AF_INET;
     sname.sin_port = PORTNUM; /* well-known port no */
     sname.sin_addr.s_addr = /* host address of the server */;
     connect(s, &sname, sizeof(sname));
```

- A connection is typically used for client-server interaction.
- A server advertizes a particular server at a well-known address and clients establish connections to that socket to avail of the offered service.
- Thus the connection establishment procedure is asymmetric.

Problems to solve

- Selection of the initial sequence number for a new connection.
- Wrap around of sequence numbers for an active connection.
- It Handle host crashes.

Releasing a connection :

1. Asymmetric

Connection broken when one party hangs up.

Abrupt! may result in data loss.

2. Symmetric

Both parties should agree to release connection.

How to reach agreement?

- **Two-army problem.**
- **Solution: three-way-handshake.**

3. Pragmatic approach

Connection = 2 unidirectional connections.

Sender can close unidirectional connection.

Connection Termination Protocol (Connection Release)

- While it creates three segments to establish a connection, it takes four segments to terminate a connection. During a TCP connection is full-duplex (that is, data flows in each direction independently of the other direction), each direction should be shut down alone.
- The rule is that either end can share a FIN when it has finished sending data.
- When a TCP receives a FIN, it should notify the application that the other end has terminated that data flow direction.
- The sending of a FIN is usually the result of the application issuing a close.
- The receipt of a FIN only means that there will be no more data flowing in that direction.
- A TCP can send data after receiving a FIN.
- The end that first issues the close (example, send the first FIN) executes the active close.
- The other end (that receives this FIN) manages the passive close.

Video Content / Details of website for further learning (if any):
https://www.tutorialspoint.com/what-is-the-tcp-connection-establishment

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 658 - 659)

Course Faculty

Verified by HOD

L 31

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **IV - Transport Layer**

Date of Lecture: 30.03.2021

Topic of Lecture: Flow Control

Introduction :

- In data communications, **flow control** is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver.
- It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Data Link Control
- Error Detection
- Error Control
- Data Transmission Concepts

Detailed content of the Lecture:

Flow Control

- Flow control is important because it is possible for a sending computer to transmit information at a faster rate than the destination computer can receive and process it.

Two categories of flow control:

1. Stop-and-wait : Send one frame at a time.

2. Sliding window : Send several frames at a time.

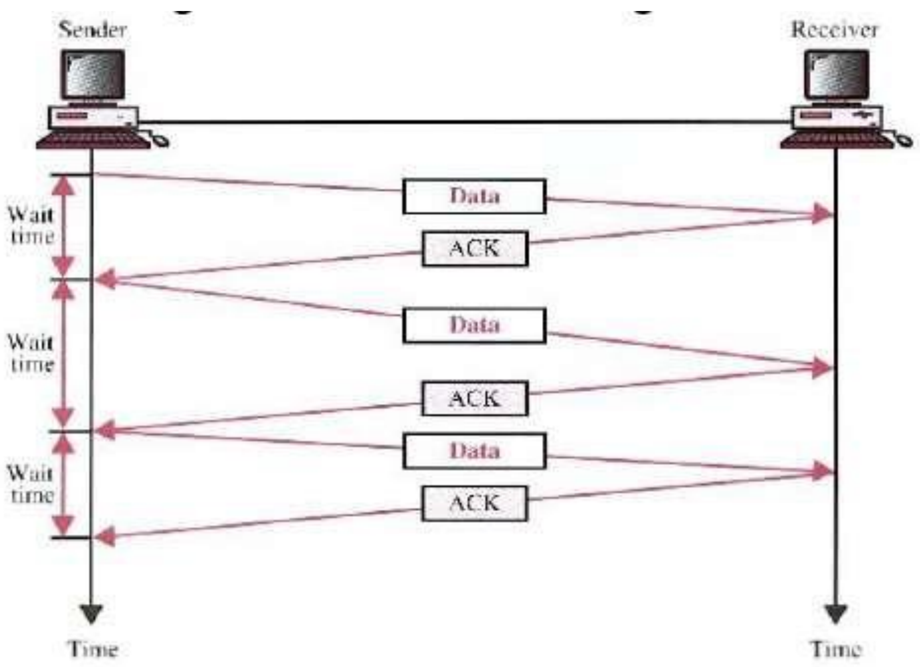
Stop-and-wait

- Sender sends one frame and waits for an acknowledgement before sending the next frame.

Operations

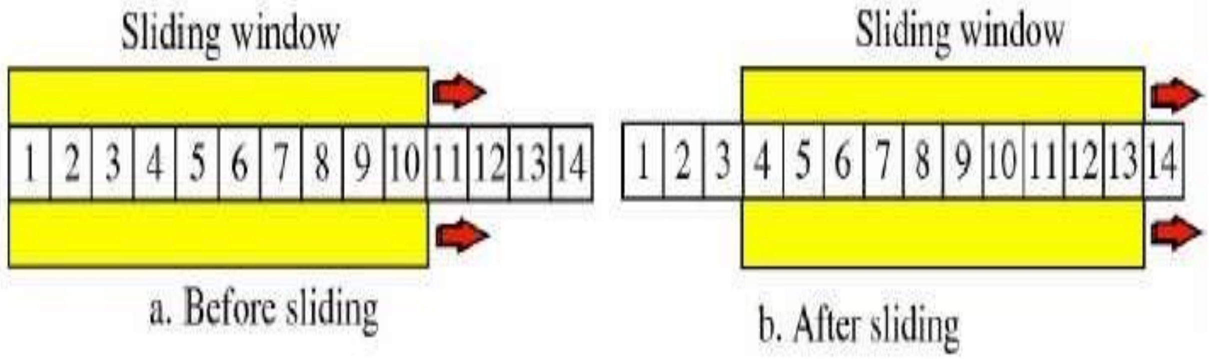
1. **Sender:** Transmits a single frame at a time.
2. Sender waits to receive ACK within time out.
3. **Receiver:** Transmits acknowledgement (ACK) as it receives a frame.
4. Go to step 1 when ACK is received, or time out is hit.

- Stop and wait can also create inefficiencies when sending longer transmissions.When longer transmissions are sent there is more likely chance for error in this protocol. If the messages are short the errors are more likely to be detected early.



Sliding window

- Sliding-window flow control is best utilized when the buffer size is limited and pre-established. During a typical communication between a sender and a receiver the receiver allocates buffer space for *n* frames (*n* is the buffer size in frames).
- The sender can send and the receiver can accept *n* frames without having to wait for an acknowledgement.
- A sequence number is assigned to frames in order to help keep track of those frames which did receive an acknowledgement.
- The receiver acknowledges a frame by sending an acknowledgement that includes the sequence number of the next frame expected. This acknowledgement announces that the receiver is ready to receive n frames, beginning with the number specified. Both the sender and receiver maintain what is called a window. The size of the window is less than or equal to the buffer size.



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

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 306 - 308)

Course Faculty

Verified by HOD

L 32

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **IV - Transport Layer**

Date of Lecture: 31.03.2021

Topic of Lecture: Transmission Control Protocol

Introduction :

- 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.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Routing
- Transport layer responsibilities
- Standards and Protocols

Detailed content of the Lecture:

TCP-Overview

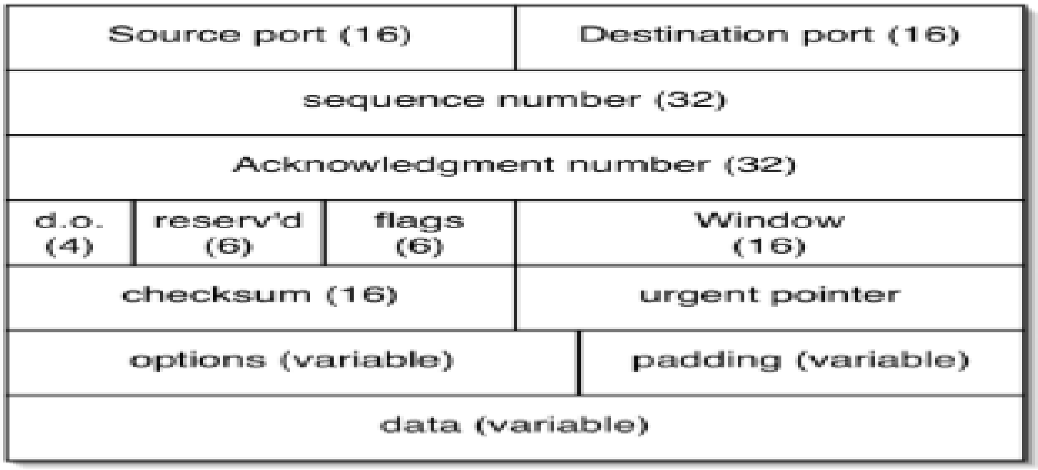
- TCP is connection-oriented, and provides for reliable, order-preserving transmission of data.
- Connection oriented – Explicit set-up and tear-down of TCP session
- Stream-of-bytes service – Sends and receives a stream of bytes, not messages – Similar to file I/O
- Reliable, in-order delivery – Checksums to detect corrupted data – Acknowledgments & retransmissions for reliable delivery – Sequence numbers to detect losses and reorder data
- Flow control – Prevent overflow of the receiver’s buffer space
- Congestion control – Adapt to network congestion for the greater good

Features

- 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) | Destination port (16)

sequence number (32)

Acknowledgment number (32)

d.o. (4) | reserv'd (6) | flags (6) | Window (16)

checksum (16) | urgent pointer

options (variable) | padding (variable)

data (variable)

Both the TCP header and the data must have a length in bits multiple of 32. The application layer must ensure that data given to the TCP protocol is multiple of 32 bits long. The TCP header has enough information to derive where padding begins.

- **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.

Addressing

TCP communication between two remote hosts is done by means of port numbers (TSAPs). Ports numbers can range from 0 – 65535 which are divided as:

- System Ports (0 – 1023)
- User Ports (1024 – 49151)
- Private/Dynamic Ports (49152 – 65535)

Connection Management

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.

Establishment

Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client’s segment which is one more than client’s Sequence number.

Client after receiving ACK of its segment sends an acknowledgement of Server’s response.

TCP Receiver Window

- Receiver window size (rwnd) .
- amount that can be sent without acknowledgment.
- Receiver can buffer this amount of data Receiver continually advertises buffer space available to sender.

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

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 723- 725)

Course Faculty

Verified by HOD

L 33

LECTURE HANDOUTS

MCA **I / II**

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **IV - Transport Layer**

Date of Lecture: 01.04.2021

Topic of Lecture: Congestion Control

Introduction :

- Congestion Control is concerned with efficiently using a network at high load.
- Congestion refers to a network state where-The message traffic becomes so heavy that it slows down the network response time.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Congestion is an important issue that can arise in Packet Switched Network.
- Congestion leads to the loss of packets in transit.
- So, it is necessary to control the congestion in network.
- It is not possible to completely avoid the congestion.

Detailed content of the Lecture:

Congestion Control

- Congestion control refers to techniques and mechanisms that can-
  - Either prevent congestion before it happens
  - Or remove congestion after it has happened
- Now, let us discuss how congestion is handled at TCP.

TCP Congestion Control

- TCP reacts to congestion by reducing the sender window size.

The size of the sender window is determined by the following two factors-

1. Receiver window size
2. Congestion window size

1. Receiver Window Size

- Sender should not send data greater than receiver window size.
- Otherwise, it leads to dropping the TCP segments which causes **TCP Retransmission**.
- So, sender should always send data less than or equal to receiver window size.
- Receiver dictates its window size to the sender through **TCP Header**.

2. Congestion Window

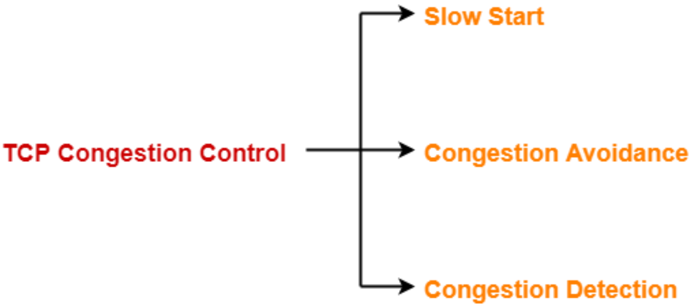
- Sender should not send data greater than congestion window size.
- Otherwise, it leads to dropping the TCP segments which causes TCP Retransmission.
- So, sender should always send data less than or equal to congestion window size.
- Different variants of TCP use different approaches to calculate the size of congestion window.
- Congestion window is known only to the sender and is not sent over the links.

So, always-

Sender window size = Minimum (Receiver window size, Congestion window size)

TCP Congestion Policy-

TCP's general policy for handling congestion consists of following three phases-



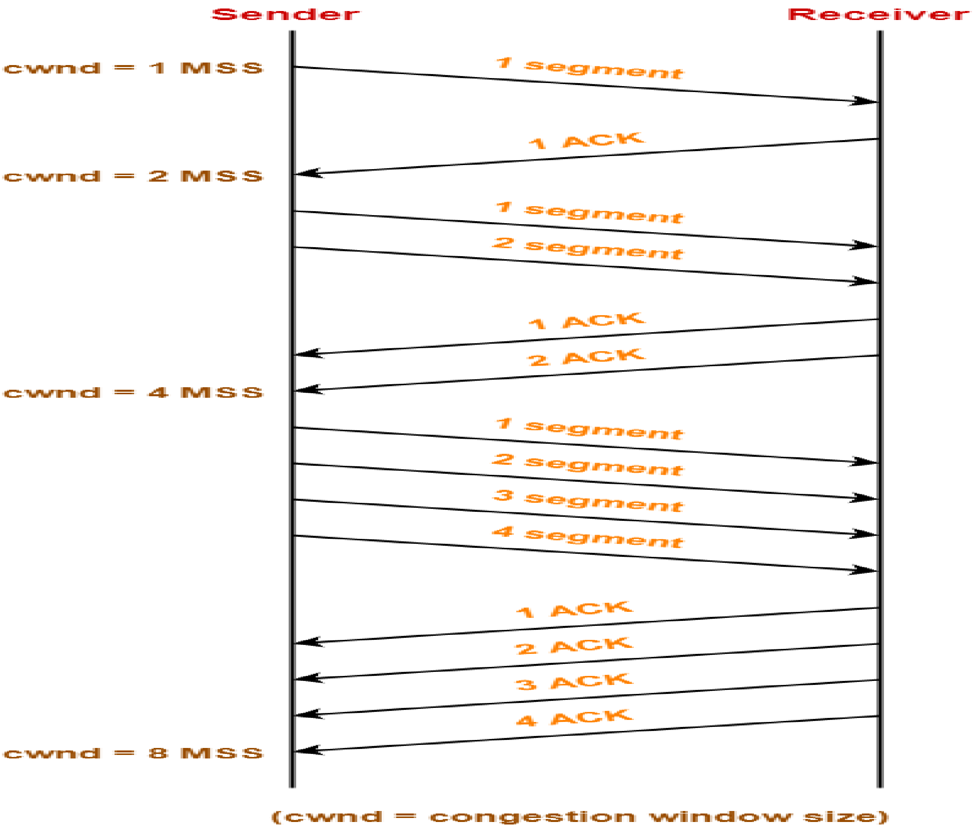
1. Slow Start
2. Congestion Avoidance
3. Congestion Detection

1. Slow Start Phase

Initially, sender sets congestion window size = Maximum Segment Size (1 MSS).

- After receiving each acknowledgment, sender increases the congestion window size by 1 MSS.
- In this phase, the size of congestion window increases exponentially.

The followed formula is- Congestion window size = Congestion window size + Maximum segment size This is shown below.



Principles of Congestion Control
Congestion:

- informally: “too many sources sending too much data too fast for network to handle”
- Different from flow control!
- End-to-end issue!
- Lost packets (buffer overflow at routers)
- Long delays (queue-ing in router buffers)

2. Congestion Avoidance Phase

After reaching the threshold,

- Sender increases the congestion window size linearly to avoid the congestion.
- On receiving each acknowledgement, sender increments the congestion window size by 1. The followed formula is-
    - Congestion window size = Congestion window size + 1

***3.* Congestion Detection Phase**

When sender detects the loss of segments, it reacts in different ways depending on how the loss is detected-

Case-01: Detection On Time Out-

- Time Out Timer expires before receiving the acknowledgement for a segment.
- This case suggests the stronger possibility of congestion in the network.
- There are chances that a segment has been dropped in the network.

Reaction-

In this case, sender reacts by-

- Setting the slow start threshold to half of the current congestion window size.
- Decreasing the congestion window size to 1 MSS.
- Resuming the slow start phase.
- Sender should not send data greater than congestion window size.
- Otherwise, it leads to dropping the TCP segments which causes TCP Retransmission.

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

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 535 - 537)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 34

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **IV - Transport Layer**

Date of Lecture: 03.04.2021

Topic of Lecture: Congestion Avoidance

Introduction :

- Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks.
- Congestion avoidance is achieved through packet dropping. Among the more commonly used congestion avoidance mechanisms is Random Early Detection (RED), which is optimum for high-speed transit networks.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Data Link Control
- Error Detection
- Error Control
- Congestion Control

Detailed content of the Lecture:

Congestion Avoidance

The following 2 Methods are used to Avoid the Congestions :

- **Random Early Discard**
- **Traffic Shaping**

1. Random Early Discard (RED)

- This is a proactive approach in which the router discards one or more packets before the buffer becomes completely full.
- Each time a packet arrives, the RED algorithm computes the average queue length, avg.
- If avg is lower than some lower threshold, congestion is assumed to be minimal or non-existent and the packet is queued.
- If avg is greater than some upper threshold, congestion is assumed to be serious and the packet is discarded.
- If avg is between the two thresholds, this might indicate the onset of congestion. The probability of congestion is then calculated.

2. Traffic Shaping

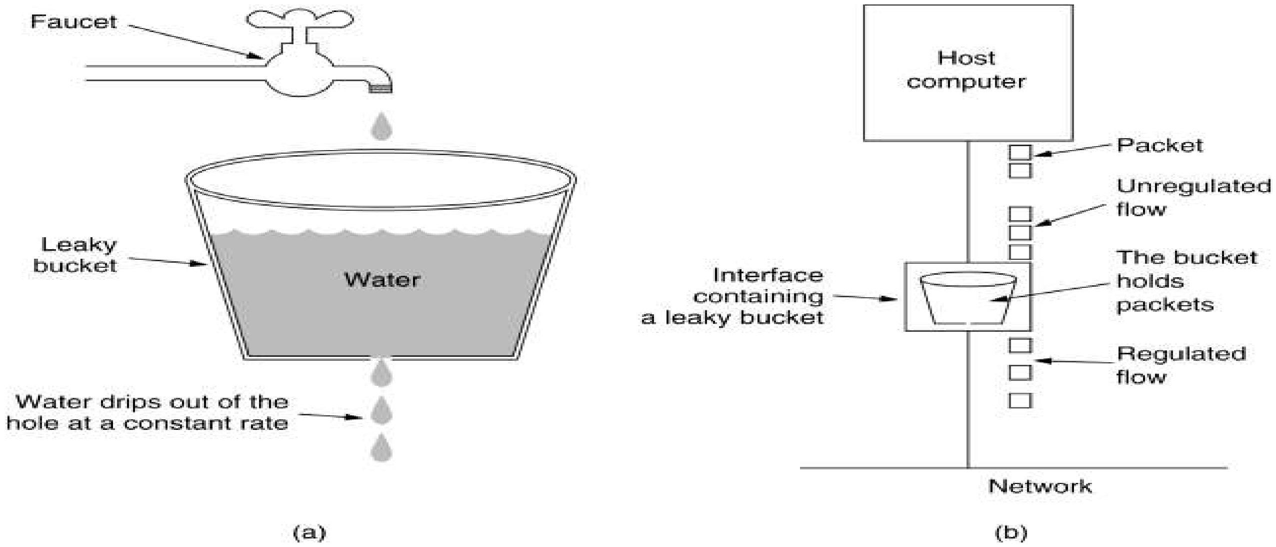
- Another method of congestion Avoidance is to "shape" the traffic before it enters the network.
- Traffic shaping controls the rate at which packets are sent (not just how many). Used in ATM and Integrated Services networks.

- At connection set-up time, the sender and carrier negotiate a traffic pattern (shape).
- Two traffic shaping algorithms are:

1. Leaky Bucket
2. Token Bucket

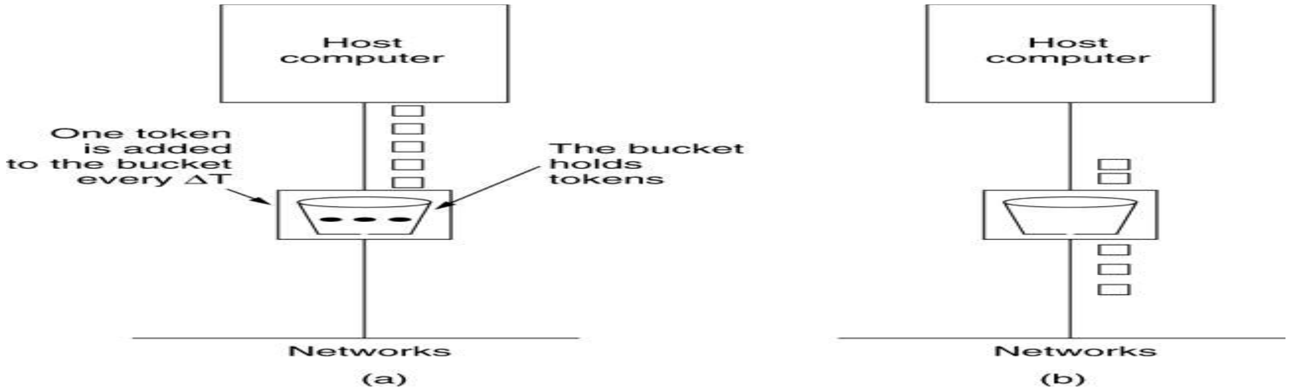
1. The Leaky Bucket Algorithm

- The Leaky Bucket Algorithm used to control rate in a network. It is implemented as a single-server queue with constant service time. If the bucket (buffer) overflows then packets are discarded.



2. Token Bucket Algorithm

- In contrast to the LB, the Token Bucket Algorithm, allows the output rate to vary, depending on the size of the burst.
- In the TB algorithm, the bucket holds tokens.To transmit a packet, the host must capture and destroy one token.
- Tokens are generated by a clock at the rate of one token every sec.



Video Content / Details of website for further learning (if any):
https://www.cisco.com/c/en/us/td/docs/ios/qos/configuration/guide/12_2sr/qos_12_2sr_book/congestion_avoidance.html

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 536 - 540)

Course Faculty

Verified by HOD

L 35

LECTURE HANDOUTS

MCA **I / II**

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **IV - Transport Layer**

Date of Lecture: 05.04.2021

Topic of Lecture: User Datagram Protocol

Introduction :

- User Datagram Protocol (UDP) is a Transport Layer protocol.
- UDP is a part of Internet Protocol suite, referred as UDP/IP suite.
- Unlike TCP, it is unreliable and Connectionless protocol. So, there is no need to establish connection prior to data transfer.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Routing
- Transport layer responsibilities
- TCP Standards and Protocols

Detailed content of the Lecture:

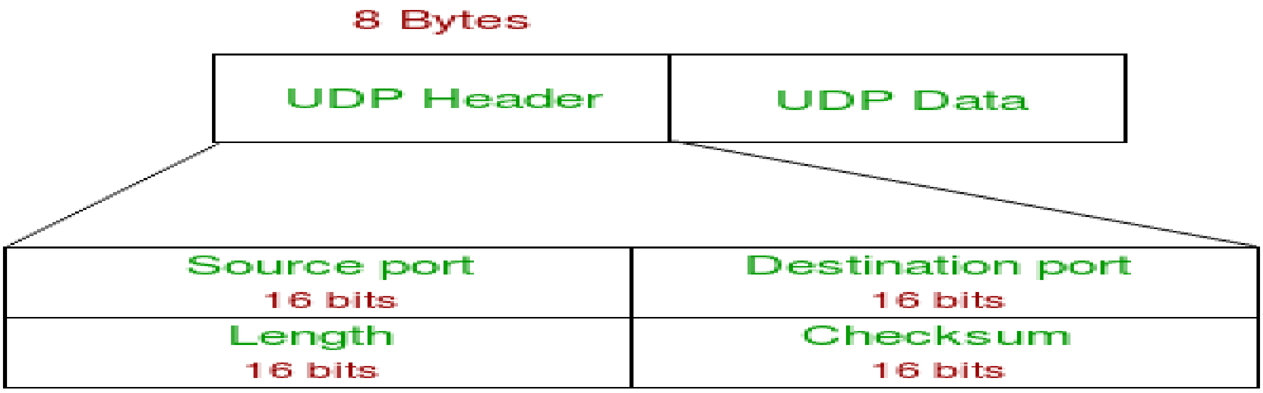
User Datagram Protocol (UDP):

- User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of Internet Protocol suite, referred as UDP/IP suite.
- Unlike TCP, it is unreliable and connectionless protocol**.** So, there is no need to establish connection prior to data transfer.
- Though Transmission Control Protocol (TCP) is the dominant transport layer protocol used with most of Internet services; provides assured delivery, reliability and much more but all these services cost us with additional overhead and latency.
- Here, UDP comes into picture. For the realtime services like computer gaming, voice or video communication, live conferences; we need UDP.
- Since high performance is needed, UDP permits packets to be dropped instead of processing delayed packets.
- There is no error checking in UDP, so it also save bandwidth.
- User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

UDP Header :

- UDP header is **8-bytes** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes.
- First 8 Bytes contains all necessary header information and remaining part consist of data.
- Port numbers help to distinguish different user requests or process.

- UDP port number fields are each 16 bits long, therefore range for port numbers defined from 0 to 65535; port number 0 is reserved.



1. **Source Port :** Source Port is 2 Byte long field used to identify port number of source.
2. **Destination Port :** It is 2 Byte long field, used to identify the port of destined packet.
3. **Length :** Length is the length of UDP including header and the data. It is 16-bits field.
4. **Checksum :** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP header and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Applications of UDP:

- Used for simple request response communication when size of data is less and hence there is lesser concern about flow and error control.
- It is suitable protocol for multicasting as UDP supports packet switching.
- UDP is used for some routing update protocols like RIP(Routing Information Protocol).
- Normally used for real time applications which cannot tolerate uneven delays between sections of a received message
- Following implementations uses UDP as a transport layer protocol:
    - NTP (Network Time Protocol)
    - DNS (Domain Name Service)
    - BOOTP, DHCP.
    - NNP (Network News Protocol)
    - Quote of the day protocol
- Application layer can do some of the tasks through UDP:
    - Trace Route
    - Record Route
    - Time stamp

- UDP takes datagram from Network Layer, attach its header and send it to the user. So, it works fast.

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.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 722 - 723)

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

L 36

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **IV - Transport Layer**

Date of Lecture: 06.04.2021

Topic of Lecture: Transport for Real Time Applications (RTP)

Introduction :

- A protocol is designed to handle real-time traffic (like audio and video) of the Internet, is known as Real Time Transport Protocol (RTP).
- RTP must be used with UDP.
- It does not have any delivery mechanism like multicasting or port numbers.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Congestion Control & Congestion Avoidance
- UDP
- TCP Standards and Protocols

Detailed content of the Lecture:

Transport for Real Time Applications (RTP) :

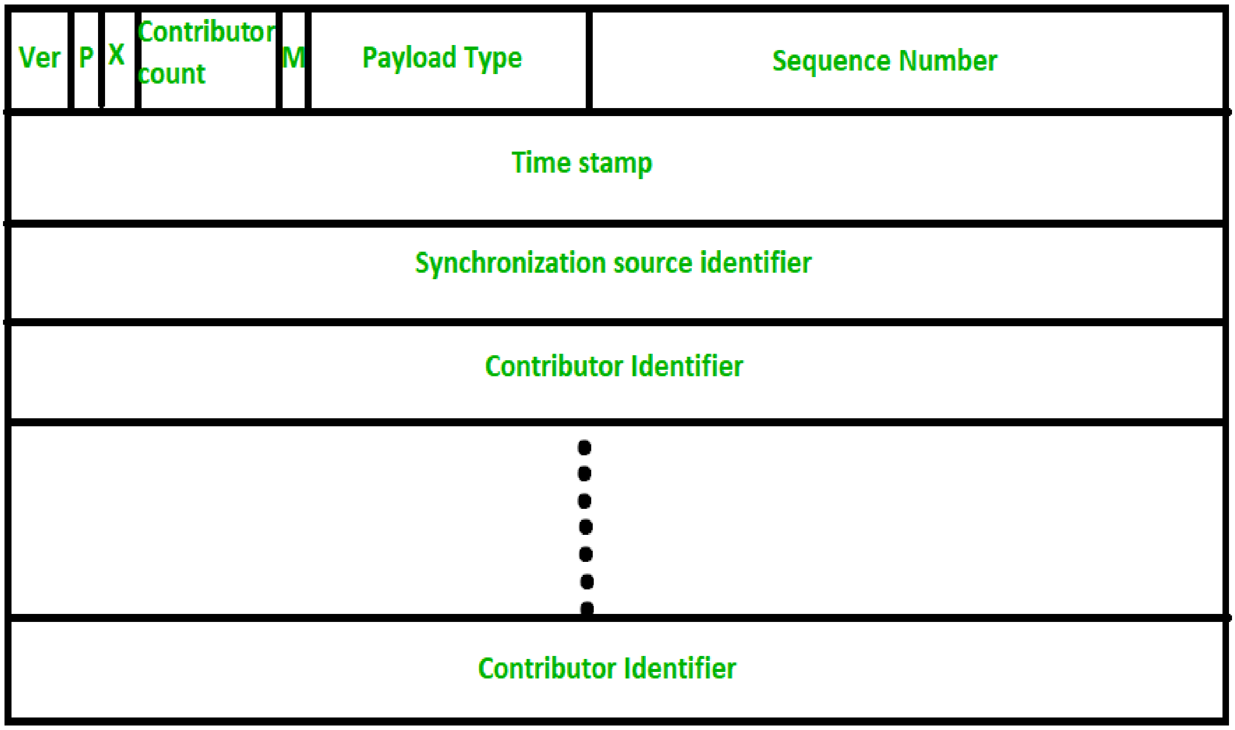
- RTP supports different formats of files like MPEG and MJPEG.
- It is very sensitive to packet delays and less sensitive to packet loss.
- RTP is first time published in 1996 and known as RFC 1889. And next it published in 2003 with name of RFC 3550.

Applications of RTP :

1. **RTP mainly helps in media mixing, sequencing and time-stamping.**
2. **Voice over Internet Protocol (VoIP)**
3. **Video Teleconferencing over Internet.**
4. **Internet Audio and video streaming.**

RTP Header Format :

- **Version :** This 2-bit field defines version number. The current version is 2.
- **P** –The length of this field is 1-bit. If value is 1, then it denotes presence of padding at end of packet and if value is 0, then there is no padding.
- **X** –The length of this field is also 1-bit. If value of this field is set to 1, then its indicates an extra extension header between data and basic header and if value is 0 then, there is no extra extension.
- **Contributor count** –This 4-bit field indicates number of contributors. Here maximum possible number of contributor is 15 as a 4-bit field can allows number form 0 to 15.



- **M** –The length of this field is 1-bit and it is used as end marker by application to indicate end of its data.
- **Payload types** –This field is of length 7-bit to indicate type of payload. We list applications of some common types of payload.
- **Sequence Number** –The length of this field is 16 bits. It is used to give serial numbers to RTP packets.
- **Time Stamp** –The length of this field is 32-bit. It is used to find relationship between times of different RTP packets.
- **Synchronization Source Identifier** –This is a 32-bit field used to identify and define the source. The value for this source identifier is a random number that is chosen by source itself.
- **Contributor Identifier** –This is also a 32-bit field used for source identification where there is more than one source present in session.
- An RTP session is established for each multimedia stream.
- Audio and video streams may use separate RTP sessions, enabling a receiver to selectively receive components of a particular stream.The RTP and RTCP design is independent of the transport protocol.

Video Content / Details of website for further learning (if any):
https://book.systemsapproach.org/e2e/rtp.html
https://en.wikipedia.org/wiki/Real-time_Transport_Protocol

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 737 - 739)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 37

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **V - Applications**

Date of Lecture: 07.04.2021

Topic of Lecture: DNS

Introduction :

- **Domain Name System** helps to resolve the host name to an address. It uses a hierarchical naming scheme and distributed database of IP addresses and associated names.
- 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.

Prerequisite knowledge for Complete understanding and learning of Topic:

- TCP/ IP Protocol
- Application layer responsibilities
- Internetworking

Detailed content of the Lecture:

Domain Name System helps to resolve the host name to an address. It uses a hierarchical naming scheme and distributed database of IP addresses and associated names

IP Address

IP address is a unique logical address assigned to a machine over the network. An IP address exhibits the following properties:

- IP address is the unique address assigned to each host present on Internet.
- IP address is 32 bits (4 bytes) long.
- IP address consists of two components: **network component** and **host component**.
- Each of the 4 bytes is represented by a number from 0 to 255, separated with dots. For example 137.170.4.124
- IP address is 32-bit number while on the other hand domain names are easy to remember names. For example, when we enter an email address we always enter a symbolic string such as webmaster@tutorialspoint.com.

Uniform Resource Locator (URL)

Uniform Resource Locator (URL) refers to a web address which uniquely identifies a document over the internet.

- This document can be a web page, image, audio, video or anything else present on the web.

For example, **www.tutorialspoint.com/internet_technology/index.html** is an URL to the index.html which is stored on tutorialspoint web server under internet_technology directory.

Absolute URL is a complete address of a resource on the web. This completed address comprises of protocol used, server name, path name and file name.

URL Types :

There are two forms of URL as listed below:

Absolute URL

Relative URL

Absolute URL

Absolute URL is a complete address of a resource on the web. This completed address comprises of protocol used, server name, path name and file name.

For example http:// www.tutorialspoint.com / internet_technology /index.htm. where:

http is the protocol.

tutorialspoint.com is the server name.

index.htm is the file name.

The protocol part tells the web browser how to handle the file. Similarly we have some other protocols also that can be used to create URL are:

FTP

https

Gopher

mailto

news

Relative URL

Relative URL is a partial address of a webpage. Unlike absolute URL, the protocol and server part are omitted from relative URL.

Relative URLs are used for internal links i.e. to create links to file that are part of same website as the Web Pages on which you are placing the link.

A Hierarchy of Servers :

The DNS system is a hierarchy of duplicated database servers worldwide that begin with the "root servers" for the top-level domains (.com, .net, .org, .gov, .edu, .mil, etc.). The root servers point to the "authoritative" servers located in ISPs,

Example :

www.yahoo.com

www --------> Host Name
Yahoo--------> Server Name
com ----------> Domain Name

Structure of DNS :

It Consists of Four Elements

1. DNS Name Space
2. DNS Database
3. Name Servers
4. DNS Resolvers

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

https://www.tutorialspoint.com/internet_technologies/internet_domain_name_system.htm

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012

(Page No : 740 - 742)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 38

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **V - Applications**

Date of Lecture: 08.04.2021

Topic of Lecture: E-Mail Protocols

Introduction :

- Electronic Mail or E-Mail is a method of sending and receiving messages (Mail) electronically over a Computer Network.
- E-Mail is a system allows a person or a group to electronically communicate to others through Internet.
- It is method of exchanging message between people using electronic devices.

Prerequisite knowledge for Complete understanding and learning of Topic:

- Application layer
- Internetworking
- WWW

Detailed content of the Lecture:

Email :

Email is a service which allows us to send the message in electronic mode over the internet. It offers an efficient, inexpensive and real time mean of distributing information among people.

E-Mail Address

Each user of email is assigned a unique name for his email account. This name is known as E-mail address. Different users can send and receive messages according to the e-mail address.

E-mail is generally of the form username@domainname. For example, webmaster@tutorialspoint.com is an e-mail address where webmaster is username and tutorialspoint.com is domain name.

- The username and the domain name are separated by @ (at) symbol.
- E-mail addresses are not case sensitive.
- Spaces are not allowed in e-mail address.

E-mail Message Components

E-mail message comprises of different components: E-mail Header, Greeting, Text, and Signature. These components are described in the following diagram:

E-mail Header

The first five lines of an E-mail message is called E-mail header. The header part comprises of following fields:

- From
- Date
- To
- Subject

Components of Email System

Mail Server

Receive, Store and Deliver the mail

DNS

Find and match the IP Address of the Mail Server

Mailbox

It is a Folder contains Emails and their information.

E-Mail Protocol

- **SMTP (Simple Mail Transfer Protocol)**
- **POP (Post Office Protocol)**
- **IMAP (Internet Mail Access Protocol)**

E-mail has proved to be powerful and reliable medium of communication. Here are the benefits of **E-mail:**

- Reliable
- Convenience
- Speed
- Inexpensive
- Printable

E-mail is very fast. However, the speed also depends upon the underlying network.

Inexpensive

The cost of sending e-mail is very low.

Printable

It is easy to obtain a hard copy of an e-mail. Also an electronic copy of an e-mail can also be saved for records.

Global

F-mail can be sent and received by a person sitting across the globe.

It is also possible to send graphics, programs and sounds with an e-mail.

Disadvantages

Apart from several benefits of E-mail, there also exists some disadvantages as discussed below:

- Forgery
- Overload
- Misdirection
- Junk
- No response

E-mail doesn’t prevent from forgery, that is, someone impersonating the sender, since sender is usually not authenticated in any way.

- Convenience of E-mail may result in a flood of mail.
- It is possible that you may send e-mail to an unintended recipient.
- Junk emails are undesirable and inappropriate emails. Junk emails are sometimes referred to as spam.
- It may be frustrating when the recipient does not read the e-mail and respond on a regular basis.

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

https://www.geeksforgeeks.org/introduction-to-electronic-mail/

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

Book : Data and Computer Communications -William Stallings, Pearson Education, 2013
(Page No : 540 - 544)

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 39

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **V - Applications**

Date of Lecture: 09.04.2021

Topic of Lecture: WWW

Introduction :

- The World Wide Web is the universe of network-accessible information.
- In simple terms, The World Wide Web is a way of exchanging information between computers on the Internet.
- The World Wide Web is based on several different Technologies : Web browsers, Hypertext Markup Language (HTML) and Hypertext Transfer Protocol (HTTP).

Prerequisite knowledge for Complete understanding and learning of Topic:

- TCP/ IP Protocol
- Application layer responsibilities
- E-Mail

Detailed content of the Lecture:

Features of WWW :

- HyperText Information System
- 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 WWW :

There are 5 Components of WWW:

1. Uniform Resource Locator (URL): serves as system for resources on web.

2. HyperText Transfer Protocol (HTTP): specifies communication of browser and server.

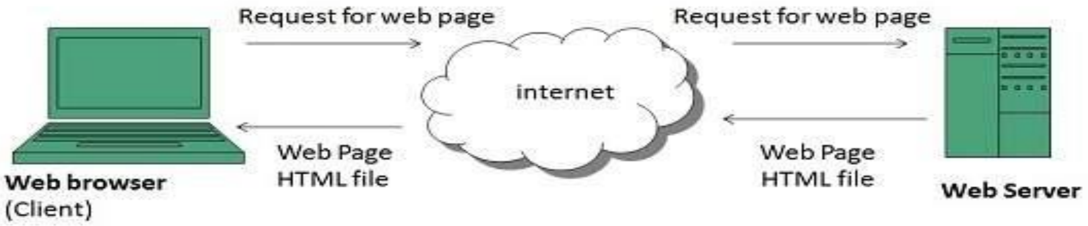
3. Hyper Text Markup Language (HTML): It Defines structure, organisation and content of webpage.

4. Web Server : A web server is computer software and underlying hardware that accepts requests via HTTP, the network protocol created to distribute web pages.

5. Web Browser : A web browser (commonly referred to as a browser or internet browser).

It is an application software for accessing the World Wide Web. When a user requests a web page from a particular website, the web browser retrieves the necessary content from a web server and then displays the page on the user's device.

- WWW Architecture



-

- Working of WWW :
- The World Wide Web is based on several different technologies :
- 1. Web browser.
- 2. Hypertext Markup Language (HTML).
- 3. Hypertext Transfer Protocol (HTTP).
- 1. Web browser : It is used to access webpages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet.
- 2. HTML : Hyperlinked resources on the World Wide Web can be accessed using software interface provided by Web browsers.
- 3. HTTP : It can be used for several tasks including : searches, mailing, transferring files, and much more. Some of the commonly used browsers are Internet Explorer, Opera Mini, Google Chrome.
- Applications of WWW :
- Online Forms
- Shopping Carts
- Word Processors
- Spreadsheets
- Video and Photo Editing
- File Conversion
- File Scanning
- E-mail programs such as Gmail, Yahoo and AOL.
- Popular Applications include Google Apps and Microsoft 365.
- WWW works on client- server approach. Following steps explains how the web works:
- User enters the URL (say, http://www.tutorialspoint.com) of the web page in the address bar of web browser.
- Then browser requests the Domain Name Server for the IP address corresponding to www.tutorialspoint.com.
- After receiving IP address, browser sends the request for web page to the web server using HTTP protocol which specifies the way the browser and web server communicates.

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

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 758 - 760)

Course Faculty

Verified by HOD

L 40

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **V - Applications**

Date of Lecture: 10.04.2021

Topic of Lecture: SNMP & SMTP

Introduction :

- Simple Network Management Protocol (SNMP) is an application–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices.
- 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.

Prerequisite knowledge for Complete understanding and learning of Topic:

- TCP/ IP Protocol
- WWW
- E-Mail

Detailed content of the Lecture:

SNMP :

SNMP is one of the widely accepted network protocols to manage and monitor network elements.

Components of SNMP :

- **SNMP Manager**
- **Managed devices**
- **SNMP agent**
- **Management Information Base (MIB)**

Basic Commands of SNMP :

GET: The GET operation is a request sent by the manager to the managed device.

GET NEXT: The significant difference is that the GET NEXT operation retrieves the value of the next MIB tree.

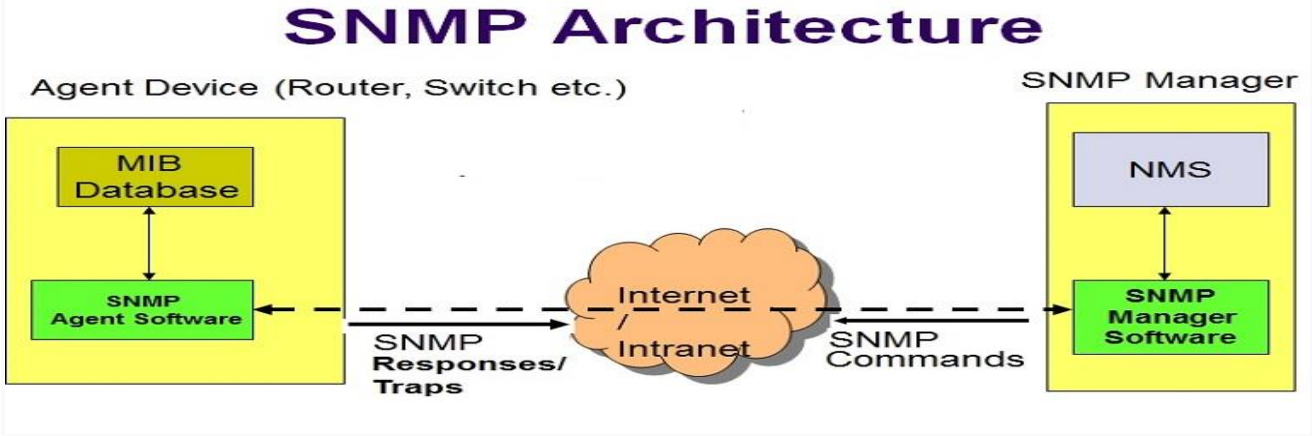
GET BULK: The GETBULK operation is used to retrieve voluminous data from large MIB table.

SET: This operation is used by the managers to modify or assign the value of the Managed device.

TRAPS: TRAPS are initiated by the Agents. It is a signal to the SNMP Manager by the Agent on the occurrence of an event.

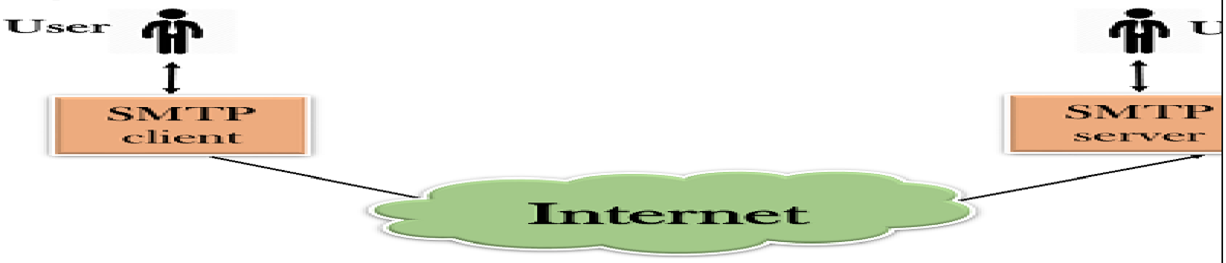
INFORM: It includes confirmation from the SNMP manager on receiving the message.

RESPONSE: It is the command used to carry back the value(s) or signal of actions directed by the SNMP Manager.



SMTP :

- 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.
- The main purpose of SMTP is used to set up communication rules between servers.
- Components of SMTP :



Working of SMTP :
It have the following Working Functionalities :

1. **Composition of Mail**
2. **Submission of Mail**
3. **Delivery of Mail**
4. **Receipt and Processing of Mail**
5. **Access and Retrieval of Mail**

Advantages:

- SMTP provides the simplest form of communicating through email message between various computers in a particular network.
- Since SMTP is developed from a simple platform , email messages may be sent easily and quickly.

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

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 747 - 753)

Course Faculty

Verified by HOD

L 41

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **V - Applications**

Date of Lecture: 12.04.2021

Topic of Lecture: Security, Threats and S ervices

Introduction :

- Network Security deals with all aspects related to the protection of the sensitive information assets existing on the network.
- It covers various mechanisms developed to provide fundamental security services for data communication.

Prerequisite knowledge for Complete understanding and learning of Topic:

- SMTP
- WWW
- E-Mail

Detailed content of the Lecture:

Security:

It describes the functioning of most common security protocols employed at different networking layers right from application to data link layer.

Goals of Network Security :

The primary goal of network security are Confidentiality, Integrity, and Availability. These three pillars of Network Security are often represented as CIA triangle.

1. Confidentiality − The function of confidentiality is to protect precious business data from unauthorized persons.

2. Integrity − It means maintaining and assuring the accuracy and consistency of data.

The function of integrity is to make sure that the data is reliable and is not changed by unauthorized persons.

3. Availability − The function of availability in Network Security is to make sure that the data, network resources/services are continuously available to the users, whenever they require it.

Security Services

fundamental security services as the following −

1. Confidentiality − E-mail message should not be read by anyone but the intended recipient.

2. Authentication − E-mail recipient can be sure of the identity of the sender.

3. Integrity − Assurance to the recipient that the e-mail message has not been altered since it was transmitted by the sender.

4. Non-repudiation − E-mail recipient is able to prove to a third party that the sender really did send the message.

5. Proof of submission − E-mail sender gets the confirmation that the message is handed to the mail delivery system.

6. Proof of delivery − Sender gets a confirmation that the recipient received the message.

Threats and Services :

- A Computer System Threat is anything that leads to loss or corruption of data or physical damage to the hardware or infrastructure.
- Security Threats can be many like Software attacks, theft of intellectual property, identity theft, theft of equipment or information.
- Threat is any activity that can lead to data loss/corruption through to delay of normal business operations.

Types of Threats

- There are physical and non-physical threats.
- Physical Threats : cause damage to computer systems hardware and infrastructure. Examples include theft, vandalism through to natural disasters.
- Non-physical Threats : Target the software and data on the computer systems.

Physical Threats

- A physical threat is a potential cause of an incident that may result in loss or physical damage to the computer systems.
- The following list classifies the physical threats into three main categories
- Internal: The threats include fire, unstable power supply, humidity in the rooms housing the hardware, etc.
- External: These threats include Lightning, floods, earthquakes, etc.
- Human: These threats include theft, vandalism of the infrastructure and hardware, accidental or intentional errors.

Non-Physical Threats

The following list is the common types of non-physical threats;

- Virus
- Trojans
- Worms
- Spyware
- Key loggers
- Adware
- Denial of Service Attacks
- Distributed Denial of Service Attacks
- Unauthorized access to computer systems resources such as data
- Phishing
- Other Computer Security Risks

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

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 793 - 796)

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

L 42

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **V - Applications**

Date of Lecture: 15.04.2021

Topic of Lecture: Cryptography

Introduction :

- Cryptography is a method of protecting information and communications through the use of codes.
- The information is intended can read and process it.
- The prefix "crypt-" means "hidden" or "vault" -- and the suffix "-graphy" stands for "writing."

Prerequisite knowledge for Complete understanding and learning of Topic:

- Security
- WWW
- E-Mail
- Threats

Detailed content of the Lecture:

Cryptography :

- Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms.

Cryptography Techniques

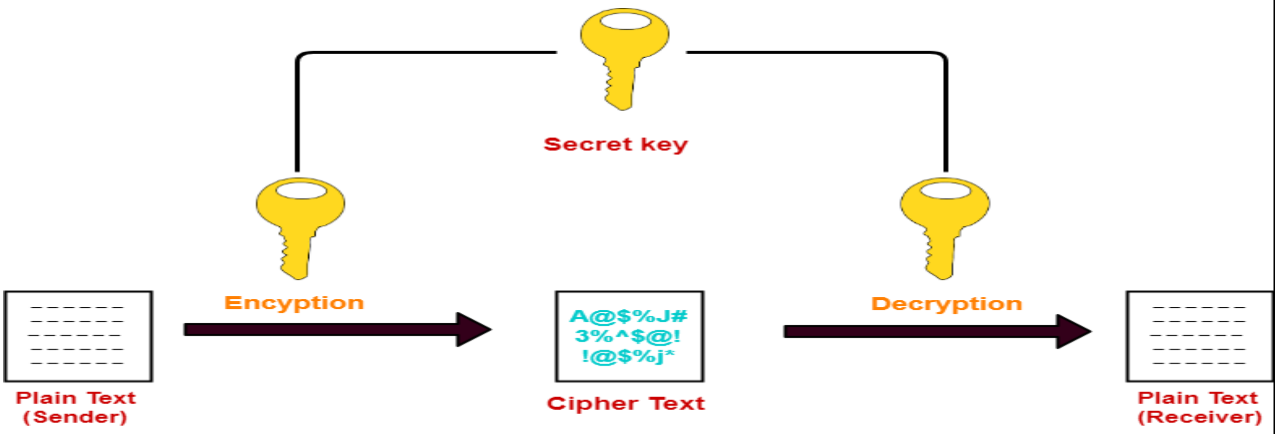
- Cryptography is closely related to the disciplines of cryptology and cryptanalysis.
- It includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit.
- Cryptography is used to convert Plaintext into Ciphertext is known as Encryption. then back again Ciphertext into Plaintext is known as Decryption.
- Encryption : Known to Unknown
- Decryption : Unknown to Known

Objectives of Cryptography

Cryptography concerns with the following Four objectives:

- **Confidentiality:** the information cannot be understood by anyone for whom it was unintended.
- **Integrity:** the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
- **Non-repudiation:** the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.
- **Authentication:** the sender and receiver can confirm each other's identity and the origin/destination of the information.

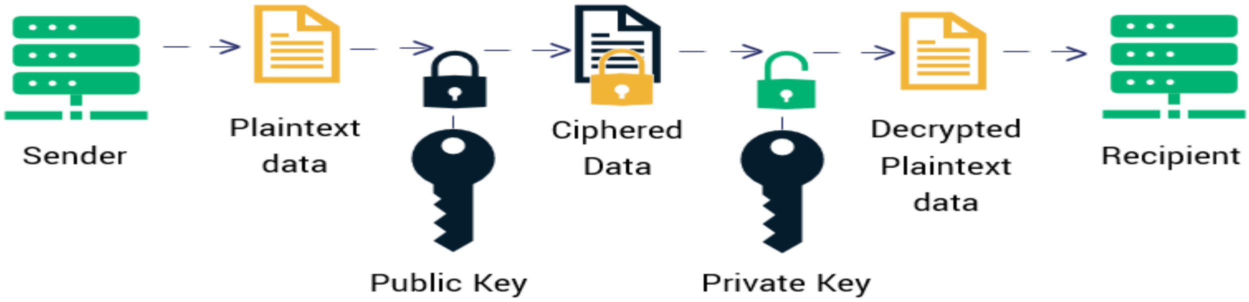
- Types of Cryptography :
- Single-key or Symmetric-key Cryptography.
- Public-key or Asymmetric-key Cryptography.
- 1. Single-key or Symmetric-key Cryptography :
- Symmetric cryptography is based on the use of just one key is used to both Encrypt and Decrypt the messages (only Private Key or Secret Key)
- 2. Public-key or Asymmetric-key Cryptography :
- Asymmetric cryptography, also known as public-key cryptography, Here Two keys are used to Encrypt and Decrypt the messages (Both Private and Public Key)
- Single-key or Symmetric-key Cryptography



Symmetric Key Cryptography

- Public-key or Asymmetric-key Cryptography

Asymmetric Encryption



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

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 794 - 798)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 43

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **V - Applications**

Date of Lecture: 17.04.2021

Topic of Lecture: DES

Introduction :

- The Data Encryption Standard is a symmetric-key algorithm for the encryption of digital data.
- The DES (Data Encryption Standard) algorithm is a symmetric-key block cipher created in the early 1970s by an IBM team and adopted by the National Institute of Standards and Technology (NIST).

Prerequisite knowledge for Complete understanding and learning of Topic:

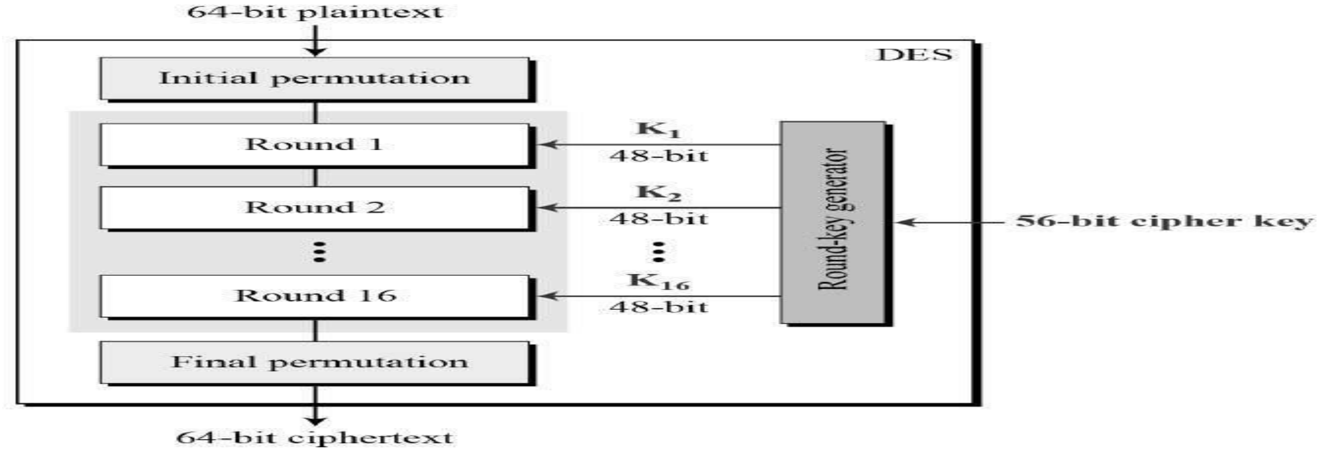
- Security
- Cryptography
- E-Mail
- Threats

Detailed content of the Lecture:

Data Encryption Standard :

- DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit.
- Key length is 64-bit.
- Since DES is based on the Feistel Cipher.
- Round function.
- Key schedule.
- Any additional processing − Initial and final permutation.

DES Algorithm



DES Algorithm Steps :

The algorithm process breaks down into the following steps:

1. The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.
2. The initial permutation (IP) is then performed on the plain text.
3. Next, the initial permutation (IP) creates two halves of the permuted block, referred to as Left Plain Text (LPT) and Right Plain Text (RPT).
4. Each LPT and RPT goes through 16 rounds of the encryption process.
5. Finally, the LPT and RPT are rejoined, and a Final Permutation (FP) is performed on the newly combined block.
6. The result of this process produces the desired 64-bit ciphertext.

DES Analysis

The DES satisfies both the desired properties of block cipher. These two properties make cipher very strong.

Avalanche effect − A small change in plaintext results in the very great change in the ciphertext.

Completeness − Each bit of ciphertext depends on many bits of plaintext.

DES Implementation

- You must choose a security provider to implement your data encryption algorithm.
- There are many available providers to choose from, but selecting one is the essential initial step in implementation.
- Your selection may depend on the language you are using, such as Java, Python, C, or MATLAB.

Lightweight Directory Access Protocol (LDAP) :

LDAP refers to Lightweight Directory Access Protocol. It is a protocol that is used for determining any individuals, organizations, and other devices during a network regardless of being on public or corporate internet.

It is practiced as Directories-as-a-Service and is the grounds for Microsoft building Activity Directory.

Some advantages of LDAP :

It is an automated protocol which makes it modernizing easier.

It supports existing technologies and allows multiple directories.

Some disadvantages of LDAP :

It requires the experience of deployment.

The directory servers are required to be LDAP obedient for deployment.

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

https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012

(Page No : 794 - 796)

Course Faculty

Verified by HOD

LECTURE HANDOUTS

L 44

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **V - Applications**

Date of Lecture: 19.04.2021

Topic of Lecture: RSA

Introduction :

- RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission.
- In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private).

Prerequisite knowledge for Complete understanding and learning of Topic:

- Security
- Cryptography
- DES
- Threats

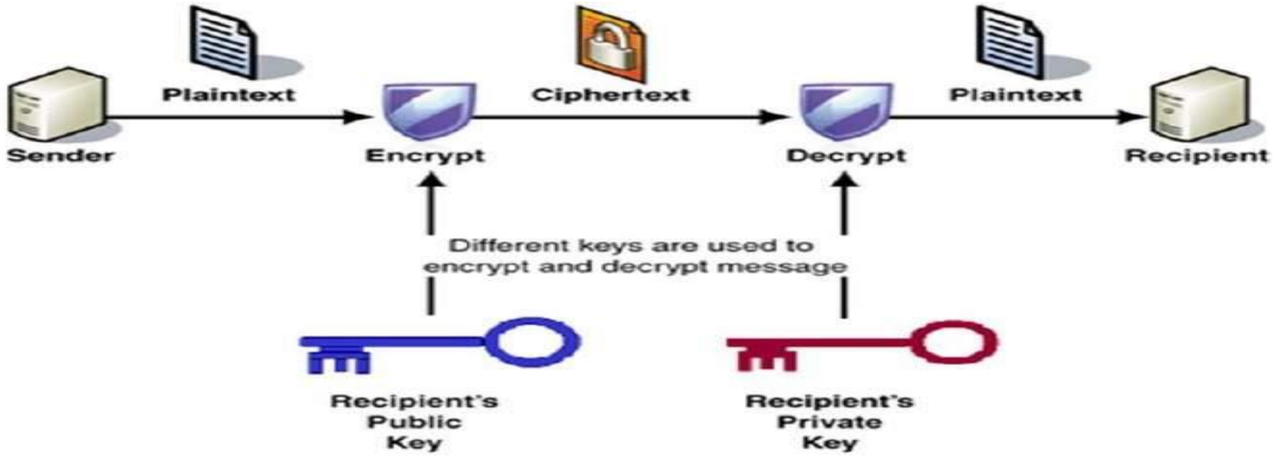
Detailed content of the Lecture:

RSA :

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.

Example :

- A client (for example browser) sends its public key to the server and requests for some data.
- The server encrypts the data using client's public key and sends the encrypted data.
- Client receives this data and decrypts it.



RSA Algorithm

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

The following steps to work on RSA algorithm :

Step 1: Generate the RSA modulus

The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N,

N=p*q

Step 2: Derived Number (e)

Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1).

Step 3: Public key

The specified pair of numbers n and e forms the RSA public key and it is made public.

Step 4: Private Key

Private Key d is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows :

ed = 1 mod (p-1) (q-1)

Encryption Formula

Consider a sender who sends the plain text message to someone whose public key is (n,e). To encrypt the plain text message in the given scenario, use the following syntax −

C = Pe mod n

Decryption Formula

The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver C has the private key d, the result modulus will be calculated as −

Plaintext = Cd mod n

Cipher

We refer to encryption and decryption algorithms as ciphers. The term cipher is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for secure communication. On the contrary, one cipher can serve millions of communicating pairs.

Key

A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key, and plaintext. These create the ciphertext. To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext. These reveal the original plaintext.

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

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

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

Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012

(Page No : 796 - 798)

Course Faculty

Verified by HOD

L 45

LECTURE HANDOUTS

MCA

I / II

Course Name with Code : **Data Communication And Networks / 19CAB09**

Course Faculty : **Mr. S.Nithyananth**

Unit : **V - Applications**

Date of Lecture:20.04.2021

Topic of Lecture: Web Security & SSL

Introduction :

- Web security is also known as "Cybersecurity". It basically means protecting a website or web application by detecting, preventing and responding to cyber threats.
- Secure Sockets Layer (SSL) is a security protocol that provides privacy, authentication, and integrity to Internet communications.

Prerequisite knowledge for Complete understanding and learning of Topic:

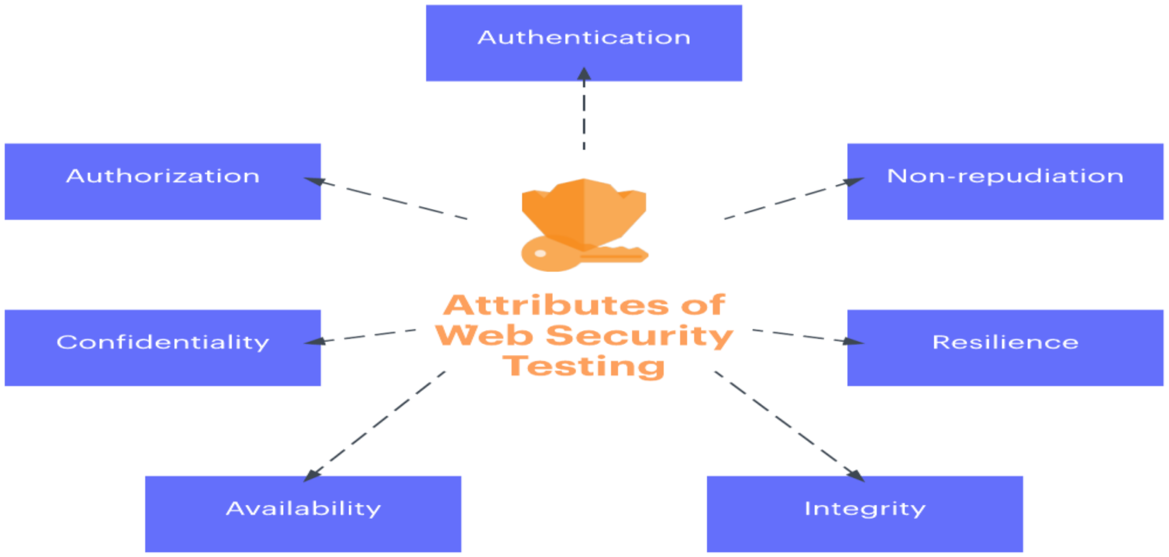
- Security
- Cryptography
- DES
- RSA

Detailed content of the Lecture:

Web Security :

web security is easy to install and it also helps the business people to make their website safe and secure.

A web application firewall prevents automated attacks that usually target small or lesser-known websites.



SSL

- Secure Sockets Layer (SSL) is a security protocol that provides privacy, authentication, and integrity to Internet communications.
- SSL eventually evolved into Transport Layer Security (TLS).
- SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol. It was first developed by Netscape in 1995.

How Does SSL Work?

- SSL encrypts data that is transmitted across the web.
- SSL initiates an authentication process called a handshake between two communicating devices to ensure that both devices are really who they claim to be.
- SSL also digitally signs data in order to provide data integrity.

SSL supports the following information security principles:

1. Encryption: protect data transmissions (e.g. browser to server, server to server, application to server, etc.)
2. Authentication: ensure the server you're connected to is actually the correct server.
3. Data integrity: ensure that the data that is requested or submitted is what is actually delivered.

Circuit-level Gateways

- Circuit-level gateways are another simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources.
- These types of firewalls typically operate at the session-level of the OSI model by verifying **TCP (Transmission Control Protocol)** connections and sessions.
- Circuit-level gateways are designed to ensure that the established sessions are protected.
- Typically, circuit-level firewalls are implemented as security software or pre-existing firewalls. Like packet-filtering firewalls, these firewalls do not check for actual data, although they inspect information about transactions.
- Therefore, if a data contains malware, but follows the correct TCP connection, it will pass through the gateway. That is why circuit-level gateways are not considered safe enough to protect our systems.

Application-level Gateways (Proxy Firewalls)

- Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called **'Application-level Gateways'**.Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server.

Video Content / Details of website for further learning (if any):
https://www.goodfirms.co/glossary/web-security/

Important Books/Journals for further learning including the page nos.:
Book : Data Communication and Networking -Forouzan, Fifth Edition, TMH 2012
(Page No : 802 - 804)

Course Faculty

Verified by HOD