University of Al-Qadisiyah
College of Computer Science and Information Technology
Information Systems Department

Computer Network I

Lecture 1

Introduction

2023

Introduction

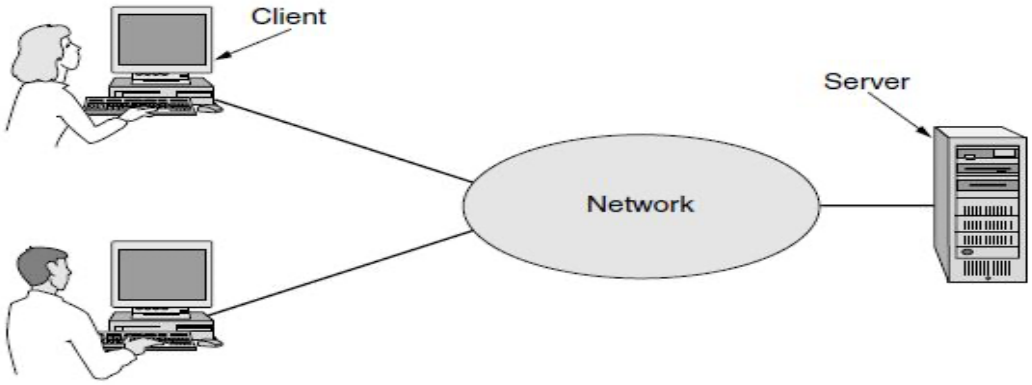
Computer network: collection of autonomous computers interconnected by a single technology.

Two computers are said to be interconnected if they are able to exchange information. The connection needs to be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used.

Resource sharing: The goal is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource or the user.

Communication medium refers to the physical channel through which data is sent and received.

Client-server model: In this model, the data are stored on powerful computers called **servers**. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simpler machines, called **clients**, on their desks, with which they access remote data, for example, to include in spreadsheets they are constructing.

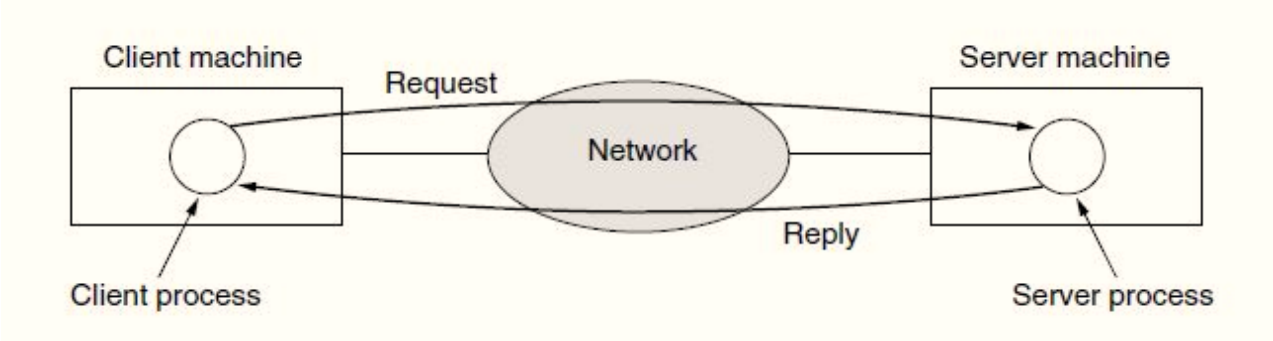


A network with two clients and one server.

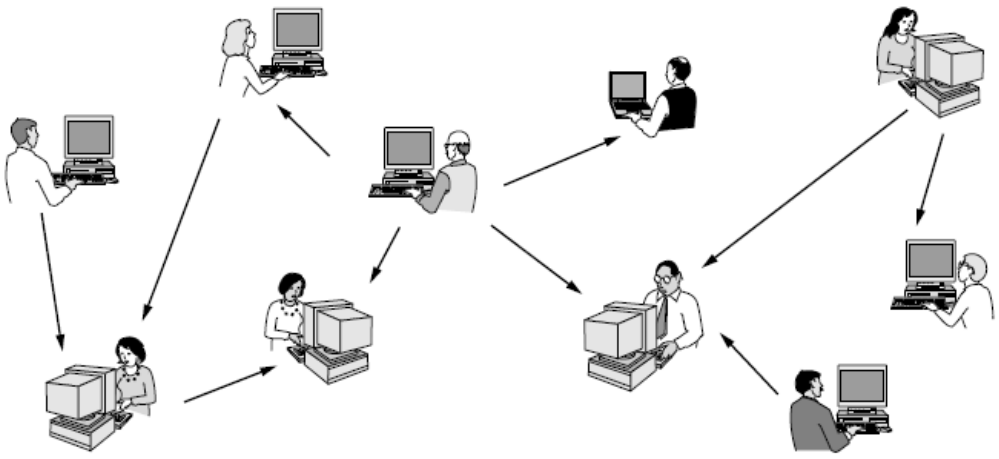
Note: Sometimes we will refer to the human user of the client machine as the ‘‘client,’’ but it should be clear from the context whether we mean the computer or its user.

Example: Web application??

The Communication between server and clients takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply.



The client-server model involves requests and replies.



In a peer-to-peer system there are no fixed clients and servers.

Peer-to-peer: popular model of communication, in which every person can communicate with one or more other people; there is no fixed division into clients and servers.

What is the idea behind using "peer-to-peer" model?

Example??

Two **important dimensions** in networks to understand: transmission technology and scale.

A- Transmission technology

There are two types of transmission technology that are in widespread use: **broadcast** links and **point-to-point (unicasting)** links.

Point-to-point links connect individual pairs of machines, this transmission with exactly one sender and exactly one receiver.

In contrast, on a **broadcast** network, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others.

Example: wireless network.

Broadcasting??

Multicasting??

B- Scale

Distance is important as a classification metric because different technologies are used at different scales.

1- **PAN** (**Personal Area Network**): Let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals.

What is the Wireless transmission media in this case??

2- **LAN** (**Local Area Network**): A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory. LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information. When LANs are used by companies, they are called **enterprise networks**.

3- **MAN (Metropolitan Area Network):** covers a city. The best-known examples of MANs are the cable television networks available in many cities.

4- **WAN** (**Wide Area Network**) spans a large geographical area, often a country or continent. The best example is a company with branch offices in different cities.

Internetwork: A collection of interconnected networks is called an **internetwork** or **internet**. It is required when people connected to one network often want to communicate with people attached to a diff

University of Al-Qadisiyah
College of Computer Science and Information Technology
Information Systems Department

Computer Network I

Lecture 2

Network Topology

2023

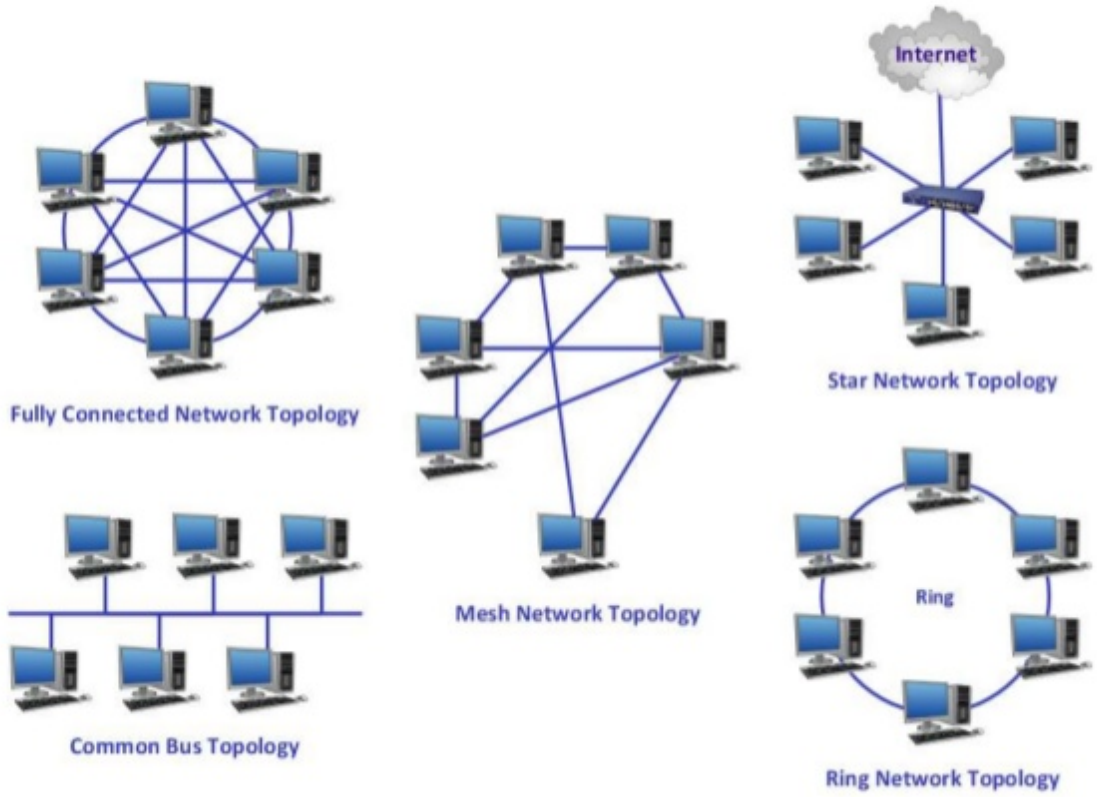
Network Topology

A network topology is the arrangement of a network, including its nodes and connecting lines. There are two ways of defining network geometry: the physical topology and the logical (or signal) topology.

- **Physical topology** describes how network devices are physically connected - in other words, how devices are actually plugged into each other. We're talking about cables, wireless connectivity, and more.
- **Logical (signal) topology** describes how network devices appear to be connected to each other.

For example, in a logical diagram of your office network, you may show a connection between location A and location B. But in the actual physical network, your data may go through switching points in several other locations as well. The logical path is a high-level representation; the physical path is the actual route.

PHYSICAL TOPOLOGIES



Star Topology: All computers and devices are connected to a centrally located hub, switch, or router. The hub or switch collects and distributes the flow of data within the network. It's better to use a switch than a hub because a switch transmits the data to the intended recipient rather than to all hosts on a network.

Bus Topology: All computers and devices are connected in series to a single linear cable called a trunk or sometimes called a backbone. Both ends of the trunk must be terminated to stop the signal from bouncing back up the cable. Because

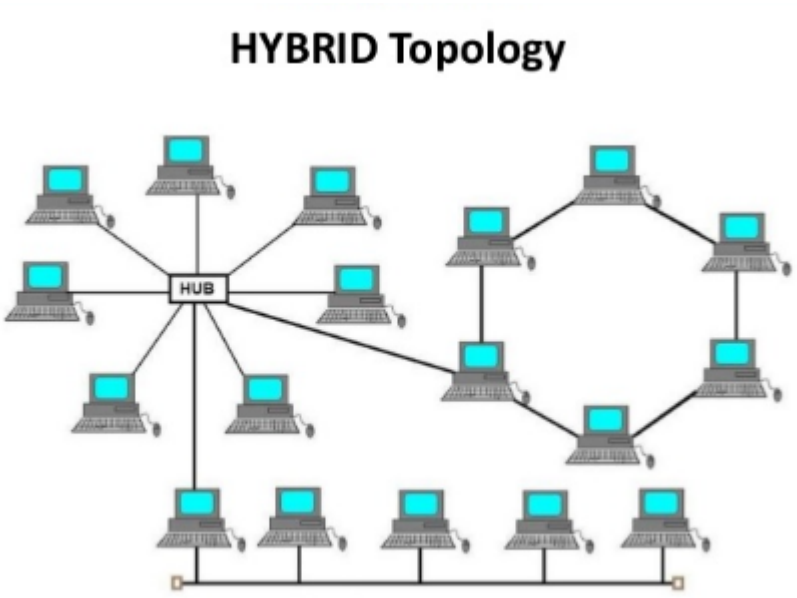
the bus topology does not have a central point it is difficult to troubleshoot problems. Also, a break at any point along the bus can cause the entire network to go down.

Ring Topology: In this topology, all computers and devices are connected to cable that forms a closed loop. Each computer on this type of topology acts like a repeater and boosts the signal before sending it to the next computer. It transmits data by passing a "token" around the network. Hence this type of network is commonly called a token ring network. Similar to the Bus topology, if one computer fails, the entire network goes down.

Mesh Topology: Employs either of two schemes, called full mesh and partial mesh. In the full mesh topology, each workstation is connected directly to each of the others. In the partial mesh topology, some workstations are connected to all the others, and some are connected only to those other nodes with which they exchange the most data.

Tree Topology: It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

Hybrid Topology: It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

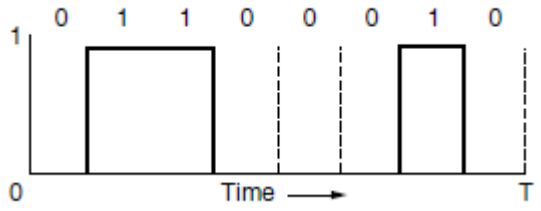


Data Communication

Information can be transmitted on wires by varying some physical property such as voltage or current. By representing the value of this voltage or current as a single-valued function of time, $f(t)$, we can model the behavior of the signal and analyze it mathematically.

Bandwidth-Limited Signals

The relevance of all of this to data communication is that real channels affect different frequency signals differently. Let us consider a specific example: the transmission of the ASCII character ‘‘b’’ encoded in an 8-bit byte. The bit pattern that is to be transmitted is 01100010.



The width of the frequency range transmitted without being strongly attenuated is called the **bandwidth**. The **bandwidth** is a physical property of the transmission medium that depends on, for example, the construction, thickness, and length of a wire or fiber.

University of Al-Qadisiyah
College of Computer Science and Information Technology
Information Systems Department

Computer Network I

Lecture 3

Network Devices

2022

Network Devices

Computer networking devices are known by different names such as networking devices, networking hardware, network equipment etc. However, all of the names mean the same but have got different purposes.

Hub

Hub is one of the basic icons of networking devices which connect networking devices physically together. Hubs are fundamentally used in networks that use **twisted pair cabling** to connect devices. They are designed to transmit the packets to the other appended devices without altering any of the transmitted packets received. They act as pathways to direct electrical signals to travel along. They transmit the information regardless of the fact if data packet is destined for the device connected or not.

Hub falls in two categories:

Active Hub: They are smarter than the passive hubs. They not only provide the path for the data signals in fact they regenerate, concentrate and strengthen the signals before sending them to their destinations. Active hubs are also termed as **'repeaters'**.

Passive Hub: They are more like point contact for the wires to built in the physical network. They have nothing to do with modifying the signals.

Switches

Switches are the linkage points of an Ethernet network. Just as in hub, devices in switches are connected to them through twisted pair cabling. But the difference shows up in the manner both the devices; hub and a switch treat the data they receive. **Hub** works by sending the data to all the ports on the device whereas a **switch** transfers it only to that port which is connected to the destination device.

Repeater

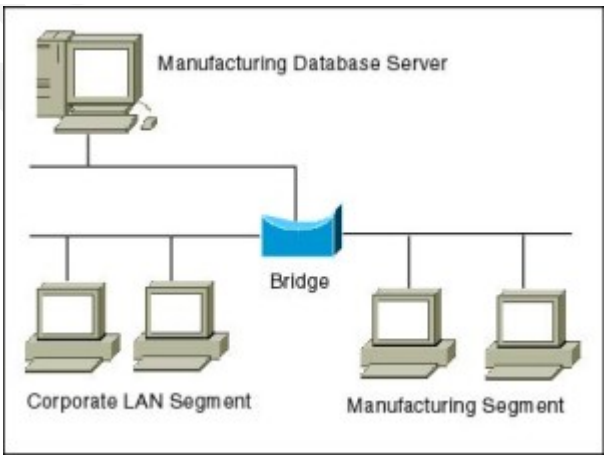
A repeater is an electronic device that amplifies the signal it receives. In other terms, you can think of repeater as a device which receives a signal and

retransmits it at a higher level or higher power so that the signal can cover longer distances.

For example, inside a college campus, the hostels might be far away from the main college where the ISP line comes in. If the college authority wants to pull a wire in between the hostels and main campus, they will have to use repeaters if the distance is much because different types of cables have limitations in terms of the distances they can carry the data for.

Bridges

A bridge is a computer networking device that builds the connection with the other bridge networks which use the same protocol. It connects two local-area networks; two physical LANs into larger logical LAN or two *segments* of the same LAN that use the same protocol.



There are mainly three types in which bridges can be characterized: Transparent Bridge, Source Route Bridge, and Translational Bridge.

Routers

Router is used to create larger complex networks by complex traffic routing. It has the ability to connect dissimilar LANs on the same protocol. It also has the ability to limit the flow of broadcasts. A router primarily comprises of a hardware device or a system of the computer which has more than one network interface and routing software.

When a router receives the data, it determines the destination address by reading the header of the packet. Once the address is determined, it searches in its **routing table** to get know how to reach the destination and then forwards the packet to the higher hop on the route. The hop could be the final destination or another router.

Routing tables play a very pivotal role in letting the router makes a decision. Thus a routing table is ought to be *updated* and *complete*.

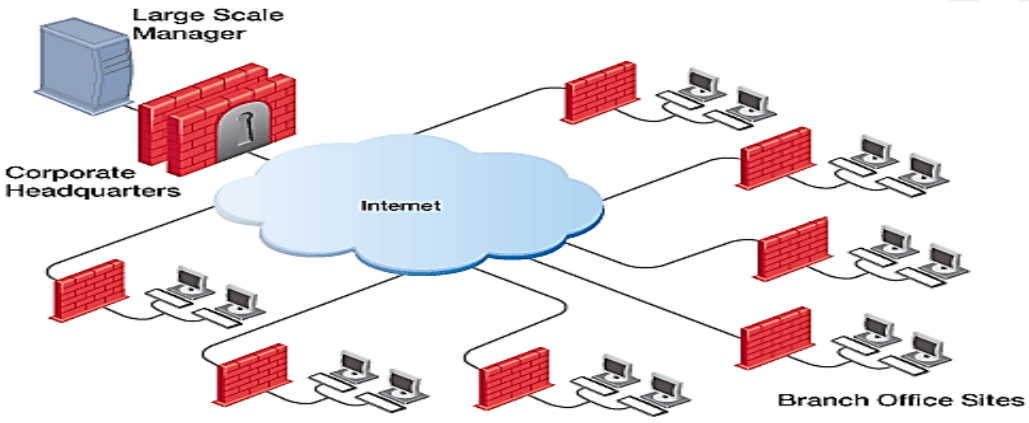
Brouters

Brouters are the combination of both the bridge and routers. They take up the functionality of the both networking devices serving as a *bridge* when forwarding data between networks, and serving as a *router* when routing data to individual systems. Brouter functions as a filter that allows some data into the local network and redirects unknown data to the other network.

Gateways

Gateway is a device which is used to connect multiple networks and passes packets from one packet to the other network. Acting as the 'gateway' between different networking systems or computer programs, a gateway is a device which forms a link between them. It allows the computer programs, either on the same

computer or on different computers to share information across the network through protocols. A router is also a gateway, since it interprets data from one network protocol to another.



Network card

Network cards also known as Network Interface Cards (NICs) are hardware devices that connect a computer with the network. They are installed on the mother board. They are responsible for developing a physical connection between the network and the computer. Computer data is translated into electrical signals send to the network via Network Interface Cards.

Modems

Modem is a device which converts the computer-generated digital signals of a computer into analog signals to enable their travelling via phone lines. The 'modulator-demodulator' or modem can be used as a dial up for LAN or to connect to an ISP. Modems can be both external, as in the device which connects to the USB or the serial port of a computer, or proprietary devices for handheld gadgets and other devices, as well as internal; in the form of add-in expansion cards for computers.

Network protocols

Network protocols define a language of instructions and conventions for communication between the network devices. It is essential that a networked computer must have one or more protocol drivers. Usually, for two computers to interconnect on a network, they must use identical protocols. At times, a computer is designed to use multiple protocols. Network protocols like HTTP, TCP/IP offer a basis on which much of the Internet stands.

University of Al-Qadisiyah
College of Computer Science and Information Technology
Information Systems Department

Computer Network I

Lecture 4

REFERENCE MODELS

2022

REFERENCE MODELS

Over the past couple of decades many of the networks that were built used different hardware and software implementations, as a result they were incompatible and it became difficult for networks using different specifications to communicate with each other. To address the problem of networks being incompatible and unable to communicate with each other, the International Organization for Standardization (ISO) researched various network schemes. The ISO recognized there was a need to create a NETWORK MODEL that would help vendors create interoperable network implementations.

A reference model is a conceptual layout that describes how communication between devices should occur. A reference model has many advantages such as it defines standards for building network components thereby permitting multiple-vendor development and also defines which functions should be performed at each layer of the model thereby promoting the standardization of network.

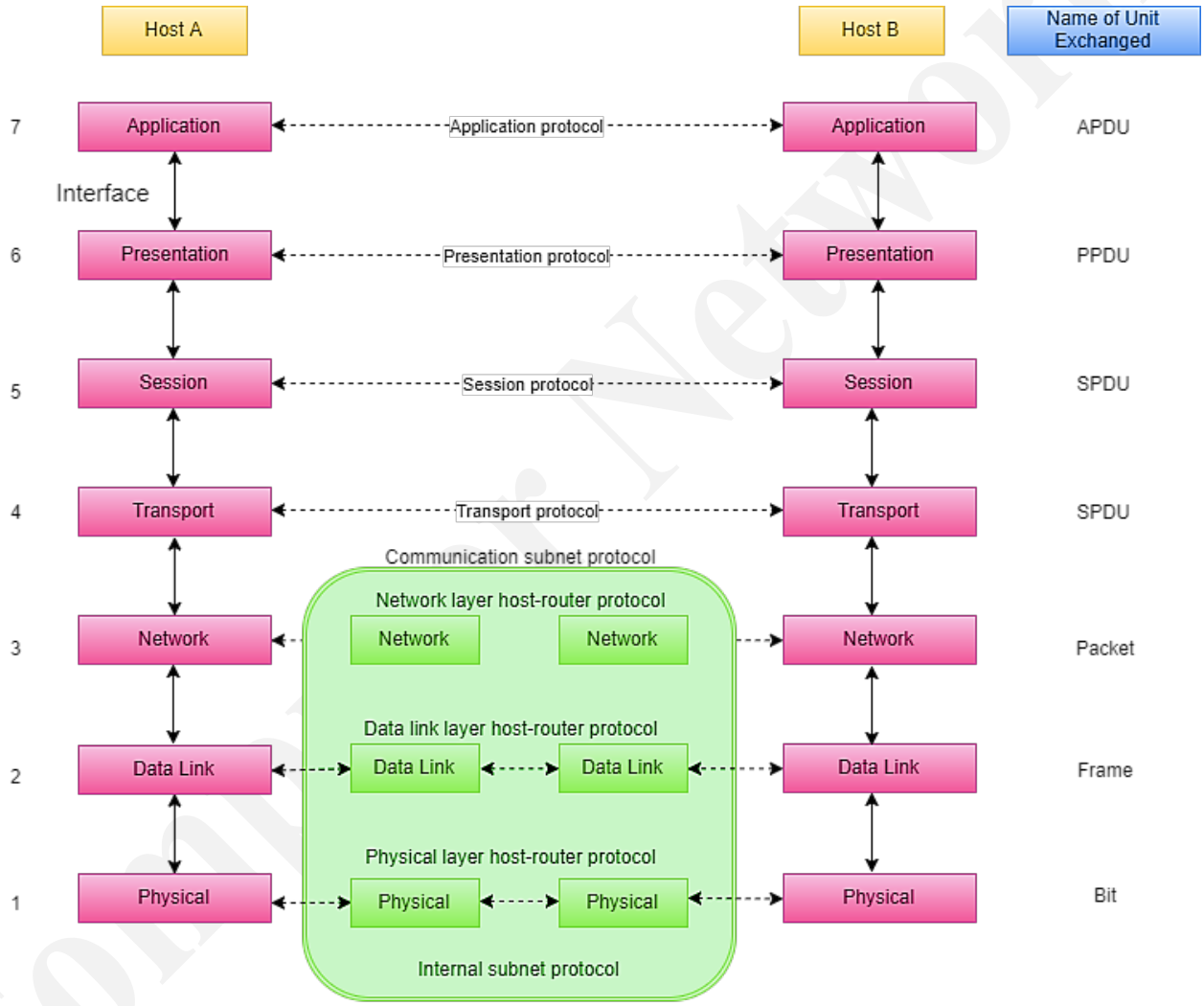
The OSI Model

There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other ISO has developed a standard. ISO stands for International organization of Standardization. This is called a model for Open System Interconnection (OSI) and is commonly known as OSI model.

The OSI model is a seven-layer architecture. It defines seven layers or levels in a

complete communication system.

Below we have the complete representation of the OSI model, showcasing all the layers and how they communicate with each other.



Feature of OSI Model

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

Following are the functions performed by each layer of the OSI model:

OSI Model Layer 1: The Physical Layer

1. Physical Layer is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

OSI Model Layer 2: Data Link Layer

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.

3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

OSI Model Layer 3: The Network Layer

1. Network Layer routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

OSI Model Layer 4: Transport Layer

1. Transport Layer decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.

4. Transport layer can be very complex, depending upon the network requirements.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

OSI Model Layer 5: The Session Layer

1. Session Layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

OSI Model Layer 6: The Presentation Layer

1. Presentation Layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It performs Data compression, Data encryption, Data conversion etc.

OSI Model Layer 7: Application Layer

1. Application Layer is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

Merits of OSI reference model

1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

University of Al-Qadisiyah
College of Computer Science and Information Technology
Information Systems Department

Computer Network I

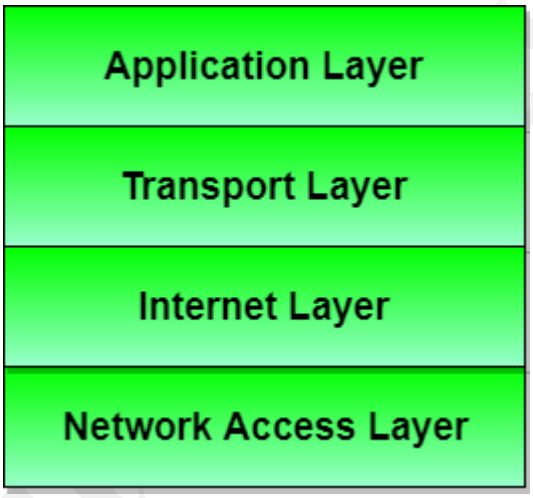
Lecture 5

The TCP/IP Reference Model

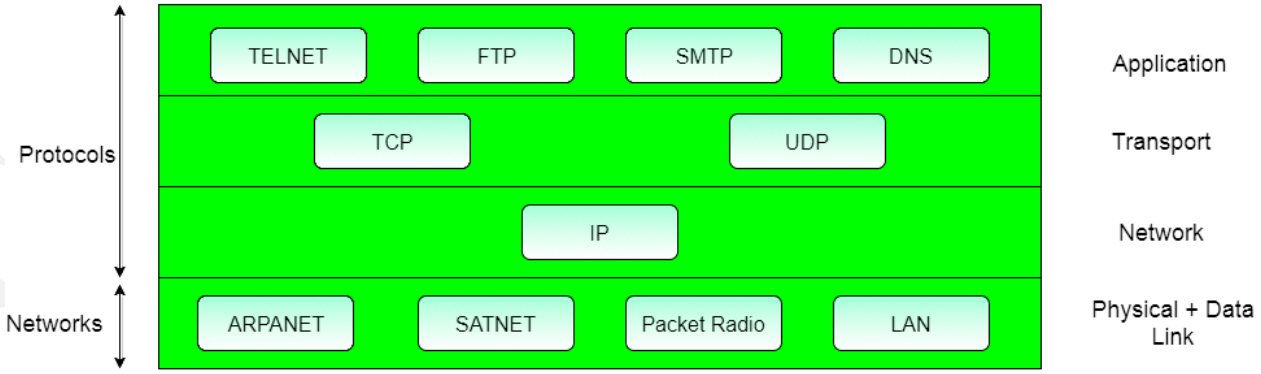
2022

The TCP/IP Reference Model

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. They also offer simple naming and addressing schemes.



Protocols and networks in the TCP/IP model:



The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Below we have discussed the 4 layers that form the TCP/IP reference model:

TCP/IP Model Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

TCP/IP Model Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called an internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.

5. IP (Internet Protocol) is used in this layer.
6. The various functions performed by the Internet Layer are:
    - Delivering IP packets
    - Performing routing
    - Avoiding congestion

TCP/IP Model Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

TCP/IP Model Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.

3. SMTP(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.
5. It allows peer entities to carry conversation.
6. It defines two end-to-end protocols: TCP and UDP
   - TCP(Transmission Control Protocol): It is a reliable connection-oriented protocol which handles byte-stream from source to destination without error and flow control.
   - UDP(User-Datagram Protocol): It is an unreliable connection-less protocol that do not want TCPs, sequencing and flow control. Eg: One-shot request-reply kind of service.

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

Differences between OSI and TCP/IP Reference Model

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. OSI model has a separate Presentation layer and Session layer.	3. TCP/IP does not have a separate Presentation layer or Session layer.
4. Transport Layer is Connection Oriented.	4. Transport Layer is both Connection Oriented and Connection less.
5. Network Layer is both Connection Oriented and Connection less.	5. Network Layer is Connection less.
6. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	6. TCP/IP model is, in a way implementation of the OSI model.
7. Network layer of OSI model provides both connection oriented and	7. The Network layer in TCP/IP model

connectionless service.	provides connectionless service.
8. OSI model has a problem of fitting the protocols into the model.	8. TCP/IP model does not fit any protocol
9. Protocols are hidden in OSI model and are easily replaced as the technology changes.	9. In TCP/IP replacing protocol is not easy.
10. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	10. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
11. It has 7 layers	11. It has 4 layers

University of Al-Qadisiyah
College of Computer Science and Information Technology
Information Systems Department

Computer Network I

Lecture 6

IP Address

2022

IP Address

IP address is a unique string of numbers separated by full stops that identifies each computer using the Internet Protocol to communicate over a network. Interconnected networks must agree on an IP addressing plan. IP addresses must be unique and generally cannot be used in different places on the Internet at the same time; otherwise, routers would not know how best to route packets to them.

IPv4 Address:

An IPv4 address (version 4) consists of 32 bits of information. These bits are divided into four sections, referred to as octets or bytes, each containing 1 byte (8 bits).

IPv4 Notation:

IPv4 address can be written by using one of these three methods:

1. Dotted-decimal, as in 172.16.30.56
2. Binary, as in 10101100.00010000.00011110.00111000
3. Hexadecimal, as in AC.10.1E.38

Example: Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number dots for separation.

a. 129.11.11.239

b. 193.131.27.255

IPv4 Classes:

The designers of the Internet decided to create classes of networks based on network size. For the small number of networks possessing a very large number of nodes, they created the rank Class **A** network. At the other extreme is the Class **C** network, which is reserved for the numerous networks with a small number of nodes. The class distinction for networks between very large and very small is predictably called the Class **B** network.

IP addresses consist of three portions:

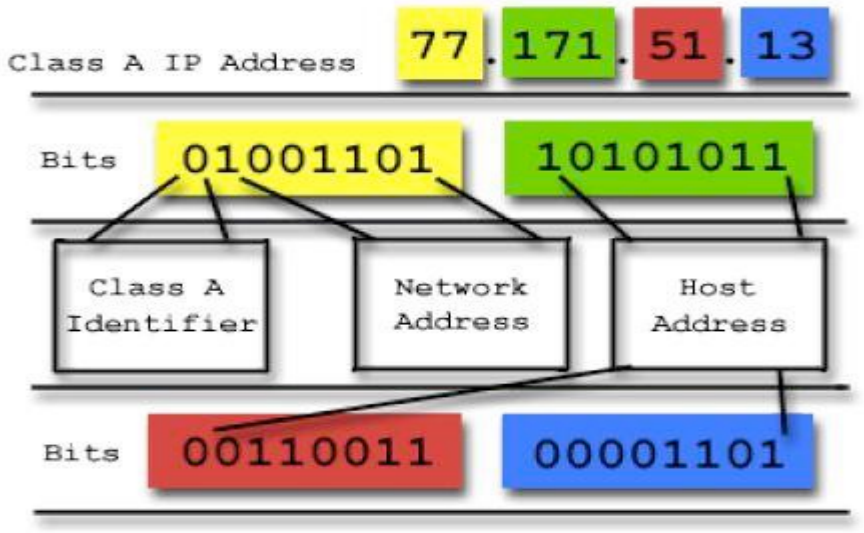
The first portion, or initial bit sequence, identifies the Address Class of the network. There are five Address Classes - Class A, B, C, D and E.

Class A: 0 - Class B: 10 - Class C: 110 - Class D: 1110 - Class E: 1111

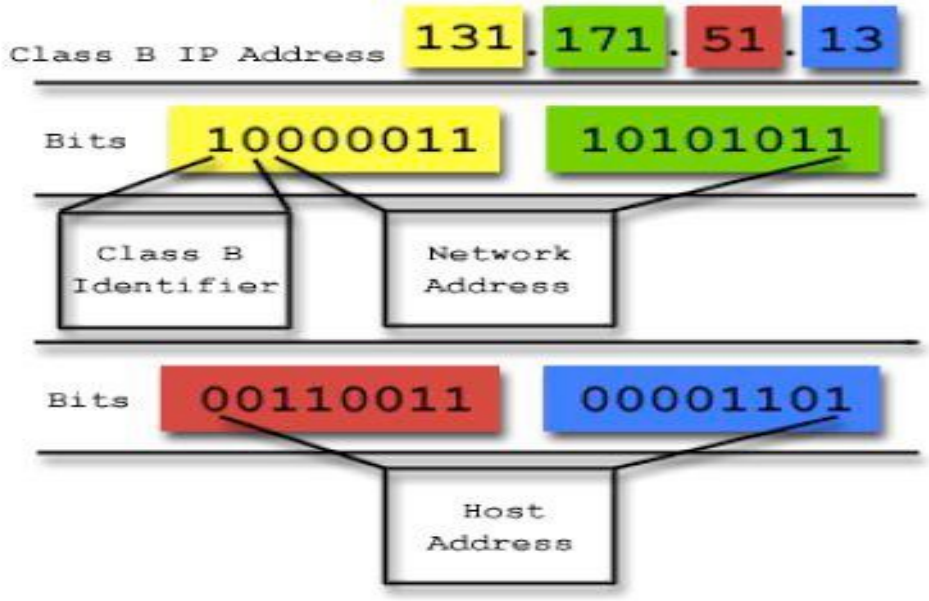
The second portion identifies the Network ID.

The last portion identifies the ID of the host within the specified network

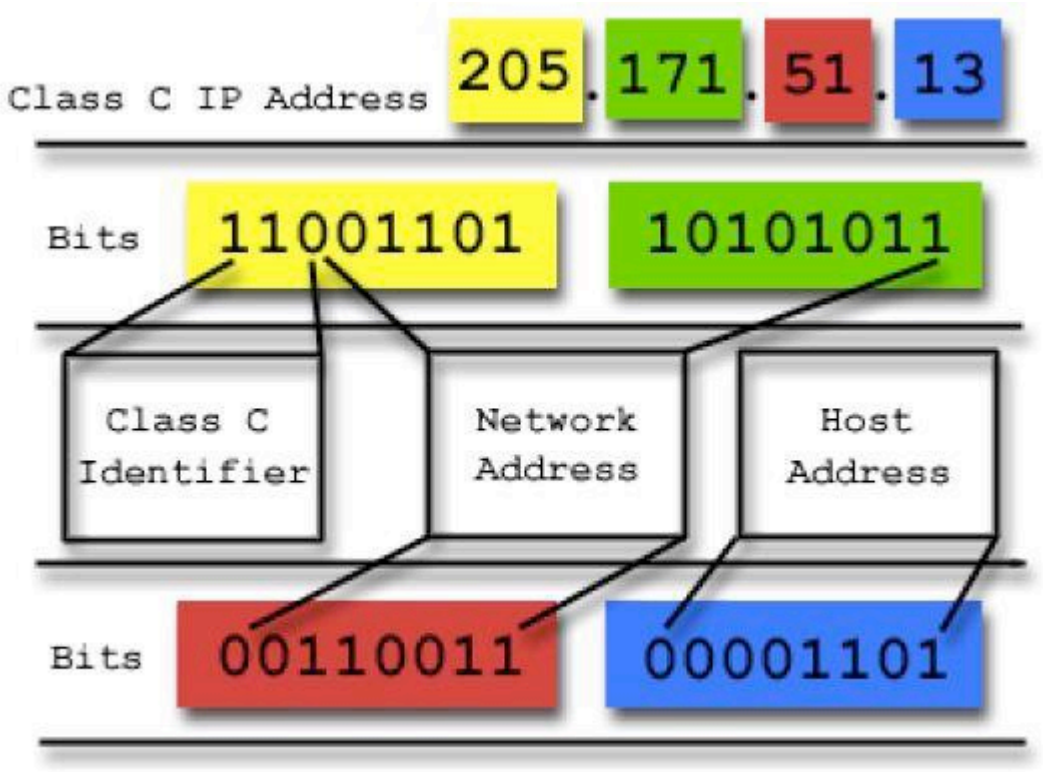
Class A: first octet 1 →126:



Class B: first octet 128 → 191



Class C: first octet 192 → 223

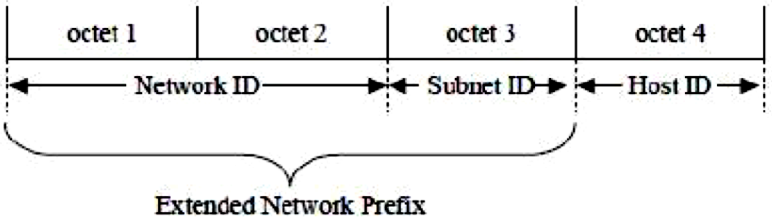


There are also Class D and Class E IP addresses, but these shouldn't be used as they are reserved for multicasting (Class D: 224 → 239) and for experimentation and testing (Class E: 240 → 254).

Subnetting:

Subnetting is used to subdivide a single class of network in to multiple smaller networks. For example your organization has a Class B IP address of 166.144.0.0 before you implement subnetting; the Network ID and Host ID are divided as follows:

To organize your network and allow for growth, you decide to use the 3rd octet to subdivide your network into subnets. Now the Network ID and Host ID are divided as follows:



IPv6 Address

Internet Protocol version 6 (IPv6) is the network community's answer to resolving some of the problems in IPv4. These problems include a somewhat limiting 32-bit address space, lack of built-in security, a sometimes complicated setup, and a lack of built-in QoS (Quality of Service).

An IPv6 address is 128 bits compared to the 32 bits in an IPv4 address. This length increases the number of possible addresses from about 4 billion in IPv4 to 3.4 x 1038 addresses (that's 34 followed by 37 zeros!) in IPv6. Unless IP addresses are assigned to every star in the universe, it's safe to say enough IPv6 addresses will be available. IPv6 is auto configuring, which means there is no IP address to assign and no subnet mask to determine.

IPv6 Address Notation:

Just as with IPv4, there is some special notation for writing down IPv6 addresses. The standard representation is x:x:x:x:x:x:x:x, where each "x" is a hexadecimal representation of a 16-bit piece of the address. An example would be 47CD:1234:4422:ACO2:0022:1234:A456:0124

Any IPv6 address can be written using this notation. Since there are a few special types of IPv6 addresses, there are some special notations that may be helpful in certain circumstances. For example, an address with a large number of contiguous 0s can be written more compactly by omitting all the 0 fields.

Thus: 47CD:0000:0000:0000:0000:0000:A456:0124

Could be written: 47CD::A456:0124

Clearly, this form of shorthand can only be used for one set of contiguous 0s in an address to avoid ambiguity.

Since there are two types of IPv6 addresses that contain an embedded IPv4 address, these have their own special notation that makes extraction of the IPv4 address easier. For example, the "IPv4-mapped IPv6 address" of a host whose IPv4 address was 128.96.33.81 could be written as:

::FFFF:128.96.33.81

That is, the last 32 bits are written in IPv4 notation, rather than as a pair of hexadecimal numbers separated by a colon. Note that the double colon at the front indicates the leading 0s.

University of Al-Qadisiyah
College of Computer Science and Information Technology
Information Systems Department

Computer Network I

Lecture 7

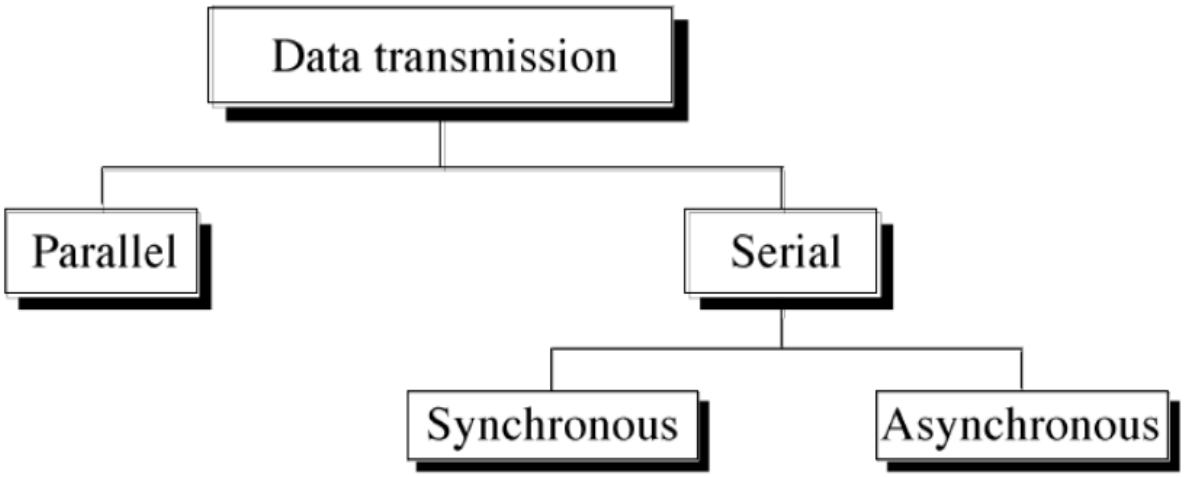
Transmission of Digital Data: Interfaces and Modems

2022

Transmission of Digital Data: Interfaces and Modems

Transmission of Digital Data

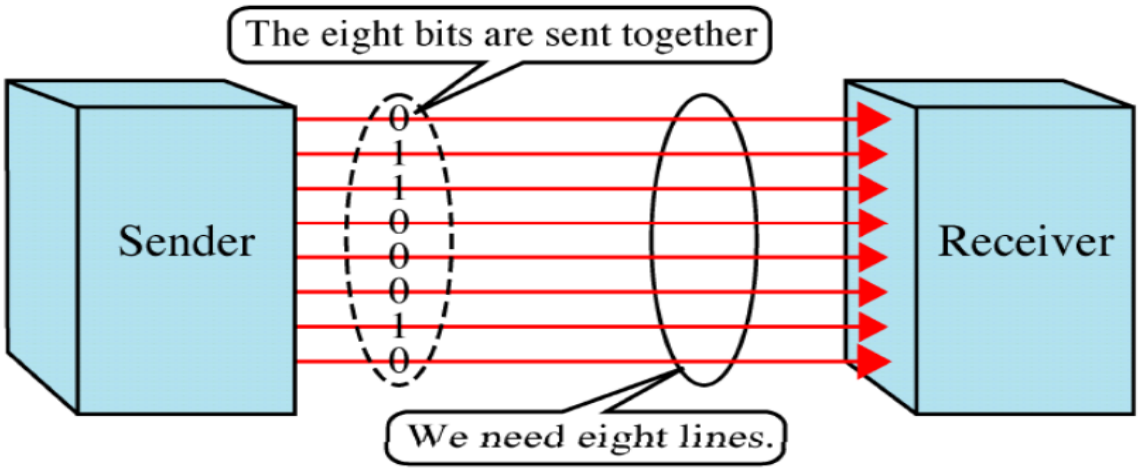
Primary concern when considering the transmission of data from one device to another is the wiring.



Transmission of Digital Data

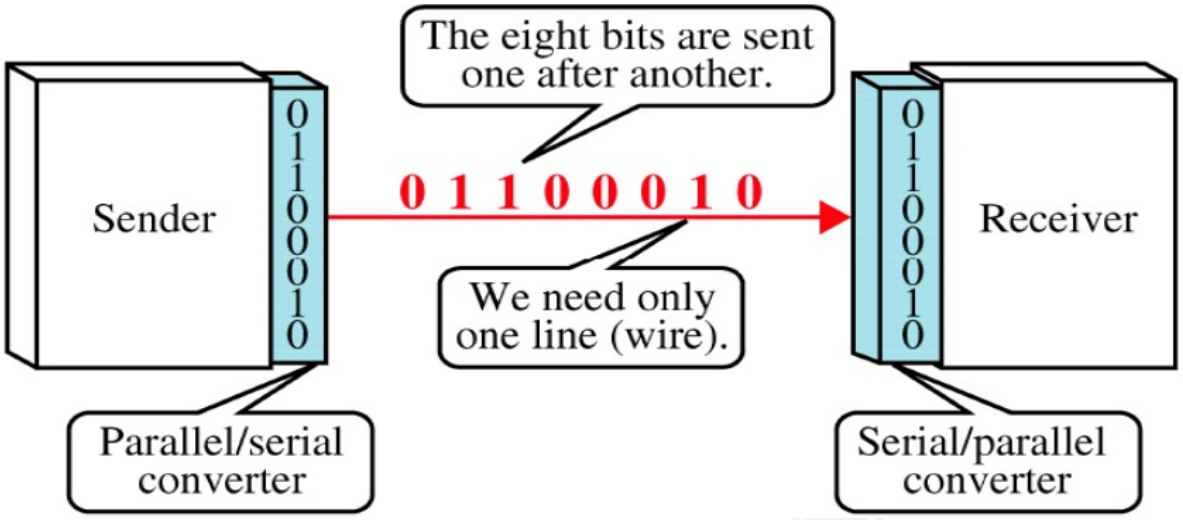
Parallel Transmission

By grouping, we can send data n bits at a time instead of one. It is speed and expansive.



Serial Transmission

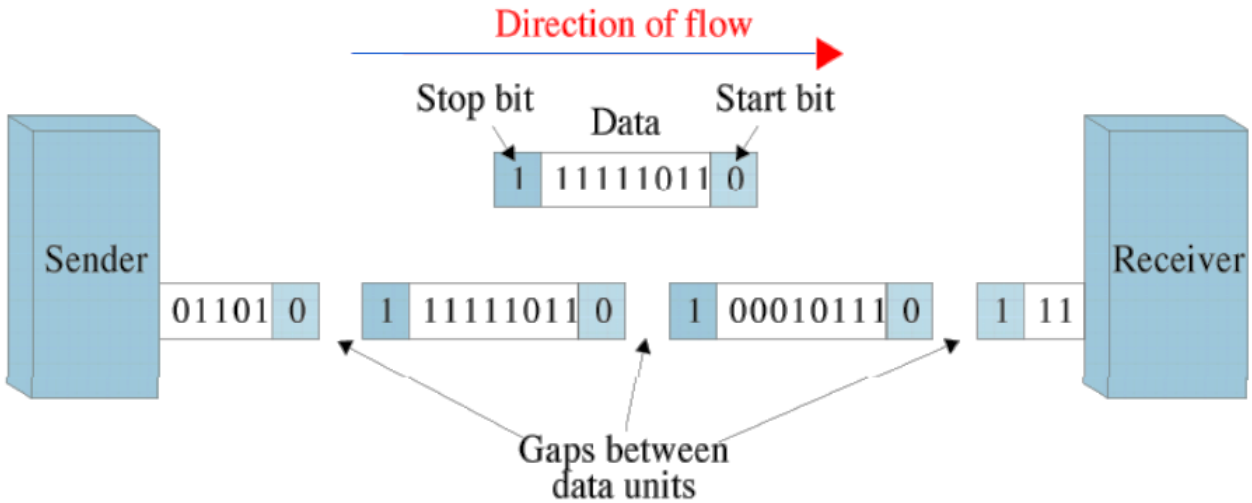
Transmit the data as one bit follows another. It uses a channel and require interface converter.



Asynchronous Transmission

Send one start bit (0) at the beginning and one or more stop bits (1) at the end of each byte. It is cheap and effective.

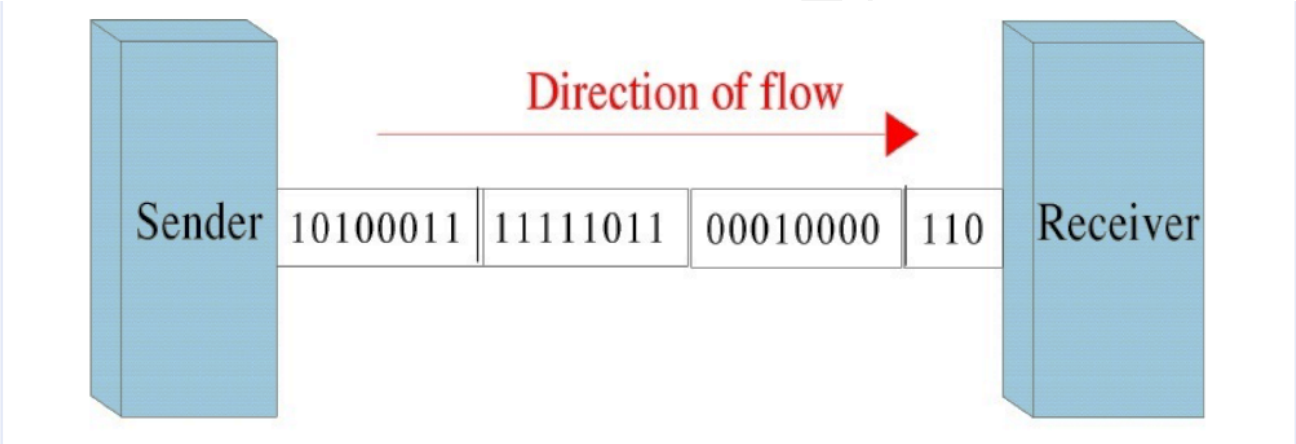
- sender provides a synchronization signal to the receiver before starting the transfer of each message



Synchronous transmission

Sending bits one after another without start/stop bits or gaps. It is the responsibility of the receiver to group the bits. The receiver counts the bits as they arrive and groups them in eight-bit units.

- Sender and receiver use the same clock signal



DTE-DCE Interface

- DTE(Data Terminal equipment)
- DCE(Data Circuit-terminating Equipment)

DTE-DCE Connection Diagram

Data Terminal Equipment (DTE): is any equipment that is either a source or destination for binary digital data. It includes terminal, microcomputer, computer, printer, fax machine and so on.

Data Circuit-Terminating Equipment (DCT): is any device (functional unit) that transmits or receives data in the form of an analog or digital signal through a network, for example: Modulator/demodulator (MODEM).

MODEM

- **Modulator:** converts a digital signal to an analog signal.
- **Demodulator:** converts an analog signal to a digital signal.

DTE do not generally communicate with each other to do so they need to use DCE to carry out the communication. DTE does not need to know how data is sent or received; the communications details are left to the DCE.

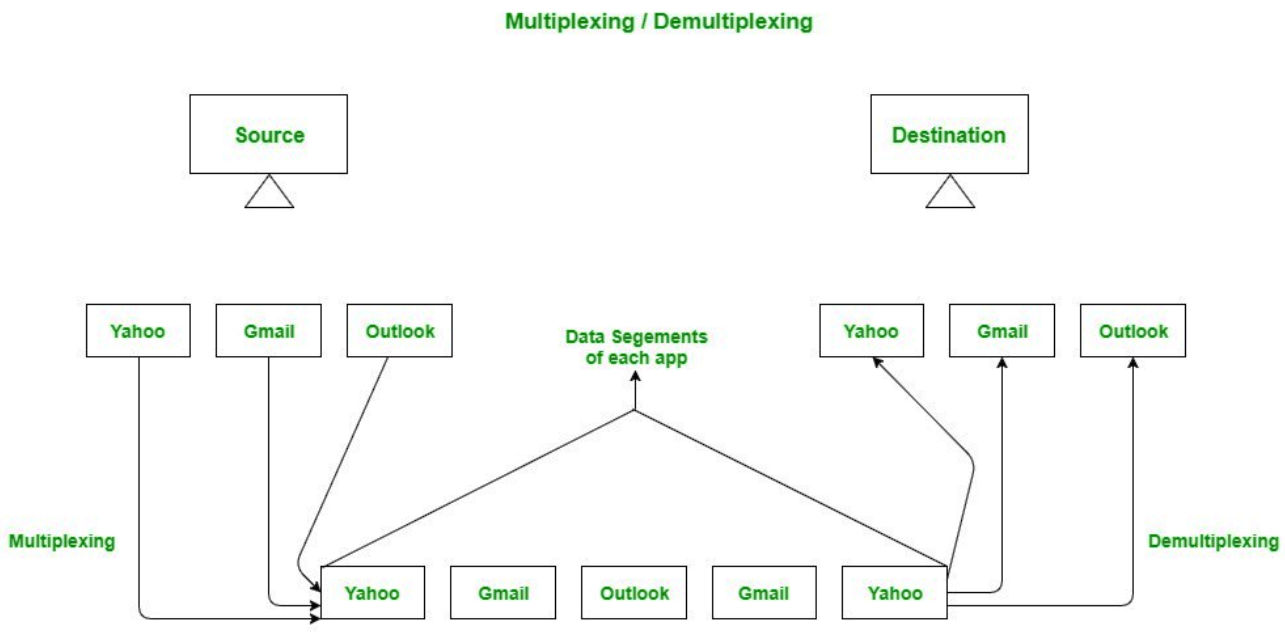
Multiplexing and Demultiplexing

Multiplexing

Gathering data from multiple application processes of sender, enveloping that data with header and sending them as a whole to the intended receiver is called as multiplexing.

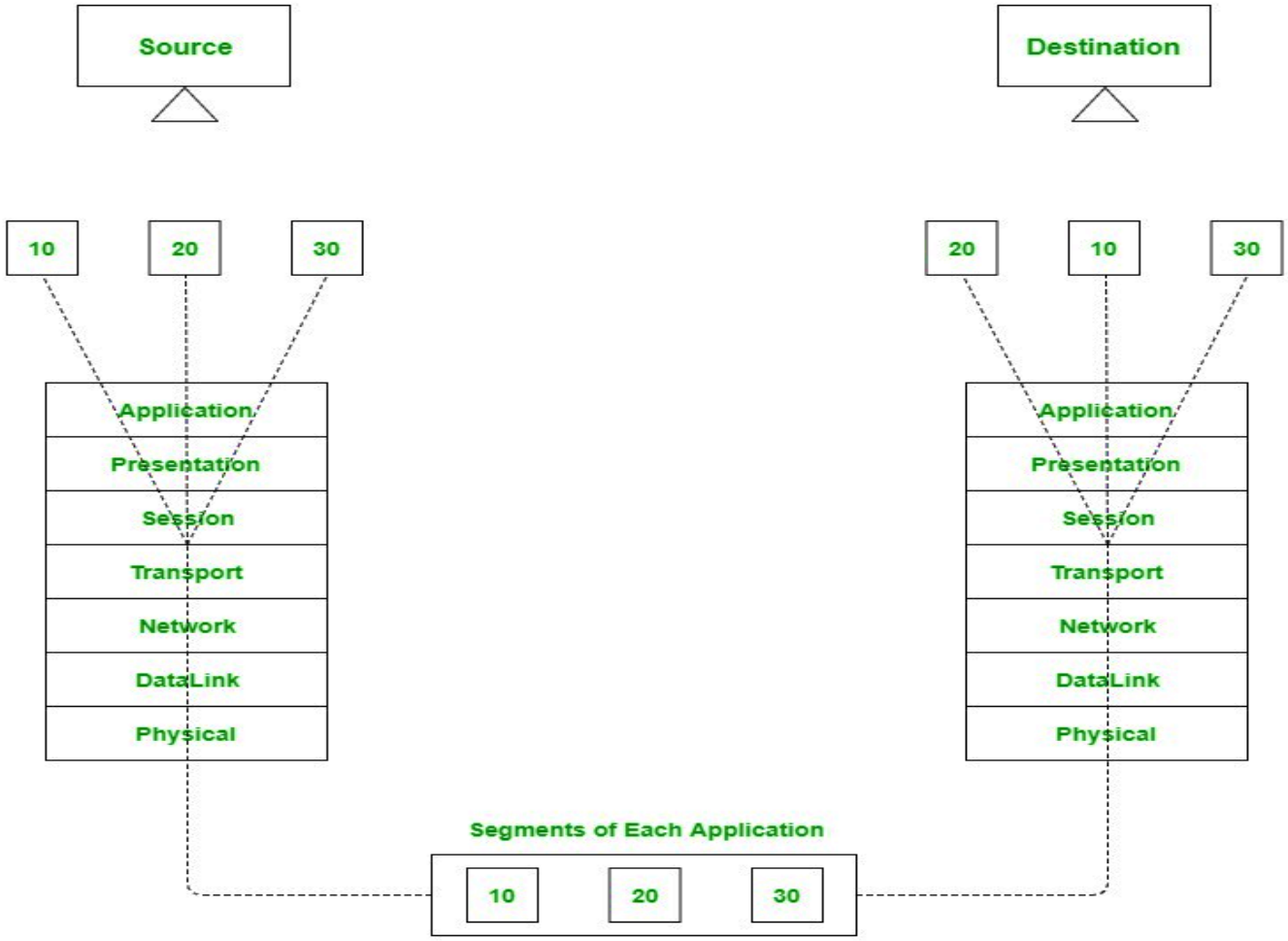
Demultiplexing

Delivering received segments at receiver side to the correct app layer processes is called as demultiplexing.



Abstract view of multiplexing and demultiplexing

Multiplexing and demultiplexing are the services facilitated by the transport layer of OSI model.



Transport layer- junction for multiplexing and demultiplexing