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

Computer Network II

Lecture 1

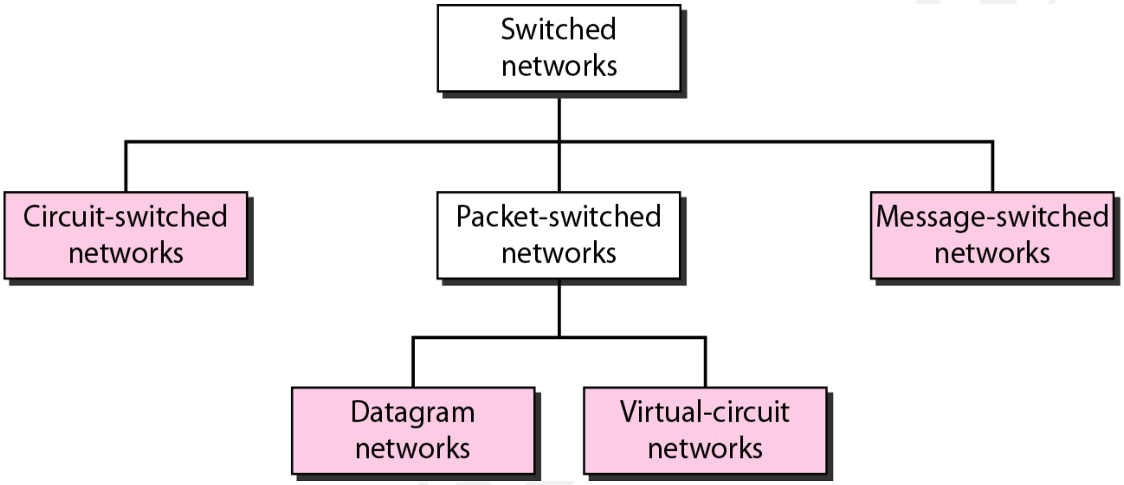
Network Switching

2023

Network Switching

What is Network Switching?

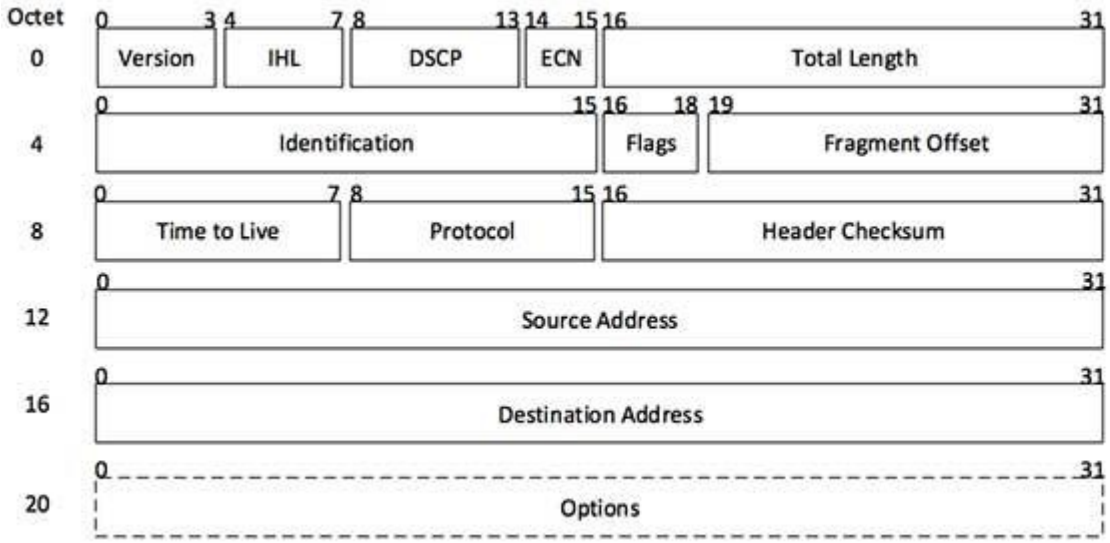
Network switching is the process of channeling data received from any number of input ports, to another designated port that will transmit the data to its desired destination. The device through with the input data passes is called a switch.



Taxonomy of switched networks

What does packet mean?

The packet is the basic unit of information in network transmission. Most networks use TCP/IP as the network protocol, or set of rules for communication between devices, and the rules of TCP/IP require information to be split into packets that contain both a segment of data to be transferred and the address where the data is to be sent. A packet consists of control information (header) and user data (payload).



[Image: IP Header]

- **Version:** Version no. of Internet Protocol used (e.g. IPv4).
- **IHL:** Internet Header Length; Length of entire IP header.
- **DSCP:** Differentiated Services Code Point; this is Type of Service.
- **ECN:** Explicit Congestion Notification; It carries information about thecongestion seen in the route.
- **Total Length:** Length of entire IP Packet (including IP header and IPPayload).
- **Identification:** If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.

- **Flags:** As required by the network resources, if IP Packet is too large to handle, these ‘flags’ tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to ‘0’.

- **Fragment Offset:** This offset tells the exact position of the fragment inthe original IP Packet.

- **Time to Live:** To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.

- **Protocol:** Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example,protocol number of ICMP is 1, TCP is 6 and UDP is 17.

- **Header Checksum:** This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.

- **Source Address:** 32-bit address of the Sender (or source) of the packet.

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

Computer Network II

Lecture 2

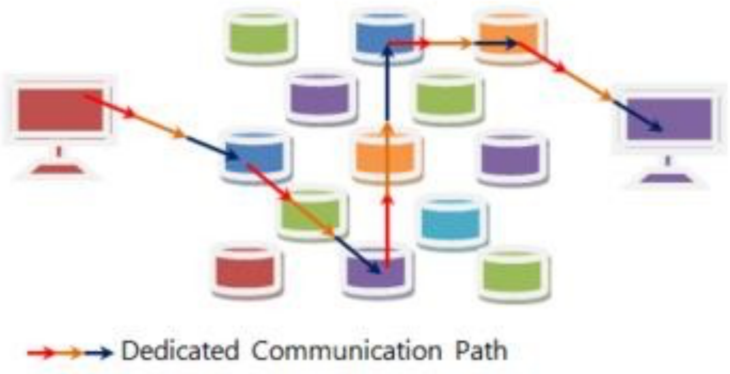
Circuit and Packet Switching

2023

1- Circuit Switching

Circuit switching is defined as the establishment of a dedicated communication path between the two parties or nodes within a physical network. This path (circuit) is established and maintained for the duration of the session. No matter the length of the communication session the circuit will remain and the data paths maintained. The circuit is only terminated when the session ends. The session consists of three phases; circuit establishment, data transfer and circuit termination/disconnect.

Figure 1: Circuit switching

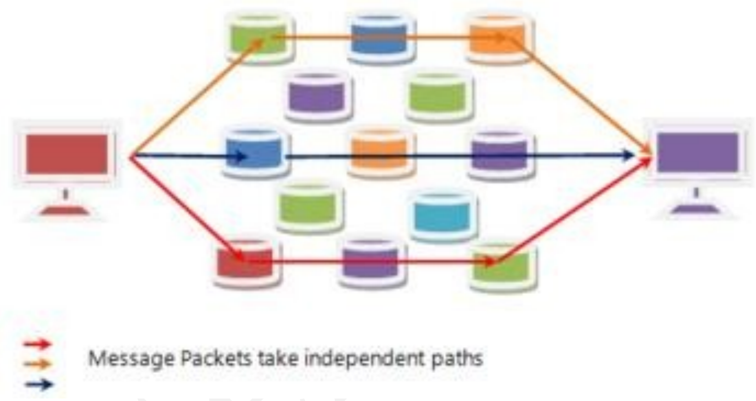


- Traditional telephone networks operate on the basis of circuit switching
- In conventional telephone networks, a circuit between two users must be established for a communication to occur
- Circuit switched networks requires resources to be reserved for each pair of end users
- The resources allocated to a call cannot be used by others for the durationof the call
- The reservation of the network resources for each user results in an inefficient use of bandwidth for applications in which information transfer is bursty or if the information is small.

2- Packet Switching

Packet switching is defined as the process of breaking down messages into small components called packets. Switching information (source and destination) is then included in the header information of the packet. Each packet then independently navigates its way using the information, through the network to its destination.

Figure 2: Packet Switching



- Packet switched networks are the building blocks of computer communication systems in which data units known as packets flow across the networks.
- It provides flexible communication in handling all kinds of connections for a wide range of applications e.g. telephone calls, video conferencing, distributed data processing etc...
- To make efficient use of available resources, packet switched

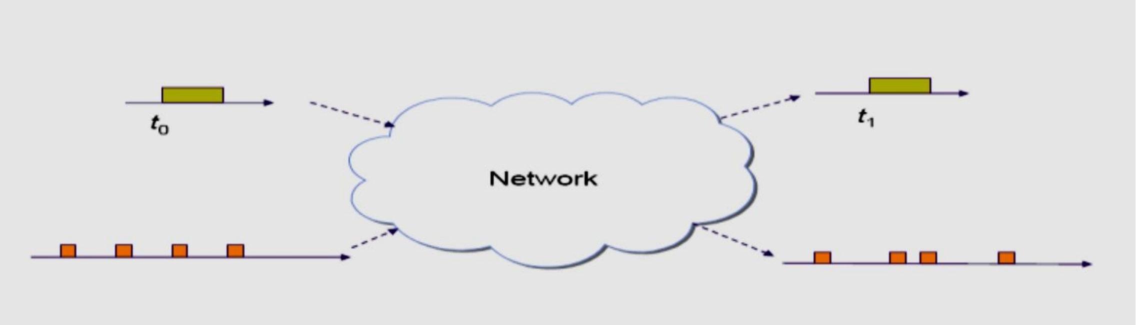
networks dynamically allocate resources only when required.

- The form of information in packet switched networks is always digital bits.

Differences between Circuit Switching and Packet Switching

Circuit switching	Packet switching
1. Call set up is required.	1. Call setup is not required.
2. Dedicated connection between two Hosts.	2. No dedicated connection between two Hosts.
3. Connection/Communication is lost, if any link in the path between the Hosts is broken.	3. Connection/Communication couldcontinue between the Hosts since data havemany routes between the Hosts.
4. Information takes the same route between the connected Hosts	4. Information could take different routes toreach the destination Host.
5. Information always arrives in order.	5. Information could arrive out of order to the destination
6. Bandwidth available is fixed.	6. Bandwidth available is variable.
7. Congestion is call based.	

- In case of single block of information, we are interested in having the block delivered correctly to destination and also interested in delay experienced intraversing the network.
- In case of sequence of blocks, we are interested not only in receive the blocks correctly and in right sequence.’



Network service can be **Connection-oriented service** or **connectionless service**

Connectionless service:

- Connectionless service is simple with two basic interactions (1) a request to network layer that it send a packet (2) an indication from the network layer that a packet has arrived
- It puts total responsibility of error control, sequencing and flow control on the end system transport layer.

Connection-oriented service

- The Transport layer cannot request transmission of information until a connection is established between end systems

- Network layer must be informed about the new flow
- Network layer maintains state information about the flows it is handling
- Connection release procedure may be required to terminate the connection

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

Computer Network II

Lecture 3

Network Security

2023

Network Security

Network security means the protection of network and data including hardware and software technologies from the threats. Most common threats include worms, spyware, Trojan horses, viruses, zero-hour attack, Denial of Service attack, and data interception and identity theft. Network Security works on multiple layers of Security.

Enforcement Mechanism

Enforcement concerns analyzing all network traffic flows and should aim to preserve the confidentiality, integrity, and availability of all systems and information on the network. These three principles compose the CIA triad:

Confidentiality – protecting assets from unauthorized entities

Integrity – ensuring the modification of assets is handled in a specified and authorized manner

Availability – a state of the system in which authorized users have continuous access to said assets.

General steps to protect Network from attacks are:

1. Analysis: The detailed requirements of the network and the threats that could imply onthat are collected and are being analyzed to determine the existing system.

2. Implementation: Once the analysis is being done now it is ready to implement a network security system that provides protection and has sufficient authorization policies.

3. Testing: When the security system is implemented it is used to perform tests on various types of threats using a large no of test cases to make sure that all of the features are working correctly and are completely protecting the network against any threats.

4. Modify: After Testing is performed the results will reveal the shortcomings of your system and where it can be changed to increase the efficiency of the security system.

Network Security Methods

There is a range of network security methods to ensure strong defense mechanisms:

Access control: This is to restrict or terminate illegitimate devices from accessing the organization's network. The users who are allowed to have permitted access to the network are also authorized to have access to a specific set of resources.

Anti-Malware: Malware includes computer worms, viruses, and trojans that try to infect theentire network and can stay on infected machines for weeks. The security system should enforce features and techniques to prevent infection and remove malware instantly.

Application security: Not all applications are genuine and malware free. Attackers use malicious and insecure applications as bait to gain access to the organizations' network. So you would need an efficient integration of software, hardware and security processes to restrictsuspicious apps.

Behavioral Analytics: Analyzing a network to understand its normal behavior is important. This would help you spot if the network is going through any abnormal behavior and hence work on any responsive protective methods.

Data loss prevention: It is vital to implement methods and techniques that restrict employeesand other users from purposefully or inadvertently sending confidential data outside the organization's network.

Email Security: Attackers use phishing emails to gain access to the network. Email securitymethods should be implemented to enable protection from such phishing emails.

Firewall: This defines a set of rules to be followed to deny or to allow internet traffic to accessyour network.

Intrusion detection and prevention: This enables to scan the traffic of the network to detectand terminate attacks.

Network segmentation: A software-related segmentation would help you to organize different categories and therefore implementing security policies becomes easier.

Web Security: This manages internal staff web use in order to terminate web-based attacksfrom exploiting potential browsers as a vector to gain access to your network.

Encryption: A Fundamental Security Technique

Cryptography is a fundamental tool in security because encryption can guarantee data confidentiality (sometimes called privacy), message authenticity, data integrity, and can prevent replay attacks. In essence, a sender applies encryption to scramble the bits of the message in such a way that only the intended recipient can unscramble them. Someone who intercepts a copy of an encrypted message will not be able to extract information.

The terminology used with encryption defines four items:

Plaintext — an original message before it has been encrypted

Cyphertext — a message after it has been encrypted

Encryption key — a short bit string used to encrypt a message

Decryption key — a short bit string used to decrypt a message

As we will see, in some technologies, the encryption key and the decryption key are identical;in others, they differ.

Mathematically, we think of encryption as a function, encrypt, that takes two arguments: a key, K1, and a plaintext message to be encrypted, M. The function produces an encrypted version of the message, cyphertext C:

$$C = \text{encrypt}\ (K1, M)$$

A decrypt function reverses the mapping to produce the original message:

$$M = \text{decrypt}\ (K2, C)$$

Mathematically, decrypt is the inverse of encrypt:

$$M = \text{decrypt}\ (K2\ ,\ \text{encrypt}\ (K1\ ,\ M))$$

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

Computer Network II

Lecture 4

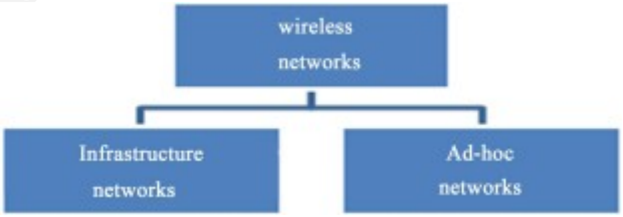
MANET & WSN

2023

Mobile Ad-Hoc Networks

- MANET – (Mobile Ad-Hoc Network) a system of mobile nodes (laptops, sensors, etc.) interfacing without the assistance of centralized infrastructure (access points, bridges, etc.).
- A Mobile Ad-hoc network is a wireless ad-hoc network which is used to exchange information.
- Each node is willing to forward data to other nodes.
- Does not rely on fixed infrastructure.

MANET is basically an organization less network of transportable devices having wireless communication capabilities that can join together at any time and at any place dynamically. In this type of network mobile hosts, sometimes, simultaneously acting as a router, are connected to one another by wireless links and they can easily move randomly hence network topology dynamically change so this makes an autonomous system of mobile nodes having no base station. In MANET each node has limited transmission range so packets are forwarded from any initiating node to any end point node in a network with the help of multiple hopes.



Classifications of wireless networks

Benefits of MANET:

Classifications of wireless networks

1- Highly suitable network in such circumstances where fixed infrastructure is too much costly, untrustworthy, not trusted and due to unavailability of such a network.

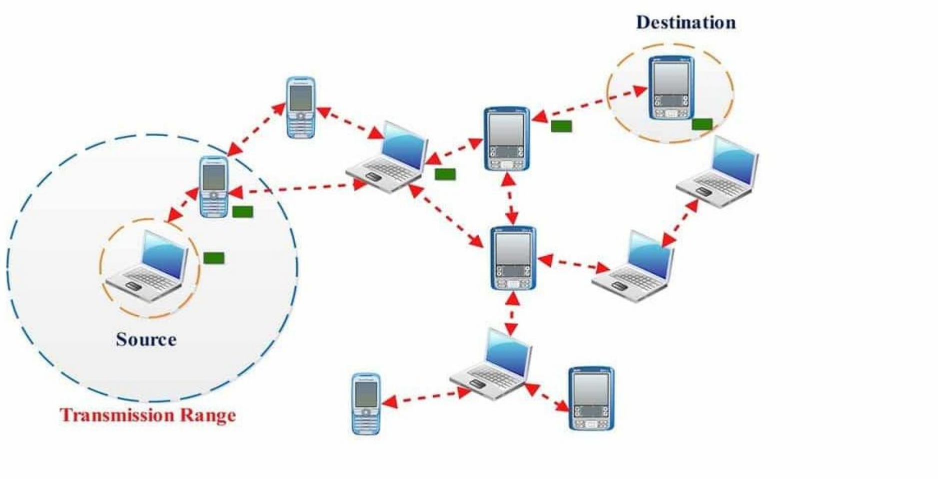
2- Quickly installation with least possible user intervention.

3- Detailed planning and installation of base stations is not required.

4- Ad hoc networks can be attached to the WWW or Internet, thereby incorporating many different devices and making possible for other users to use available services.

5- Capacity, range and energy arguments promote their use in tandem with existing cellular infrastructures as they can extend coverage and interconnectivity.

6- MANET also fitted to use the future 4G architecture and their services, aims to provide ubiquitous computer environments that support users in completing their tasks, accessing information and communicating anywhere, anytime and from any device.

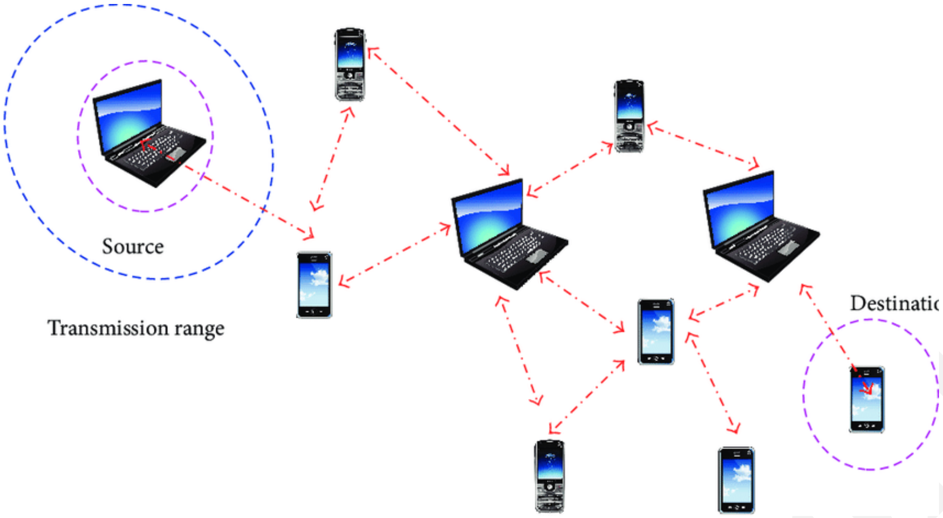


Applications of MANETs:

- Day-to-day applications: like email and file transfer can be easily deployable within an ad hoc network environment
- Web Services: can also be implemented with ad hoc networks, where any node in the network can serve as a gateway to the outside world.
- Military Applications: Ad Hoc networks were developed by keeping in mind military applications. Infrastructure network is almost impossible to establish or maintain in the battle field in an unknown region. The ad hoc networks having self-organizing capability can be effectively used in these situations.
- Crisis Management: In case of crisis management, infrastructure may be destroyed, in such cases ad hoc networks are useful.
- Personal Area Networking: managing personal things like printers, cell phones, PDAs, laptops, headsets, and so on. (ad hoc network can be replaced with Bluetooth).

another distinctive MANET application include:

- **Educational sector:** arrangement of communications facilities for computer- generated conference rooms or classrooms or laboratories.
- **Sensor Networks:** managing home appliances with MANETs in both the case like nearby and distantly. Tracking of objects like creatures. Weather sensing related activities.
- **Business Sector:** Ad-hoc network could be used for rescuing and emergency processes for adversity assistance struggles, for instance, in flood, fire or earthquake. Emergency saving procedures should take place where damaged and non-existing transmissions structure and quick preparation of a transmission network is required.


Source
Transmission range
Destinatio

Wireless Sensor Networks:

A wireless sensor network (WSN) is a wireless network; consist of spatially distributed autonomous devices using sensor to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutes, at different locations.

Sensor: A transducer, converts physical phenomenon e.g. heat, light, motion, vibration, and sound into electrical signals.

sensor node: basic unit in sensor network. contains on-board sensors, processor, memory, transceiver, and power supply.

Sensor network:

consists of a large number of sensor nodes.

nodes deployed either inside or very close to the sensed phenomenon.

Wireless Sensor Networks Applications:

1- Military Applications.
2- Environmental Applications.
3- Health Applications.
4- Home and Office Applications.
5- Environmental control in office buildings
6- Interactive museums
7- Detecting and monitoring car thefts
8- Managing inventory control
9- Vehicle tracking and detection

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

Computer Network II

Lecture 5

Internet Assigned Numbers Authority (IANA)

2023

The Internet Assigned Numbers Authority (IANA)

A company or organization that wishes to have network hosts accessible from the Internet must have a block of public addresses assigned. The use of these public addresses is regulated and the company or organization must have a block of addresses allocated to it. This is true for IPv4, IPv6, and multicast addresses. The IANA is the master holder of the IP addresses. The IP multicast addresses and the IPv6 addresses are obtained directly from IANA.

The Internet Service Providers (ISPs):

To get access to the services of the Internet, we have to connect our data network to the Internet using an Internet Service Provider (ISP). ISPs have their own set of internal data networks to manage Internet connectivity and to provide related services. Among the other services that an ISP generally provides to its customers are DNS services, e-mail services, and a website. Depending on the level of service required and available, customers use different tiers of an ISP.

There are three levels for the ISPs:

- Level 1 - These ISPs are large national or international ISPs that are directly connected to the Internet backbone. The customers of level 1 ISPs are either lower-tiered ISPs or large companies and organizations. Because they are at the top of Internet connectivity, they engineer highly reliable connections and services. Among the technologies used to support this reliability are multiple connections to the Internet backbone.
- Level 2 - Level 2 ISPs acquire their Internet service from level 1 ISPs and give their service to level 3 ISPs.

- Level 3 - Level 3 ISPs purchase their Internet service from level 2 ISPs. The focus of these ISPs is the retail and home markets in a specific locale.

IP v6 (Internet Protocol Version 6):

In its early years, the Internet was largely used by universities, high-tech industry. With the explosion of interest in the Internet starting in the mid-1990s, it began to be used by different group of people, especially by people with different requirements producing a billion machines being used. Under these circumstances it became apparent that IP had to evolve and become more flexible. In 1990 the Internet Engineering Task Force (IETF) started work on a new version of IP, one which would never run out of addresses, would solve a variety of other problems, and be more flexible and efficient as well. Its major goals were:

1. Support billions of hosts, even with inefficient address space allocation.
2. Reduce the size of the routing table.
3. Simplify the protocol, to allow routers to process packets faster.
4. Provide better security (authentication and privacy) than current IP.
5. Pay more attention to the type of service, particularly for real-time data.
6. Allow the protocol to evolve in the future.

In general, IPv6 is not compatible with IPv4, but it is compatible with other auxiliary protocols, including TCP, UDP, etc. the main features of IPv6 are discussed below:

First, IPv6 has longer addresses than IPv4, they are 16 bytes long, which solves the problem that IPv6 set out to solve: provide an effectively unlimited supply of Internet addresses.

The **second** major improvement of IPv6 is the simplification of the header. It contains only seven fields (versus 13 in IPv4). This change allows routers to process packets faster and thus improve throughput and delay.

The **third** improvement was better support for options. This change was essential

with the new header because fields that previously were required are now optional. In addition, the way options are represented is different, making them it simple for routers to skip over options not intended for them. This feature speeds up packet processing time.

The **fourth** area in which IPv6 represents a big advance is in security. Authentication and privacy are the key features of the new IP.

Finally, more attention has been paid to the quality of service.

Domain Name System (DNS):

Although programs theoretically could refer to hosts, mailboxes, and other resources by their network (e.g., IP) address, these addresses are hard for people to remember. Consequently, ASCII names were introduced to decouple machine names from machine addresses. Nevertheless, the network itself understands only numerical addresses, so some mechanism is required to convert the ASCII strings to network addresses. To solve these problems DNS was invented.

The DNS Name Space:

Conceptually the Internet is divided into over 200 top-level domains, where each domain covers many hosts. Each domain is partitioned into subdomains, and these are further partitioned, and so on. All these domains can be represented by a tree, as shown in the following figure. The leaves of the tree represent domains they have no subdomains. A leaf domain may contain a single host, or it may represent a company and contain thousands of hosts The top level domains come in two flavors: generic and countries. The original generic domains were com (commercial), edu (educational institutions), gov (Governmental), int (ceratin international orgaqnizations), mil (military), net (network providers) and org (nonprofit organizations). The country domain include one entry for every country, as defined in ISO 3166. In November 2000, four new general purpose top level domains were approved, biz (business), info (information), name (people's names), and pro (professionals such as doctors and lawyers).in addition to some certain industries. These are aero (aerospace industry), coop (co-operatives), and museum (museums). Other top-level domains will be added in the future.

In general, getting a second level-level domain, such as name-ofcompany.com, is easy. It merely requires going to a registrar for the corresponding top-level domain (com in the case) to check if the desired name is available and not somebody else's trademark. If there are no problems, the requester pays a small annual fee and gets the name.

Each domain is named by the path upward from it to the (unnamed) root. The components are separated by periods (dots). Thus, the engineering department at Sun Microsystems might be eng.sun.com.

Domain names can be either absolute or relative. An absolute domain name always ends with a period (e.g., eng.sun.com.), whereas a relative one does not. Relative names have to be interpreted in some context to uniquely determine their true meaning. In both cases, a named domain refers to a specific node in the tree and all the nodes under it. There is no rule against registering under two top level domains (e.g. sony.com and sony.nl).

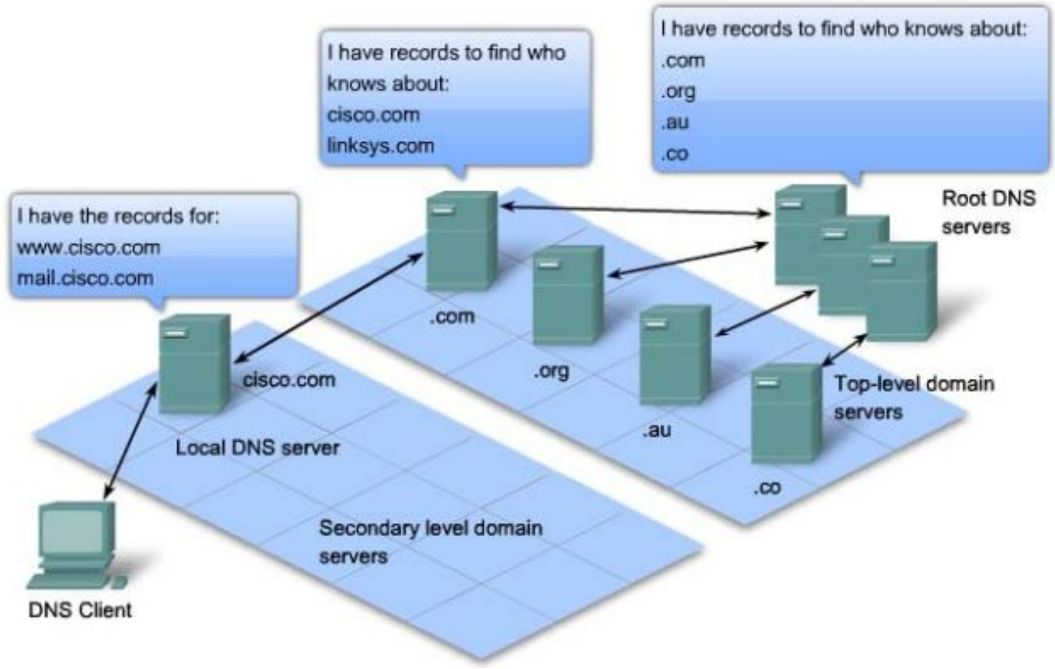
Resource Records

Every domain, whether it is a single host or a top-level domain, can have a set of **resource records** associated with it. For a single host, the most common resource record is just its IP address. When a resolver gives a domain name to **DNS**, what it gets back are the resource records associated with that name. Thus, the primary function of **DNS** is to map domain names onto resource records.

Name Servers

In theory at least, a single name server could contain the entire **DNS** database and respond to all queries about it. In practice, this server would so overloaded as to be useless. Furthermore, if it ever went down, the entire Internet would be crippled.

To avoid the problem associated with having only a single source of information, the **DNS** name space is divided into nonoverlapping **zones** (as shown in the figure). Each zone contains some part of the tree and also contains name servers holding the information about that zone. Normally, a zone will have one primary name server, which gets its information from a file on its disk, and one or more secondary name servers, which get their information from the primary server.



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

Computer Network II

Lecture 6

Quality of Service

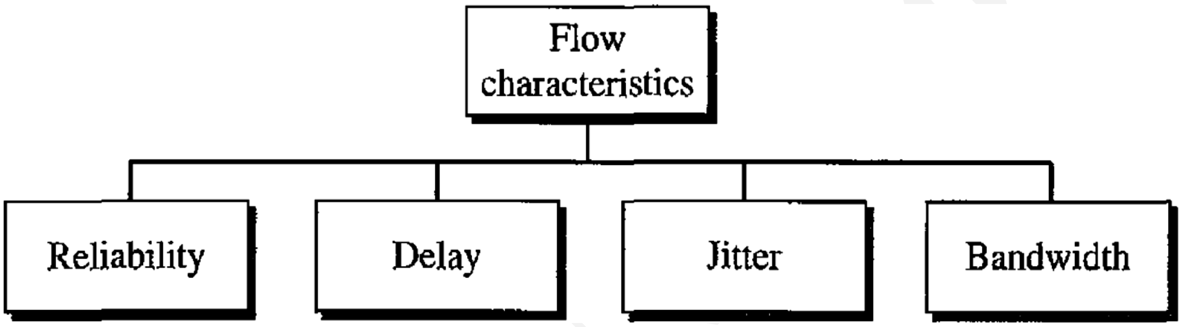
2023

Quality of Service

Quality of service (QoS) is an internetworking issue that has been discussed more than defined. We can informally define quality of service as something a flow seeks to attain.

Flow Characteristics.

Traditionally, four types of characteristics are attributed to a flow: reliability, delay, jitter, and bandwidth, as shown in Figure below.



Flow characteristics

1-Reliability

Reliability is a characteristic that a flow needs. Lack of reliability means losing a packet or acknowledgment, which entails retransmission. However, the sensitivity of application programs to reliability is not the same. For example, it is more important that electronic mail, file transfer, and Internet access have reliable transmissions than telephony or audio conferencing.

2-Delay

Source-to-destination delay is another flow characteristic. Again applications can tolerate delay in different degrees. In this case, telephony, audio conferencing, video conferencing, and remote log-in need minimum delay, while delay in file transfer or e-mail is less important.

3-Jitter

Jitter is the variation in delay for packets belonging to the same flow. For example, if four packets depart at times 0, 1, 2, 3 and arrive at 20, 21, 22, 23, all have the same delay, 20 units of time. On the other hand, if the above four packets arrive at 21, 23, 21, and 28, they will have different delays: 21,22, 19, and 24. For applications such as audio and video, the first case is completely acceptable; the second case is not.

High jitter means the difference between packet delays is large.

Low jitter means the variation in the packet delay is small.

4- Bandwidth

Different applications need different bandwidths. In video conferencing we need to send millions of bits per second to refresh a color screen while the total number of bits in an e- mail may not reach even a million.

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

Computer Network II

Lecture 7

Transmission of Digital Data: Interfaces and Modems

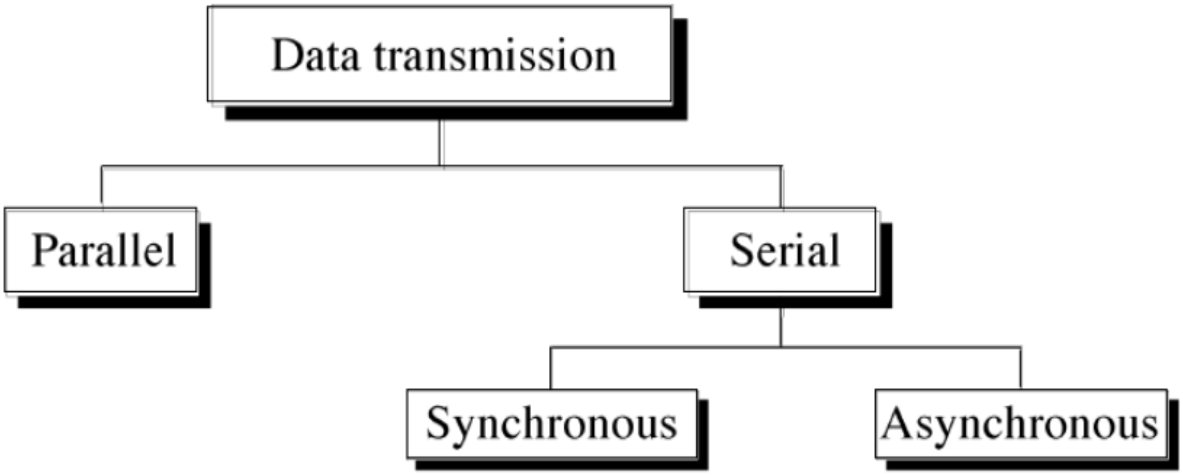
Dr. Alaa Taima

2022

Transmission of Digital Data: Interfaces and Modems

Transmission of Digital Data

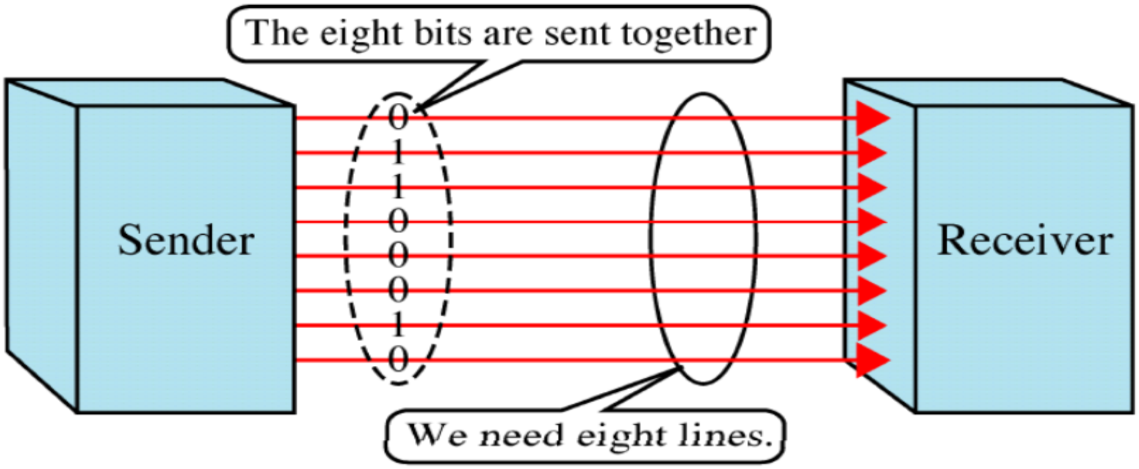
Primary concern when considering the transmission of data from one device to another is the wiring.



Transmission of Digital Data

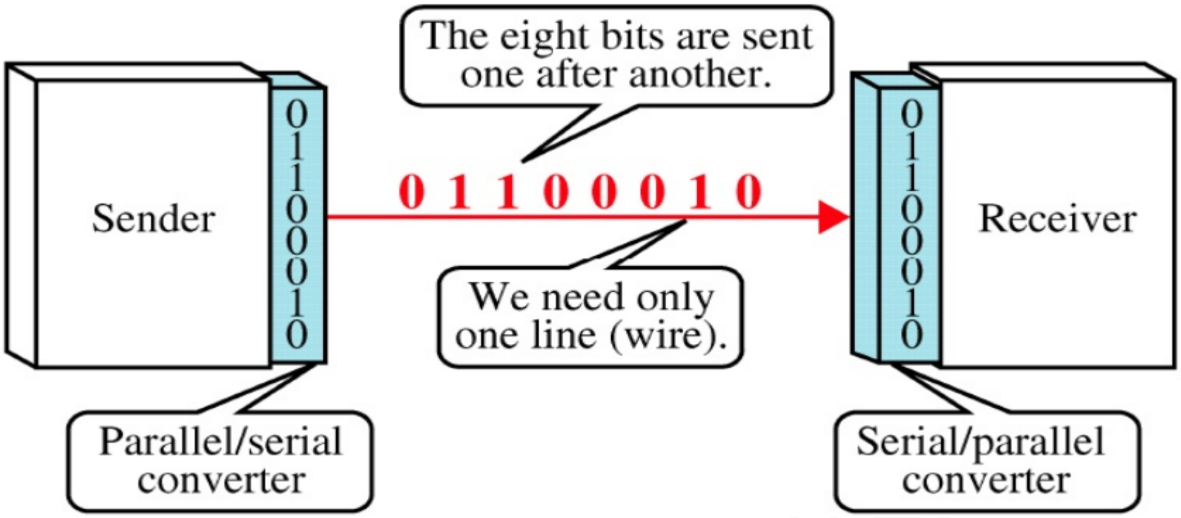
Parallel Transmission

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



Serial Transmission

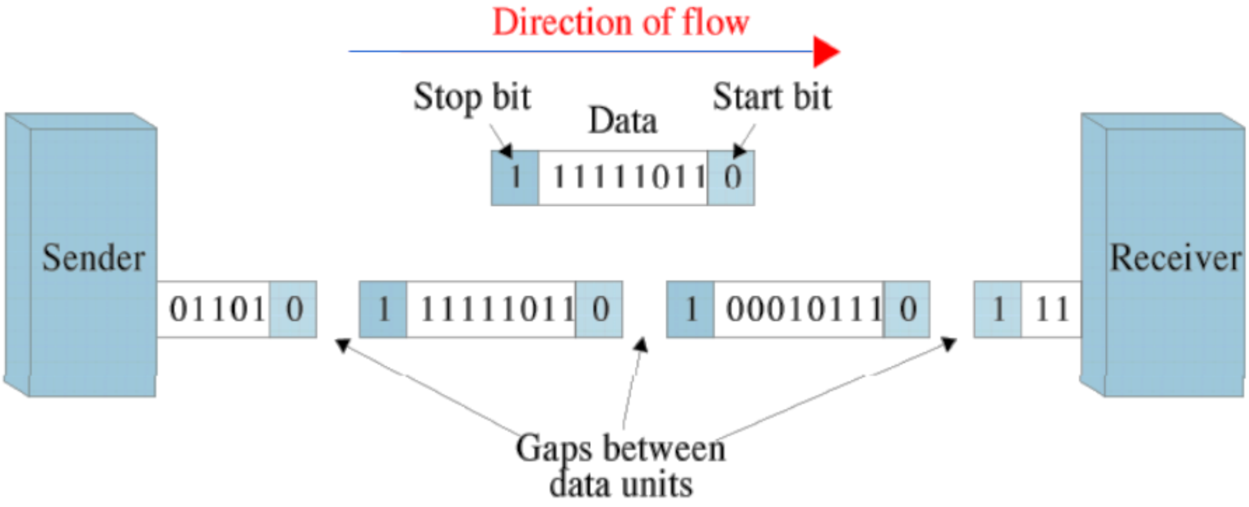
Transmit the data as one bit follows another. It uses a channel and require interface converter.


The eight bits are sent one after another.
Sender
0 1 1 0 0 0 1 0
Receiver
We need only one line (wire).
Parallel/serial converter
Serial/parallel 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.

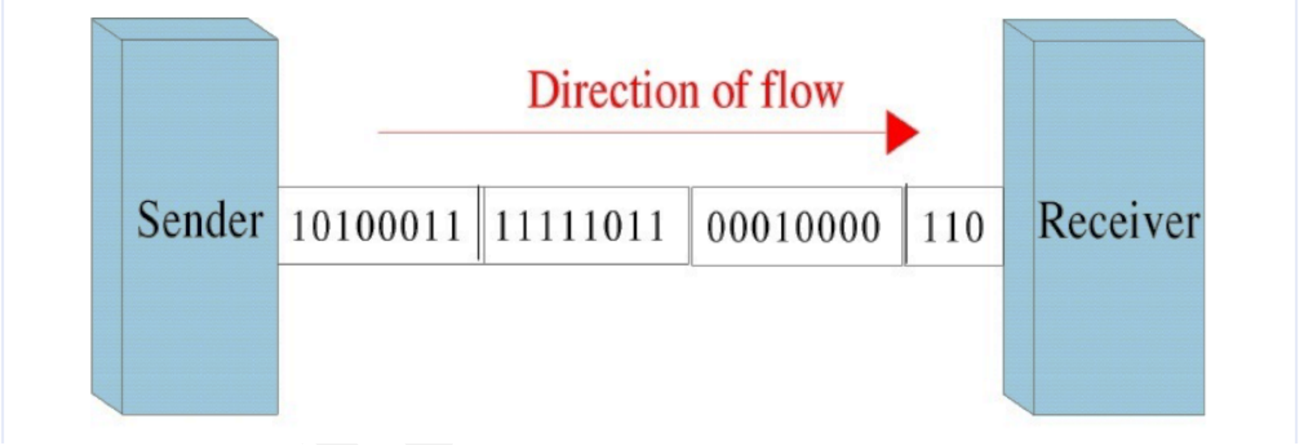
- sender provides a synchronization signal to the receiver before starting the transfer of each message



Synchronous transmission

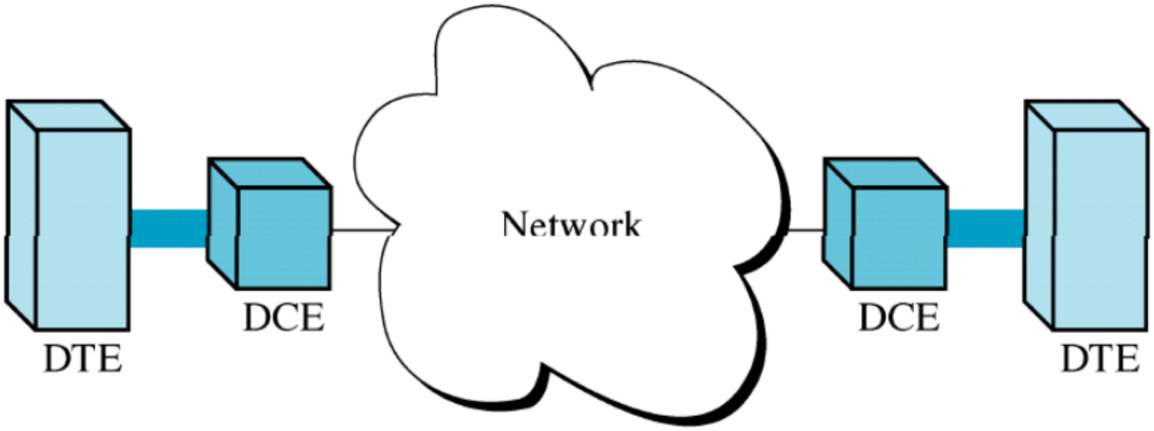
Sending bits one after another without start/stop bits or gaps. It is the responsibility of the receiver to group the bits. The receiver counts the bits as they arrive and groups them in eight-bit units.

- 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 (DCE): 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.

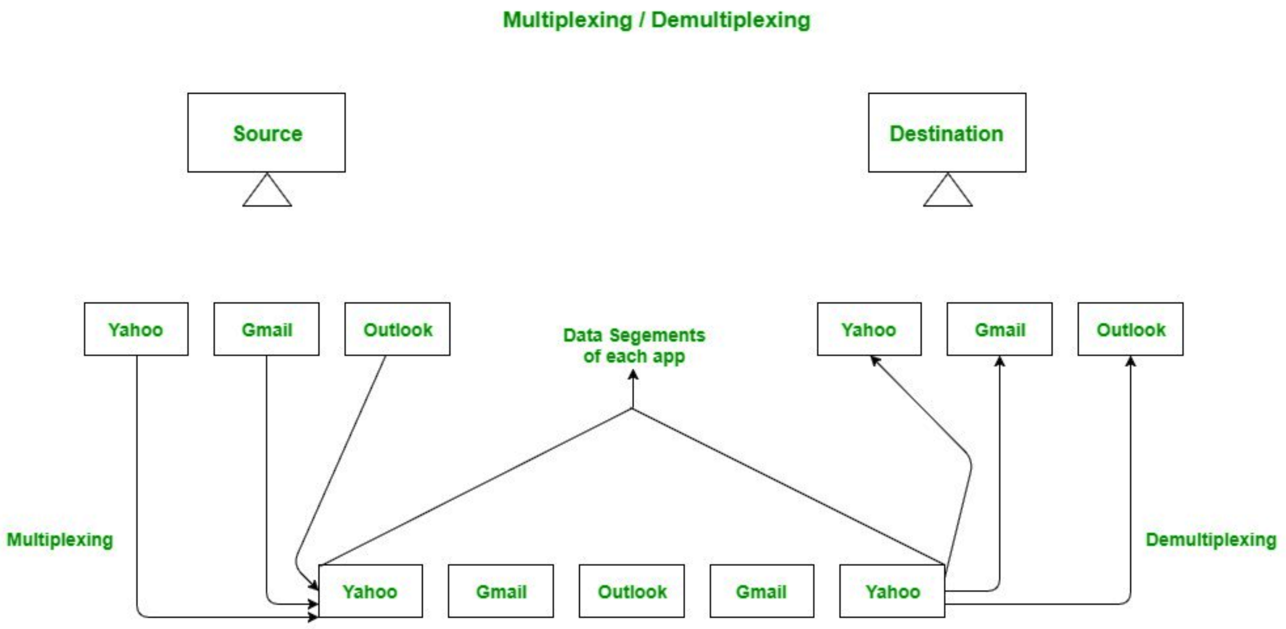
Multiplexing and Demultiplexing

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.

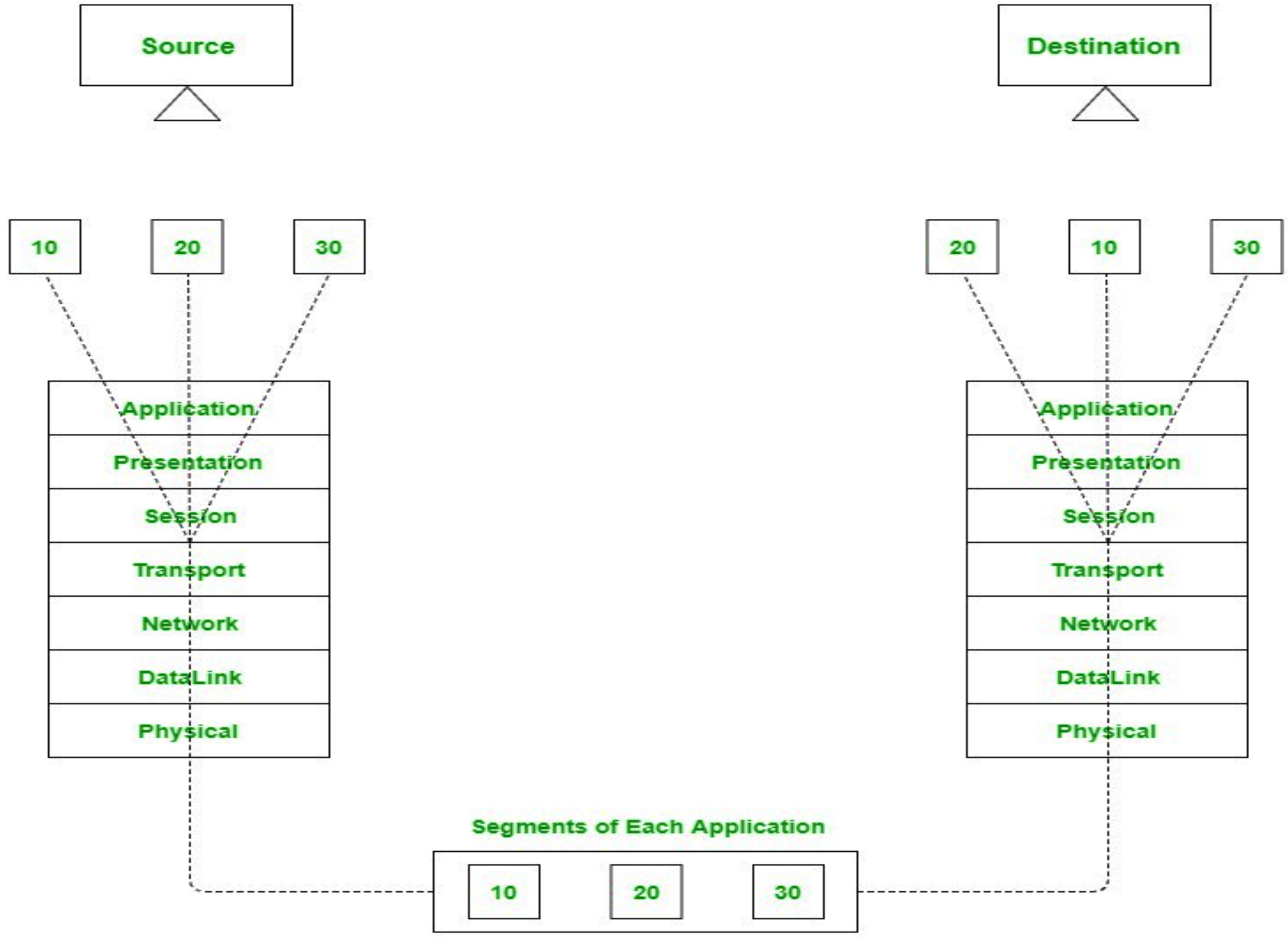
Demultiplexing

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