Lecture 5: TCP/IP PROTOCOL SUITE

The main objectives of lecture 5:

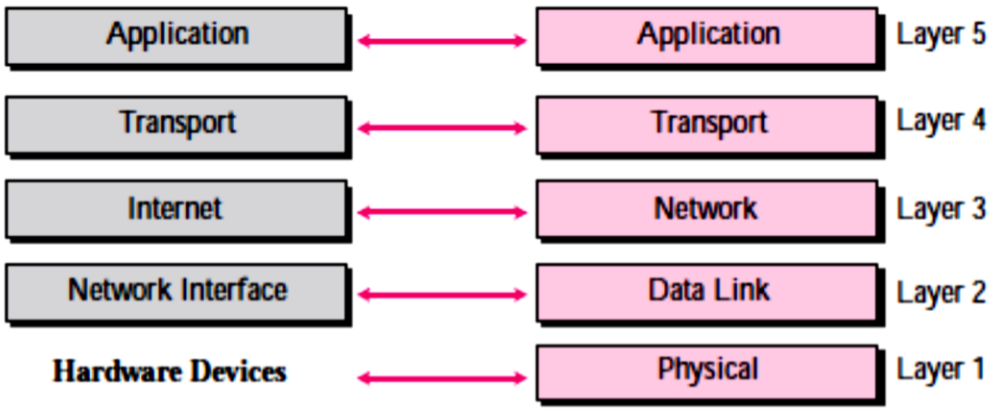
On Completion of this lesson, the students will be able to:

Explain the layers of TCP/IP reference model.

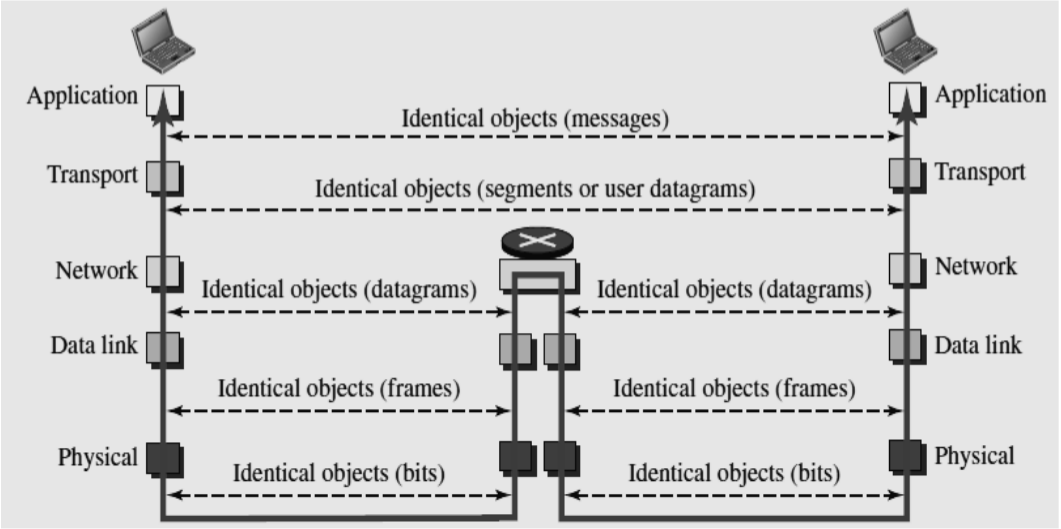
Discuss the main functions of each layer.

classify and describe the various types of the addressing

The **TCP/IP protocol suite** was ***developed prior*** to the OSI model. The next Figure shows both configurations.



1. TCP/IP layers:

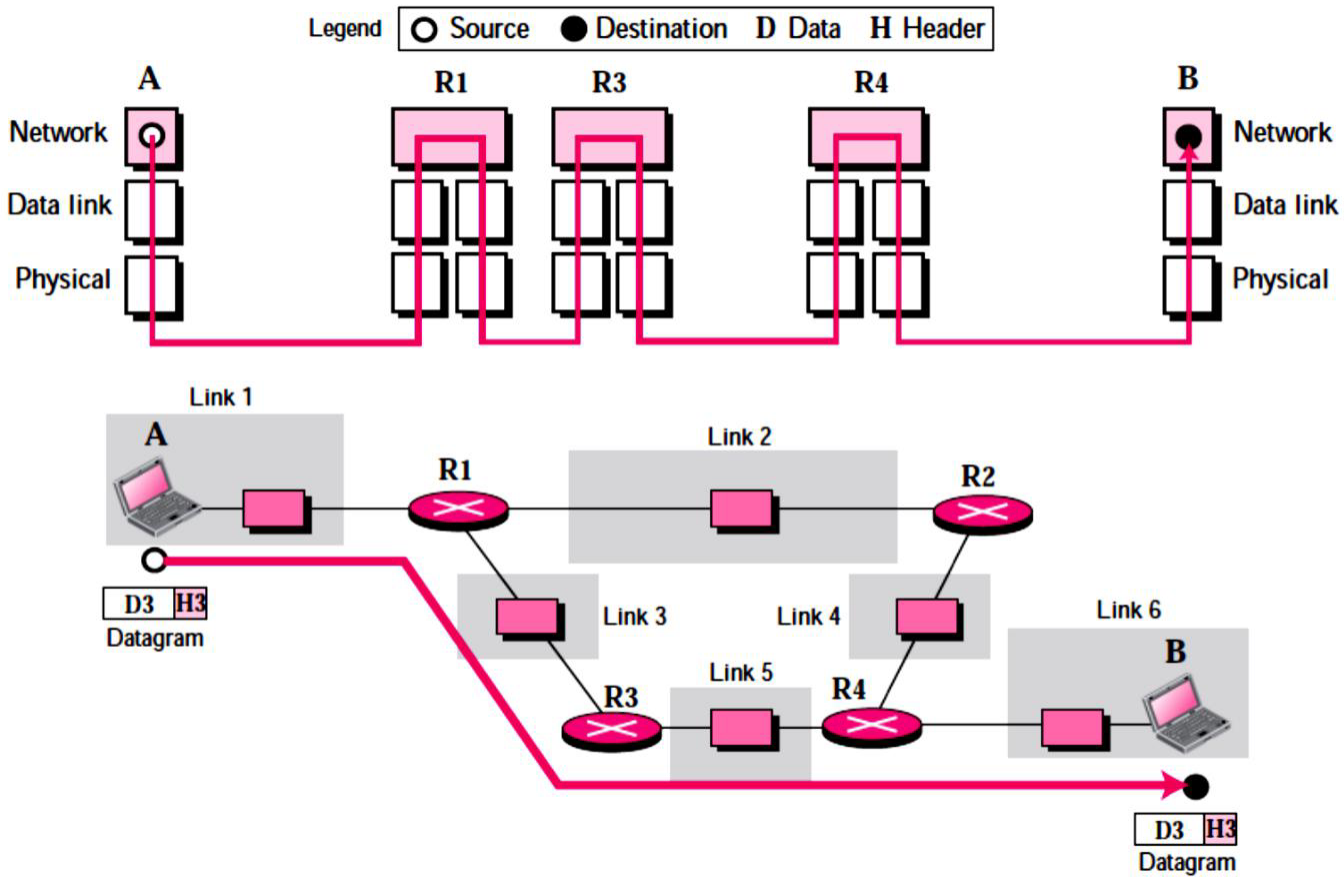


1. Physical and Data Link Layers

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 a local-area network or a wide-area network. Note that:

2. Network Layer

At the network layer (or, more accurately, the internetwork layer), TCP/IP supports the Internetworking Protocol. IP transports data in packets called **datagrams.** Datagrams can travel along different routes and can arrive out of sequence or be duplicated.



IP uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

2.1. Internetworking Protocol (IP): it is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol-a

best-effort delivery service. The term best effort means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees. IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

2.2. Address Resolution Protocol (ARP): it is used to associate a logical address with a physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address, usually imprinted on the network interface card (NIC). ARP is used to find the physical address of the node when its Internet address is known.

2.3. Reverse Address Resolution Protocol (RARP): it allows a host to discover its Internet address when it knows only its physical address. It is used when a computer is connected to a network for the first time or when a diskless computer is booted.

2.4. Internet Control Message Protocol: it is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

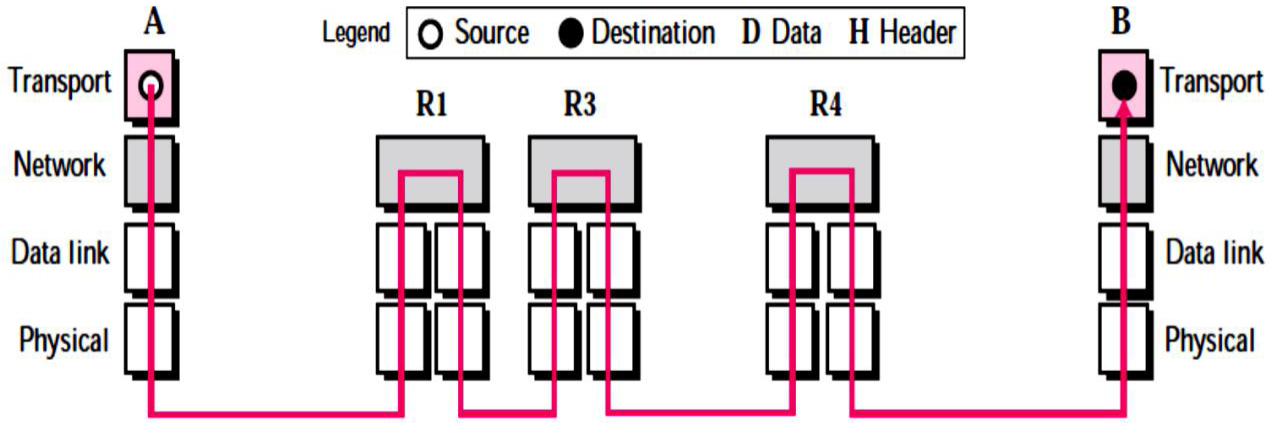
2.5. Internet Group Message Protocol: it is used to facilitate the simultaneous transmission of a message to a group of recipients.

Transport Layer:

As the network layer is responsible for sending individual datagrams from computer A to computer B; the transport layer is responsible for

delivering the whole message, which is called a segment, a user datagram, or a packet, from A to B. A segment may consist of a few or tens of datagrams.

The segments need to be broken into datagrams and each datagram has to be delivered to the network layer for transmission.



Traditionally it was represented in TCP/IP by two protocols: TCP and UDP. 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, has been devised to meet the needs of some newer applications.

3.1. User Datagram Protocol: it 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.

3.2. Transmission Control Protocol: it provides full transport-layer services to applications. TCP is a reliable stream transport protocol (connection-oriented). At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP

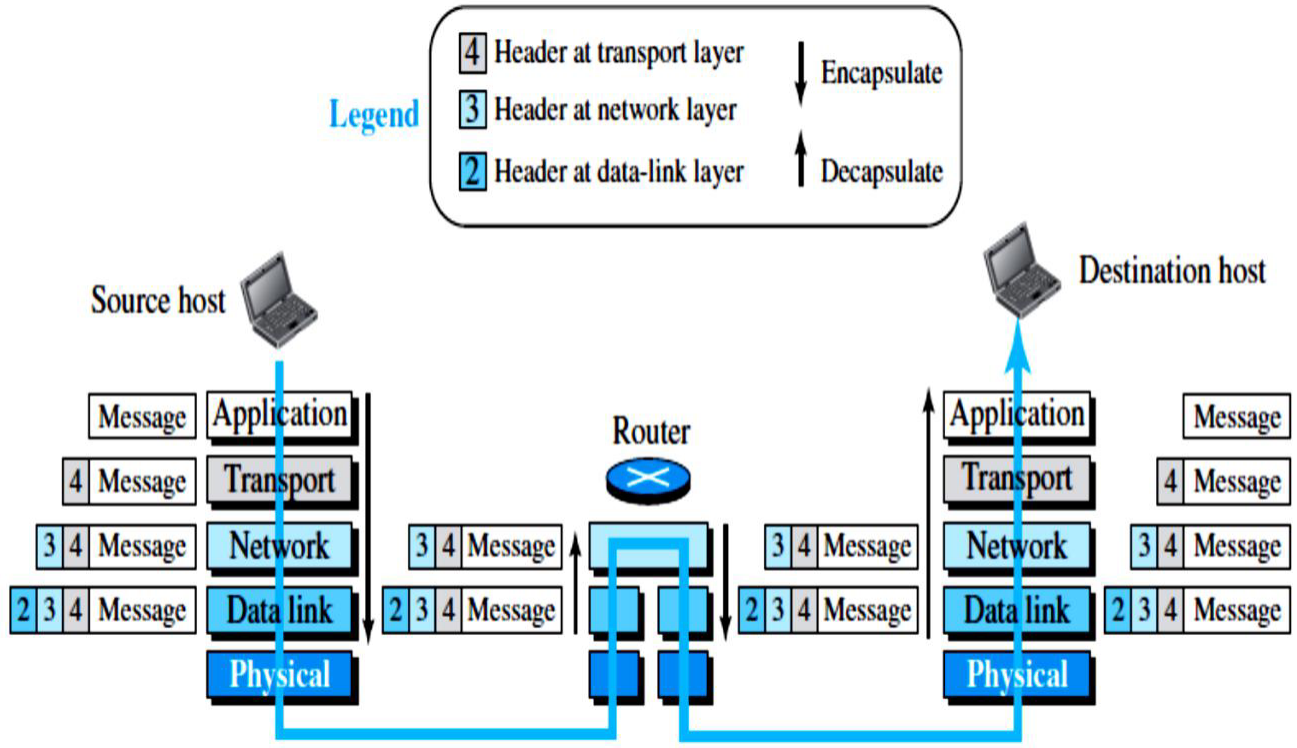
collects each segment as it comes in and reorders the transmission based on sequence numbers.

3.3. Stream Control Transmission Protocol (SCTP): it 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.

4. Application Layer

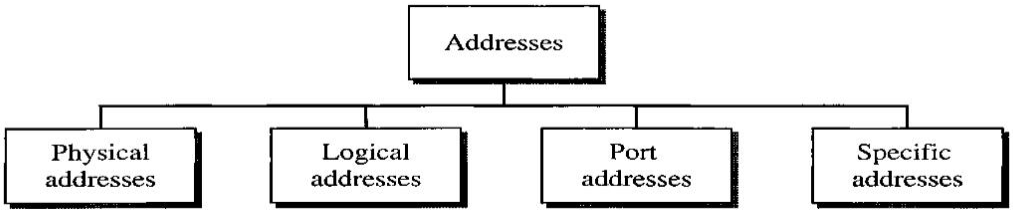
The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model

2. Encapsulation and Decapsulation

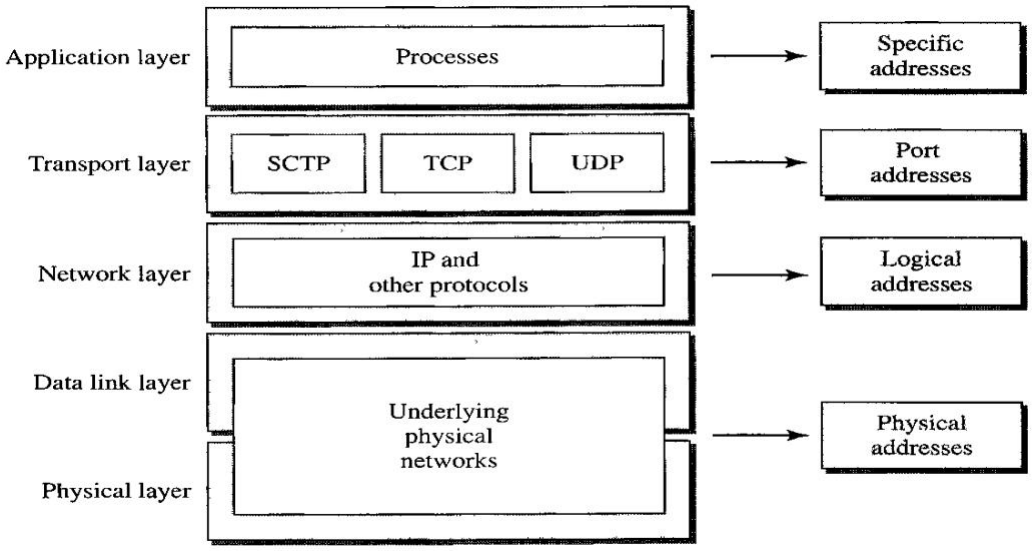


3. Addressing:

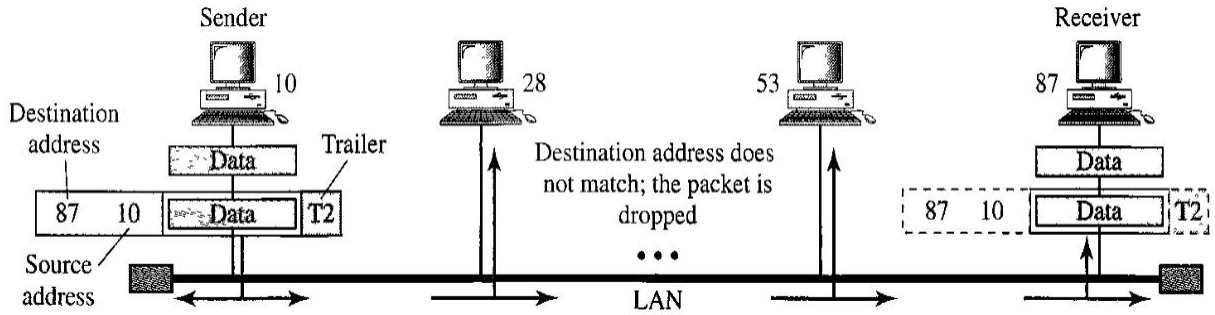
Four levels of addresses are used in an internet employing the TCP/IP protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses (see the following figure)



Each address is related to a specific layer in the TCP/IP architecture, as shown in the next figure.



4.1. Physical Addresses: The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address. The physical addresses have authority over the network (LAN or WAN). The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC). Local Talk (Apple), however, has a 1-byte dynamic address that changes each time the station comes up.

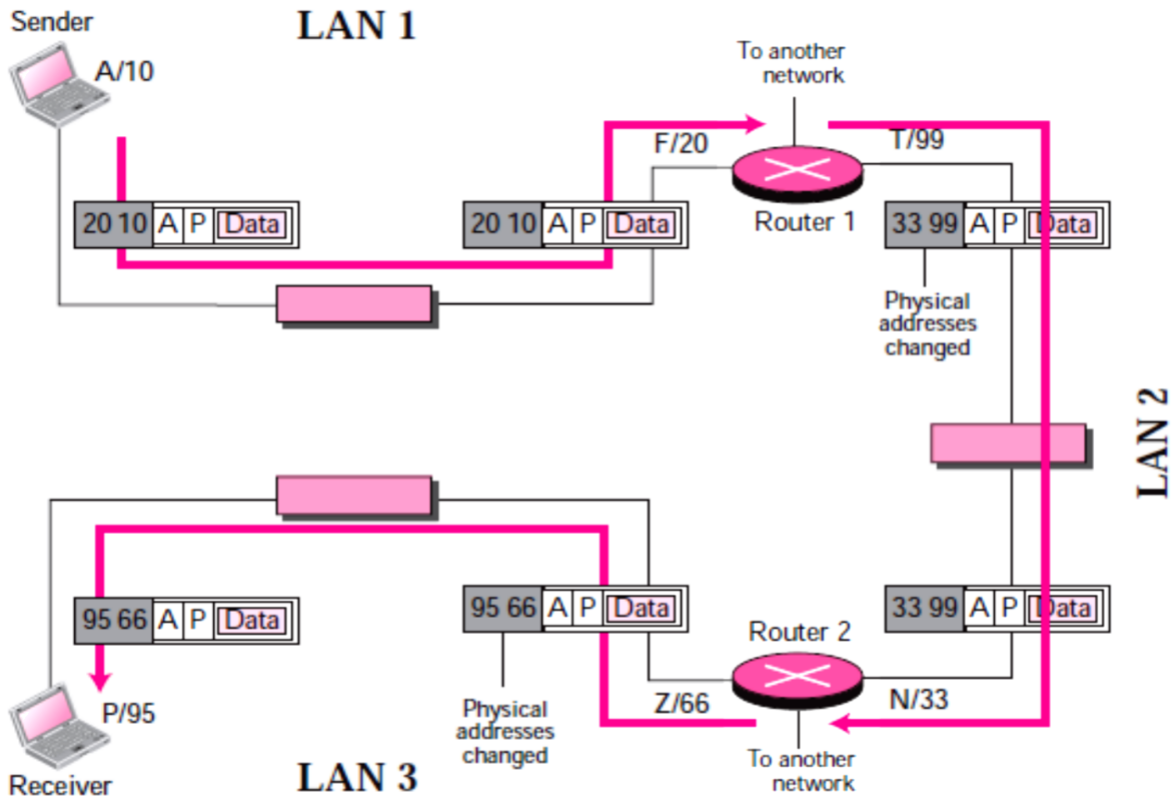


4.2. Logical Addresses: Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

Example:

The next figure shows a part of an internet with two routers connecting three LANs.

The computer with logical address **A** and physical address **10** needs to send a packet to the computer with logical address **P** and physical address **95**. The sender encapsulates its data in a packet at the network layer and adds two logical addresses (**A** and **P**).



The network layer, however, needs to find the physical address of the next hop before the packet can be delivered. The network layer consults its routing table and finds the logical address of the next hop (router 1) to be F. Another protocol, **Address Resolution Protocol** (ARP) finds the physical address of router 1 that corresponds to its logical address (20). Now the network layer passes this address to the data link layer, which in turn, encapsulates the packet with physical destination address 20 and physical source address 10.

The frame is received by every device on LAN 1, but is discarded by all except router 1, which finds that the destination physical address in the frame matches with its own physical address. The router decapsulates the packet from the frame to read the logical destination address P. Since the logical destination address does not match the router's logical address, the router knows that the

packet needs to be forwarded. The router

consults its routing table and ARP to find the physical destination address of the next hop (router 2), creates a new frame, encapsulates the packet, and sends it to router 2.

The source physical address changes from 10 to 99. The destination physical address changes from 20 (router 1 physical address) to 33 (router 2 physical address). The logical source and destination addresses must remain the same; otherwise the packet will be lost.

At router 2 we have a similar scenario. The physical addresses are changed, and a new frame is sent to the destination computer. When the frame reaches the destination, the packet is decapsulated. The destination

logical address **P** matches the logical address of the computer. The data are decapsulated from the packet and delivered to the upper layer. Note that although physical addresses will change from hop to hop, logical addresses remain the same from the source to destination.

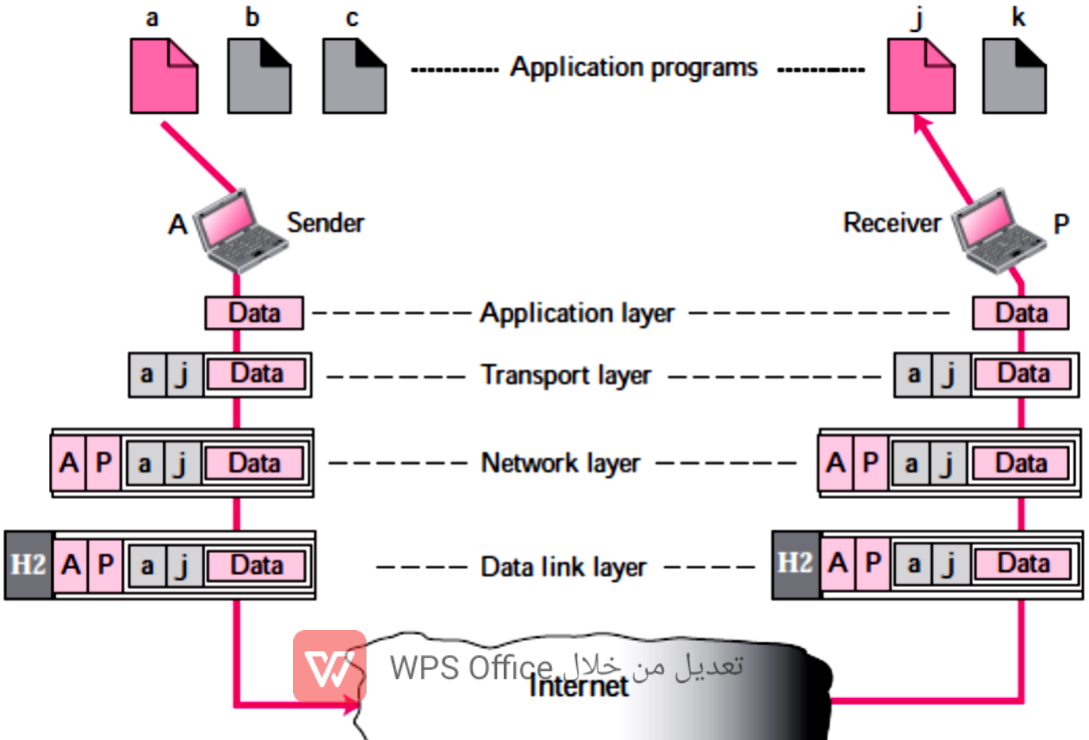
4.3. Port Addresses: The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. A system that sends nothing but data from one computer to another is not complete. Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data instantaneously, we need a method to

label the different processes. In other words, they need

addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length.

Example:

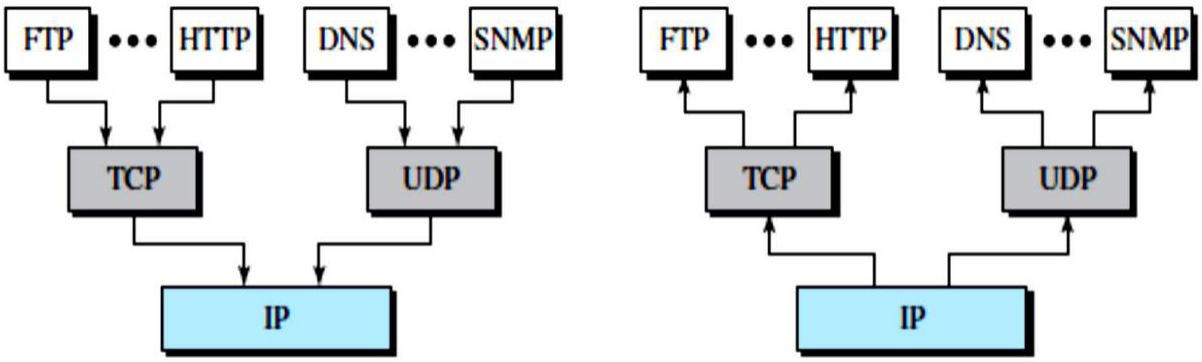
The following figure shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses **a**, **b**, and **c**. The receiving computer is running two processes at this time with port addresses **j** and **k**. Process **a** in the sending computer needs to communicate with process **j** in the receiving computer. Note that although both computers are using the same application, FTP. To show that data from process **a** need to be delivered to process **j**, and not **k**, the transport layer encapsulates data from the application layer in a packet and adds two port addresses (**a** and **j**), source and destination. The packet from the transport layer is then encapsulated in another packet at the network layer with logical source and destination addresses (A and P). Finally, this packet is encapsulated in **a** frame with the physical source and destination addresses of the next hop.



4.4. Specific Addresses: Some applications have user-friendly addresses that are designed for that specific address. For example: www.Ibbuniv.edu.ye.

Multiplexing and Demultiplexing

Since the TCP/IP protocol suite uses several protocols at some layers, we can say that we have ***multiplexing*** at the ***source*** and ***demultiplexing*** at the ***destination***. Multiplexing in this case means that a protocol at a layer can encapsulate a packet from ***several next-higher*** layer protocols (one at a time); demultiplexing means that a protocol can ***decapsulate*** and ***deliver*** a ***packet*** to ***several next-higher*** layer protocols (one at a time). The next figure shows the concept of multiplexing and demultiplexing at the three upper layers.



a. Multiplexing at source b. Demultiplexing at destination