COMPUTER NETWORKS

MODULE I. REVIEW OF NETWORK MODELS

1.1 Understand TCP/IP Protocol
- 1.1.1 Illustrate computer networks
- 1.1.2 Identify TCP/IP Protocol suite.
- 1.1.3 Explain the functionalities of layers in TCP/IP
- 1.1.4 Define Addressing of TCP/IP.
- 1.1.5 Describe about Wired LAN – Ethernet
- 1.1.6 State IEEE 802 project
- 1.1.7 Illustrate standard Ethernet
- 1.1.8 Describe about Wireless LAN.
- 1.1.9 State IEEE 802.11
- 1.1.10 Explain LAN connecting devices.
- 1.1.11 Explain the architecture of Virtual LANs.

MODULE I – TCP/IP PROTOCOL

Introduction to computer networks – physical structure, topology, types - TCP/IP – architecture, Description of layers, addressing – wired LAN – Ethernet protocol – IEEE project 802 – Standard Ethernet – characteristics, addressing, implementation – wireless LAN – architectural comparison, characteristics, access control – IEEE 802.11 – architecture – LAN connecting devices – hub, switch, router – virtual LAN – architecture, membership, configuration

---

Computer network

Definition: A **computer network** is a set of computers connected together for the purpose of sharing resources. Computers on a network are called **nodes**. The connection between computers can be done via cabling, most commonly the Ethernet cable, or wirelessly through radio waves. Connected computers can share resources, like access to the Internet, printers, file servers, and others.

Physical Structures

Some network attributes are:

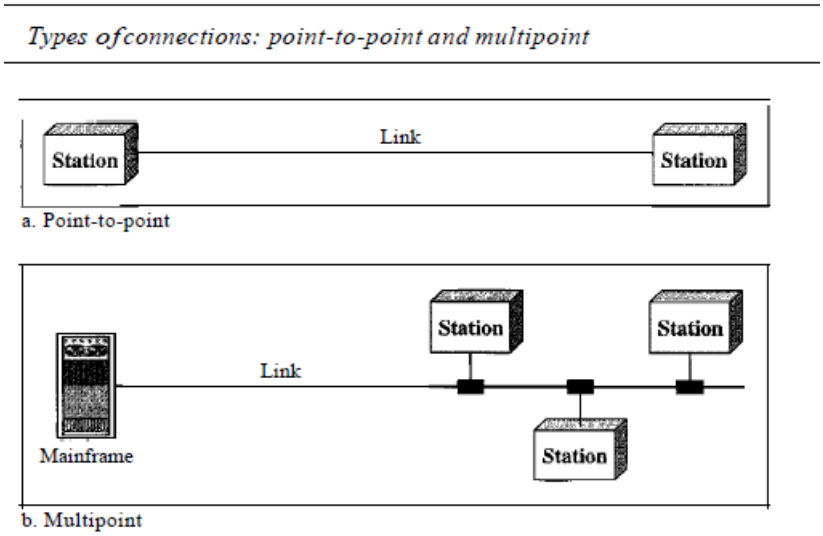
Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another.

There are two possible types of connections: point-to-point and multipoint.

Point-to-Point: A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices.

Multipoint: A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.



TCP/IP PROTOCOL SUITE

- The TCP/IP (Transmission Control Protocol and Internet Protocol) 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
  - application.
- However, when TCP/IP is compared to OSI, we can say that the
  - Host-to-network layer is equivalent to the combination of the physical and data link layers.
  - The internet layer is equivalent to the network layer.
  - Application layer is roughly doing the job of the session, presentation, and application layers.
  - Transport layer do the functionalities as in OSI model.

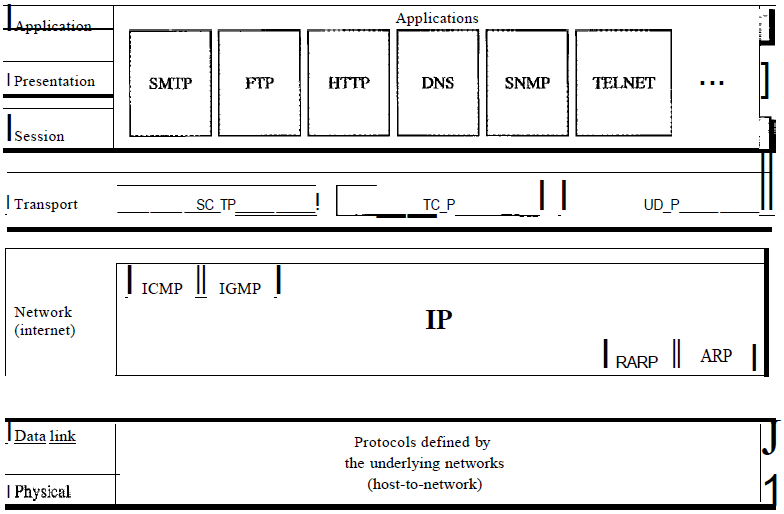


Fig: TCP/IP protocol suite

Application Layer

The *application layer* in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model. The application layer is concerned with providing network services to applications. There are many application network processes and protocols that work at this layer, including HyperText Transfer Protocol (HTTP), Simple Mail Transport Protocol (SMTP) and File Transfer Protocol (FTP) etc.

Transport Layer

This layer is concerned with the transmission of the data. The main protocols that used in this layer are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP is regarded as being the reliable transmission protocol and it guarantees that the proper data transfer will take place. UDP is not as complex as TCP and as such is not designed to be reliable or guarantee data delivery. UDP is generally thought of as being a best effort data delivery, i.e. once the data is sent, UDP will not carry out any checks to see that it has safely arrived.

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.

Network Layer
This is the layer that contains the packet construct that will be transmitted. This takes the form of the Internet Protocol (IP) which describes a packet that contains a source IP Address, destination IP Address and the actual data to be delivered. At the network layer *TCP/IP* uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

Internetworking Protocol or internet protocol (IP)
The Internetworking Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless protocol-a best-effort delivery service. 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.

Address Resolution Protocol (ARP)

Delivery of a packet to a host or router requires two levels of addresses: logical and physical. A **physical address** is a 48-bit address that identifies a host or router at the physical level. **Logical address** in the internet is currently a 32-bit address that can uniquely define a host connected to the internet. Mapping of a logical address to a physical address can be static or dynamic. Static mapping involves a list of logical and physical address correspondences; maintenance of the list requires high overhead.

The address resolution protocol (ARP) is a dynamic mapping method that finds a physical address given a logical address.

Reverse Address Resolution Protocol (RARP)
The reverse address resolution protocol (RARP) is a dynamic mapping method that finds a logical address given a physical address.

Internet Control Message Protocol (ICMP)
The Internet Control Message Protocol (ICMP) 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.

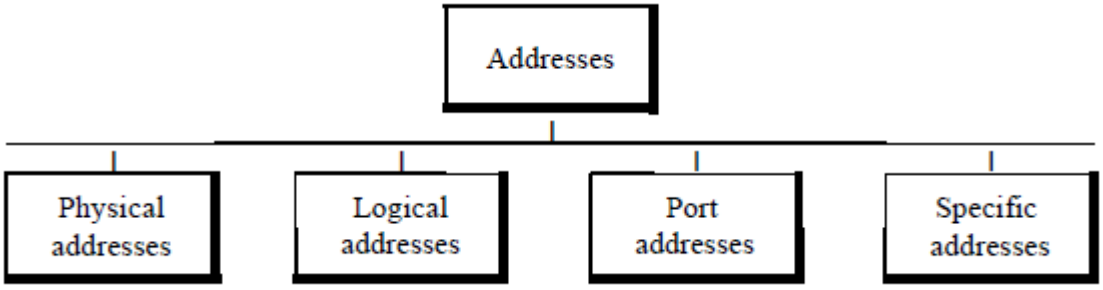
Internet Group Message Protocol (IGMP)
The Internet Group Message Protocol (IGMP) is used to facilitate the simultaneous transmission of a message to a group of recipients.

Physical and Data Link Layers

This is the lowest level of the TCP/IP protocol stack and functions carried out here include encapsulation of IP packets into frames for transmission, mapping IP addresses to physical hardware addresses (MAC Addresses) and the use of protocols for the physical transmission of data.

ADDRESSING of TCP/IP

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



Each address is related to a specific layer in the TCPIIP architecture, as shown in Figure below

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 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). LocalTalk (Apple), however, has a I-byte dynamic address that changes each time the station comes up.

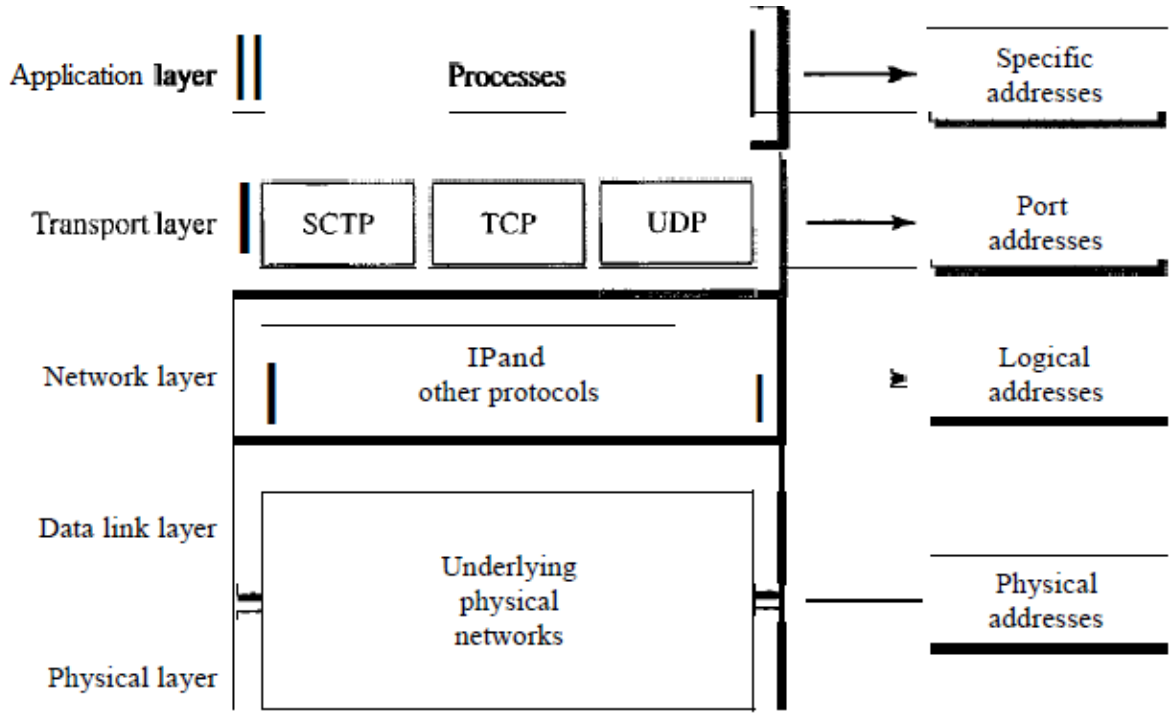


Figure 2. *Relationship of layers and addresses in TCP/IP*

Logical Addresses (IP address)

- 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.
- The physical addresses will change from hop to hop, but the logical addresses usually remain the same.

Port address

- 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 simultaneously, 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.
- Port address in TCP/IP is **16 bits** in length.
- The port address identifies a process on a host.

Specific Addresses

- A specific address is a **user-friendly address**.
- Examples include the e-mail address (for example, forouzan@fhda.edu) and the Universal Resource Locator (URL) (for example, www.mhhe.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web.

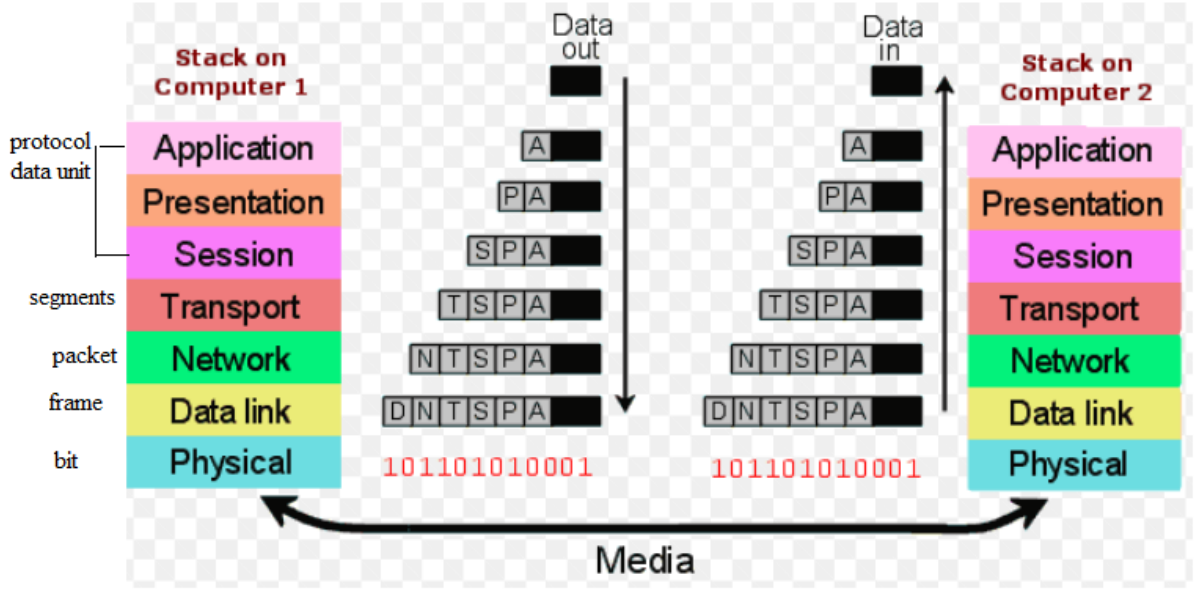
Merits of TCP/IP model

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

Demerits of TCP/IP model

1. In this, transport layer does not guarantee delivery of packets.
2. Relacing of protocol is not easy.

OSI Model



Layer	Name	Description
7	Application	Serves the application process, providing features such as file sharing, network transparency, and distributed processing.
6	Presentation	Performs services generally required by applications, such as data conversions, encryption, and compression.
5	Session	Negotiates and manages communications sessions between network processes.
4	Transport	Accepts data from the session layer and determines how to present it to the network layer. Takes data from the network layer and redistributes it to the appropriate applications or other entities on the upper layers.
3	Network	Routes data between adjacent or local network devices in the form of *packets*. A *packet* is the fundamental unit of data transmitted between network layers on two nodes.
2	Data Link	Provides an interface to a communications medium on the physical layer. Changes packets of data into *frames* and vice versa. A *frame* is the elementary unit of information transferred across the data link layer. Packets are contained within frames. The data link layer may provide error detection and correction.
1	Physical	Transmits raw bits over a physical medium, such as cable, microwave, or fiber optic. Converts frames to electronic signals, pulses, or other physical forms, and the reverse.

IEEE 802 Project

IEEE- institute of Electrical and Electronics Engineers.

IEEE STANDARDS

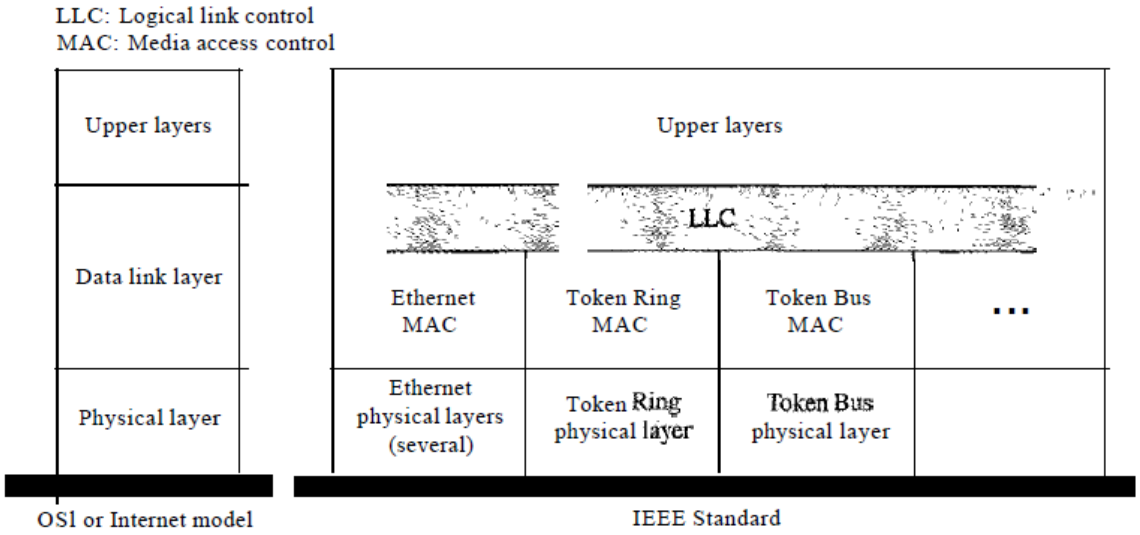
In 1985, the Computer Society of the IEEE started a project, called Project 802. It is a networking standards and proceedures for implementing and creating network related equipment.

A list of IEEE 802 standards are

802.1 – internetworking
802.2 – Logical link control(LLC)
802.3 – Ethernet
802.4 –Token bus
802.5 - Token ring
802.6 - MAN(Metropolitian Area Networks)
802.7 – Broadband technical advisory group
802.8 – Fiber optic technical advisory group
802.9 - integrated voice and data networks
802.10 – network security

802.11 – wireless networking

Figure 13.1 *IEEE standardfor LANs*



The relationship of the 802 Standard to the traditional OSI model is shown in Figure 13.1. The IEEE has subdivided the data link layer into two sublayers: logical link control (LLC) and media access control (MAC). IEEE has also created several physical layer standards for different LAN protocols.

Wired LANs: ETHERNET

ETHERNET STANDARDS

Ethernet standards are written and maintain by the IEEE. Different standards having different suffix letters.

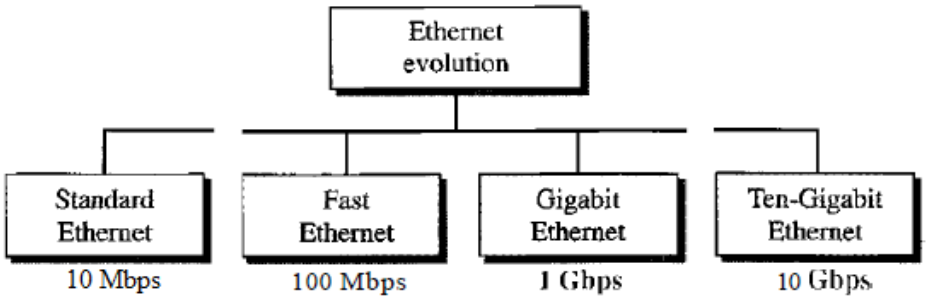
802.3a – 10 Base 2(thin Ethernet)
802.3i – 10 Base t(twisted pair)
802.3j – 10 Base F (fiber optic)
802.3x- Full duplex
802.3ae-10 Gigabyte Ethernet

ETHERNET FORMATS
First number specifies transmission speed in megabitsper seconds(Mbps). The second term indicates transmission time.ie base means baseband. The last term indicates segment length. 5 means 500m. In the more recent versions of IEEE 802 standard letters replace numbers Example 10 base T means UTP, 100 base T4 indicates 4 twisted pair.

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: Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (l Gbps), and Ten-Gigabit Ethernet (l0 Gbps), as shown in Figure 13.3.

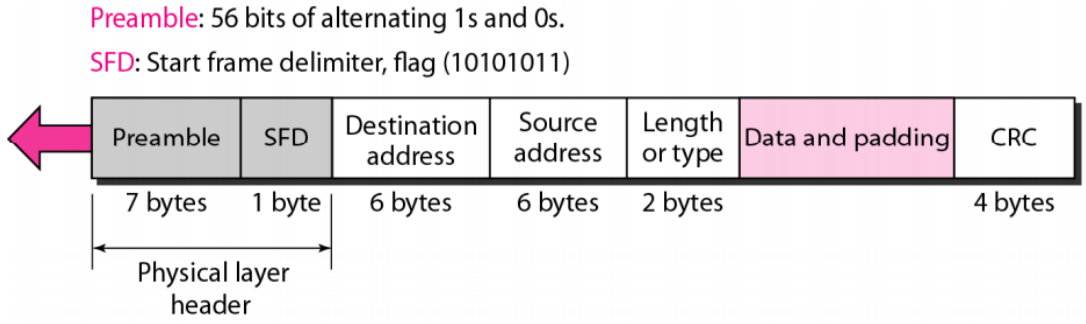
Figure 13.3 *Ethernet evolution through four generations*



MAC Sublayer

In Standard Ethernet, the MAC sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer.

Figure 13.4 ***802.3 MAC frame***



Frame Format

The Ethernet frame contains seven fields: preamble, SFD, DA, SA, length or type of protocol data unit (PDU), upper-layer data, and the CRC. Ethernet does not provide any mechanism for acknowledging received frames thus it is unreliable. Acknowledgments must be implemented at the higher layers. The format of the MAC frame is shown in Figure 13.4.

Preamble. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating 0's and 1's that alerts the receiving system to the coming frame and enables it to synchronize its input timing.

Start frame delimiter (SFD). The second field (l byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address

Destination address (DA). The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.

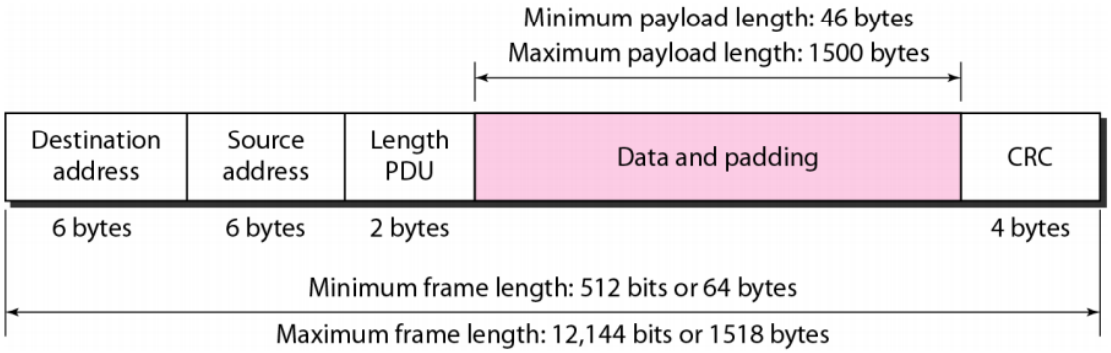
Source address (SA). The SA field is also 6 bytes and contains the physical address of the sender of the packet.

Length or type. This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.

Data. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes, as we will see later.

CRC. The last field contains error detection information.

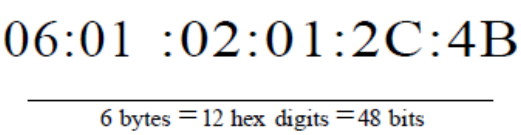
Frame Length



Addressing

Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6-byte physical address. As shown in Figure 13.6, the Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes.

Figure 13.6 *Example of an Ethernet address in hexadecimal notation*



Unicast, Multicast, and Broadcast Addresses: A source address is always a unicast address-the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. Figure 13.7 shows how to distinguish a unicast address from a multicast address. If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.

A unicast destination address defines only one recipient; the relationship between the sender and the receiver is one-to-one. A multicast destination address defines a group of addresses; the relationship between the sender and the receivers is one-to-many. The broadcast address is a special case of the multicast address; the recipients are all the stations on the LAN. A broadcast destination address is forty-eight 1s.

Example:

Define the type of the following destination addresses:

a. 4A:30:10:21:1O:1A

b. 47:20:1B:2E:08:EE

c. FF:FF:FF:FF:FF:FF

Solution

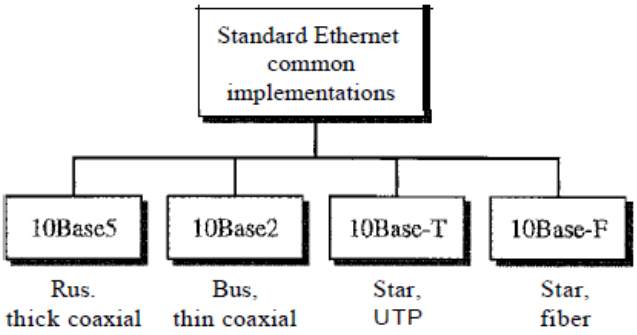
To find the type of the address, we need to look at the second hexadecimal digit from the left. If it is even, the address is unicast. If it is odd, the address is multicast. If all digits are F's, the address is broadcast. Therefore, we have the following:

a. This is a unicast address because A in binary is 1010 (even).

b. This is a multicast address because 7 in binary is 0111 (odd).

c. This is a broadcast address because all digits are F's.

Categories of Standard Ethernet



10 Base5: Thick Ethernet

The first implementation is called **10Base5, thick Ethernet, or Thicknet.** The nickname derives from the size of the cable. 10Base5 was the first Ethernet specification to use a bus topology with an external **transceiver** (transmitter/receiver) connected via a tap to a thick coaxial cable. Figure 13.10 shows a schematic diagram of a 10Base5 implementation.

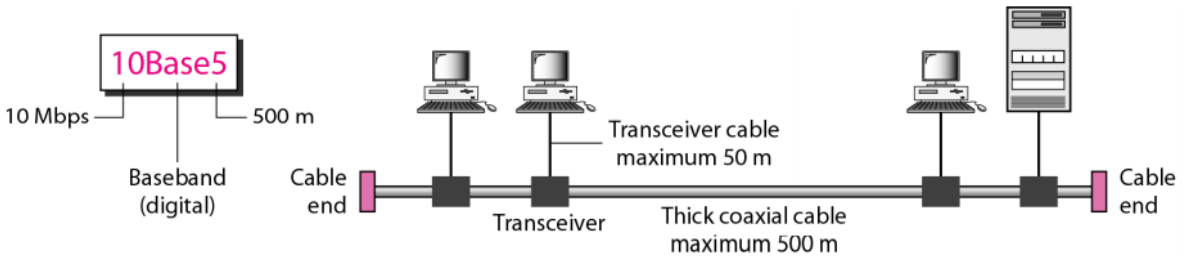
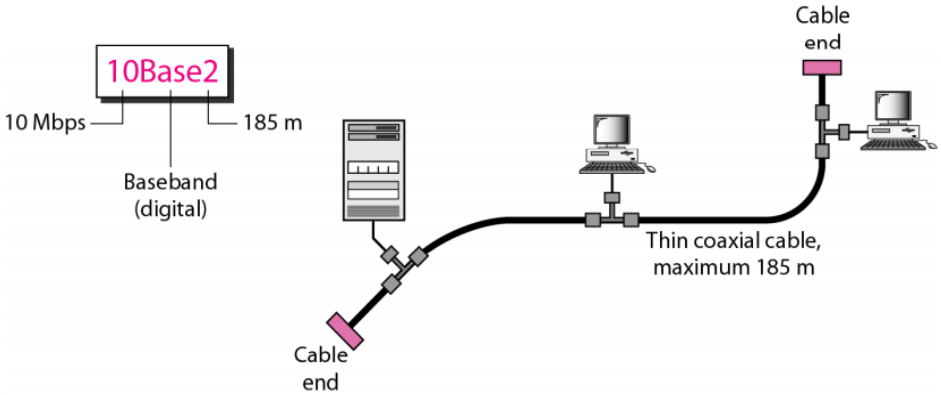


Fig. 10Base5 implementation

The transceiver is responsible for transmitting, receiving, and detecting collisions. The transceiver is connected to the station via a transceiver cable that provides separate paths for sending and receiving. This means that collision can only happen in the coaxial cable. The maximum length of the coaxial cable must not exceed *500* m, otherwise, there is excessive degradation of the signal. If a length of more than *500* m is needed, up to five segments, each a maximum of 500-meter, can be connected using repeaters.

10Base2: Thin Ethernet



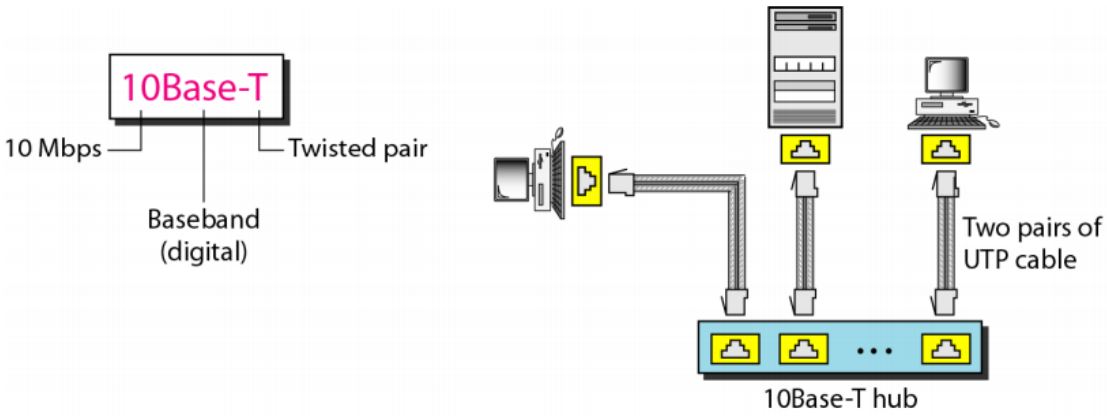
The second implementation is called 10Base2, **thin** Ethernet, or Cheapernet. 10Base2 also uses a bus topology, but the cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station. Figure shows the schematic diagram of a 10Base2 implementation.

Note that the collision here occurs in the thin coaxial cable. This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps. Installation is simpler because the thin coaxial cable is very flexible. However, the length of each segment cannot exceed *185* m (close to 200 m) due to the high level of attenuation in thin coaxial cable.

10Base-T: Twisted-Pair Ethernet

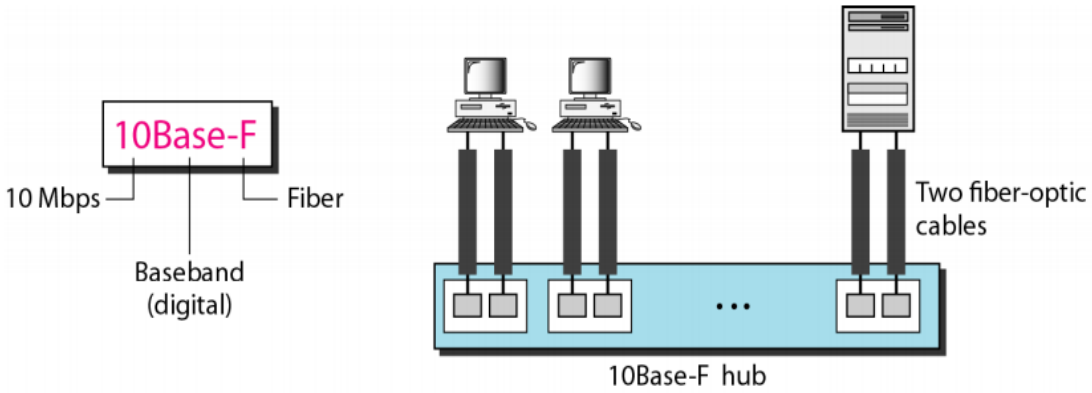
The third implementation is called 10Base-T or twisted-pair Ethernet. 10Base-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable, as shown in Figure.

Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub. Any collision here happens in the hub.
Compared to 10BaseS or 10Base2, we can see that the hub actually replaces the coaxial cable as far as a collision is concerned. The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.



10Base-F: Fiber Ethernet

lOBase-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables, as shown in Figure 13.13.



Summary of Standard Ethernet implementations

Characteristics	*10Base5*	*10Base2*	*10Base-T*	*10Base-F*
Media	Thick coaxial cable	Thin coaxial cable	2 UTP	2 Fiber
Maximum length	500 m	185 m	100 m	2000 m
Line encoding	Manchester	Manchester	Manchester	Manchester

Important points:

- Ethernet is the most widely used local area network protocol
- The IEEE 802.3 Standard defines I-persistent *CSMA/CD* as the access method for first-generation 10-Mbps Ethernet.
- The data link layer of Ethernet consists of the LLC sublayer and the MAC sublayer.
- The MAC sublayer is responsible for the operation of the *CSMA/CD* access method and framing.
- Each station on an Ethernet network has a unique 48-bit address imprinted on its network interface card (NIC).
- The minimum frame length for 10-Mbps Ethernet is 64 bytes; the maximum is 1518 bytes.

- The common implementations of 10-Mbps Ethernet are 10Base5 (thick Ethernet), 10Base2 (thin Ethernet), 10Base-T (twisted-pair Ethernet), and 10Base-F (fiber Ethernet).
- The 10Base5 implementation of Ethernet uses thick coaxial cable. lOBase2 uses thin coaxial cable. 10Base-T uses four twisted-pair cables that connect each station to a common hub. 10Base-F uses fiber-optic cable.
- A bridge can increase the bandwidth and separate the collision domains on an Ethernet LAN.
- A switch allows each station on an Ethernet LAN to have the entire capacity of the network to itself.
- Full-duplex mode doubles the capacity of each domain and removes the need for the *CSMA/CD* method.
- Fast Ethernet has a data rate of 100 Mbps.
- **In** Fast Ethernet, autonegotiation allows two devices to negotiate the mode or data rate of operation.
- The common Fast Ethernet implementations are 100Base-TX (two pairs of twisted pair cable), 100Base-FX (two fiber-optic cables), and 100Base-T4 (four pairs of voice-grade, or higher, twisted-pair cable).
- Gigabit Ethernet has a data rate of 1000 Mbps.
- Gigabit Ethernet access methods include half-duplex mode using traditional *CSMA/*CD (not common) and full-duplex mode (most popular method).
- The common Gigabit Ethernet implementations are 1000Base-SX (two optical fibers and a short-wave laser source), 1000Base-LX (two optical fibers and a long-wave laser source), and 1000Base-T (four twisted pairs).
- The latest Ethernet standard is Ten-Gigabit Ethernet that operates at 10 Gbps. The three common implementations are lOGBase-S, 10GBase-L, and 10GBase-E. These implementations use fiber-optic cables in full-duplex mode.

Wireless LAN - *IEEE 802.11*

Architecture

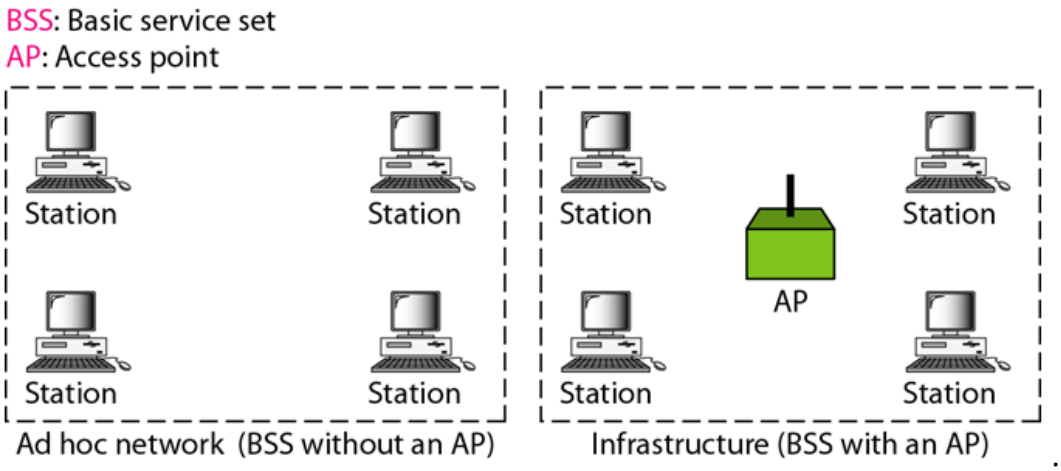
The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

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, known as the access point (AP). Figure 14.1 shows two sets in this standard.

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

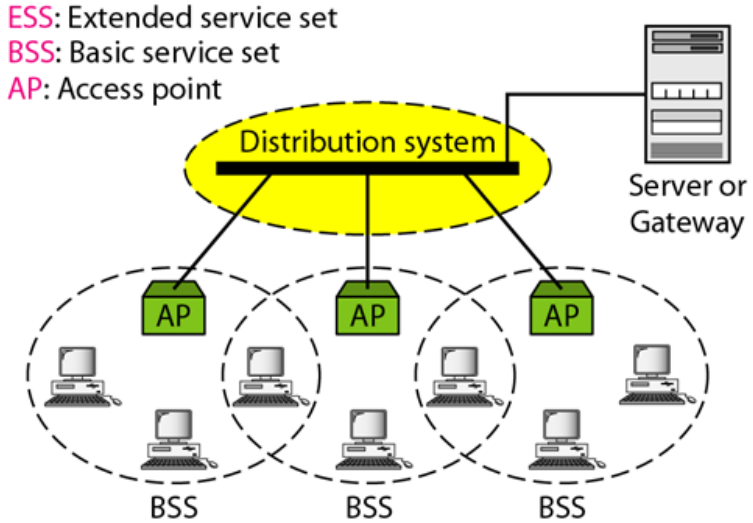
Figure 14.1 *Basic service sets (BSSs)*



Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a *distribution system*, which is usually a wired LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN. Figure 14.2 shows an ESS.

Figure 14.2 *Extended service sets (ESSs)*



When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs. The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a base station. Note that a mobile station can belong to more than one BSS at the same time.

Station Types

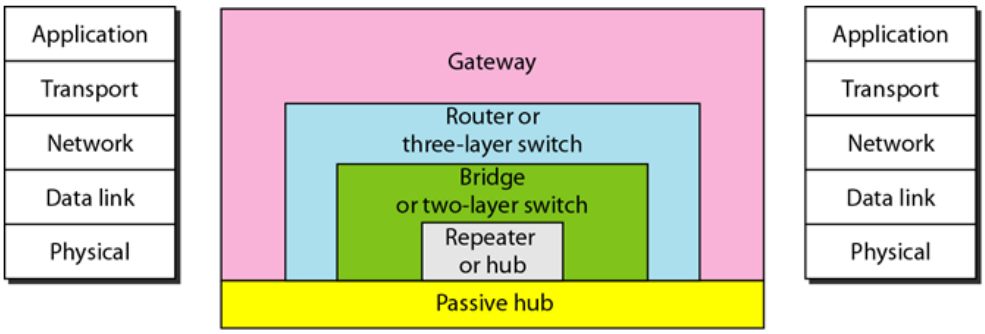
IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN: no-transition, BSS·transition, and ESS-transition mobility. A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS. A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS. A station with ESS-transition mobility can move from one ESS to another. However, IEEE 802.11 does not guarantee that communication is continuous during the move.

LAN Connecting Devices

In this section, we divide connecting devices into five different categories based on the layer in which they operate in a network.

The five categories contain devices which can be defined as
1. Those which operate below the physical layer such as a passive hub.
2. Those which operate at the physical layer (a repeater or an active hub).
3. Those which operate at the physical and data link layers (a bridge or a two-layer switch).
4. Those which operate at the physical, data link, and network layers (a router or a three-layer switch).
5. Those which can operate at all five layers (a gateway).

Figure 15.1 *Five categories of connecting devices*

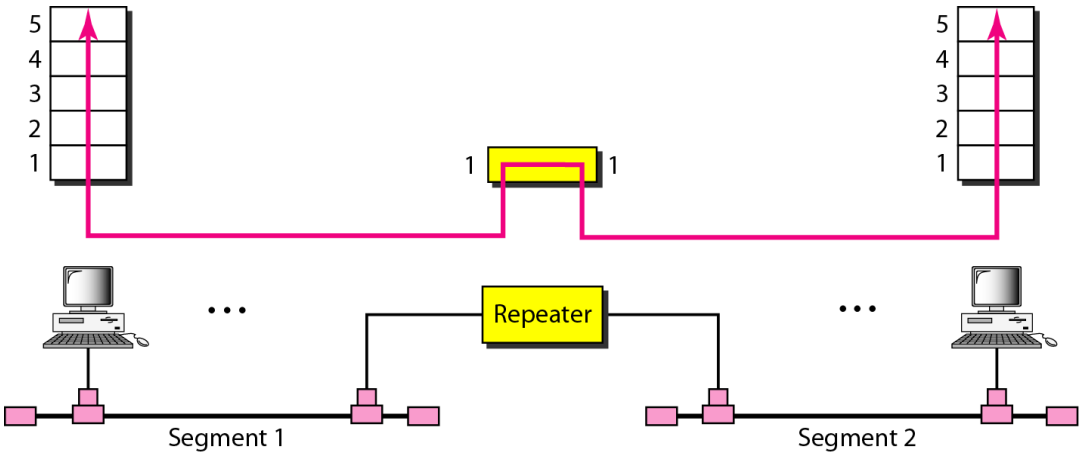


Passive Hubs

A passive hub is just a connector. It connects the wires coming from different branches. In a star-topology Ethernet LAN, a passive hub is just a point where the signals coming from different stations collide; the hub is the collision point. its location in the Internet model is below the physical layer.

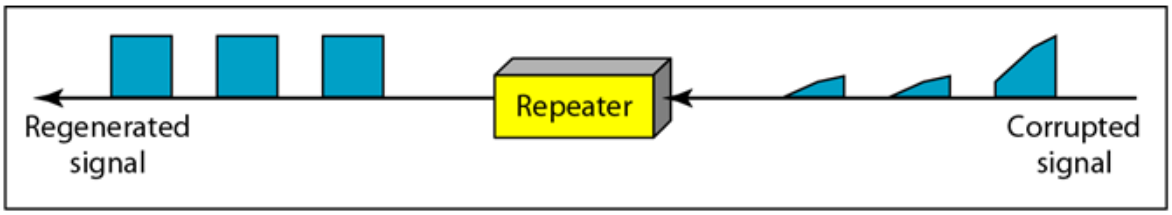
Repeaters

A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data. A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern. The repeater then sends the refreshed signal. A repeater can extend the physical length of a LAN, as shown in Figure 15.2.

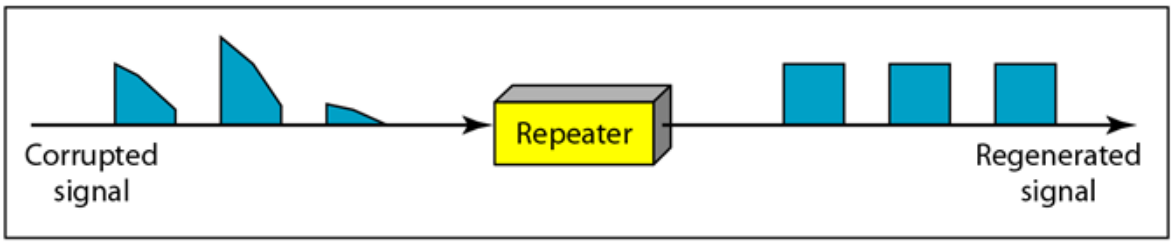


A repeater connects segments of a LAN.
A repeater forwards every frame – there is no filtering.
A repeater is a regenerator, not an amplifier.

Figure 15.3 ***Function of a repeater***



a. Right-to-left transmission.



b. Left-to-right transmission.

Active Hubs

An active hub is actually a multipart repeater. It is normally used to create connections between stations in a physical star topology. Hubs can also be used to create multiple levels of hierarchy, as shown in Figure 15.4. The hierarchical use of hubs removes the length limitation of 10Base-T (100 m).

Bridges

A bridge operates in both the physical and the data link layer. As a physical layer device, it regenerates the signal it receives. As a data link layer device, the bridge can check the physical (MAC) addresses (source and destination) contained in the frame.

Let us give an example. In Figure 15.5, two LANs are connected by a bridge. If a frame destined for station 712B13456142 arrives at port 1, the bridge consults its table to find the

departing port. According to its table, frames for 7l2B13456142 leave through port 1; therefore, there is no need for forwarding, and the frame is dropped. On the other hand, if a frame for 712B13456141 arrives at port 2, the departing port is port 1 and the frame is forwarded. In the first case, LAN 2 remains free of traffic; in the second case, both LANs have traffic. In our example, we show a two-port bridge; in reality a bridge usually has more ports.

A bridge has a table used in filtering decisions.

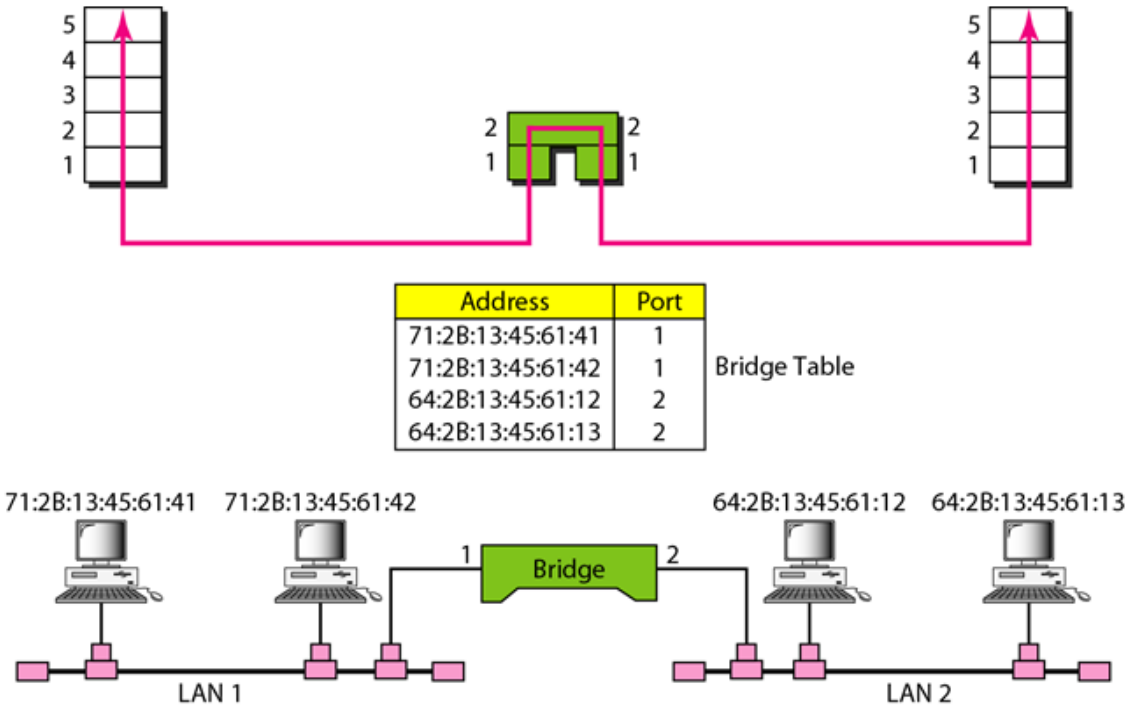
A bridge does not change the physical (MAC) addresses in a frame.

Types:
A transparent bridge
Source Routing Bridges

Two-Layer Switches

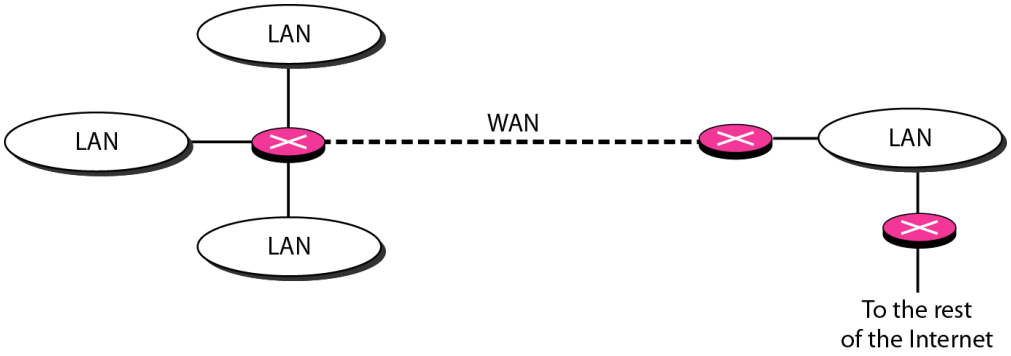
The **two-layer switch** performs at the physical and data link layers. A two-layer switch is a bridge, a bridge with many ports and a design that allows better (faster) performance. A bridge with a few ports can connect a few LANs together. A bridge with many ports may be able to allocate a unique port to each station, with each station on its own independent entity. This means no competing traffic (no collision).

Figure 15.5 ***A bridge connecting two LANs***



Routers

A router is a three-layer device that routes packets based on their logical addresses (host-to-host addressing). A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route. The routing tables are normally dynamic and are updated using routing protocols



Three-Layer Switches

A three-layer switch is a router, but a faster and more sophisticated. The switching fabric in a three-layer switch allows faster table lookup and forwarding. In this book, we use the terms *router* and *three-layer switch* interchangeably.

Gateway

A gateway is normally a computer that operates in all five layers of the Internet or seven layers of OSI model. A gateway takes an application message, reads it, and interprets it. This means that it can be used as a connecting device between two internetworks that use different models. For example, a network designed to use the OSI model can be connected to another network using the Internet model.

Network topology and virtual LAN