
Module 2:

Basics of Network Devices

2.1 Network Devices

Networking hardware, also known as network equipment or computer networking devices, are electronic devices which are required for communication and interaction between devices on a computer network. Specifically, they mediate data transmission in a computer network. Units which are the last receiver or generate data are called hosts, end systems or data terminal equipment.

All but the most basic of networks require devices to provide connectivity and functionality. Understanding how these networking devices operate and identifying the functions they perform are essential skills for any network administrator and requirements for a Network candidate.

2.1.1 NIC (Network Interface Card):

This is also known as Network Interface Unit (NIU). A network interface card (NIC) is a hardware component, typically a circuit board or chip, which is installed on a computer so that it can connect to a network. Modern NICs provide functionality to computers such as support for I/O interrupt, direct memory access (DMA) interfaces, data transmission, network traffic engineering and partitioning.

- A NIC provides a computer with a dedicated, full-time connection to a network by implementing the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi.
- Each card represents a device and can prepare, transmit and control the flow of data on the network. The NIC uses the OSI model to send signals at the physical layer, transmit data packets at the network layer and operate as an interface at the TCP/IP layer.
- Network cards can communicate with each other over the same network using a network switch, or if two computers are directly connected. When computers need to connect to a different network (e.g., the Internet), they must use a router to route the network packets to the correct network.

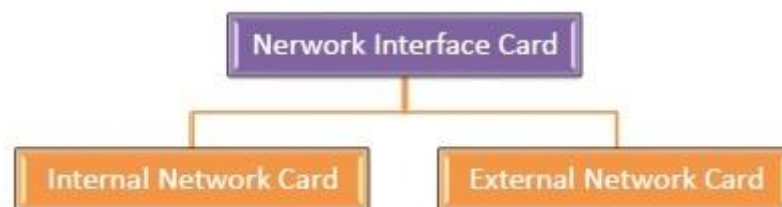
The network card operates as a middleman between a computer and a data network. For example, when a user requests a web page, the computer will pass the request to the network card which converts it into electrical impulses. Those impulses are received by a web server on the internet and responds by sending the web page back to the network card as electrical signals. The card gets these signals and translates them into the data that the computer displays.

Functions of NIC:

- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Installing NIC:

NIC cards are of two types –

**Internal Network Cards**

In internal networks cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).



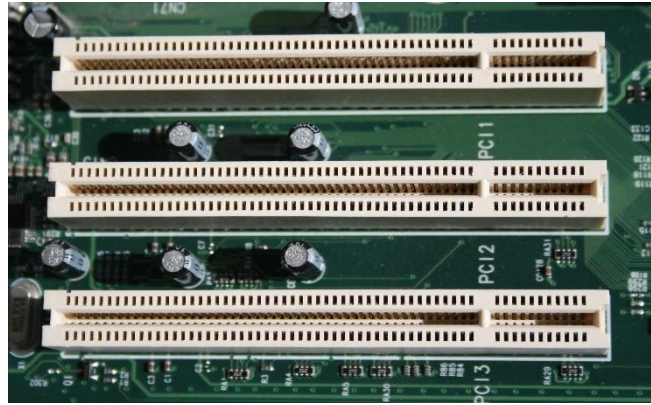
External Network Cards

In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.

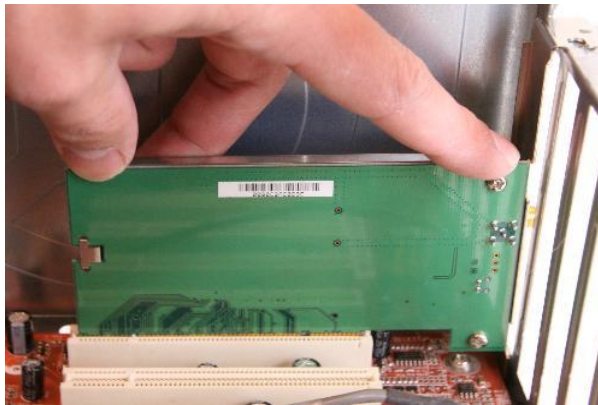


Steps of NIC installation:

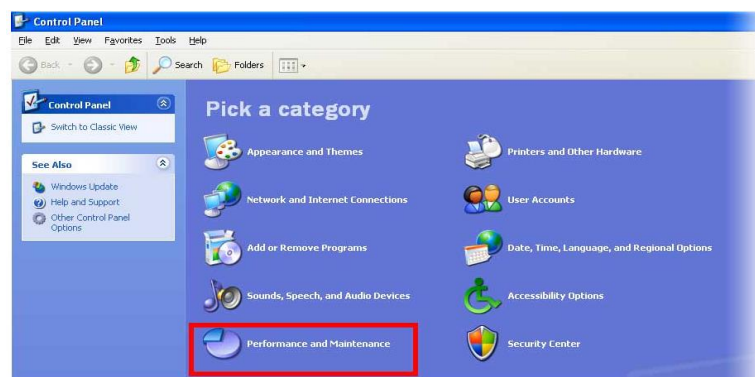
- First step is to read the user's guide and familiarize yourself with the new card.
- Power down PC and remove the AC power cord.
- Open the computer case.
- Find an available Peripheral Component Interconnect (PCI) slot on the motherboard and remove slot insert if one exists.



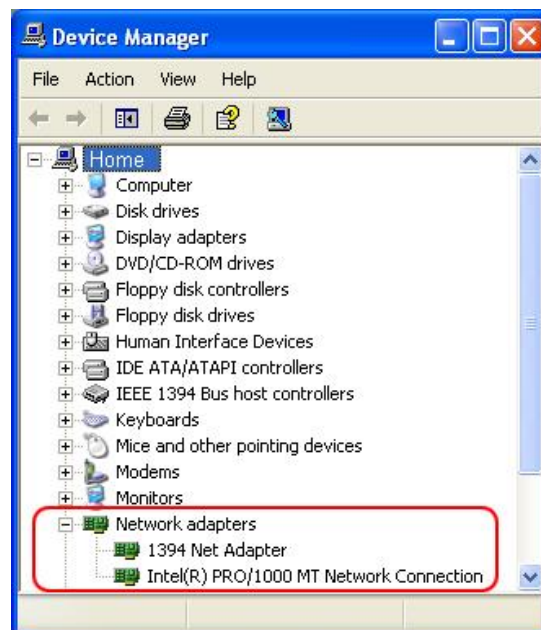
- Carefully remove the network card from its static-proof plastic envelope, and slide it into the slot.
- Seat the card in the slot firmly with gentle pressure along the length of the card, especially right about the slot itself.



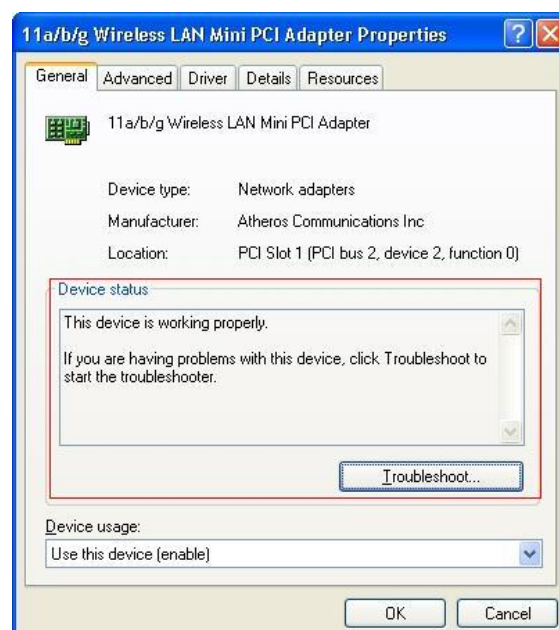
- Snugly, screw the card to the computer frame, but do not over tighten.
- Close the computer case.
- Plug your computer in and power it up.
- Click Start, then click Control Panel.
- In Category View (vs. Classic View) click Performance and Maintenance.



- Click "System" icon at bottom of window.
- Click the Hardware tab.
- Click the Device Manager button.
- Double-click Network Adapters.



- Beneath it should appear the name of your Ethernet card.
- Next, double click the name of your Ethernet adapter. If the text in the "Device Status" box says "This device is working properly.", then you successfully installed the card and are finished.



- If the text in the "Device status" box doesn't say "This device is working properly.", then write down on a piece of paper what it says and continue with next step.
- Click the Troubleshoot. Button and follow instructions. Double check you followed the directions above. Install the most up to date device drivers.

2.1.2 Repeater

- A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.
- When an electrical signal is transmitted via a channel, it gets attenuated depending upon the nature of the channel or the technology. This poses a limitation upon the length of the LAN or coverage area of cellular networks. This problem is alleviated by installing repeaters at certain intervals.

Installing the repeater:

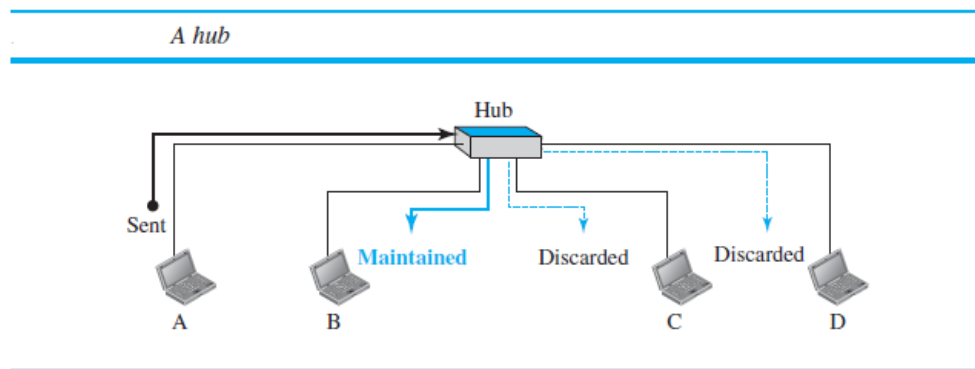
1. Choose a placement that is free of the same sorts of obstructions that can interfere with your router's signal. Thick concrete walls pose more of a problem than wood or glass, for example.
2. Plug the repeater into a working AC power outlet in your chosen location within range of your existing Wi-Fi coverage.
3. Using a nearby computer or laptop, connect the repeater. Do this by connecting an Ethernet cable directly from the repeater to your PC, a method that is often recommended by the manufacturer, or by connecting to the repeater's wireless network, often called something like *Wi-Fi Repeater* or containing the brand name of the product's manufacturer.
4. When they are connected, open your computer's local area network properties. On Windows, select Start > Control Panel > View Network Status and Tasks > Manage Network Connections. Then, right-click Local Area

Network and choose Properties, followed by Internet Protocol Version 4 and Properties again.

5. Check the repeater's instructions to be sure, but the default IP address you need to enter in the respective blank field is usually 192.168.10.1. Here, you'll also enter common number strings for the subnet mask (255.255.255.0) and default gateway (192.168.10.1).
6. Open a web browser and type `http://192.168.10.1` in the address bar. If asked to enter a DNS server address, leave the field blank. If asked for a username and password, try entering admin in both fields or admin in the username field and password in the password field. This brings you to the Setup Wizard.
7. Choose Wireless Repeater Mode and click Repeater – OneKey Setting. When it appears, select the Wireless Network Selection button and click Refresh List.
8. Choose your main router's wireless network to connect the repeater to the router and click Next.
9. Enter your Wi-Fi network's password in the Pre-Shared Key field when prompted if the network is secured. Now click Apply and Reboot and OK.

2.1.3 Hub

- A **hub** 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* and *retimes* the original bit pattern. The repeater then sends the refreshed signal. In the past, when Ethernet LANs were using bus topology, a repeater was used to connect two segments of a LAN to overcome the length restriction of the coaxial cable.
- Today, however, Ethernet LANs use star topology. In a star topology, a repeater is a multiport device, often called a *hub* that can be used to serve as the connecting point and at the same time function as a repeater.
- Figure shows that when a packet from station A to station B arrives at the hub, the signal representing the frame is regenerated to remove any possible corrupting noise, but the hub forwards the



Installing a hub:

1. Connect the hub's power cable into the socket on the back of the device. Plug the power adapter into the power outlet, and then power on the hub.
2. Insert the blue Ethernet cable that came with the hub into one of the numbered Ethernet ports on the rear panel of your Internet router.
3. Plug the other end of the blue Ethernet cable into the "Uplink" port on the hub. If you can't see a port marked with "Uplink," then your hub will instead use auto-sensing ports that detect the uplink connection from the router. In this situation, plug the cable into any Ethernet port on the rear of the hub or switch.
4. Connect each computer, printer or other network device to the free ports on the rear of the hub with an Ethernet cable.
5. Launch a Web browser or any other online application on a computer connected to the hub to access the Internet.

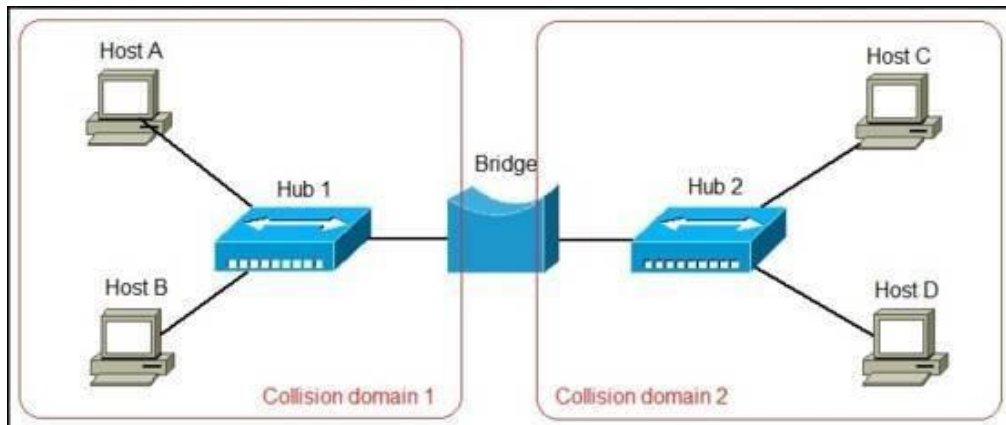
2.1.4 Bridge

- A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination.
- It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

Types of Bridges

- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges:-** In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The host can

discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.



- In the picture above we have a network of four computers. The network is divided into segments by a bridge.
- Each segment is a separate collision domain with its own bandwidth. Let's say that Host A wants to communicate with Host C. Host A will send the frame with the Host C's destination MAC address to the bridge. The bridge will inspect the frame and forward it to the segment of the network Host C is on.
- Network bridges offer substantial improvements over network hubs, but they are not widely used anymore in modern LANs. Switches are commonly used instead.

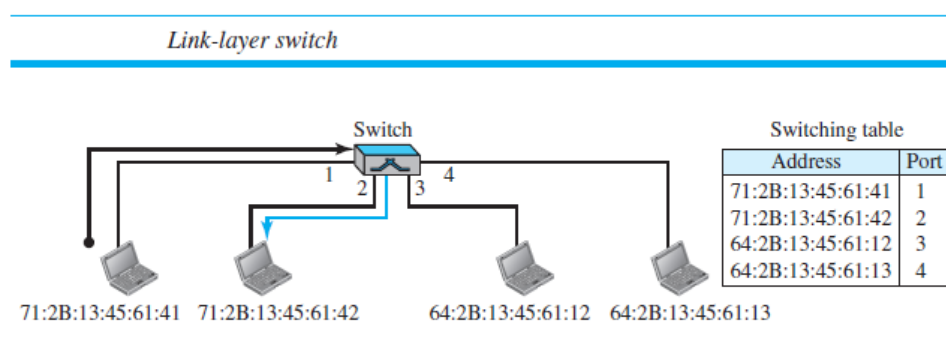
2.1.5 Switch

- A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance.
- A switch is a data link layer device.
- The switch can perform error checking before forwarding data that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.
- In other words, switch divides collision domain of hosts, but broadcast domain remains same.

Filtering

One may ask what the difference in functionality is between a link-layer switch and a hub. A link-layer switch has **filtering** capability. It can check the destination address of a frame and can decide from which outgoing port the frame should be sent.

For example. In Figure, we have a LAN with four stations that are connected to a link-layer switch. If a frame destined for station 71:2B:13:45:61:42 arrives at port 1, the link-layer switch consults its table to find the departing port. According to its table, frames for 71:2B:13:45:61:42 should be sent out only through port 2; therefore, there is no need for forwarding the frame through other ports.



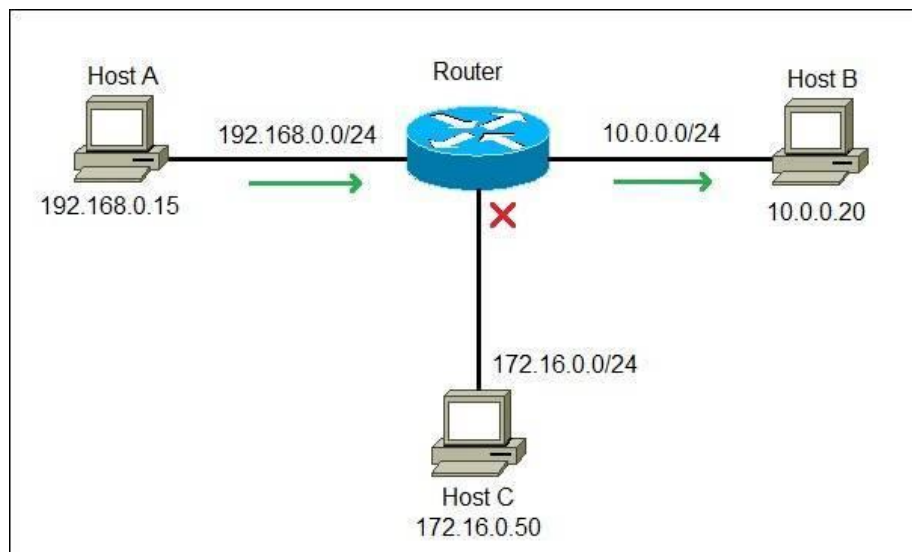
2.1.6 Routers

A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.

Installation of a network router:

- Connect the router's WAN port to your internet source, such as a DSL or cable modem, using the first network cable. All home routers have just one WAN port (sometimes labeled the internet port); this port is always separate from the other network ports and often is a different color to further differentiate it. Note: If you do not have internet access at home, or want to have an isolated (non internet-enabled) network, you can skip this step. Later on you can always complete this step when the internet is available or needed.
- Connect one of the router's LAN ports (most routers have four LAN ports) to the computer using the second network cable

- Plug the router into the power outlet using its power adapter, as you would with most electronics. If the router has an on-off switch, make sure the router is on. Many routers don't have this switch and will turn on as you plug it in.



We have a network of three computers. Note that each computer is on a different network. Host A wants to communicate with Host B and sends a packet with Host B's IP address (**10.0.0.20**) to the default gateway (the router). The router receives the packet, compares the packet's destination IP address to the entries in its routing table and finds a match. It then sends the packet out the interface associated with that network. Only Host B will receive the packet. In fact, Host C will not even be aware that the communication took place.

2.1.7 Gateway

- A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models.
- They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.
- Network gateway provides interoperability between networks and contains devices, such as protocol translators, impedance matchers, rate converters, fault isolators, or signal translators.
- A network gateway requires the establishment of mutually acceptable administrative procedures between the networks using the gateway.
- Network gateways, known as protocol translation gateways or mapping gateways, can perform protocol conversions to connect networks with different network protocol technologies.

- For example, a network gateway connects an office or home intranet to the Internet. If an office or home computer user wants to load a web page, at least two network gateways are accessed—one to get from the office or home network to the Internet and one to get from the Internet to the computer that serves the web page.

2.1.8 CSU/DSU:

- A Channel Service Unit/Digital Service Unit (CSU/DSU), sometimes called Data Service Unit, is a device that converts the digital signal format used on LANs into one used on WANs.
- Such translation is necessary because the networking technologies used on WANs are different from those used on LANs.
- The CSU/DSU sits between the LAN and the access point provided by the telecommunications company.
- Many router manufacturers are now incorporating CSU/DSU functionality into their products.
- The channel service unit (CSU) is responsible for the connection to the telecommunication network, while the data service unit (DSU) is responsible for managing the interface with the data terminal equipment (DTE).

2.1.9 MODEM:

- A modem, short for modulator/demodulator, is a device that converts the digital signals generated by a computer into analog signals that can travel over conventional phone lines.
- The modem at the receiving end converts the signal back into a format the computer can understand. Modems can be used as a means to connect to an ISP or as a mechanism for dialing up to a LAN.
- A modem modulates one or more carrier wave signals to encode digital information for transmission and demodulates signals to decode the transmitted information.

- The goal is to produce a signal that can be transmitted easily and decoded reliably to reproduce the original digital data. Modems can be used with almost any means of transmitting analog signals from light-emitting diodes to radio.
- A common type of modem is one that turns the digital data of a computer into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

Table1: Network devices summary

Device	Function/Purpose	Key Points
Hub	Connects devices on a twisted-pair network	A hub does not perform any tasks besides signal regeneration.
Switch	Connects devices on a twisted-pair network.	A switch forwards data to its destination by using the MAC address embedded in each packet.
Bridge	Divides networks to reduce overall network traffic	A bridge allows or prevents data from passing through it by reading the MAC address.
Router	Connects networks together.	A router uses the software-configured network address to make forwarding decisions.
Gateway	Translates from one data format to another.	Gateways can be hardware or software based. Any device that translates data formats is called a gateway
CSU/DSU	Translates digital signals used on a LAN to those used on a WAN.	CSU/DSU functionality is sometimes incorporated into other devices, such as a router with a WAN connection.
NIC	Enables systems to connect to the network.	Network interfaces can be add-in expansion cards, PCMCIA cards, or built-in interfaces.
MODEM	Provides serial communication capabilities across phone lines.	Modems modulate the digital signal into analog at the sending end and perform the reverse function at the receiving end.

2.2 Data Link Layer:

The data-link layer is located between the physical and the network layers. The data link layer provides services to the network layer; it receives services from the physical layer.

- The duty scope of the data-link layer is node-to-node. When a packet is travelling in the Internet, the data-link layer of a node (host or router) is responsible for delivering a datagram to the next node in the path.
- For this purpose, the data-link layer of the sending node needs to encapsulate the datagram received from the network in a frame, and the data-link layer of the receiving node needs to decapsulate the datagram from the frame. In other words, the data-link layer of the source host needs only to encapsulate, the data-link layer of the destination host needs to decapsulate, but each intermediate node needs to both encapsulate and decapsulate.
- One may ask why we need encapsulation and decapsulation at each intermediate node. The reason is that each link may be using a different protocol with a different frame format. Even if one link and the next are using the same protocol, encapsulation and decapsulation are needed because the link-layer addresses are normally different.
- The data link layer provides error-free transmission of data frames from one node to another over the physical layer. It allows the above layers to assume virtually error-free transmission over the link.
- It provides link establishment and termination, Physical addressing, Frame traffic control, Frame sequencing, Frame acknowledgment, Detects and recovers from errors that occur in the physical layer, Frame delimiting, Frame error checking and Media access management.
- The data link layer is partitioned into the **Logical Link Control (LLC)** and the **media access control (MAC) sublayers**. The LLC is common to all LANs and handles functions such as connection setup, initialization, data formatting, address recognition, error control, flow control and connection termination. Thus this sublayer supervises the transmission of a packet between nodes. The MAC layer handles access to the shared medium and is specific to the type of LAN that is implemented.

2.2.1 Ethernet:

Ethernet is a family of computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN) and wide area networks (WAN). It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3. Ethernet has since retained a good deal of backward compatibility and has been refined to support higher bit rates, a greater number of nodes, and longer link distances. Over time, Ethernet has largely replaced competing wired LAN technologies such as Token Ring, FDDI and ARCNET.

2.2.1.1 Ethernet standards

The IEEE 802 LAN/MAN (Metropolitan Area Network) Standards Committee develops and maintains networking standards and recommended practices for local, metropolitan, and other area networks, using an open and accredited process, and advocates them on a global basis. The most extensively used standards are for Ethernet, Bridging and Virtual Bridged LANs, Wireless LAN, Wireless Personal Area Network (PAN), Wireless MAN, Wireless Coexistence, Media Independent Handover Services, and Wireless Rural Area Network (RAN).

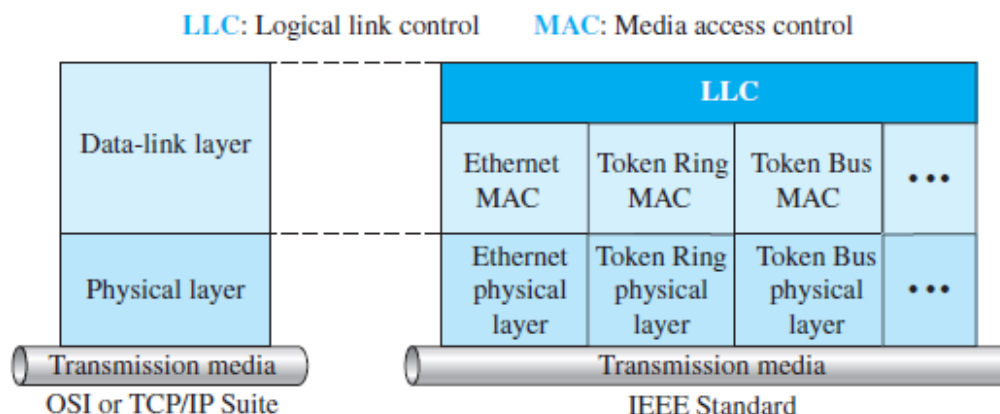
The relationship of the 802 Standard to the TCP/IP protocol suite is shown in Figure down below. The IEEE has subdivided the data-link layer into two sublayers: **logical link control (LLC)** and **media access control (MAC)**.

- **Logical Link Control (LLC)**

In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control (LLC). Framing is handled in both the LLC sublayer and the MAC sublayer. The LLC provides a single link-layer control protocol for all IEEE LANs. This means LLC protocol can provide interconnectivity between different LANs because it makes the MAC sublayer transparent.

- **Media Access Control (MAC)**

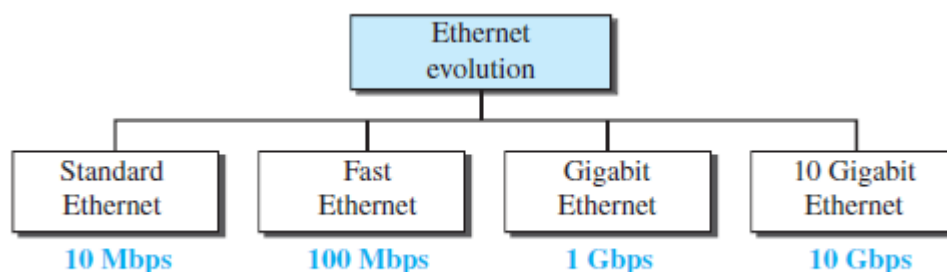
IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN. For example, it defines CSMA/CD as the media access method for Ethernet LANs and defines the token-passing method for Token Ring and Token Bus LANs. As we mentioned in the previous section, part of the framing function is also handled by the MAC layer.



2.2.1.2 Ethernet Evolution

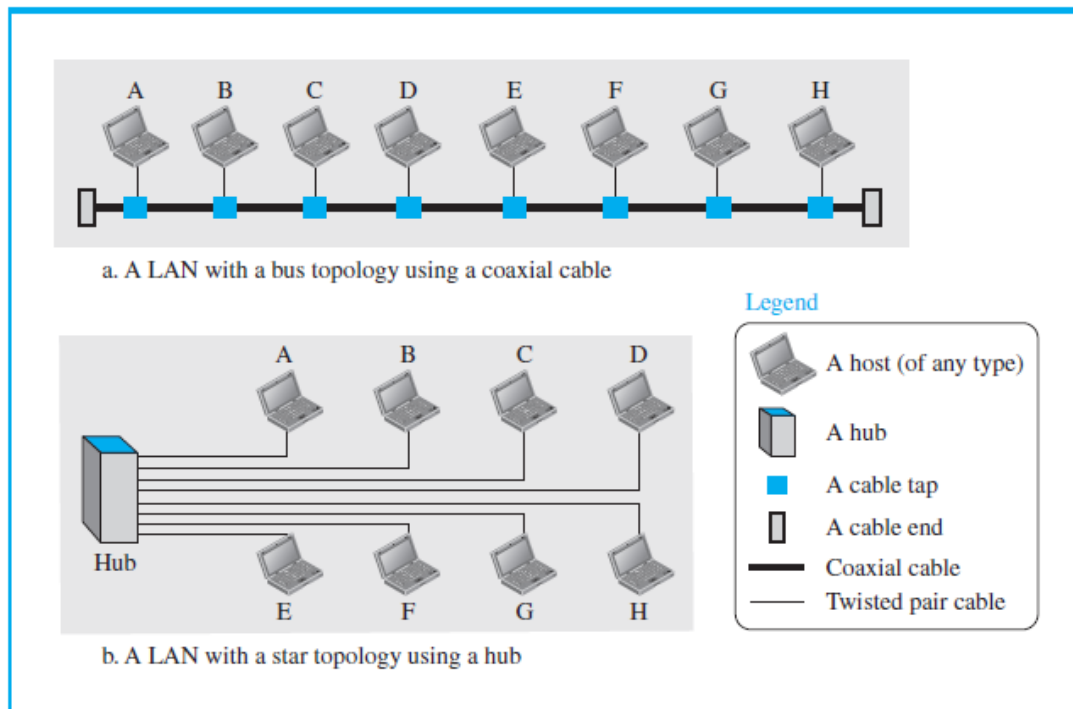
The Ethernet LAN was developed in the 1970s by Robert Metcalfe and David Boggs. Since then, it has gone through four generations as shown in Figure:

- Standard Ethernet (10 Mbps)
- Fast Ethernet (100 Mbps)
- Gigabit Ethernet (1 Gbps)
- 10 Gigabit Ethernet (10 Gbps)



2.2.2 Standard Ethernet

We refer to the original Ethernet technology with the data rate of 10 Mbps as the Standard Ethernet. Although most implementations have moved to other technologies in the Ethernet evolution, there are some features of the Standard Ethernet that have not changed during the evolution. We discuss this standard version to pave the way for understanding the other three technologies.



2.2.2.1 Characteristics

1. Connectionless and Unreliable Service

- Ethernet provides a connectionless service, which means each frame sent is independent of the previous or next frame. Ethernet has no connection establishment or connection termination phases.
- The sender sends a frame whenever it has it; the receiver may or may not be ready for it. The sender may overwhelm the receiver with frames, which may result in dropping frames.
- If a frame drops, the sender will not know about it. Since IP, which is using the service of Ethernet, is also connectionless, it will not know about it either.
- If the transport layer is also a connectionless protocol, such as UDP, the frame is lost and salvation may only come from the application layer.
- However, if the transport layer is TCP, the sender TCP does not receive acknowledgment for its segment and sends it again. Ethernet is also unreliable like IP and UDP.
- If a frame is corrupted during transmission and the receiver finds out about the corruption, which has a high level of probability of happening because of the CRC-32, the receiver drops the frame silently. It is the duty of high-level protocols to find out about it.

2. Frame Format

The Ethernet frame contains seven fields,

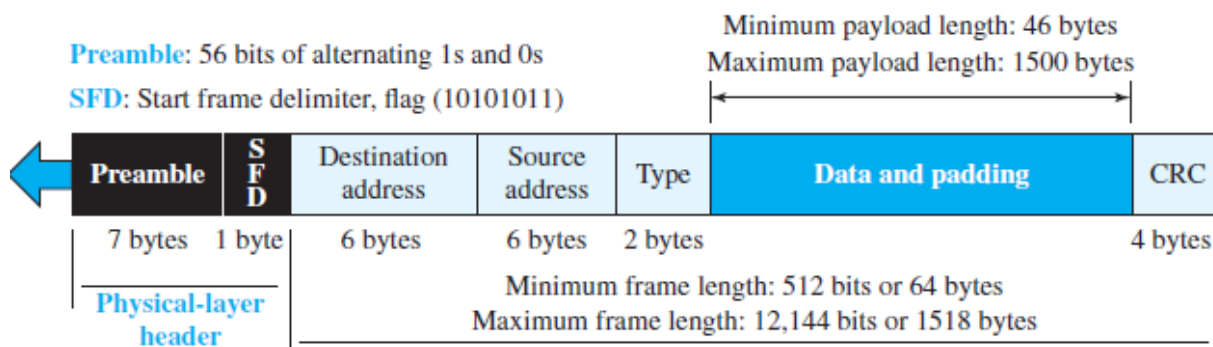


Figure: Ethernet Frame

- **Preamble.** This field contains 7 bytes (56 bits) of alternating 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its clock if it's out of synchronization. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.
- **Start frame delimiter (SFD).** This field (1 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 are (11)2 and alert the receiver that the next field is the destination address. This field is actually a flag that defines the beginning of the frame. We need to remember that an Ethernet frame is a variable-length frame. It needs a flag to define the beginning of the frame. The SFD field is also added at the physical layer.
- **Destination address (DA).** This field is six bytes (48 bits) and contains the link layer address of the destination station or stations to receive the packet. We will discuss addressing shortly. When the receiver sees its own link-layer address, or a multicast address for a group that the receiver is a member of, or a broadcast address, it decapsulates the data from the frame and passes the data to the upper layer protocol defined by the value of the type field.
- **Source address (SA).** This field is also six bytes and contains the link-layer address of the sender of the packet. We will discuss addressing shortly.
- **Type.** This field defines the upper-layer protocol whose packet is encapsulated in the frame. This protocol can be IP, ARP, OSPF, and so on. In other words, it serves the

same purpose as the protocol field in a datagram and the port number in a segment or user datagram. It is used for multiplexing and de-multiplexing.

- **Data.** This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes. We discuss the reason for these minimum and maximum values shortly. If the data coming from the upper layer is more than 1500 bytes, it should be fragmented and encapsulated in more than one frame. If it is less than 46 bytes, it needs to be padded with extra 0s. A padded data frame is delivered to the upper-layer protocol as it is (without removing the padding), which means that it is the responsibility of the upper layer to remove or, in the case of the sender, to add the padding. The upper-layer protocol needs to know the length of its data. For example, a datagram has a field that defines the length of the data.
- **CRC.** The last field contains error detection information, in this case a CRC-32. The CRC is calculated over the addresses, types, and data field. If the receiver calculates the CRC and finds that it is not zero (corruption in transmission), it discards the frame

3. Frame Length

Ethernet has imposed restrictions on both the minimum and maximum lengths of a frame. The minimum length restriction is required for the correct operation of CSMA/CD, as we will see shortly. An Ethernet frame needs to have a minimum length of 512 bits or 64 bytes. Part of this length is the header and the trailer.

4. 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 link-layer address. The Ethernet address is 6 bytes (48 bits), normally written in hexadecimal notation, with a colon between the bytes. For example, the following shows an Ethernet MAC address:

4A:30:10:21:10:1A

5. Transmission of Address Bits

The way the addresses are sent out online is different from the way they are written in hexadecimal notation. The transmission is left to right, byte by byte; however, for each byte, the least significant bit is sent first and the most significant bit is sent last. This means that the

bit that defines an address as unicast or multicast arrives first at the receiver. This helps the receiver to immediately know if the packet is unicast or multicast.

2.2.2 Point-to-Point Protocol (PPP):

One of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP). Point-to-Point Protocol (PPP) is a data link layer communications protocol between two routers directly without any host or any other networking in between.

- It can provide connection authentication, transmission encryption, and compression. Today, millions of Internet users who need to connect their home computers to the server of an Internet service provider use PPP.
- The majority of these users have a traditional modem; they are connected to the Internet through a telephone line, which provides the services of the physical layer. But to control and manage the transfer of data, there is a need for a point-to-point protocol at the data-link layer.
- PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links such as SONET.
- Internet service providers (ISPs) have used PPP for customer dial-up access to the Internet, since IP packets cannot be transmitted over a modem line on their own, without some data link protocol that can identify where the transmitted frame starts and where it ends.
- Two derivatives of PPP, Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over ATM (PPPoA), are used most commonly by ISPs to establish a digital subscriber line (DSL) Internet service connection with customers.

Services

- The designers of PPP have included several services to make it suitable for a point-to-point protocol, but have ignored some traditional services to make it simple.
- Services Provided by PPP defines the format of the frame to be exchanged between devices.

- It also defines how two devices can negotiate the establishment of the link and the exchange of data.
- PPP is designed to accept payloads from several network layers (not only IP). Authentication is also provided in the protocol, but it is optional.
- The new version of PPP, called Multilink PPP, provides connections over multiple links. O
- ne interesting feature of PPP is that it provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

PPP functionalities

1. Encapsulation

The PPP encapsulation provides for multiplexing of different network-layer protocols simultaneously over the same link. The PPP encapsulation has been carefully designed to retain compatibility with most commonly used supporting hardware. Only 8 additional octets are necessary to form the encapsulation when used within the default HDLC-like framing. In environments where bandwidth is at a premium, the encapsulation and framing may be shortened to 2 or 4 octets.

2. Link Control Protocol

In order to be sufficiently versatile to be portable to a wide variety of environments, PPP provides a Link Control Protocol (LCP). The LCP is used to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, detect a looped-back link and other common misconfiguration errors, and terminate the link. Other optional facilities provided are authentication of the identity of its peer on the link, and determination when a link is functioning properly and when it is failing.

3. Network Control Protocols

Point-to-Point links tend to exacerbate many problems with the current family of network protocols. For instance, assignment and management of IP addresses, which is a problem even in LAN environments, is especially difficult over circuit-

switched point-to-point links (such as dial-up modem servers). These problems are handled by a family of Network Control Protocols (NCPs), which each manage the specific needs required by their respective network-layer protocols. These NCPs are defined in companion documents.

PPP Configuration

It is intended that PPP links be easy to configure. By design, the standard defaults handle all common configurations. The implementer can specify improvements to the default configuration, which are automatically communicated to the peer without operator intervention. Finally, the operator may explicitly configure options for the link which enable the link to operate in environments where it would otherwise be impossible.

PPP Frame format

PPP uses a character-oriented (or byte-oriented) frame. Figure below shows the format of a PPP frame. The description of each field follows:

- **Flag.** A PPP frame starts and ends with a 1-byte flag with the bit pattern 01111110.

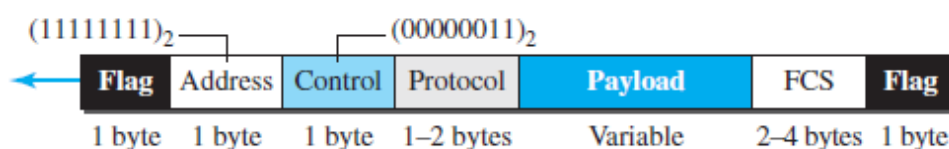


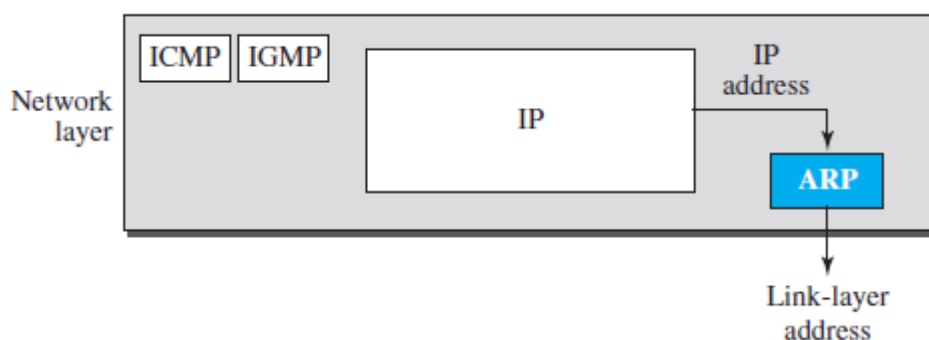
Figure: PPP Frame format

- **Address.** The address field in this protocol is a constant value and set to 11111111 (broadcast address).
- **Control.** This field is set to the constant value 00000011 (imitating unnumbered frames in HDLC). As we will discuss later, PPP does not provide any flow control. Error control is also limited to error detection.
- **Protocol.** The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only 1 byte.

- **Payload field.** This field carries either the user data or other information that we will discuss shortly. The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation. The data field is byte-stuffed if the flag byte pattern appears in this field. Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.
- **FCS.** The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRC.

2.2.3 Address Resolution Protocol

- The **Address Resolution Protocol (ARP)** is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.
- Anytime a node has an IP datagram to send to another node in a link, it has the IP address of the receiving node. The source host knows the IP address of the default router.
- Each router except the last one in the path gets the IP address of the next router by using its forwarding table. The last router knows the IP address of the destination host. However, the IP address of the next node is not helpful in moving a frame through a link; we need the link-layer address of the next node.
- This is the time when the **Address Resolution Protocol (ARP)** becomes helpful. The ARP protocol is one of the auxiliary protocols defined in the network layer, as shown in Figure.
- ARP accepts an IP address from the IP protocol, maps the address to the corresponding link-layer address, and passes it to the data-link layer.



Anytime a host or a router needs to find the link-layer address of another host or router in its network, it sends an ARP request packet. The packet includes the link-layer and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the link-layer address of the receiver, the query is broadcast over the link using the link-layer broadcast address, which we discuss for each protocol later.

*(working of ARP is explained in the 1st module)

Packet Format of ARP

Figure shows the format of an ARP packet. The names of the fields are self-explanatory.

- The *hardware type* field defines the type of the link-layer protocol; Ethernet is given the type 1.
- The *protocol type* field defines the network-layer protocol: IPv4 protocol is (0800)16. The source hardware and source protocol addresses are variable-length fields defining the link-layer and network-layer addresses of the sender.
- The destination hardware address and destination protocol address fields define the receiver link-layer and network-layer addresses.
- An ARP packet is encapsulated directly into a data-link frame. The frame needs to have a field to show that the payload belongs to the ARP and not to the network-layer datagram.

0	8	16	31
Hardware Type		Protocol Type	
Hardware length	Protocol length	Operation Request:1, Reply:2	
Source hardware address			
Source protocol address			
Destination hardware address (Empty in request)			
Destination protocol address			

Hardware: LAN or WAN protocol
Protocol: Network-layer protocol

2.3 Wireless Networking:

2.3.1 Wireless Technology:

- Wireless communication is one of the fastest-growing technologies.
- The demand for connecting devices without the use of cables is increasing everywhere. Wireless technology has helped to simplify networking by enabling multiple computer users to simultaneously share resources in a home or business without additional or intrusive wiring.
- These resources might include a broadband Internet connection, network printers, data files, and even streaming audio and video.
- This kind of resource sharing has become more prevalent as computer users have changed their habits from using single, stand-alone computers to working on networks with multiple computers, each with potentially different operating systems and varying peripheral hardware.
- U.S. Robotics wireless networking products offer a variety of solutions to seamlessly integrate computers, peripherals, and data. Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

2.3.2 Benefits of Wireless Technology:

- Wireless networking enables the same capabilities and comparable speeds of a wired 10BASE-T network without the difficulties associated with laying wire, drilling into walls, or stringing Ethernet cables throughout an office building or home.
- Laptop users have the freedom to roam anywhere in the office building or home without having to hunt down a connector cable or available jack. Every room in a wireless home or office can be “connected” to the network, so adding more users and growing a network can be as simple as installing a new wireless network adapter.

Reasons to choose wireless networking over traditional wired networks include:

- Running additional wires or drilling new holes in a home or office could be prohibited (because of rental regulations), impractical (infrastructure limitations), or too expensive
- Flexibility of location and data ports is required

- Roaming capability is desired; e.g., maintaining connectivity from almost anywhere inside a home or business
- Network access is desired outdoors; e.g., outside a home or office building

2.2.3 Types of Wireless Networks:

- The IEEE 802.11 has two basic modes of operation: **infrastructure and ad hoc mode**. In ad hoc mode, mobile units transmit directly peer-to-peer.
- In infrastructure mode, mobile units communicate through an access point that serves as a bridge to other networks (such as Internet or LAN).
- Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also included encryption mechanisms: Wired Equivalent Privacy (WEP, now insecure), Wi-Fi Protected Access (WPA, WPA2, WPA3), to secure wireless computer networks.

Infrastructure Mode

- Most Wi-Fi networks are deployed in infrastructure mode.
- In infrastructure mode, a base station acts as a wireless access point hub, and nodes communicate through the hub. The hub usually, but not always, has a wired or fiber network connection, and may have permanent wireless connections to other nodes.
- Wireless access points are usually fixed, and provide service to their client nodes within range.
- Wireless clients, such as laptops and smartphones, connect to the access point to join the network.
- Sometimes a network will have a multiple access points, with the same 'SSID' and security arrangement. In that case connecting to any access point on that network joins the client to the network. In that case, the client software will try to choose the access point to try to give the best service, such as the access point with the strongest signal.

Peer-to-peer communication (Ad-hoc mode)

Ad-hoc mode is also known as “peer-to-peer” mode. Ad-hoc networks don’t require a centralized access point. Instead, devices on the wireless network connect directly to each other. If you set up the two laptops in ad-hoc wireless mode, they’d connect directly to each other without the need for a centralized access point.

- An ad hoc network is a network where stations communicate only peer to peer (P2P). There is no base and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).
- A WiFi Direct network is another type of network where stations communicate peer to peer.
- In a Wi-Fi P2P group, the group owner operates as an access point and all other devices are clients.
- There are two main methods to establish a group owner in the Wi-Fi Direct group. In one approach, the user sets up a P2P group owner manually. This method is also known as Autonomous Group Owner (autonomous GO). In the second method, also called negotiation-based group creation, two devices compete based on the group owner intent value.
- A peer-to-peer network allows wireless devices to directly communicate with each other.
- Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network. This can basically occur in devices within a closed range.

2.3.4 Types of Wireless Communication

The different types of wireless communication mainly include, IR wireless communication, satellite communication, broadcast radio, Microwave radio, Bluetooth, Zigbee etc.

Bluetooth Technology

- A Bluetooth technology is a high speed low powered wireless technology link that is designed to connect phones or other portable equipment together.
- Bluetooth is a wireless technology that uses low-energy radio waves to send wireless data between Bluetooth-enabled devices. It's similar to Wi-Fi in that it operates over radio waves.
- It is a specification (IEEE 802.15.1) for the use of low power radio communications to link phones, computers and other network devices over short distance without wires.
- Wireless signals transmitted with Bluetooth cover short distances, typically up to 30 feet (10 meters).

- It is achieved by embedded low cost transceivers into the devices. It supports on the frequency band of 2.45GHz and can support upto 721KBps along with three voice channels.
- This frequency band has been set aside by international agreement for the use of industrial, scientific and medical devices (ISM).rd-compatible with 1.0 devices.

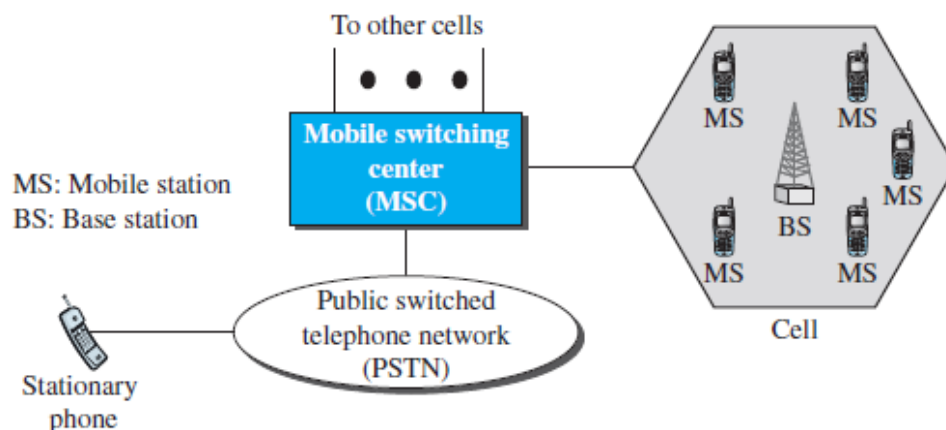
WiMAX

- WiMAX stands for Worldwide Interoperability for Microwave Access
- The Worldwide Interoperability for Microwave Access (WiMAX) has been designed for these types of applications.
- WiMAX refers to interoperable implementations of the IEEE 802.16 family of wireless-networks standards ratified by the WiMAX Forum.
- The scalable physical layer architecture that allows for data rate to scale easily with available channel bandwidth and range of WiMAX make it suitable for the following potential applications:
 1. Providing portable mobile broadband connectivity across cities and countries through various devices.
 2. Providing a wireless alternative to cable and digital subscriber line (DSL) for "last mile" broadband access.
 3. Providing data, telecommunications (VoIP) and IPTV services (triple play).
 4. Providing Internet connectivity as part of a business continuity plan.
 5. Smart grids and metering.

Cellular Telephony

- **Cellular telephony** is designed to provide communications between two moving units, called *mobile stations (MSs)*, or between one mobile unit and one stationary unit, often called a *land unit*.

- A service provider must be able to locate and track a caller, assign a channel to the call, and transfer the channel from base station to base station as the caller moves out of range.
- To make this tracking possible, each cellular service area is divided into small regions called *cells*.
- Each cell contains an antenna and is controlled by a solar- or AC powered network station, called the *base station* (BS). Each base station, in turn, is controlled by a switching office, called a **mobile switching center (MSC)**. The MSC coordinates communication between all the base stations and the telephone central office. It is a computerized center that is responsible for connecting calls, recording call information, and billing (see Figure).



Satellite Networks

- A *satellite network* is a combination of nodes, some of which are satellites, that provides communication from one point on the Earth to another.
- A node in the network can be a satellite, an Earth station, or an end-user terminal or telephone. Although a natural satellite, such as the moon, can be used as a relaying node in the network, the use of artificial satellites is preferred because we can install electronic equipment on the satellite to regenerate the signal that has lost its energy during travel.
- Another restriction on using natural satellites is their distances from the Earth, which create a long delay in communication.
- Satellite networks are like cellular networks in that they divide the planet into cells.

- Satellites can provide transmission capability to and from any location on Earth, no matter how remote.
- This advantage makes high-quality communication available to undeveloped parts of the world without requiring a huge investment in ground-based infrastructure.

2.3.5 Wireless network Components:

Wireless LANs consist of components similar to traditional Ethernet-wired LANs. In fact, wireless LAN protocols are similar to Ethernet and comply with the same form factors. The big difference, however, is that wireless LANs don't require wire.

User Devices

- Users of wireless LANs operate a multitude of devices, such as PCs, laptops, and PDAs. The use of wireless LANs to network stationary PCs is beneficial because of limited needs for wiring.
- Laptops and PDAs, however, are commonly equipped with wireless LAN connectivity because of their portable nature.
- User devices might consist of specialized hardware as well. For example, bar code scanners and patient monitoring devices often have wireless LAN connectivity.

Radio NICs

- A major part of a wireless LAN includes a radio NIC that operates within the computer device and provides wireless connectivity.
- A wireless LAN radio NIC, sometimes referred to as a radio card, often implements the 802.11 standard. The cards generally implement one particular physical layer, such as 802.11a or 802.11b/g. As a result, the radio card must utilize a version of the standard that is compatible with the wireless LAN.
- Wireless LAN radio cards that implement multiple versions of the standard and provide better interoperability are becoming more common.
- Radio cards come in a variety of form factors, including: ISA, PCI, PC card, mini-PCI, and CF. PCs generally utilize ISA and PCI cards; but PDAs and laptops use PC cards, mini-PCI, and CF adapters.

Access Points

- An access point contains a radio card that communicates with individual user devices on the wireless LAN, as well as a wired NIC that interfaces to a distribution system, such as Ethernet.
- System software within the access point bridges together the wireless LAN and distribution sides of the access point.
- The system software differentiates access points by providing varying degrees of management, installation, and security functions. Figure 5-1 shows an example of access-point hardware.



Figure : Wireless LAN Access Points Connect Wireless LANs to Wired Networks

- In most cases, the access point provides an http interface that enables configuration changes to the access point through an end-user device that is equipped with a network interface and a web browser.
- Some access points also have a serial RS-232 interface for configuring the access point through a serial cable as well as a user device running terminal emulation and Telnet software, such as hyper terminal.

2.3.6 Wireless LAN standards:

1. IEEE 802.11

- IEEE 802.11 is part of the IEEE 802 set of LAN protocols, and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies.
- They are the world's most widely used wireless computer networking standards, used in most home and office networks to allow laptops, printers, and smartphones to talk to each other and access the Internet without connecting wires.
- They are created and maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments.

2. IEEE 802.11a:

- 802.11a, published in 1999, uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer).
- It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s.
- It has seen widespread worldwide implementation, particularly within the corporate workspace.

3. IEEE 802.11b:

- The 802.11b standard has a maximum raw data rate of 11 Mbit/s (Megabits per second), and uses the same media access method defined in the original standard.
- 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard.
- The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

4. IEEE 802.11g:

- In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a.
- It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput.
- 802.11g hardware is fully backward compatible with 802.11b hardware, and therefore is encumbered with legacy issues that reduce throughput by ~21% when compared to 802.11a.

2.3.7 Wireless LAN modulation techniques:

- The process of modulation is the varying in a signal or a tone called a carrier signal. Data is then added to this carrier signal in a process known as encoding.
- Imagine that you are singing a song. Words are written on a sheet of music. If you just read the words, your tone is soft and does not travel far. To convey the words to a large group, you use your vocal chords and modulation to send the words farther. While you are singing the song, you encode the written words into a waveform and let your vocal cords modulate it. People hear you singing and decode the words to understand the meaning of the song.
- **Modulation** is what **wireless** networks use to send data. It enables the sending of encoded data using radio signals. **Wireless** networks use **modulation** as a carrier signal, which means that the **modulated** tones carry data. A modulated waveform consists of three parts:

Amplitude: The volume of the signal

Phase: The timing of the signal between peaks

Frequency: The pitch of the signal

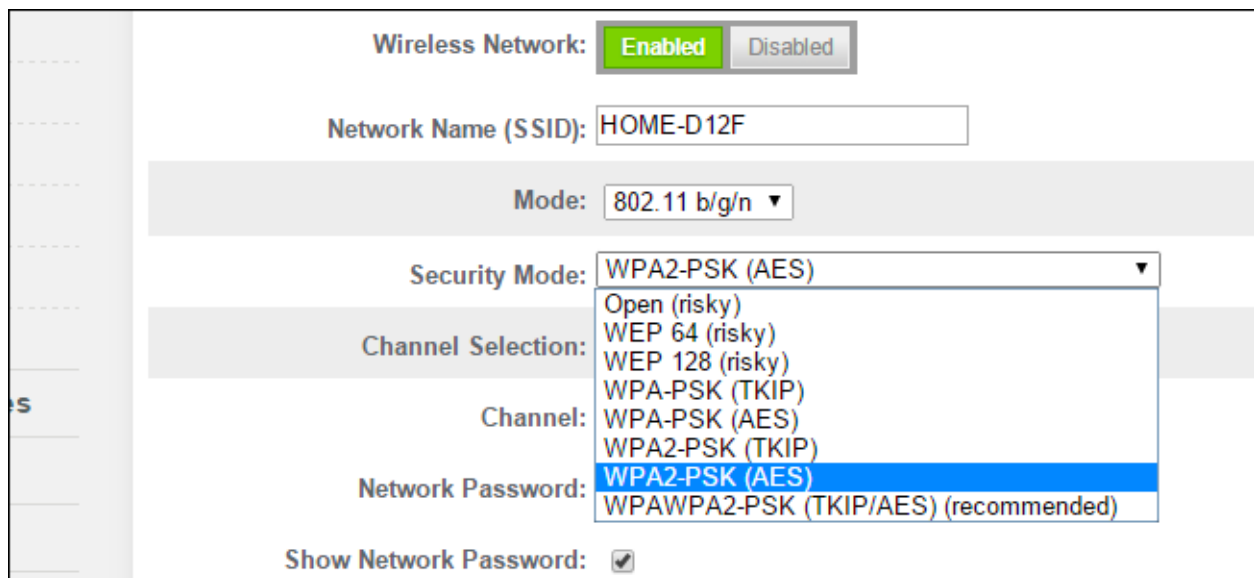
- Wireless networks use a few different modulation techniques, including the above mentioned : DSSS (direct-sequence spread spectrum), OFDM (Orthogonal Frequency Division Multiplexing)
- DSSS is the modulation technique that 802.11b devices use to send the data. In DSSS, the transmitted signal is spread across the entire frequency spectrum that is being used.
- Orthogonal frequency division multiplexing (OFDM) is a modulation and multiplexing technique. Modulation is the process by which data is encoded onto a carrier signal, which is then amplified and applied to an antenna.

2.3.8 Wireless security Protocols:

Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. The most common type is **Wi-Fi security**, which includes

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA).
- IEEE 802.1X

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.



The screenshot displays a wireless network configuration window. At the top, the 'Wireless Network' status is set to 'Enabled'. Below this, the 'Network Name (SSID)' is 'HOME-D12F'. The 'Mode' is set to '802.11 b/g/n'. The 'Security Mode' dropdown menu is open, showing a list of options: 'Open (risky)', 'WEP 64 (risky)', 'WEP 128 (risky)', 'WPA-PSK (TKIP)', 'WPA-PSK (AES)', 'WPA2-PSK (TKIP)', 'WPA2-PSK (AES)', and 'WPAWPA2-PSK (TKIP/AES) (recommended)'. The 'Channel Selection' is set to 'Channel: WPA2-PSK (AES)'. The 'Network Password' field is empty. At the bottom, the 'Show Network Password' checkbox is checked.

Figure: Wireless security protocols versions can be seen

1. Wired Equivalent Privacy (WEP)

- Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks.

- WEP, recognizable by its key of 10 or 26 hexadecimal digits (40 or 104 bits), was at one time widely in use and was often the first security choice presented to users by router configuration tools.
- Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication.
- In Open System authentication, the WLAN client does not provide its credentials to the Access Point during authentication. Any client can authenticate with the Access Point and then attempt to associate.
- In effect, no authentication occurs. Subsequently, WEP keys can be used for encrypting data frames. At this point, the client must have the correct keys.

2. Wi-Fi Protected Access (WPA)

- Wi-Fi Protected Access (WPA) is a security standard for users of computing devices equipped with wireless internet connections.
- WPA was developed by the Wi-Fi Alliance to provide more sophisticated data encryption and better user authentication than Wired Equivalent Privacy (WEP), the original Wi-Fi security standard.
- Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3) are three security and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.
- Despite various improvements, work-rounds, and other attempts to shore up the WEP system, it remains highly vulnerable. As computing power increased, it became easier and easier to exploit those flaws.
- WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999.
- However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.

3. IEEE 802.1X:

- IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols.
- It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
- The IEEE 802.1X standard defines a client and server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports.
- The authentication server authenticates each client connected to a switch port and assigns the port to a VLAN before making available any services offered by the switch or the LAN.
- 802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The **supplicant** is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator.
- The **authenticator** is a network device which provides a data link between the client and the network and can allow or block network traffic between the two, such as an Ethernet switch or wireless access point; and the **authentication server** is typically a trusted server that can receive and respond to requests for network access, and can tell the authenticator if the connection is to be allowed, and various settings that should apply to that client's connection or setting.

2.3.9 Installing a wireless LAN

1. **Find the best location for the wireless router.** The optimal placement is in a central location of your home, free from obstructions that could cause wireless interference.
2. **Turn off the modem.** Power off the cable or DSL modem from your internet service provider before connecting your equipment

3. **Connect the router to the modem.** Plug an Ethernet cable (typically provided with the router) into the router WAN port. Then, connect the other end of the Ethernet cable to the modem
4. **Connect a laptop or computer to the router.** Plug one end of another Ethernet cable into the router LAN port (any port will work) and the other end of the Ethernet cable into the Ethernet port of a laptop.
5. **Power up the modem, router, and computer.** It's important that these devices be turned on in the proper order. Turn on the modem first. When the modem lights are all on, turn on the router. When the router is on, turn on the computer.
6. **Go to the management web page for the router.** Open a browser and enter the IP address of the router administration page. This information is provided in the router documentation (it's usually something like 192.168.1.1). The login information is also in the manual.
7. **Change the default administrator password (and username) for the router.** This setting is usually found in the router administration page in a tab or section called Administration. Use a strong password that you won't forget.
8. **Add WPA2 security.** This step is essential. Find this setting in the wireless security section of the router administration page. Select which type of encryption to use and enter a passphrase of at least 8 characters. The more characters and the more complex the password, the better.
9. **Change the wireless network name (SSID).** To make it easy for you to identify your network, choose a descriptive name for your SSID (**Service Set Identifier**) in the wireless network information section of the router administration page.
10. **Set up the wireless adapter on the computer.** After saving the configuration settings on the router, unplug the cable that connects the computer to the router. Then, plug a USB or PC card wireless adapter into the laptop, if it doesn't have a wireless adapter installed or built-in.

11. **Connect to the new wireless network.** On your computer and other wireless-enabled devices, find the new network you set up and connect to the network.