**UNIT-IV** **12 Hours**

Bit Local Area Network: Overview, LAN Protocol Architecture, Bridges, Layer 2 and Layer 3 Switches. High-Speed LANs: The Emergence of High-Speed LANs. Wireless LANs: Overview, Wireless LAN Technology, IEEE 802.11-Architecture and Services, Modems and Types.

**Learning Outcomes**: At the end of this unit the students will be able to

1. Define and interpret the LAN architecture and its variants.

2. Recognize the importance of High-speed LAN and its applications.

**What is Layer 2 switching?**

- The term Layer 2 is adopted from the Open System Interconnect (OSI) model, which is a reference model for explaining and describing network communications.

- It is the process of using devices and MAC addresses on a LAN to segment a network. Switches and bridges are mostly used for Layer 2 switching.
- They help to break up large size collision domain into separate smaller ones.
- Layer 2 CISCO switches are similar to bridges.
- They interconnect networks at layer 2, mostly at the MAC sub-layer, and operate as bridges. It builds tables for the transfer of frames among systems.
- Layer 2 ethernet switches are faster compared to routers, as they do not take much time for evaluation at the network layer header information.
- Instead, they should look at the frame's hardware addresses, which helps you decide what action needs to take like forward, flood, or drop it.

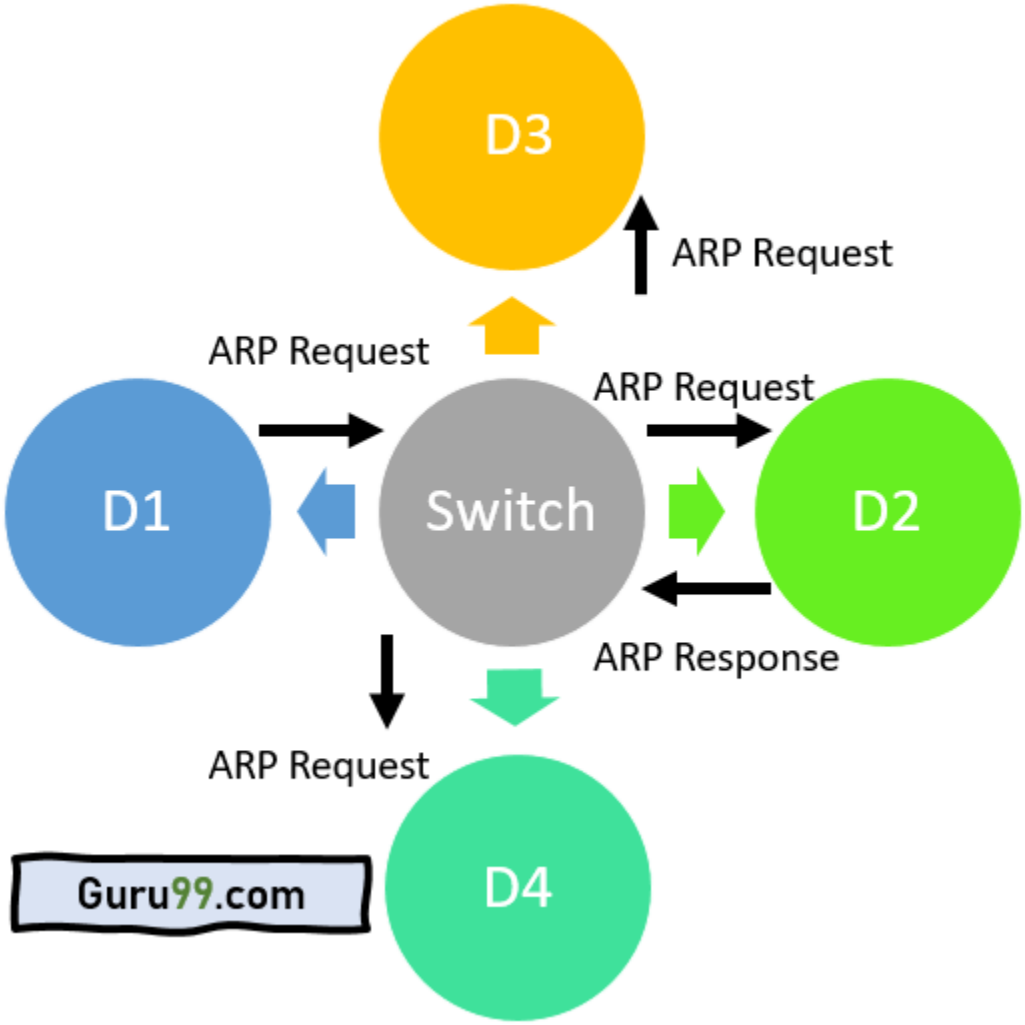
**What is Layer 3 Switching?**

A Layer 3 switch is a switch that performs routing functions in addition to switching. A client computer needs a default gateway for layer 3 connectivity to any remote subnets.

This type of layer helps you to combine the functionality of a switch and a router. It acts as a switch to connect devices that are on the same subnet or virtual LAN.

This type of CISCO network switches support routing protocols. It helps to inspect incoming packets and makes routing decisions based on the source and destination addresses. That is how layer 3 switch acts as both for switch and a router.

**How Layer 2 Switching works?**




Layer2 switching

Here is an example of a network where a switch is connected to four host devices known as D1, D2, D3, and D4.

- D1 wants to send a data packet to D2 for the first time.
- D1 knows the IP address of D2 as they are communicating for the first time. However, it does not know the MAC (hardware) address of the recipient host.
- Thus D1 uses an ARP to discover the MAC address of D2.
- The Layer switch sends the ARP request to all the ports that exclude the port on which D1 is connected.
- D2, when receives the ARP request, replies to the ARP response message with its MAC address. D2 also gathers the MAC address of D1.
- Here, with the help of the above-given messages, switch learns which MAC addresses are assigned to which ports.
- Similarly, D2 also sends its MAC address in the ARP message,the switch now takes the MAC address of D2 and banks it into the MAC address table.
- It also stores the MAC address of D1 in the address table as it was sent by D1 to switch with the ARP request message.
- So, whenever D1 wants to send any data to D2, the switch will check the table and forward it to the other destination port of D2.
- Similarly, the Layer Switch will keep on maintaining the hardware address of each connecting host.

**Functions of layer 2 switching**

Here are important functions of Layer 2 switching:

- MAC addresses are known from all the incoming frames source addresses.
- Bridges and switches communicate with each other using the STP to remove bridging loops.
- Frames designed for unknown locations are overflowed out to all ports except the one that received the frame.
- It performs the same function as a transparent bridge.
- Frames are forwarded using specialized hardware, which is known as Application-Specific Integrated Circuits (ASIC).
- Layer-2 switches also perform the switching function to re-arrange the data frames from the source to its destination network.
- Layer-2 Switch splits a complicated LAN (local area network) into small VLAN networks.

**Functions of layer 3 switching**

Here are important functions of Layer 3 switching:

- Define paths based on logical addressing

- Provide Security
- Run layer three checksums
- Process and respond to any option information
- Allows you to update simple Network Management
- Information Base (MIB) information

**Applications of Layer-2 Switches**

Here are some important applications of Layer 2 switches.

- You can send a data frame from the source to the destination that is situated in the same VLAN without being physically connected.
- Servers of IT companies can be put centrally at one place. The clients located at some other locations can access the data link layer without latency, which saves the server cost and time.
- Companies also used it for internal communications by configuring the hosts on the same VLAN by using Layer 2 switches without any internet connection.
- Software professionals also use these switches for sharing their tools by keeping them centrally at one server location.

**Difference between Layer 2 and Layer 3 Switches**

Here are some important difference between Layer 2 and Layer 3 switching:

| Layer 2 | Layer 3 |
|---|---|
| Layer 2 switching is used to reduce traffic on the local network. | It is mostly used to Implement VLAN. |
| In Layer 2, switching packets are rerouted from the source to the destination port. | In Layer 3 switching, switches use a little time to check data packets before finding the best available route to direct data packets to the destination port. |
| Layer 2 uses the Address Resolution Protocol (ARP) to discover other devices' MAC addresses. | Layer 3 devices utilize IP addresses for routing within Virtual LANs (VLANs). |
| Layer 2 switch comes with a little tendency of switching packets from one port to another. | Layer 3 switching helps devices to communicate outside the networks as well. |
| Layer 2 switch does simple switching by finding and maintain a table of MAC addresses. | Layer 3 switch is a specialized device that is designed for routing of data packets through IP addresses. |

**Layer 2 vs. Layer 3 Switch**

| Item | Layer 2 Switch | Layer 3 Switch |
|---|---|---|
| Routing Function | Mac address only | Supports higher routing such as static routing and dynamic routing, |
| VLAN Tagging Based on IP Address | No | Yes |
| Inter-VLAN | No | Yes |
| Application | Pure Layer 2 domain | Aggregate multiple access switches |

**Advantage of Layer2 Switching**

Here are the pros/benefits of Layer2 Switching switches:

- Helps to forward packets based on unique MAC addresses
- Does not offer any setup or management
- It can be quickly deployed at a lower cost
- L2 switches flow accounting capabilities
- Low latency and improved security

**Advantage of Layer3 Switching**

Here are the pros/benefits of Layer3 Switching:

- L3 support routing between virtual LANs.
- Improve fault isolation.
- Provide ease of security management.
- Reduce broadcast traffic volumes.
- Ease the configuration process for VLANs, as a separate router is not needed between each VLAN.
- Separate routing tables, and as a result, segregate traffic better.
- Offers flow accounting and high-speed scalability.
- Lower network latency as a packet that does not make extra hops to go through a router.

**Limitation of Layer2 Switching**

Here are the cons/drawback of Layer2 switching:

- The layer 2 switches must break up the collision domains correctly.
- It does not break up broadcast domains by default.
- L2 switches does not allow you to implement any intelligence while forwarding packets.
- Does not helps you to perform switching or IP address-based routing.
- Never given guarantee required bandwidth to VoIP users

**Limitation of Layer3 Switching**

Here are the cons/drawbacks of Layer2 switching:

- The cost of the L3 switch is quite high compared to the Layer 2 switch.
- Layer 3 switch does not offer WAN functionality.
- Multiple tenants and virtualization.
- Does not offer any functionality.

**Summary:**

- Layer2 is the process of using devices and MAC addresses on a LAN to segment a network.
- A Layer 3 switch is a switch that performs routing functions in addition to switching.
- Layer 2 switches perform the switching function to re-arrange the data frames from the source to its destination network.
- Layer 3 switches define paths based on logical addressing.
- Layer 2 switches are used to reduce traffic on the local network, whereas Layer 3 switches mostly used to Implement VLAN.
- The advantage of Layer 2 switches is that it helps to forward packets based on unique MAC addresses
- The advantage of Layer 3 switches offers flow accounting and high-speed scalability.
- The main drawback of Layer 2 switches is that it does not allow you to implement any intelligence while forwarding packets.
- The main drawback of the Layer 3 switch does not offer WAN functionality.

## High Speed LANs

- Fast Ethernet and Gigabit Ethernet: The extension of 10-Mbps CSMA/CD (carrier sense multiple access with collision detection) to higher speeds is a logical strategy, because it tends to preserve the investment in

existing systems.

- Fibre Channel: This standard provides a low-cost, easily scalable approach to achieving very high data rates in local areas.

- High-speed wireless LANs: Wireless LAN technology and standards have at last come of age, and high- speed standards and products are being introduced.

**Need of High Speed LANs**

In recent years, two significant trends have altered the role of the personal computer, increased the volume of data to be handled over LANs, and therefore the requirements on the LAN:

- The speed and computing power of personal computers has continued to enjoy explosive growth

- MIS organizations have recognized the LAN as a viable and indeed essential computing platform, resulting in the focus on network computing.

The following are examples of requirements that call for higher-speed LANs:

- Centralized server farms: In many applications, there is a need for user, or client, systems to be able to draw huge amounts of data from multiple centralized servers, called server farms.. As the performance of the servers themselves has increased, the bottleneck has shifted to the network.

- Power workgroups: These groups typically consist of a small number of cooperating users who need to draw massive data files across the network. In such cases, large amounts of data are distributed to several workstations, processed, and updated at very high speed for multiple iterations.

- High-speed local backbone: As processing demand grows, LANs proliferate at a site, and high-speed interconnection is necessary.

Ethernet (CSMA/CD)

- The most widely used high-speed LANs today are based on Ethernet and were developed by the IEEE
- 802.3 standards committee.
- As with other LAN standards, there is both a medium access control layer and a physical layer. The media access uses CSMA/CD.
- This and its precursors can be termed random access, or contention, techniques. They are random access in the sense that there is no predictable or scheduled time for any station to transmit; station transmissions are ordered randomly.
- They exhibit contention in the sense that stations contend for time on the shared medium.

**CSMA**

- The foregoing observations led to the development of carrier sense multiple access (CSMA). With CSMA, a station wishing to transmit first listens to the medium to determine if another transmission is in progress (carrier sense)
- . If the medium is in use, the station must wait.
- If the medium is idle, the station may transmit. It may happen that two or more stations attempt to transmit at about the same time.
- If this happens, there will be a collision; the data from both transmissions will be garbled and not received successfully.
- To account for this, a station waits a reasonable amount of time after transmitting for an acknowledgment, taking into account the maximum round-trip propagation delay and the fact that the acknowledging station must also contend for the channel to respond.
- If there is no acknowledgment, the station assumes that a collision has occurred and retransmits. This strategy is effective for networks in which the average frame transmission time is much longer than the propagation time.
- Collisions can occur only when more than one user begins transmitting within a short time interval (the period of the propagation delay).
- If a station begins to transmit a frame, and there are no collisions during the time it takes for the leading edge of the packet to propagate to the farthest station, then there will be no collision for this frame because all other stations are now aware of the transmission.
- The maximum utilization achievable using CSMA can far exceed that of ALOHA or slotted ALOHA. The maximum utilization depends on the length of the frame and on the propagation time; the longer the frames or the shorter the propagation time, the higher the utilization.

**Nonpersistent CSMA**

With CSMA, an algorithm is needed to specify what a station should do if the medium is found busy. One algorithm is nonpersistent CSMA. A station wishing to transmit listens to the medium and obeys the following rules:

1. If the medium is idle, transmit; otherwise, go to step 2.
2. If the medium is busy, wait an amount of time drawn from a probability distribution (the retransmission delay) and repeat step 1.

The use of random delays reduces the probability of collisions. To see this, consider that two stations become ready to transmit at about the same time while another transmission is in progress; if both stations delay the same amount of time before trying again, they will both attempt to transmit at about the same time. A problem with nonpersistent CSMA is that capacity is wasted because the medium will generally remain idle following the end of a transmission even if there are one or more stations waiting to transmit.

**1-persistent CSMA**

To avoid idle channel time, the 1-persistent protocol can be used. A station wishing to transmit listens to the medium and obeys the following rules:

1. If the medium is idle, transmit; otherwise, go to step 2.

2. If the medium is busy, continue to listen until the channel is sensed idle; then transmit immediately.

Whereas nonpersistent stations are deferential, 1-persistent stations are selfish. If two or more stations are waiting to transmit, a collision is guaranteed. Things get sorted out only after the collision.

**P-persistent CSMA**

A compromise that attempts to reduce collisions, like nonpersistent, and reduce idle time, like 1- persistent, is p-persistent. The rules are:

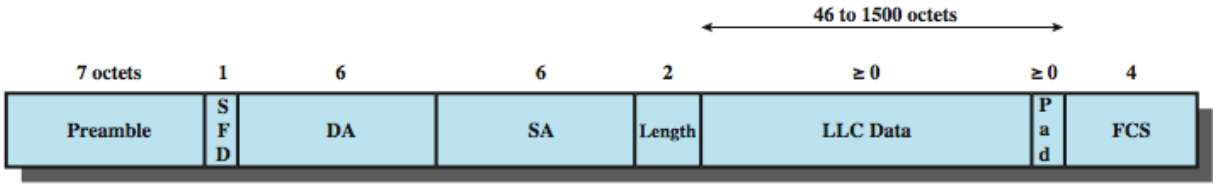
**1.** If the medium is idle, transmit with probability p, and delay one time unit with probability (1 – p). The time unit is typically equal to the maximum propagation delay.

**2.** If the medium is busy, continue to listen until the channel is idle and repeat step 1.

**3.** If transmission is delayed one time unit, repeat step 1.

The question arises as to what is an effective value of p. The main problem to avoid is one of instability under heavy load.

## IEEE 802.3 Frame Format




SFD = Start of frame delimiter
DA = Destination address
SA = Source address
FCS = Frame check sequence

It consists of the following fields:

- Preamble: A 7-octet pattern of alternating 0s and 1s used by the receiver to establish bit synchronization.

- Start Frame Delimiter (SFD): The sequence 10101011, which indicates the actual start of the frame and enables the receiver to locate the first bit of the rest of the frame.

- Destination Address (DA): Specifies the station(s) for which the frame is intended. It may be a unique physical address, a group address, or a global address.

- Source Address (SA): Specifies the station that sent the frame.

- Length/Type: Length of LLC data field in octets, or Ethernet Type field, depending on whether the frame conforms to the IEEE 802.3 standard or the earlier Ethernet specification. In either case, the maximum frame size, excluding the Preamble and SFD, is 1518 octets.

- LLC Data: Data unit supplied by LLC.

- Pad: Octets added to ensure that the frame is long enough for proper CD operation.

- Frame Check Sequence (FCS): A 32-bit cyclic redundancy check, based on all fields except preamble, SFD, and FCS.

**10Mbps Specification (Ethernet)**

Non Return to Zero Inverted (NRZI) is a data recording and transmission method that ensures clock synchronization

The IEEE 802.3 committee has defined a number of alternative physical configurations. This is both good and bad. On the good side, the standard has been responsive to evolving technology. On the bad side, the customer, not to mention the potential vendor, is faced with a bewildering array of options.
However, the committee has been at pains to ensure that the various options can be easily integrated into a configuration that satisfies a variety of needs. Thus, the user that has a complex set of requirements may find the flexibility and variety of the 802.3 standard to be an asset. To distinguish the various implementations that are available, the committee has developed a concise notation: <data rate in Mbps> <signaling method><max segment length in hundreds of meters>

The defined alternatives for 10-Mbps are:

- 10BASE5: Specifies the use of 50-ohm coaxial cable and Manchester digital signaling. The maximum length of a cable segment is set at 500 meters. Can extend using up to 4 repeaters.

- 10BASE2: lower-cost alternative to 10BASE5 using a thinner cable, with fewer taps over a shorter distance than the 10BASE5 cable.

- 10BASE-T: Uses unshielded twisted pair in a star-shaped topology, with length of a link is limited to 100 meters. As an alternative, an optical fiber link may be used out to 500 m.

- 10BASE-F: Contains three specifications using optical fibre

| | 10BASE5 | 10BASE2 | 10BASE-T | 10BASE-FP |
|---|---|---|---|---|
| Transmission medium | Coaxial cable (50 ohm) | Coaxial cable (50 ohm) | Unshielded twisted pair | 850-nm optical fiber pair |
| Signaling technique | Baseband (Manchester) | Baseband (Manchester) | Baseband (Manchester) | Manchester/on-off |
| Topology | Bus | Bus | Star | Star |
| Maximum segment length (m) | 500 | 185 | 100 | 500 |
| Nodes per segment | 100 | 30 | — | 33 |

| | | | | |
|---|---|---|---|---|
| Cable diameter (mm) | 10 | 5 | 0.4 to 0.6 | 62.5/125 µm |

100Mbps Fast Ethernet

Fast Ethernet refers to a set of specifications developed by the IEEE 802.3 committee to provide a low- cost, Ethernet-compatible LAN operating at 100 Mbps. The blanket designation for these standards is 100BASE-T. The committee defined a number of alternatives to be used with different transmission media. Stallings DCC8e Table 16.3 summarizes key characteristics of the 100BASE-T options. All of the 100BASE-T options use the IEEE 802.3 MAC protocol and frame format. 100BASE-X refers to a set of options that use two physical links between nodes; one for transmission and one for reception.
100BASE-TX makes use of shielded twisted pair (STP) or high-quality (Category 5) unshielded twisted pair (UTP). 100BASE-FX uses optical fiber. For all of the 100BASE-T options, the topology is similar to that of 10BASE-T, namely a star-wire topology.

In many buildings, any of the 100BASE-X options requires the installation of new cable. For such cases, 100BASE-T4 defines a lower-cost alternative that can use Category 3, voice-grade UTP in addition to the higher-quality Category 5 UTP. To achieve the 100-Mbps data rate over lower-quality cable, 100BASE-T4 dictates the use of four twisted-pair lines between nodes, with the data transmission making use of three pairs in one direction at a time.

| | **100BASE-TX** | | **100BASE-FX** | **100BASE-T4** |
|---|---|---|---|---|
| **Transmission medium** | 2 pair, STP | 2 pair, Category 5 UTP | 2 optical fibers | 4 pair, Category 3, 4, or 5 UTP |
| **Signaling technique** | MLT-3 | MLT-3 | 4B5B, NRZI | 8B6T, NRZ |
| **Data rate** | 100 Mbps | 100 Mbps | 100 Mbps | 100 Mbps |
| **Maximum segment length** | 100 m | 100 m | 100 m | 100 m |
| **Network span** | 200 m | 200 m | 400 m | 200 m |

100BASE-X

Fiber Distributed Data Interface (FDDI) is a standard for data transmission in a local area network

For all of the transmission media specified under 100BASE-X, a unidirectional data rate of 100 Mbps is achieved transmitting over a single link (single twisted pair, single optical fiber). For all of these media, an efficient and effective signal encoding scheme is required. The one chosen is referred to as 4B/5B- NRZI. This scheme is further modified for each option. The 100BASE-X designation includes two physical medium specifications, one for twisted pair, known as 100BASE-TX, and one for optical fiber, known as 100-BASE-FX.

100BASE-TX makes use of two pairs of twisted-pair cable, one pair used for transmission and one for reception. Both STP and Category 5 UTP are allowed. The MTL-3 signaling scheme is used.

100BASE-FX makes use of two optical fiber cables, one for transmission and one for reception. With 100BASE-FX, a means is needed to convert the 4B/5B-NRZI code group stream into optical signals. The technique used is known as intensity modulation. A binary 1 is represented by a burst or pulse of light; a binary 0 is represented by either the absence of a light pulse or a light pulse at very low intensity.

100BASE-T4

100BASE-T4 is designed to produce a 100-Mbps data rate over lower-quality Category 3 cable, thus taking advantage of the large installed base of Category 3 cable in office buildings. The specification also indicates that the use of Category 5 cable is optional. 100BASE-T4 does not transmit a continuous signal between packets, which makes it useful in battery-powered applications. For 100BASE-T4 using voice- grade Category 3 cable, it is not reasonable to expect to achieve 100 Mbps on a single twisted pair.
Instead, 100BASE-T4 specifies that the data stream to be transmitted is split up into three separate data streams, each with an effective data rate of Mbps. Four twisted pairs are used. Data are transmitted using three pairs and received using three pairs. Thus, two of the pairs must be configured for bidirectional transmission. As with 100BASE-X, a simple NRZ encoding scheme is not used for 100BASE- T4. This would require a signaling rate of 33 Mbps on each twisted pair and does not provide synchronization. Instead, a ternary signaling scheme known as 8B6T is used

## Introduction to Wireless LAN

- Wireless LAN stands for **Wireless Local Area Network**. It is also called LAWN (**Local Area Wireless Network**). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection

- The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm.
- Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.
- In some instance wireless LAN technology is used to save costs and avoid laying cable, while in other cases, it is the only option for providing high-speed internet access to the public. Whatever the reason, wireless solutions are popping up everywhere.
- Examples of WLANs that are available today are NCR's waveLAN and Motorola's ALTAIR.

## Advantages of WLANs

- **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
- **Design:** Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.
- **Robustness:** Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.
- **Cost:** The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost. And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.
- **Ease of Use:** Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

## Disadvantages of WLANs

- **Quality of Services:** Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.

- **Proprietary Solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.
- **Restrictions:** Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.
- **Global operation:** Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.
- **Low Power:** Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.
- **License free operation:** LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.
- **Robust transmission technology:** If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.).Wireless LAN transceivers cannot be adjusted for perfect transmission is a standard office or production environment.

IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

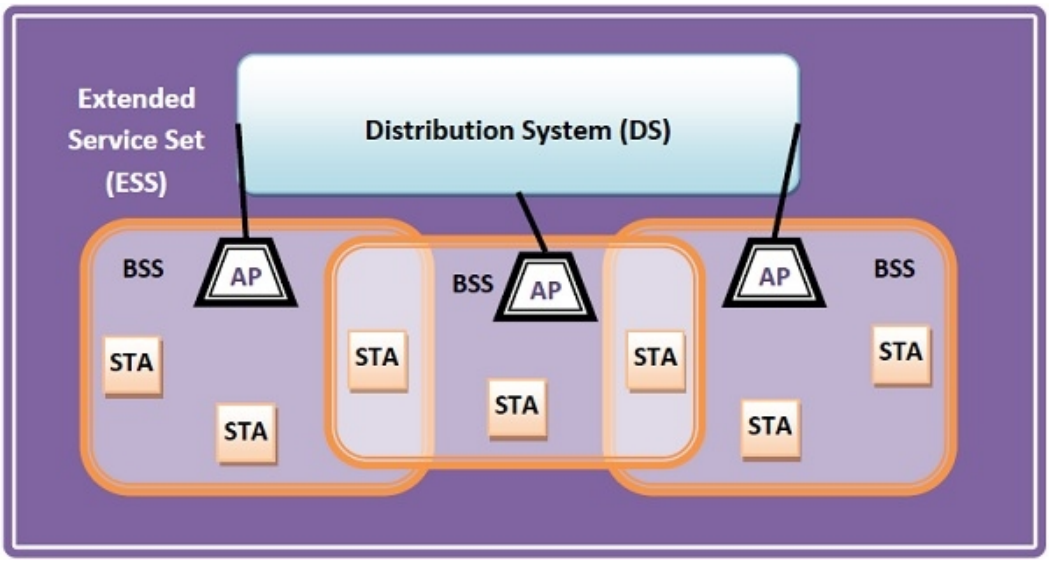
**IEEE 802.11 Architecture**

The components of an IEEE 802.11 architecture are as follows −

- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. A station can be of two types−
    - Wireless Access Point (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
    - Client. Clients are workstations, computers, laptops, printers, smartphones, etc.
- Each station has a wireless network interface controller.
- **Basic Service Set (BSS)** − A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories depending upon the mode of operation−

- Infrastructure BSS − Here, the devices communicate with other devices through access points.
- Independent BSS − Here, the devices communicate in a peer-to-peer basis in an ad hoc manner.

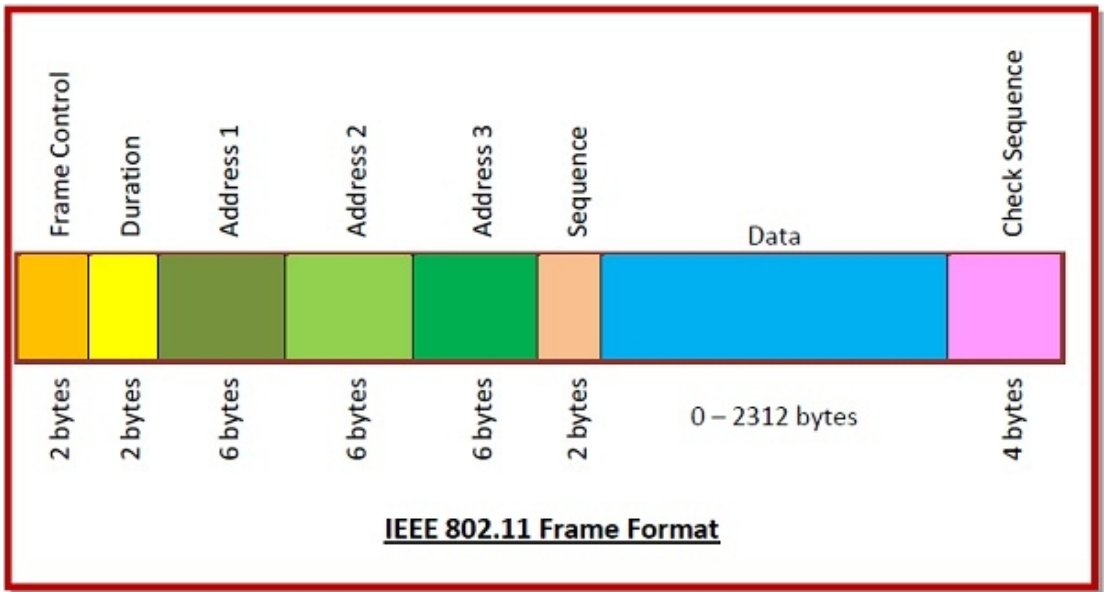
- **Extended Service Set (ESS)** − It is a set of all connected BSS.
- **Distribution System (DS)** − It connects access points in ESS.




**Frame Format of IEEE 802.11**

The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are −

- **Frame Control** − It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.
- **Duration** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.
- **Address fields** − There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.
- **Sequence** − It a 2 bytes field that stores the frame numbers.
- **Data** − This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.
- **Check Sequence** − It is a 4-byte field containing error detection information.




**Modems and types of Modems**

Modem stands for Modulator and Demodulator. It is a device that modulates signals to encode digital information for transmission and demodulates signals to decode the transmitted information.

A modem transmits data in bits per second (bps).

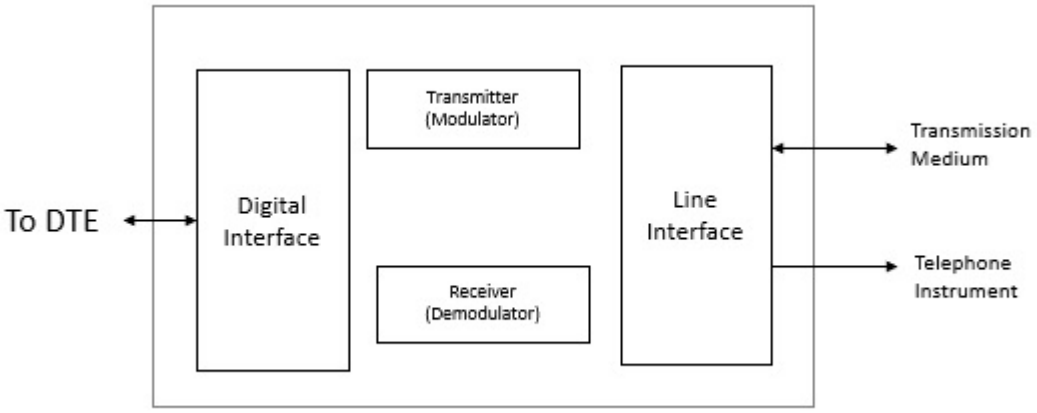
It is necessary for communication between digital devices and Analog devices.

Modem is necessary because it acts as a translator between the devices and rapidly transmits the information.

It converts the digital signal to Analog and vice versa to communicate between devices.

It encodes the signal and decodes at the other end and vice versa between the devices.

Building blocks of modem are shown in the diagram below −



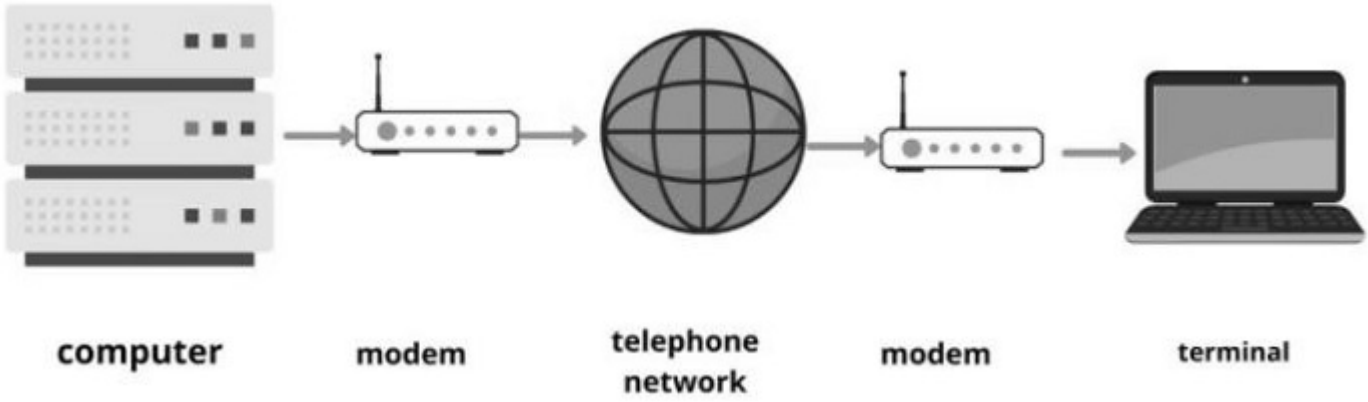
**Types of Modems**

The different types of modems used to access the internet at home are as follows −

## Telephone modem

A computer is connected through telephone lines to access the network of other computers. It is cheaper when compared to other modems because it does not have any installation cost and also the monthly fee of a telephone modem is low. It can be used in any house if a telephone network is provided.

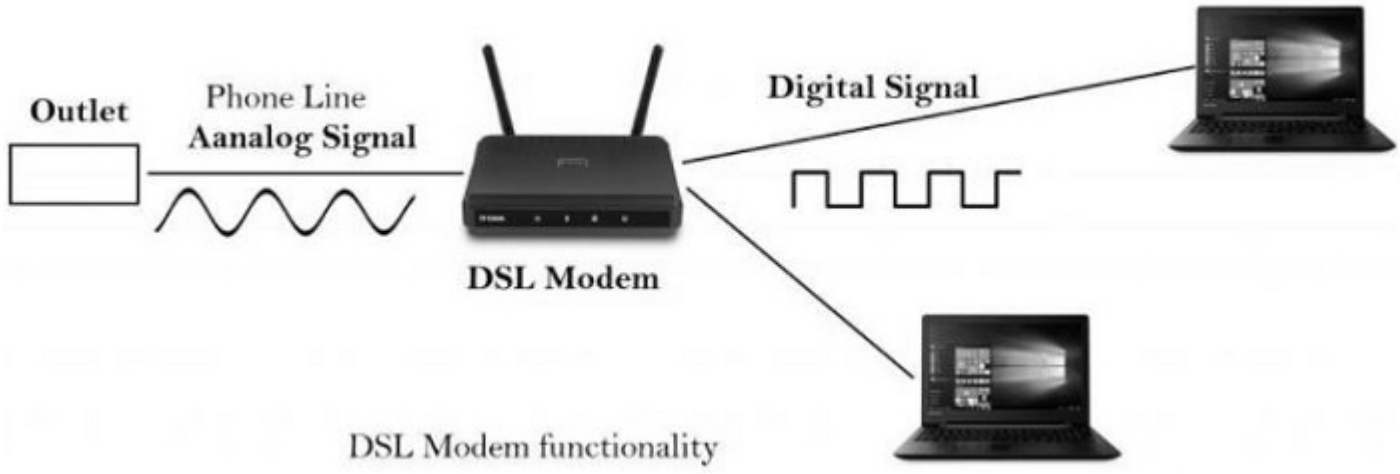
Given below is the diagram of telephone modem −




## Digital subscriber Line

It provides high speed internet connection through telephone lines. It is expensive when compared to a telephone modem. The DSL is also connected with phone lines similar to telephone modem, but the difference is in DSL voice communication and internet service is used simultaneously whereas in telephone modem it is not provided.

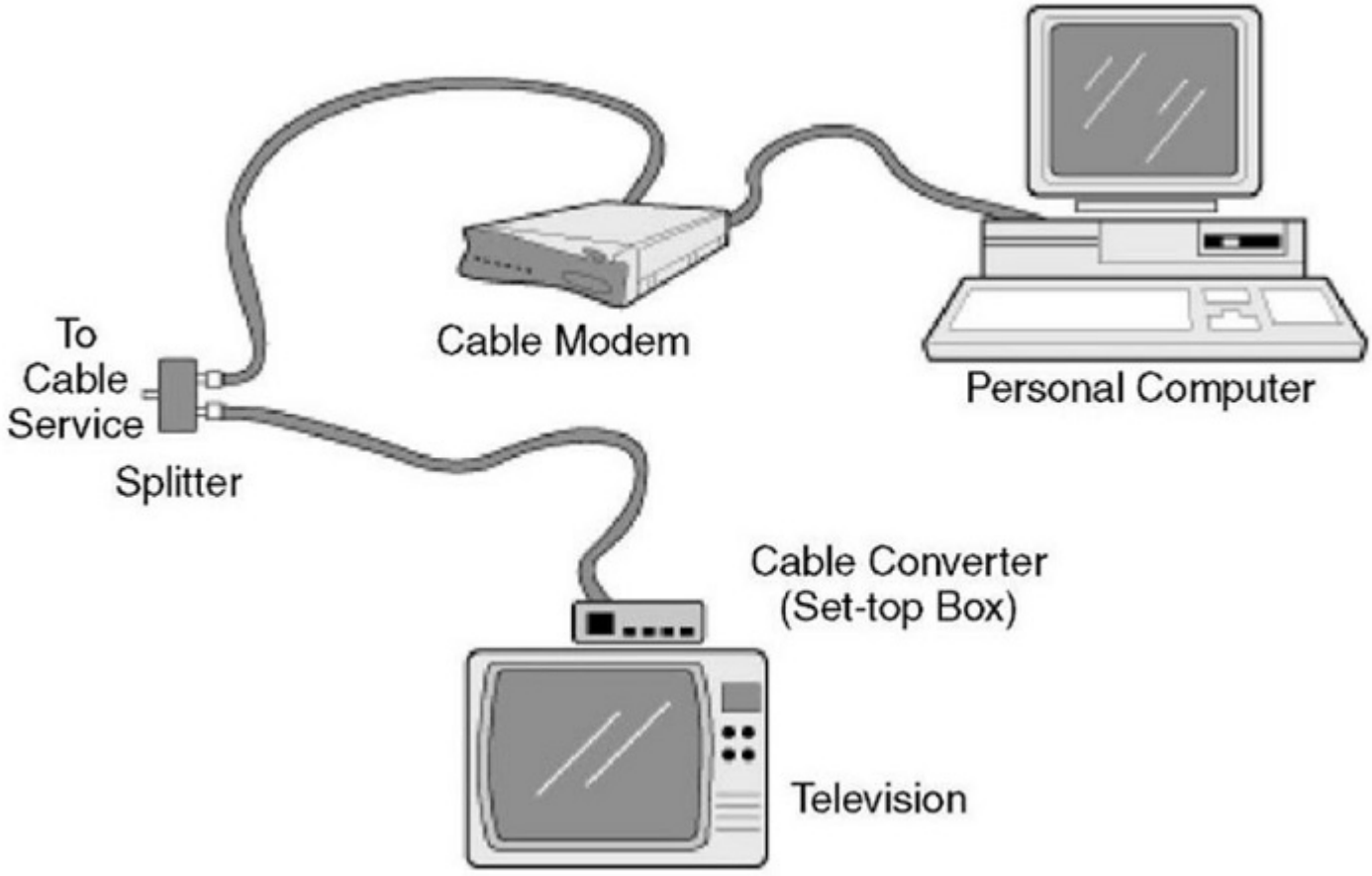
Given below is the diagram of digital subscriber line (DSL) −




## Cable modem

Cable Modem is a device that allows high-speed data access via a cable TV (CATV) network. Most cable modems are currently external devices that connect to the PC through a standard 10 BASE-T Ethernet card and twisted-pair wiring.

Given below is the diagram of cable modem −




## Satellite modem

It is a device that provides internet connection through satellite dishes. It transfers the input bits to output radio signals and then executes vice versa. It is costlier when compared to all other modems but provides better reliability to the internet network.