Contents

1) Introduction to Networking

1.1 What is a Network?

A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

In the world of Information Technology (IT) information is the building block for effective communication. Communication is a medium that helps us to drive our day to day professional and personal operations. Where computer networking acts as the base of everything as the best and most important IT solutions. Below is a list of points that we do with the help of computer networks, or things that we benefit from with the help of computer networks or that have become possible or effective due to computer networks. Provides the best way of business communication.

- Streamline communication.
- Cost-effective resource sharing.
- Improving storage efficiency and volume.
- Cut costs on software.
- Cut costs on hardware.
- Utilizes Centralized Database.
- Increase in efficiency.
- Optimize convenience and flexibility.
- Allows File sharing.
- sharing of peripherals and internet access.
- Network gaming.
- Voice over IP (VoIP).
- Media Center Server.
- Centralized network administration, meaningless IT support.
- Flexibility.
- Allowing information sharing.
- Supporting distributed processing.
- User communication.
- Overcoming geographic separation.

1.2 Network Topologies

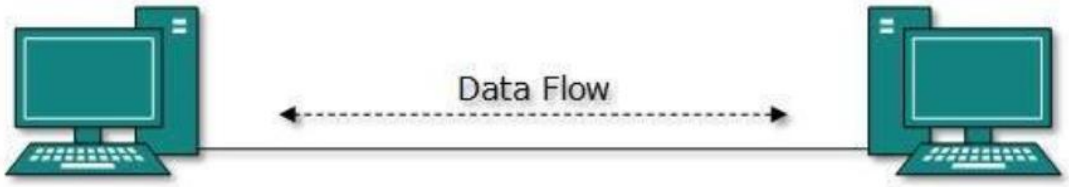
Network topology refers to how various nodes, devices, and connections on your network are physically or logically arranged in relation to each other. Think of your network as a city, and the topology as the road map. Just as there are many ways to arrange and maintain a city—such as making sure the avenues and boulevards can facilitate passage between the parts of town getting the most traffic—there are several ways to arrange a network. Each has advantages and disadvantages and depending on the needs of your company, certain arrangements can give you a greater degree of connectivity and security.

There are two approaches to network topology: physical and logical. Physical network topology, as the name suggests, refers to the physical connections and interconnections between nodes and the network—the wires, cables, and so forth. Logical network topology is a little more abstract and strategic, referring to the conceptual understanding of how and why the network is arranged the way it is, and how data moves through it.

Here are the well-known network topologies.

Point-to-Point

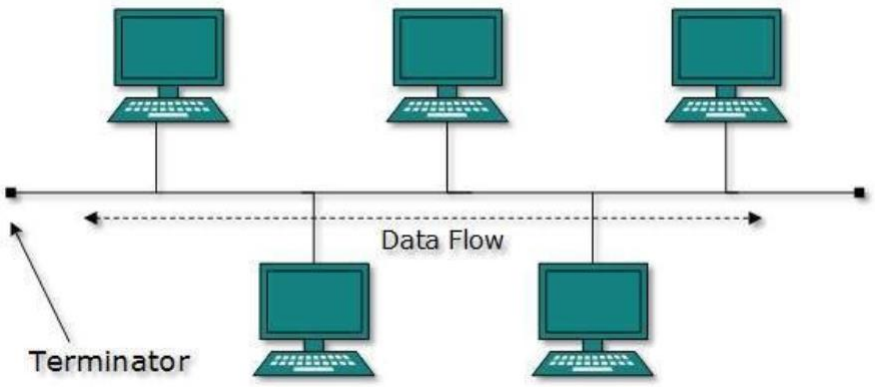
Point-to-point networks contain exactly two hosts such as computers, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to the sending end of the other and vice-versa.



If the hosts are connected point-to-point logically, then they may have multiple intermediate devices. But the end hosts are unaware of the underlying network and see each other as if they are connected directly.

Bus Topology

In case of Bus topology, all devices share a single communication line or cable. Bus topology may have problems while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.



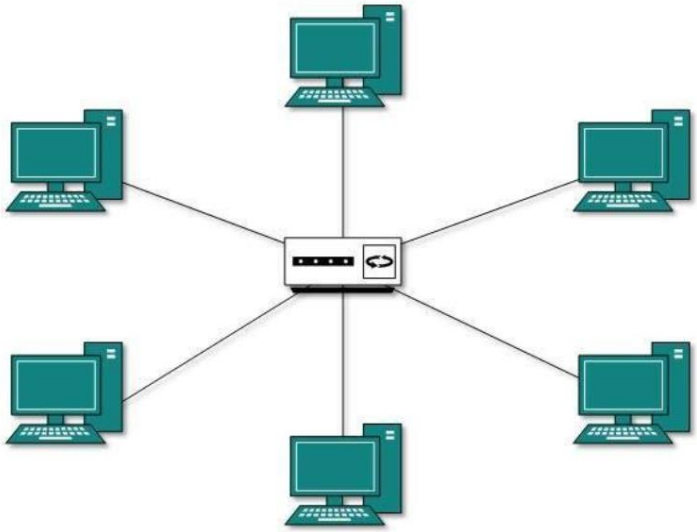
Both ends of the shared channel have a line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

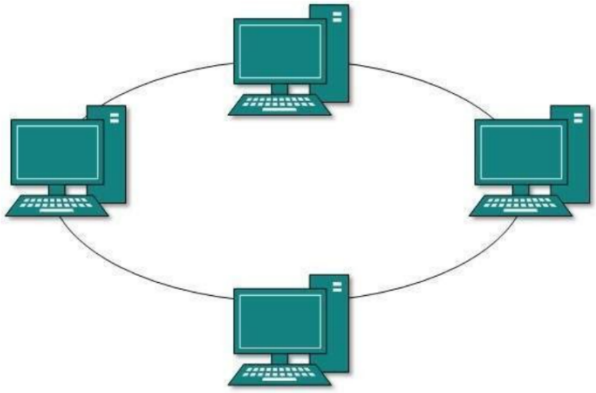
- Layer-1 device such as hub or repeater
- Layer-2 device such as switch or bridge
- Layer-3 device such as router or gateway

As in Bus topology, the hub acts as a single point of failure. If the hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts takes place through only the hub. Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.



Ring Topology

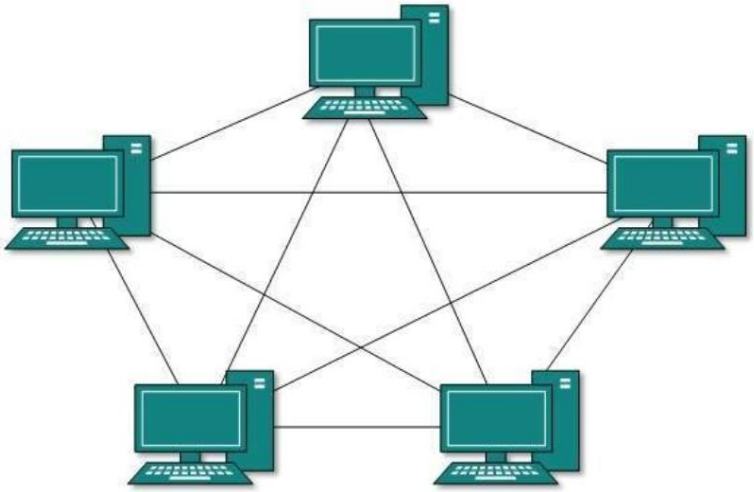
In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.



Failure of any host results in failure of the whole ring. Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

Mesh Topology

In this type of topology, a host is connected to one or multiple hosts. This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.

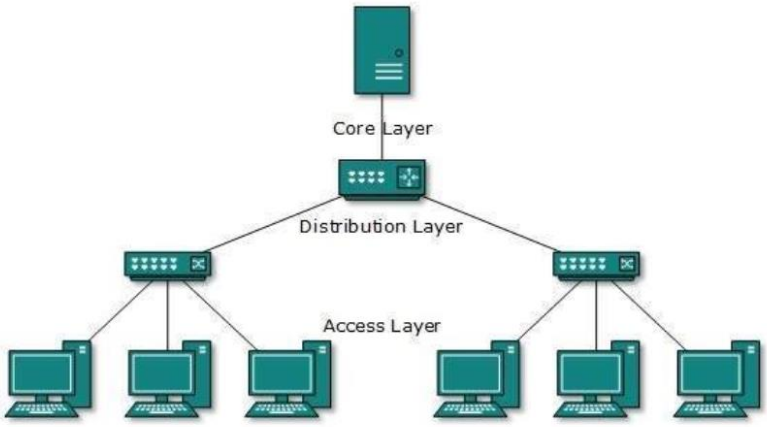


Hosts in Mesh topology also work as relays for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

- Full Mesh: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.
- Partially Mesh: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrary fashion. This topology exists where we need to provide reliability to some hosts out of all.

Tree Topology

Also known as Hierarchical Topology, this is the most common form of network topology in use presently. This topology imitates as extended Star topology and inherits properties of bus topology.



This topology divides the network in to multiple levels/layers of the network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is an access-layer where computers are attached. The middle layer is known as the distribution layer, which works as a mediator between upper layer and lower layer. The highest layer is known as the core layer, and is the central point of the network, i.e. root of the tree from which all nodes fork.

All neighboring hosts have point-to-point connection between them. Similar to the Bus topology, if the root goes down, then the entire network suffers even. Though it is not the single point of failure. Every connection serves as a point of failure, failing which divides the network into unreachable segments.

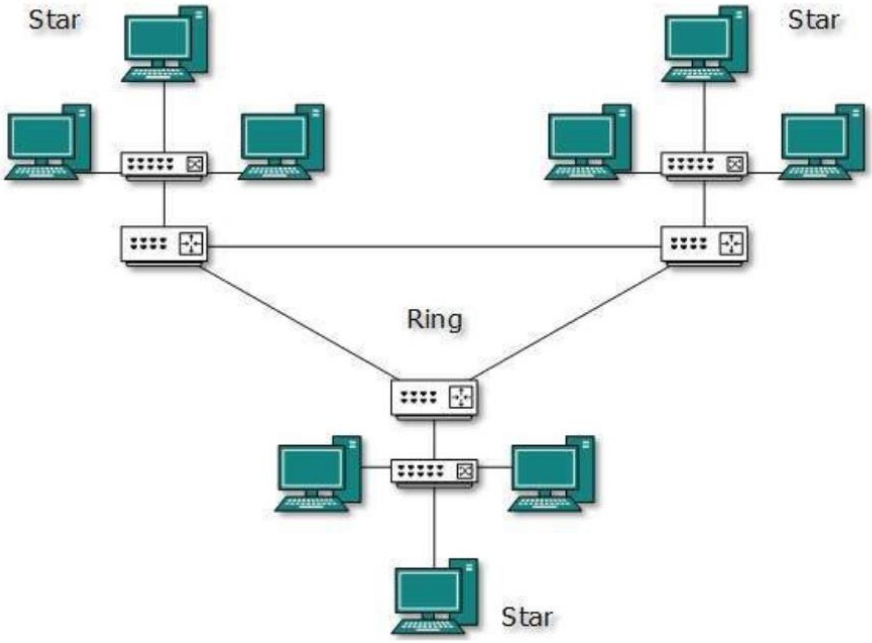
Daisy Chain

This topology connects all the hosts in a linear fashion. Similar to Ring topology, all hosts are connected to two hosts only, except the end hosts. Means, if the end hosts in daisy chain are connected then it represents Ring topology.

Each link in daisy chain topology represents single point of failure. Every link failure splits the network into two segments. Every intermediate host works as relay for its immediate hosts.

Hybrid Topology

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.



The above picture represents an arbitrarily hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology.

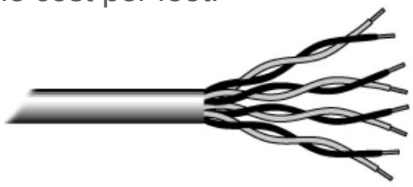
1.3 What is Network Cabling?

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

The following sections discuss the types of cables used in networks and other related topics.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Cable Installation Guides

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks. The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot.



Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector. A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

Shielded Twisted Pair (STP) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

Shielded twisted pair cable is available in three different configurations:

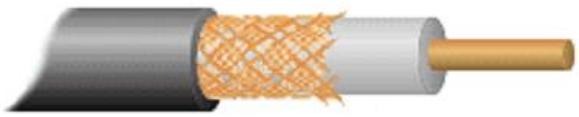
1) Each pair of wires is individually shielded with foil.
2) There is a foil or braid shield inside the jacket covering all wires (as a group).
3) There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield. The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

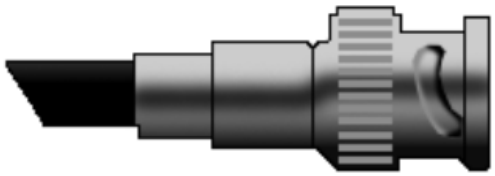


Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayonet-Neill-Concelman (BNC) connector. Different types of adapters are available for BNC connectors, including a T-connector,

barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.



Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials. It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pairs. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers. A plastic coating then cushions the fiber center, and Kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket is made of Teflon or PVC.

There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

1.4 Types of Computer Networks

Personal Area Network

PAN is a computer network formed around a person. It generally consists of a computer, mobile, or personal digital assistant. PAN can be used for establishing communication among these personal devices for connecting to a digital network and the internet.

Characteristics of PAN

- It is mostly personal devices network equipped within a limited area.
- Allows you to handle the interconnection of IT devices at the surrounding of a single user.
- PAN includes mobile devices, tablet, and laptop.
- It can be wirelessly connected to the internet called WPAN.
- Appliances use for PAN: cordless mice, keyboards, and Bluetooth systems.

Advantages of PAN

Here, are important pros/benefits of using PAN network:

- PAN networks are relatively secure and safe
- It offers only short-range solution up to ten meters
- Strictly restricted to a small area

Disadvantages of PAN

Here are important cons/ drawback of using PAN network:

- It may establish a bad connection to other networks at the same radio bands.
- Distance limits.

Local Area Network

A Local Area Network (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other applications. The simplest type of LAN network is to connect computers and a printer in someone's home or office. In general, LAN will be used as one type of transmission medium.

It is a network which consists of less than 5000 interconnected devices across several buildings.

Characteristics of LAN

Here are important characteristics of a LAN network:

- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.
- There are various kinds of media access control methods like token ring and Ethernet.

Advantages of LAN

Here are pros/benefits of using LAN:

- Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.

- You can use the same software over the network instead of purchasing the licensed software for each client in the network.
- Data of all network users can be stored on a single hard disk of the server computer.
- You can easily transfer data and messages over networked computers.
- It will be easy to manage data at only one place, which makes data more secure.
- Local Area Network offers the facility to share a single internet connection among all the LAN users.

Disadvantages of LAN

Here are the important cons/ drawbacks of LAN:

- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
- Unauthorized users can access critical data of an organization in case LAN admin is not able to secure a centralized data repository.
- Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

Wide Area Network

WAN (Wide Area Network) is another important computer network that which is spread across a large geographical area. WAN network system could be a connection of a LAN which connects with other LAN's using telephone lines and radio waves. It is mostly limited to an enterprise or an organization.

Characteristics of WAN:

- The software files will be shared among all the users; therefore, all can access the latest files.
- Any organization can form its global integrated network using WAN.

Advantages of WAN

Here are the benefits/ pros of using WAN:

- WAN helps you to cover a larger geographical area. Therefore, business offices situated at longer distances can easily communicate.
- Contains devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.
- WLAN connections work using radio transmitters and receivers built into client devices.

Disadvantage of WAN

Here are drawbacks/cons of using WAN:

- The initial setup cost of investment is very high.

- It is difficult to maintain the WAN network. You need skilled technicians and network administrators.
- There are more errors and issues because of the wide coverage and the use of different technologies.
- It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.
- Offers lower security compared to other types of networks.

WLAN (Wireless Local Area Network)

WLAN (Wireless Local Area Network) helps you to link single or multiple devices using wireless communication within a limited area like home, school, or office building. It gives users an ability to move around within a local coverage area which may be connected to the network. Today most modern day's WLAN systems are based on IEEE 802.11 standards.

In 1997, the Institute of Electrical and Electronics Engineers created the first WLAN standard. They called it 802.11 after the name of the group formed to oversee its development. Unfortunately, 802.11 only supported a maximum network bandwidth of 2 Mbps—too slow for most applications. For this reason, ordinary 802.11 wireless products are no longer manufactured. However, an entire family has sprung up from this initial standard.

The best way to look at these standards is to consider 802.11 as the foundation, and all other iterations as building blocks upon that foundation that focus on improving both small and large aspects of the technology. Some building blocks are minor touch-ups while others are quite large.

The largest changes to wireless standards come when the standards are "rolled up" to include most or all small updates. So, for example, the most recent rollup occurred in December 2016 with 802.11-2016. Since then, however, minor updates are still occurring and, eventually, another large roll-up will encompass them.

Below is a brief look at the most recently approved iterations, outlined from newest to oldest. Other iterations, like 802.11be (Wi-Fi 7), are still in the approval process.

802.11ax: Branded as Wi-Fi 6, the 802.11ax standard went live in 2019 and will replace 802.11ac as the de facto wireless standard. Wi-Fi 6 maxes out at 10 Gbps, uses less power, is more reliable in congested environments, and supports better security.

802.11aj: Known as the China Millimeter Wave, this standard applies in China and is basically a rebranding of 802.11ad for use in certain areas of the world. The goal is to maintain backward compatibility with 802.11ad.

802.11ah: Approved in May 2017, this standard targets lower energy consumption and creates extended-range Wi-Fi networks that can go beyond the reach of a typical 2.4 GHz or 5 GHz networks. It is expected to compete with Bluetooth given its lower power needs.

802.11ad: Approved in December 2012, this standard is freakishly fast. However, the client device must be located within 30 feet of the access point.

Keep in mind when distances are mentioned that ranges can be greatly impacted by obstacles that block the signal, so the range mentioned refers to situations where there is absolutely no interference.

802.11ac: The generation of Wi-Fi that first signaled popular use, 802.11ac uses dual-band wireless technology, supporting simultaneous connections on both 2.4 GHz and 5 GHz Wi-Fi devices. 802.11ac offers backward compatibility to 802.11a/b/g/n and bandwidth rated up to 1300 Mbps on the 5 GHz band plus up to 450 Mbps on 2.4 GHz. Most home wireless routers are compliant with this standard.

802.11ac is the most expensive to implement; performance improvements only noticeable in high-bandwidth applications

802.11n: 802.11n (also sometimes known as Wireless N) was designed to improve on 802.11g in the amount of bandwidth it supports, by using several wireless signals and antennas (called MIMO technology) instead of one. Industry standards groups ratified 802.11n in 2009 with specifications providing for up to 600 Mbps of network bandwidth. 802.11n also offers a somewhat better range over earlier Wi-Fi standards due to its increased signal intensity, and it is backward-compatible with 802.11a/b/g gear.

- Pros of 802.11n: Significant bandwidth improvement from previous standards; wide support across devices and network gear
- Cons of 802.11n: More expensive to implement than 802.11g; use of multiple signals may interfere with nearby 802.11b/g based networks

802.11g: In 2002 and 2003, WLAN products supporting a newer standard called 802.11g emerged on the market. 802.11g attempts to combine the best of both 802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 GHz frequency for greater range. 802.11g is backward compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

- Pros of 802.11g: Supported by essentially all wireless devices and network equipment in use today; least expensive option
- Cons of 802.11g: Entire network slows to match any 802.11b devices on the network; slowest/oldest standard still in use

802.11a: While 802.11b was in development, IEEE created a second extension to the original 802.11 standard called 802.11a. Because 802.11b gained in popularity much faster than did 802.11a, some folks believe that 802.11a was created after 802.11b. In fact, 802.11a was created at the same time. Due to its higher cost, 802.11a is usually found on business networks whereas 802.11b better serves the home market.

802.11a supports bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz. This higher frequency compared to 802.11b shortens the range of 802.11a networks. The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions.

Because 802.11a and 802.11b use different frequencies, the two technologies are incompatible with each other. Some vendors offer hybrid 802.11a/b network gear, but these products merely implement the two standards side by side (each connected device must use one or the other).

802.11b: IEEE expanded on the original 802.11 standard in July 1999, creating the 802.11b specification. 802.11b supports a theoretical speed up to 11 Mbps. A more realistic bandwidth of 2 Mbps (TCP) and 3 Mbps (UDP) should be expected.

802.11b uses the same unregulated radio signaling frequency (2.4 GHz) as the original 802.11 standard. Vendors often prefer using these frequencies to lower their production costs. Being unregulated, 802.11b gear can incur interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz range. However, by installing 802.11b gear a reasonable distance from other appliances, interference can easily be avoided.

Standard	Speed	Range	Range (meter)	Frequency
802.11b	11 Mbps	150 Feet	45.72 M	2.4 GHz
802.11g	54 Mbps	50 Feet	15.24 M	2.4 GHz
802.11a*	54 Mbps	50 Feet	15.24 M	5 GHz
802.11n	300 Mbps 450 Mbps	175 Feet	51.85 M	2.4/5 GHz