Protocol and Standard in Computer Networks

Last Updated : 13 Sep, 2024

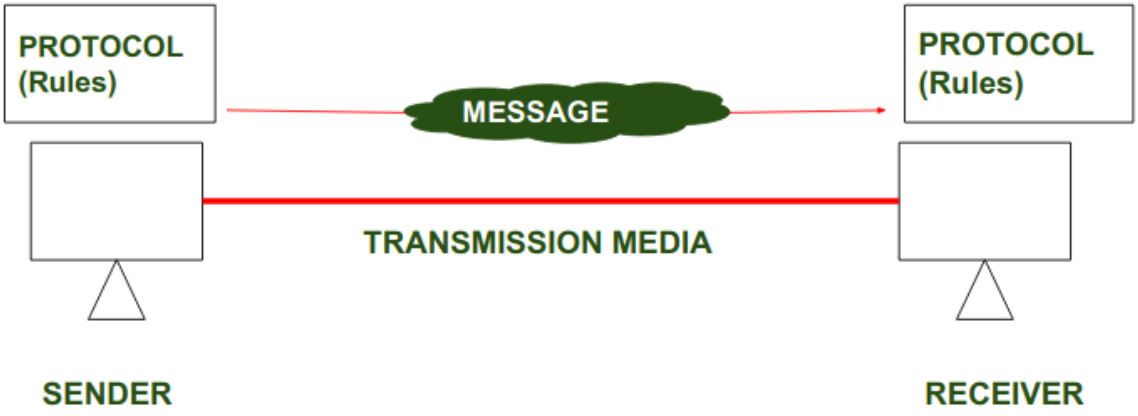
Protocols and standards are important in computer networks. They are like the rules and guidelines that allow different devices and systems to communicate and work together smoothly. Protocols define how data is sent, received, and processed, while standards ensure that various technologies are compatible with each other. This coordination is critical for the Internet and other networks to function constantly and efficiently.

Network protocol ensures that different technologies and components of the network are compatible with one another, reliable, and able to function together. In this article, we are going to discuss every point about protocols and standards in computer networks.

What is Protocol?

A protocol is a set of rules that determines how data is sent and received over a network. The protocol is just like a language that computers use to talk to each other, ensuring they understand and can respond to each other's messages correctly. Protocols help make sure that data moves smoothly and securely between devices on a network.

To make communication successful between devices, some rules and procedures should be agreed upon at the sending and receiving ends of the system. Such rules and procedures are called Protocols. Different types of protocols are used for different types of communication.



Protocols

In the above diagrams, Protocols are shown as a set of rules. Communication between the Sender and Receiver is not possible without Protocol.

Key Elements of Protocol

- **Syntax:** Syntax refers to the structure or the format of the data that gets exchanged between the devices. Syntax of the message includes the type of data, composition of the message, and sequencing of the message. The starting 8 bits of data are considered as the address of the sender. The next 8 bits are considered to be the address of the receiver. The remaining bits are considered as the message itself.
- **Semantics:** Semantics defines data transmitted between devices. It provides rules and norms for understanding message or data element values and actions.
- **Timing:** Timing refers to the synchronization and coordination between devices while transferring the data. Timing ensures at what time data should be sent and how fast data can be sent. For example, If a sender sends 100 Mbps but the receiver can only handle 1 Mbps, the receiver will overflow and lose data. Timing ensures preventing of data loss, collisions, and other timing-related issues.
- **Sequence Control:** Sequence control ensures the proper ordering of data packets. The main responsibility of sequence control is to acknowledge the data while it get received, and the retransmission

of lost data. Through this mechanism, the data is delivered in correct order.

- **Flow Control:** Flow control regulates device data delivery. It limits the sender's data or asks the receiver if it's ready for more. Flow control prevents data congestion and loss.
- **Error Control:** Error control mechanisms detect and fix data transmission faults. They include error detection codes, data resend, and error recovery. Error control detects and corrects noise, interference, and other problems to maintain data integrity.
- **Security :** Network security protects data confidentiality, integrity, and authenticity. which includes encryption, authentication, access control, and other security procedures. Network communication's privacy and trustworthiness are protected by security standards.

Types of Protocol

- **Network Layer Protocols :** Network layer protocols operate in the network layer which is also known as the Layer 3 of the network architecture. Network layer protocols are responsible for packet routing, forwarding, and addressing of data packets throughout the network. IP and ICMP are the network layer protocols.
- **Transport Layer Protocols**: Transport layer protocols work in the transport layer which provides end-to-end service ensuring data transfer across apps on different devices. TCP and UDP are the most popular transport layer protocols.
- **Application Layer Protocol:** Application layer protocol working in the application layer of the network architecture provides communication between applications running on different devices. The application layer protocols enable cross-device communication. They format, exchange, and interpret application data. HTTP, FTP, and SMTP are examples.
- **Wireless Protocols:** Wireless protocols basically used in wireless communication which enables data transfer through wireless networks. Bluetooth, Wi-Fi, and LTE protocols are examples.
- **Routing Protocols:** Routing protocol establishes the best/optimal network pathways through a network for fastest data

transmission. Routers share information to develop and maintain routing tables. RIP, OSPF, and BGP are examples.

- **Security Protocols :** security protocol protects data confidentiality, integrity, and authenticity while transmission of data over the network. They include SSL and TLS, encryption methods, and authentication protocols for providing data security.
- **Internet Protocols :** IP identifies devices uniquely. Internet protocol provides data communication through routing and forwarding data packets from one device to another by unique addressing scheme.

Important Protocols Used in Computer Network

Here are some key protocols that are widely used in computer networks:

- **TCP (Transmission Control Protocol):** Ensures data is sent and received accurately by breaking it into packets, sending them, and reassembling them at the destination.
- **IP (Internet Protocol):** Addresses and routes the packets to make sure they reach the right destination.
- **HTTP/HTTPS (HyperText Transfer Protocol/Secure):** HTTP used for transferring web pages on the internet. When you browse a website, your browser uses HTTP to request and display web pages. And HTTPs is a secure version of HTTP that encrypts data to protect it from being intercepted.
- **FTP (File Transfer Protocol):** Used for transferring files between computers on a network. It allows users to upload and download files.**SMTP (Simple Mail Transfer Protocol):** Used for sending emails. It transfers emails from a client to a server or between servers.
- **DNS (Domain Name System):** It is used to translates human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on the network.
- **DHCP (Dynamic Host Configuration Protocol):** Automatically assigns IP addresses to devices on a network, ensuring each device has a unique address.

- **SSH (Secure Shell):** Provides a secure way to access and manage devices over a network. It encrypts the data, making it safe from eavesdropping.
- **SNMP (Simple Network Management Protocol):** Used for managing and monitoring network devices like routers, switches, and servers. It collects and organizes information about these devices

How are Protocols Used in Cyber Attacks?

Attackers can misuse the rules of how data is sent over the internet to cause problems for systems. One common way they do this is through distributed denial-of-service (DDoS) attacks.

For example, in a SYN flood attack, attackers exploit the TCP protocol. Normally, a device sends a SYN packet to a server to start a connection, and the server responds, expecting a final response to complete the connection. Attackers send many SYN packets but never complete the connections. This overloads the server, preventing it from working properly for real users.

Cloudflare offers solutions to stop these kinds of attacks. One of their services, Cloudflare Magic Transit, protects against attacks targeting different levels of the network system. In the case of a SYN flood attack, Cloudflare manages the TCP connections for the server, so the server doesn't get overwhelmed and can continue to serve real users.

What is Standards?

Standards are the set of rules for data communication that are needed for the exchange of information among devices. It is important to follow Standards which are created by various Standard Organizations like IEEE, ISO, ANSI, etc.

Types of Standards

- **De Facto Standard:** The meaning of the word *" De Facto "* is " By Fact " or "By Convention". These are the standards that have not been approved by any Organization but have been adopted as Standards because of their widespread use. Also, sometimes these standards are often established by M

For example : Apple and Google are two companies that established their own rules for their products which are different. Also, they use some same standard rules for manufacturing their products.

- **De Jure Standard:** The meaning of the word *"De Jure"* is "By Law" or "By Regulations".Thus, these are the standards that have been approved by officially recognized bodies like ANSI, ISO, IEEE, etc. These are the standards that are important to follow if it is required or needed.
  For example : All the data communication standard protocols like SMTP, TCP, IP, UDP etc. are important to follow the same when we need them.

Protocol and Standard Compliance in Network Security

- **Interoperability:** Protocols and standards allow devices and systems to communicate. These protocols ensure network components can function together, avoiding risks and security gaps produced by incompatible or unsupported systems.
- **Security Baseline :** Protocols and standards contain security principles and best practices that help secure network infrastructure. These protocols allow organizations to protect sensitive data via encryption, authentication, and access controls.
- **Vulnerability Management :** Network security protocols and standards help organizations find and fix vulnerabilities. Many standards requires regular security assessments, vulnerability scanning, and penetration testing to discover network infrastructure flaws. Organizations can prevent cyberattacks and address vulnerabilities by following these compliance criteria.

Best Practices for Ensuring Protocol and Standard Compliance

- Use cryptography tools to secure personal data transported across your network, making sure that data encryption methods exceed industry requirements.

- Perform frequent security checks on all network devices to discover vulnerabilities and verify they fulfil compliance standards.
- Restrict user access to specified network zones to ensure secure data sharing and prevent unauthorized access.

Conclusion

Protocols and standards enable secure and efficient computer network communication. They regulate data exchange, formatting, endpoints, and reliable device communication. These protocols and standards ensure network security and performance. Compliance can prevent data breaches and system breakdowns.

Frequently Asked Question on Protocol and Standards – FAQs

What is the role of organizations like the IEEE and the IETF in protocol development?

> *Organizations such as the IEEE and the IETF play important roles in defining and maintaining networking protocols and standards. They provide platforms for experts to cooperate, analyze suggestions, and reach agreements on new protocols or changes to current ones.*

Why are protocols and standards important in networking?

> *Protocols and standards ensure that devices from multiple companies may communicate with one another effectively. They also contribute to consistent and reliable data transfer, resulting in efficient networking operations.*

What are some common networking protocols?

- *TCP/IP*
- *FTP*
- *SMTP*
- *HTTP*

How do protocols ensure data integrity and security?

Protocols usually include systems for error detection, correction, and encryption to assure data integrity and security during transmission. TCP, for example, uses sequence numbers and acknowledgment messages to ensure that data is delivered reliably.

Next Article

Examples of Data Link Layer Protocols

Similar Reads

Difference between Stop and Wait protocol and Sliding Window...

Both the Stop and Wait protocol and the Sliding Window protocol are the techniques to the solution of flow control handling. The main difference...

5 min read

Difference between Spanning Tree Protocol (STP) and Rapid...

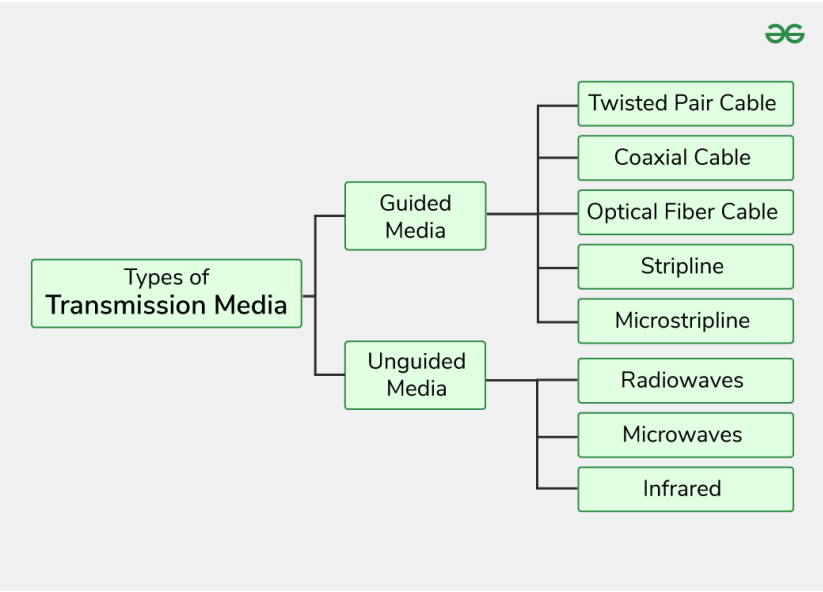
Types of Transmission Media

Last Updated : 21 Mar, 2025

Transmission media refers to the physical medium through which data is transmitted from one device to another within a network. These media can be wired or wireless. The choice of medium depends on factors like distance, speed, and interference. In this article, we will discuss the transmission media. In this article we will see types of transmission media in detail.

What is Transmission Media in Computer Networks?

A transmission media is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one device to another. Transmission Media is broadly classified into the following types:



Types of Transmission Media

1. Guided Media

Guided Media is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

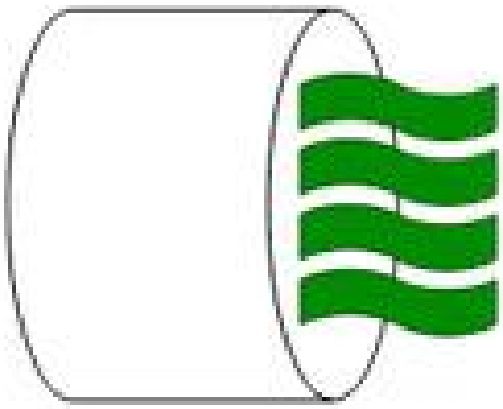
- High Speed
- Secure
- Used for comparatively shorter distances

There are 3 major types of Guided Media:

Twisted Pair Cable

It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP):**UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.



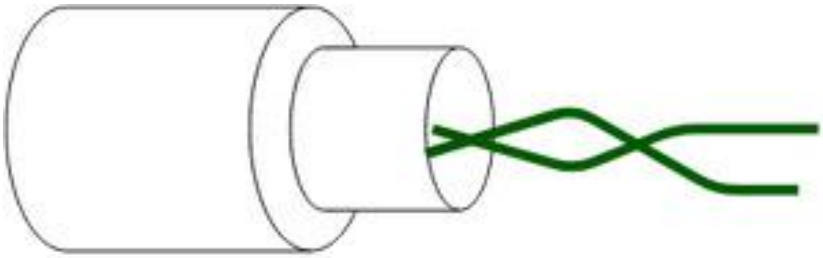
Unshielded Twisted Pair

Advantages of Unshielded Twisted Pair

- Least expensive
- Easy to install
- High-speed capacity

Disadvantages of Unshielded Twisted Pair

- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation



Shielded Twisted Pair

Shielded Twisted Pair (STP): Shielded Twisted Pair (STP) cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.

Advantages of Shielded Twisted Pair

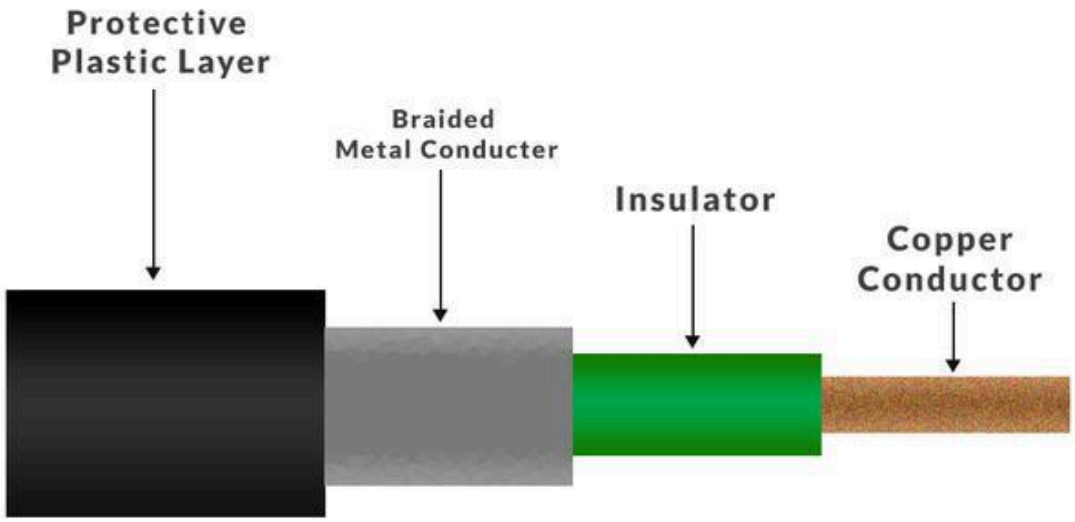
- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster

Disadvantages of Shielded Twisted Pair

- Comparatively difficult to install and manufacture
- More expensive
- Bulky

Coaxial Cable

Coaxial cable has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.



Advantages of Coaxial Cable

- Coaxial cables has high bandwidth .
- It is easy to install.
- Coaxial cables are more reliable and durable.
- Less affected by noise or cross-talk or electromagnetic inference.
- Coaxial cables support multiple channels

Disadvantages of Coaxial Cable

- Coaxial cables are expensive.
- The coaxial cable must be grounded in order to prevent any crosstalk.
- As a Coaxial cable has multiple layers it is very bulky.
- There is a chance of breaking the coaxial cable and attaching a “t-joint” by hackers, this compromises the security of the data.

Optical Fiber Cable

Optical Fibre Cable uses the concept total internal reflection of light through a core made up of glass. The core is surrounded by a less dense glass or plastic covering called the coating. It is used for the transmission of large volumes of data. The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.

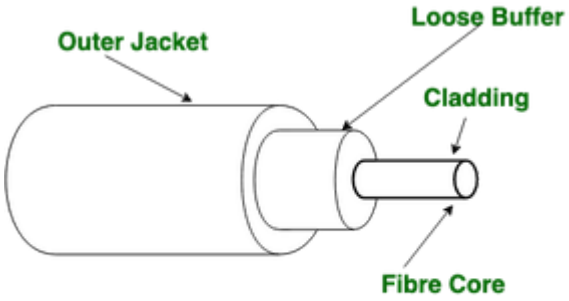


Figure of Optical Fibre Cable

Advantages of Optical Fibre Cable

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials

Disadvantages of Optical Fibre Cable

- Difficult to install and maintain
- High cost

Applications of Optical Fibre Cable

- **Medical Purpose:** Used in several types of medical instruments.
- **Defence Purpose:** Used in transmission of data in aerospace.
- **For Communication:** This is largely used in formation of internet cables.
- **Industrial Purpose:** Used for lighting purposes and safety measures in designing the interior and exterior of automobiles.

Stripline

Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett of the Air Force Cambridge Research Centre in the 1950s. Stripline is the earliest form of the planar transmission line. It uses a conducting material to transmit high-

frequency waves it is also called a waveguide. This conducting material is sandwiched between two layers of the ground plane which are usually shorted to provide EMI immunity.

Microstripline

A **microstripline** is a type of transmission media used to carry high-frequency signals, commonly found in microwave and radio frequency circuits. It consists of a flat, narrow conducting strip (usually made of metal) placed on top of a dielectric material (an insulating layer), with a metal ground plane on the other side.

2. Unguided Media

It is also referred to as Wireless or Unbounded transmission media . No physical medium is required for the transmission of electromagnetic signals.

Features of Unguided Media

- The signal is broadcasted through air
- Less Secure
- Used for larger distances

There are 3 types of Signals transmitted through unguided media:

Radio Waves

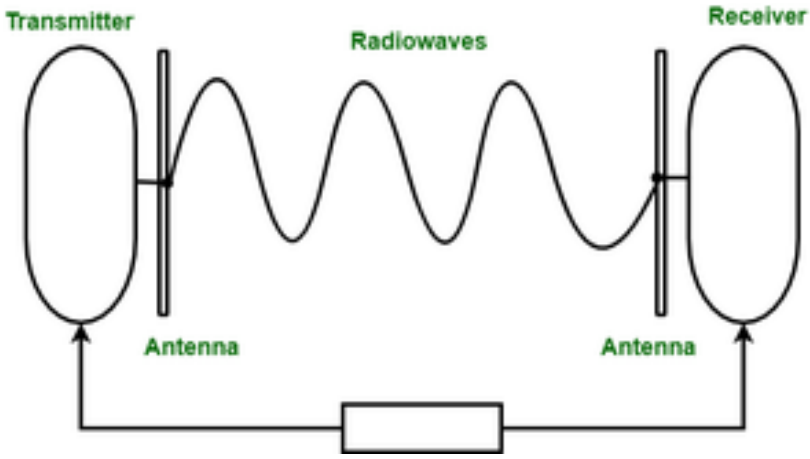
Radio waves are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.

Types of Radio Waves:

- **Short Wave:** AM Radio
- **VHF (Very High Frequency):** FM Radio/TV
- **UHF (Ultra High Frequency):** TV

Radio Wave Components:

- **Transmitter:** Responsible for encoding the signal.
- **Receiver:** Responsible for decoding the signal.



Microwaves

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. **Micro waves** are majorly used for mobile phone communication and television distribution.

Advanges:

- Cheaper than using cables
- Freedom from land acquisition
- Ease of communication in difficult terrains
- Communication over oceans

Disadvanges:

- Insecure communication.
- Out-of-phase signal.
- Susceptible to weather conditions.
- Bandwidth is limited.
- High cost of design, implementation, and maintenance.

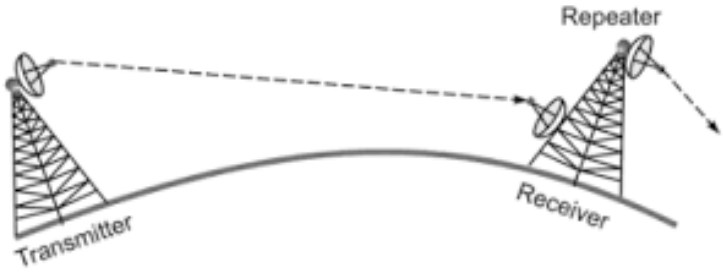
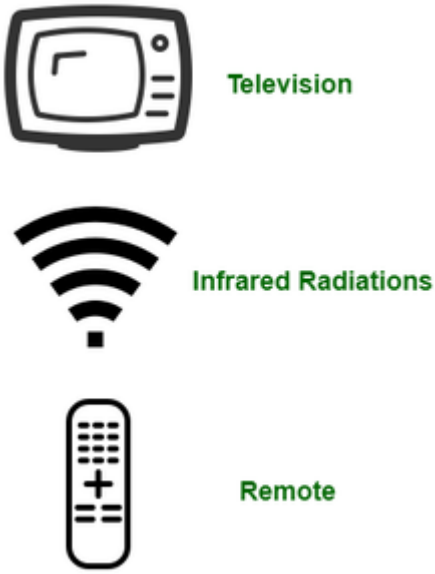


Fig: Microwave Transmission

Infrared

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.



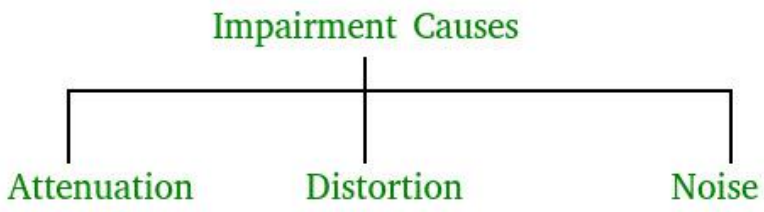
Difference Between Radio Waves, Micro Waves, and Infrared Waves

Basis	Radiowave	Microwave	Infrared wave
Direction	These are omni-directional in nature.	These are unidirectional in nature.	These are unidirectional in nature.
Penetration	At low frequency,	At low frequency, they	They cannot penetrate

Basis	Radiowave	Microwave	Infrared wave
	can penetrate through solid objects and walls but high frequency they bounce off the obstacle.	can penetrate through solid objects and walls. at high frequency, they cannot penetrate.	through any solid object and walls.
Frequency range	Frequency range: 3 KHz to 1GHz.	Frequency range: 1 GHz to 300 GHz.	Frequency range: 300 GHz to 400 GHz.
Security	These offers poor security.	These offers medium security.	These offers high security.
Attenuation	Attenuation is high.	Attenuation is variable.	Attenuation is low.
Government License	Some frequencies in the radio-waves require government license to use these.	Some frequencies in the microwaves require government license to use these.	There is no need of government license to use these waves.
Usage Cost	Setup and usage Cost is moderate.	Setup and usage Cost is high.	Usage Cost is very less.
Communication	These are used in long distance communication.	These are used in long distance communication.	These are not used in long distance communication.

Causes of Transmission Impairment

Transmission impairment refers to the loss or distortion of signals during data transmission, leading to errors or reduced quality in communication. Common causes include signal distortion, attenuation, and noise all of which can affect the clarity and reliability of transmitted data.



Transmission Impairment

- **Attenuation:** It means loss of energy. The strength of signal decreases with increasing distance which causes loss of energy in overcoming resistance of medium. This is also known as attenuated signal. Amplifiers are used to amplify the attenuated signal which gives the original signal back and compensate for this loss.
- **Distortion:** It means changes in the form or shape of the signal. This is generally seen in composite signals made up with different frequencies. Each frequency component has its own propagation speed travelling through a medium. And thats why it delay in arriving at the final destination Every component arrive at different time which leads to distortion. Therefore, they have different phases at receiver end from what they had at senders end.
- **Noise:** The random or unwanted signal that mixes up with the original signal is called noise. There are several types of noise such as induced noise, crosstalk noise, thermal noise and impulse noise which may corrupt the signal.

Factors Considered for Designing the Transmission Media

- **Bandwidth:** Assuming all other conditions remain constant, the greater a medium's bandwidth, the faster a signal's data transmission rate.

- **Transmission Impairment** : Transmission Impairment occurs when the received signal differs from the transmitted signal. Signal quality will be impacted as a result of transmission impairment.
- **Interference:** Interference is defined as the process of disturbing a signal as it travels over a communication media with the addition of an undesired signal.

Applications of Transmission Media in Computer Networks

Transmission media in computer networks are used to connect devices and transfer data. Here are some common applications:

Transmission Media	Application
Unshielded Twisted Pair (UTP)	Local Area Networks (LAN), telephones
Shielded Twisted Pair (STP)	Industrial networks, environments with high interference
Optical Fiber Cable	Long-distance communication, internet backbones
Coaxial Cable	Cable TV, broadband internet, CCTV
Stripline	Printed Circuit Boards (PCBs), microwave circuits
Microstripline	Antennas, satellite communication, RF circuits
Radio	Wireless communication, AM/FM radio, mobile phones
Infrared	Remote controls, short-range communication

Transmission Media	Application
Microwave	Satellite communication, radar, long-distance links

Conclusion

In conclusion, transmission media are fundamental ways for data transmission in networks, and they are classified as directed (wired) or unguided (wireless). Guided media, such as twisted pair cables, coaxial cables, and optical fibers, provide secure, fast, and dependable data transmission over short distances. Unguided media, such as radio waves, microwaves, and infrared, provide wireless communication at various distances, with security and attenuation trade-offs. The choice of transmission media is determined by bandwidth, transmission impairment, and interference.

Frequently Asked Questions on Transmission Media – FAQ's

What are three options for signal transmission on a network?

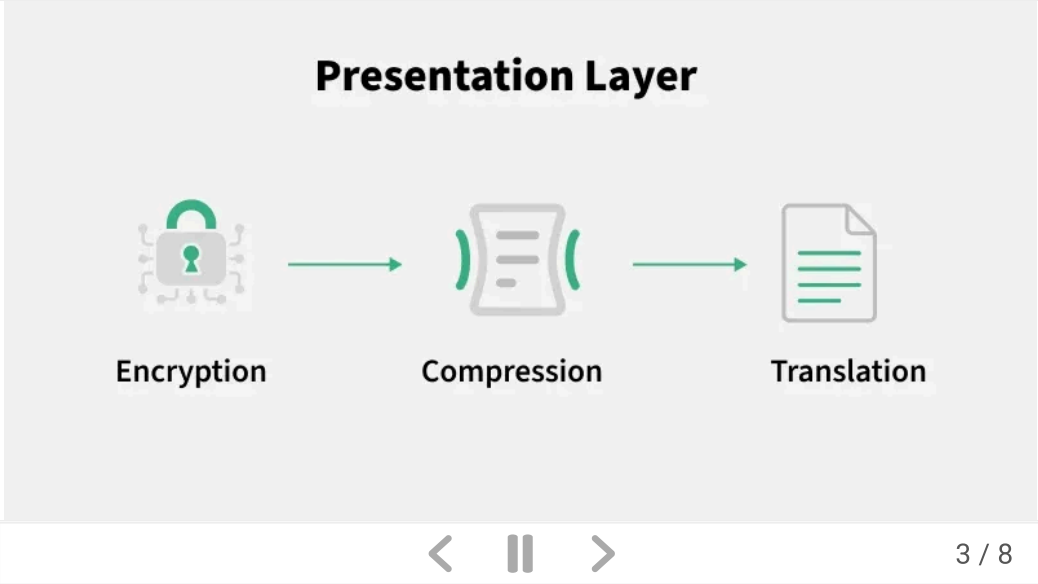
There are three common ways to send signals over a network:

1. *Electrical signals: Data is sent as electrical pulses through copper wires.*
2. *Optical signals: Electrical signals are changed into light pulses to carry data.*
3. *Wireless signals: Data is sent through the air using infrared, microwaves, or radio waves.*

What is OSI Model? – Layers of OSI Model

Last Updated : 20 Jan, 2025

The **OSI (Open Systems Interconnection)** Model is a set of rules that explains how different computer systems communicate over a network. OSI Model was developed by the **International Organization for Standardization (ISO)**. The OSI Model consists of 7 layers and each layer has specific functions and responsibilities. This layered approach makes it easier for different devices and technologies to work together. OSI Model provides a clear structure for data transmission and managing network issues. The OSI Model is widely used as a reference to understand how network systems function.



Layers of the OSI Model

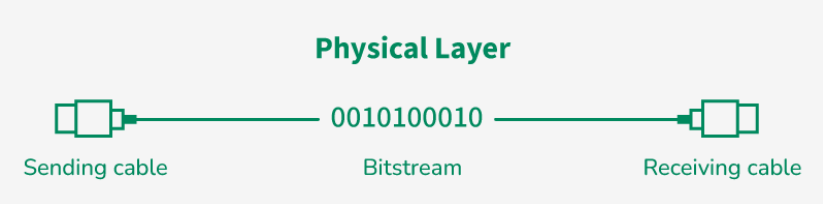
There are 7 layers in the OSI Model and each layer has its specific role in handling data. All the layers are mentioned below:

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer

- Presentation Layer
- Application Layer

Layer 1 – Physical Layer

The lowest layer of the OSI reference model is the **Physical Layer**. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** Physical Layer is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together. Common physical layer devices are Hub, Repeater, Modem, and Cables.



Physical Layer

Functions of the Physical Layer

- **Bit Synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
- **Bit Rate Control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- **Physical Topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus topology, star topology, or mesh topology.
- **Transmission Mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full duplex.

Layer 2 – Data Link Layer (DLL)

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer

is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address. Packet in the Data Link layer is referred to as Frame. Switches and Bridges are common Data Link Layer devices.

The Data Link Layer is divided into two sublayers:

- Logical Link Control (LLC)
- Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of the **NIC (**Network Interface Card**)**. DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP (Address Resolution Protocol) request onto the wire asking, "Who has that IP address?" and the destination host will reply with its MAC address.

Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- **Physical Addressing:** After creating frames, the Data link layer adds physical addresses (MAC **addresses)** of the sender and/or receiver in the header of each frame.
- **Error Control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
- **Access Control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

Layer 3 – Network Layer

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender and receiver's IP address are placed in the header by the network layer. Segment in the Network layer is referred to as Packet**.** Network layer is implemented by networking devices such as routers and switches.

Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- **Logical Addressing:** To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender and receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Layer 4 – Transport Layer

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as **Segments**. It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found. Protocols used in Transport Layer are TCP, UDP NetBIOS, PPTP.

At the sender's side, the transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow and error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

- Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a

web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

At the Receiver's side, Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

Functions of the Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus, by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services Provided by Transport Layer

- Connection-Oriented Service
- Connectionless Service

Layer 5 – Session Layer

Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices. It also provides authentication and security. Protocols used in the Session Layer are NetBIOS, PPTP.

Functions of the Session Layer

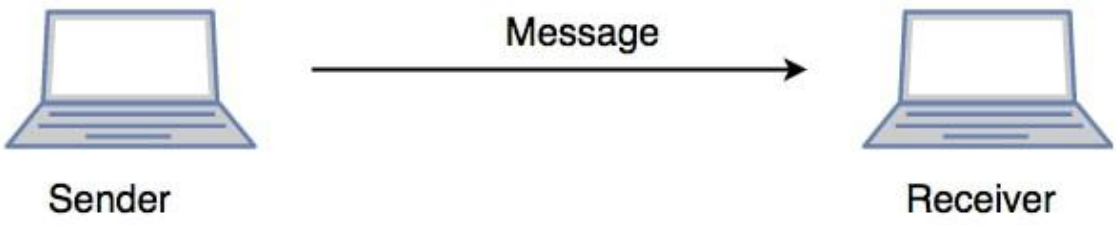
- **Session Establishment, Maintenance, and Termination:** The layer allows the two processes to establish, use, and terminate a

connection.

- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely, and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full duplex.

Example

Let us consider a scenario where a user wants to send a message through some Messenger application running in their browser. The "**Messenger**" here acts as the application layer which provides the user with an interface to create the data. This message or so-called **Data** is compressed, optionally encrypted (if the data is sensitive), and converted into bits (0's and 1's) so that it can be transmitted.



Communication in Session Layer

Layer 6 – Presentation Layer

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. Protocols used in the Presentation Layer are JPEG, MPEG, GIF, TLS/SSL, etc.

Functions of the Presentation Layer

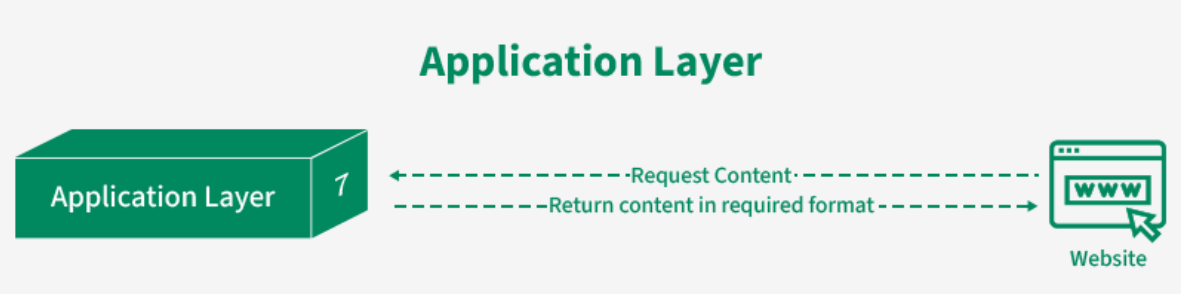
- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the

ciphertext, and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

- **Compression:** Reduces the number of bits that need to be transmitted on the network.

Layer 7 – Application Layer

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user. Protocols used in the Application layer are SMTP, FTP, DNS, etc.



Application Layer

Functions of the Application Layer

The main functions of the application layer are given below.

- **Network Virtual Terminal (NVT):** It allows a user to log on to a remote host.
- **File Transfer Access and Management (FTAM):** This application allows a user to access files in a remote host, retrieve files in a remote host, and manage or control files from a remote computer.
- **Mail Services:** Provide email service.
- **Directory Services:** This application provides distributed database sources and access for global information about various objects and services.

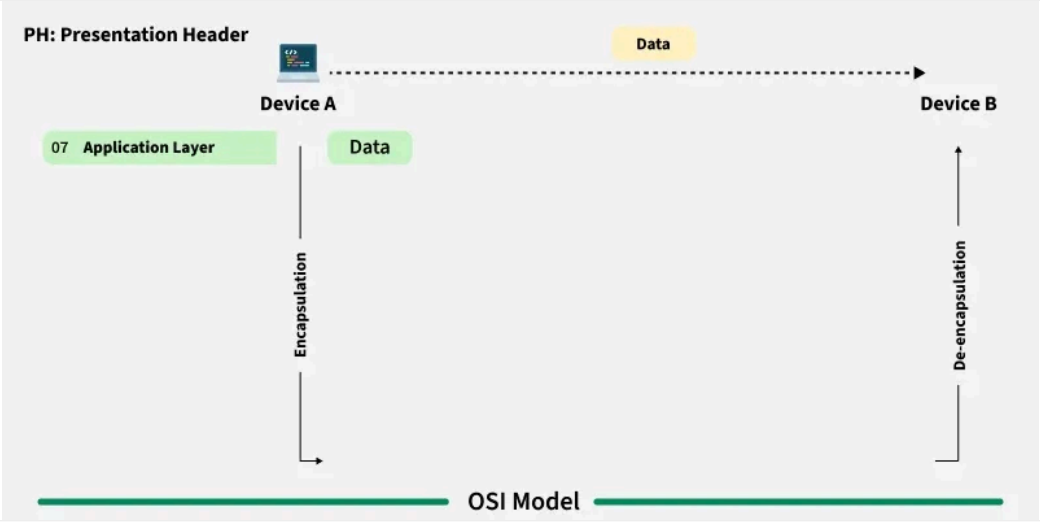
How Data Flows in the OSI Model?

When we transfer information from one device to another, it travels through 7 layers of OSI model. First data travels down through 7 layers from the sender's end and then climbs back 7 layers on the receiver's end.

Data flows through the OSI model in a step-by-step process:

- **Application Layer:** Applications create the data.
- **Presentation Layer:** Data is formatted and encrypted.
- **Session Layer:** Connections are established and managed.
- **Transport Layer:** Data is broken into segments for reliable delivery.
- **Network Layer:** Segments are packaged into packets and routed.
- **Data Link Layer:** Packets are framed and sent to the next device.
- **Physical Layer:** Frames are converted into bits and transmitted physically.

Each layer adds specific information to ensure the data reaches its destination correctly, and these steps are reversed upon arrival.



We can understand how data flows through OSI Model with the help of an example mentioned below.

Let us suppose, **Person A** sends an e-mail to his friend **Person B**.

Step 1: Person A interacts with e-mail application like **Gmail**, **outlook**, etc. Writes his email to send. (This happens at **Application Layer**).

Step 2: At Presentation Layer, Mail application prepares for data transmission like encrypting data and formatting it for transmission.

Step 3: At Session Layer, there is a connection established between the sender and receiver on the internet.

Step 4: At Transport Layer, Email data is broken into smaller segments. It adds sequence number and error-checking information to maintain the reliability of the information.

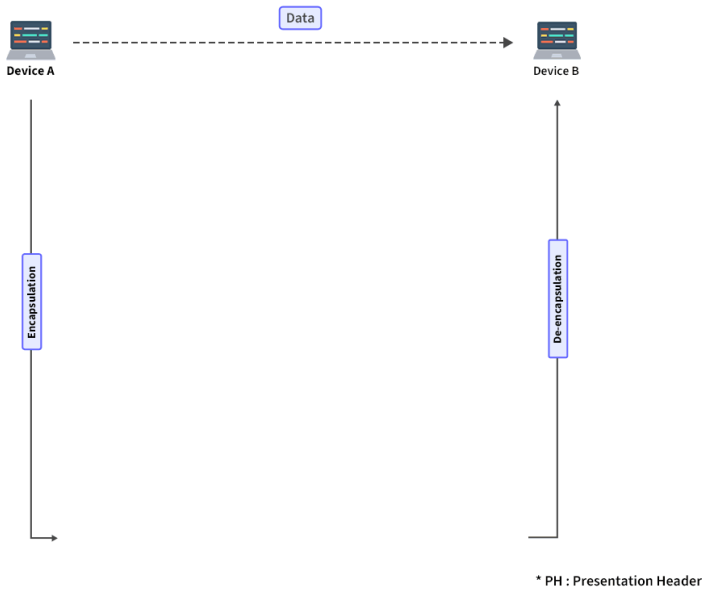
Step 5: At Network Layer, addressing of packets is done in order to find the best route for transfer.

Step 6: At Data Link Layer, data packets are encapsulated into frames, then MAC address is added for local devices and then it checks for error using error detection.

Step 7: At Physical Layer, Frames are transmitted in the form of electrical/ optical signals over a physical network medium like ethernet cable or WiFi.

After the email reaches the receiver i.e. **Person B**, the process will reverse and decrypt the e-mail content. At last, the email will be shown on **Person B** email client.

Please refer the below animation for detailed flow.



Protocols Used in the OSI Layers

Layer	Working	Protocol Data Unit	Protocols
1 – Physical Layer	Establishing Physical Connections between Devices.	Bits	USB, SONET/SDH, etc.
2 – Data Link Layer	Node to Node Delivery of Message.	Frames	Ethernet, PPP, etc.
3 – Network Layer	Transmission of data from one host to another, located in different networks.	Packets	IP, ICMP, IGMP, OSPF, etc.
4 – Transport Layer	Take Service from Network Layer and provide it to the Application Layer.	Segments (for TCP) or Datagrams (for UDP)	TCP, UDP, SCTP, etc.
5 – Session Layer	Establishes Connection, Maintenance, Ensures Authentication and Ensures security.	Data	NetBIOS, RPC, PPTP, etc.
6 – Presentation Layer	Data from the application layer is extracted and manipulated in the required format for transmission.	Data	TLS/SSL, MIME, JPEG, PNG, ASCII, etc.

Layer	Working	Protocol Data Unit	Protocols
7 – Application Layer	Helps in identifying the client and synchronizing communication.	Data	FTP, SMTP, DNS, DHCP, etc.

Why Does the OSI Model Matter?

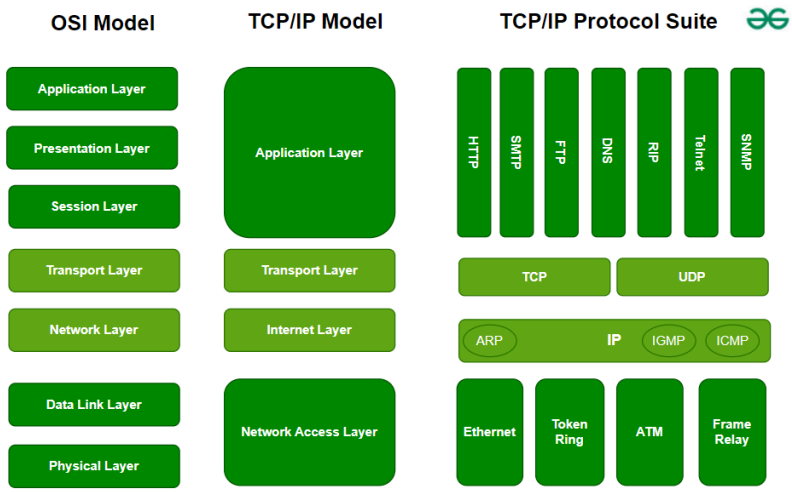
The OSI Model matters because it provides the user a clear structure of “how the data moves in the network?”. As the OSI Model consists of 7 layers, each layer has its specific role, and due to which it helps in understanding, identifying and solving the complex network problems easily by focusing on one of the layers not the entire network.

As the modern Internet does not prefer the OSI Model, but still, the OSI Model is still very helpful for solving network problems. It helps people understanding network concepts very easily.

Difference Between OSI and TCP/IP Model

OSI Model	TCP/IP Model
OSI stands for Open Systems Interconnection.	TCP/IP stands for Transmission Control Protocol/Internet Protocol.
OSI model has 7 layers.	TCP/IP model consists of 4 layers.
Package delivery is guaranteed in OSI Model.	Package delivery is not guaranteed in the TCP/IP Model.

OSI Model	TCP/IP Model
In the OSI model, only layers 1,2 and 3 are necessary for data transmission.	All layers of the TCP/IP model are needed for data transmission.
Protocols at each layer is independent of the other layer.	Layers are integrated; some layers are required by other layers of TCP/IP model.
OSI Model is a conceptual framework, less used in practical applications.	Widely used in actual networks like Internet and Communication Systems.



OSI vs TCP/IP

Advantages of OSI Model

The OSI Model defines the communication of a computing system into 7 different layers. Its advantages include:

- It divides network communication into 7 layers which makes it easier to understand and troubleshoot.
- It standardizes network communications, as each layer has fixed functions and protocols.
- Diagnosing network problems is easier with the **OSI model.**

- It is easier to improve with advancements as each layer can get updates separately.

Disadvantages of OSI Model

- The OSI Model has seven layers, which can be complicated and hard to understand for beginners.
- In real-life networking, most systems use a simpler model called the Internet protocol suite (TCP/IP), so the OSI Model is not always directly applicable.
- Each layer in the OSI Model adds its own set of rules and operations, which can make the process more time-consuming and less efficient.
- The OSI Model is more of a theoretical framework, meaning it's great for understanding concepts but not always practical for implementation.

Conclusion

In conclusion, the OSI (Open Systems Interconnection) model helps us understand how data moves in networks. It consists of seven distinct layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Each layer has specific responsibilities and interacts with the layers directly above and below it. Since it is a conceptual model, but the OSI framework is still widely used to troubleshoot and understand networking issues.

Frequently Asked Questions on OSI Model – FAQs

Can OSI layers work independently?

> *No, OSI layers do not work independently. Each layer depends on the services provided by the layer below it and, in turn, provides services to the layer above it. This layered approach ensures that data is transmitted smoothly from the source to the destination.*

How does the OSI Model help in troubleshooting network issues?

Types of Computer Networks

Last Updated : 08 Jul, 2024

A computer network is a cluster of computers over a shared communication path that works to share resources from one computer to another, provided by or located on the network nodes. In this article, we will discuss computer networks and their types.

What is a Computer Network?

A computer network is a system that connects many independent computers to share information (data) and resources. The integration of computers and other different devices allows users to communicate more easily. A computer network is a collection of two or more computer systems that are linked together. A network connection can be established using either cable or wireless media. Hardware and software are used to connect computers and tools in any network.

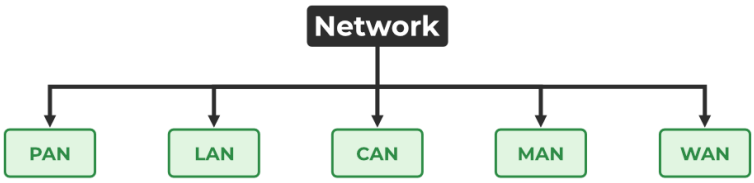
Uses of Computer Networks

- Communicating using email, video, instant messaging, etc.
- Sharing devices such as printers, scanners, etc.
- Sharing files.
- Sharing software and operating programs on remote systems.
- Allowing network users to easily access and maintain information.

Types of Computer Networks

There are mainly five types of Computer Networks

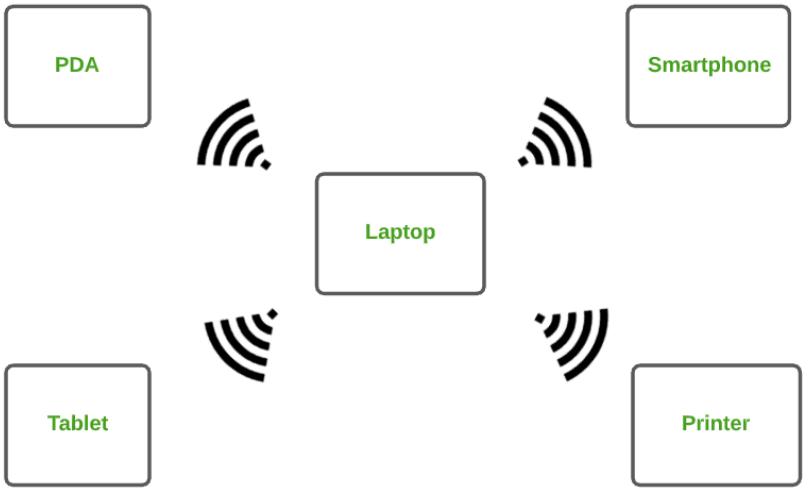
1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Campus Area Network (CAN)
4. Metropolitan Area Network (MAN)
5. Wide Area Network (WAN)



Types of Computer Networks

1. Personal Area Network (PAN)

PAN is the most basic type of computer network. It is a type of network designed to connect devices within a short range, typically around one person. It allows your personal devices, like smartphones, tablets, laptops, and wearables, to communicate and share data with each other. PAN offers a network range of 1 to 100 meters from person to device providing communication. Its transmission speed is very high with very easy maintenance and very low cost. This uses Bluetooth, IrDA, and Zigbee as technology. Examples of PAN are USB, computer, phone, tablet, printer, PDA, etc.



Personal Area Network (PAN)

Types of PAN

- **Wireless Personal Area Networks:** Wireless Personal Area Networks are created by simply utilising wireless technologies such as WiFi

and Bluetooth. It is a low-range network.
- **Wired Personal Area Network:** A wired personal area network is constructed using a USB.

Advantages of PAN

- PAN is relatively flexible and provides high efficiency for short network ranges.
- It needs easy setup and relatively low cost.
- It does not require frequent installations and maintenance
- It is easy and portable.
- Needs fewer technical skills to use.

Disadvantages of PAN

- Low network coverage area/range.
- Limited to relatively low data rates.
- Devices are not compatible with each other.
- Inbuilt WPAN devices are a little bit costly.

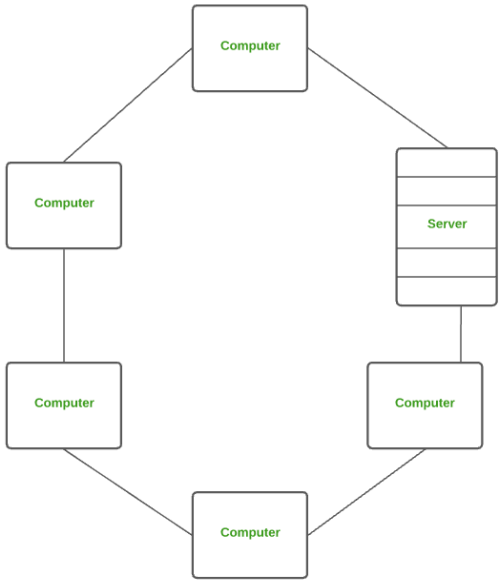
Applications of PAN

- Home and Offices
- Organizations and the Business sector
- Medical and Hospital
- School and College Education
- Military and Defense

2. Local Area Network (LAN)

LAN is the most frequently used network. A LAN is a computer network that connects computers through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are Ethernet and Wi-fi. It ranges up to 2km & transmission speed is very high with easy maintenance

and low cost. Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.



Local Area Network (LAN)

Advantages of a LAN

- **Privacy:** LAN is a private network, thus no outside regulatory body controls it, giving it a privacy.
- **High Speed:** LAN offers a much higher speed(around 100 mbps) and data transfer rate comparatively to WAN.
- **Supports different transmission mediums:** LAN support a variety of communications transmission medium such as an Ethernet cable (thin cable, thick cable, and twisted pair), fiber and wireless transmission.
- **Inexpensive and Simple:** A LAN usually has low cost, installation, expansion and maintenance and LAN installation is relatively easy to use, good scalability.

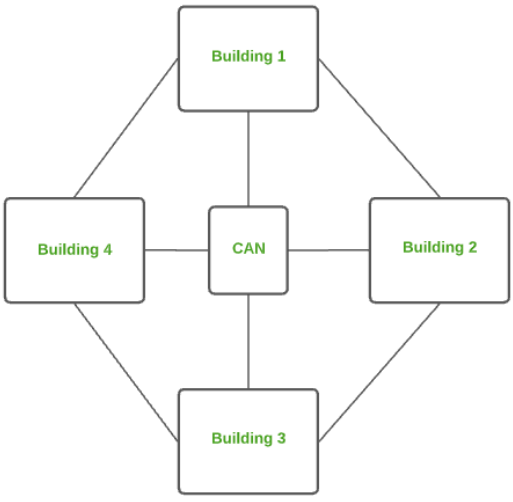
Disadvantages of LAN

- The initial setup costs of installing Local Area Networks is high because there is special software required to make a server.
- Communication devices like an ethernet cable, switches, hubs, routers, cables are costly.

- LAN administrator can see and check personal data files as well as Internet history of each and every LAN user. Hence, the privacy of the users are violated
- LANs are restricted in size and cover only a limited area
- Since all the data is stored in a single server computer, if it can be accessed by an unauthorized user, can cause a serious data security threat.

3. Campus Area Network (CAN)

CAN is bigger than a LAN but smaller than a MAN. This is a type of computer network that is usually used in places like a school or colleges. This network covers a limited geographical area that is, it spreads across several buildings within the campus. CAN mainly use Ethernet technology with a range from 1km to 5km. Its transmission speed is very high with a moderate maintenance cost and moderate cost. Examples of CAN are networks that cover schools, colleges, buildings, etc.



Campus Area Network (CAN)

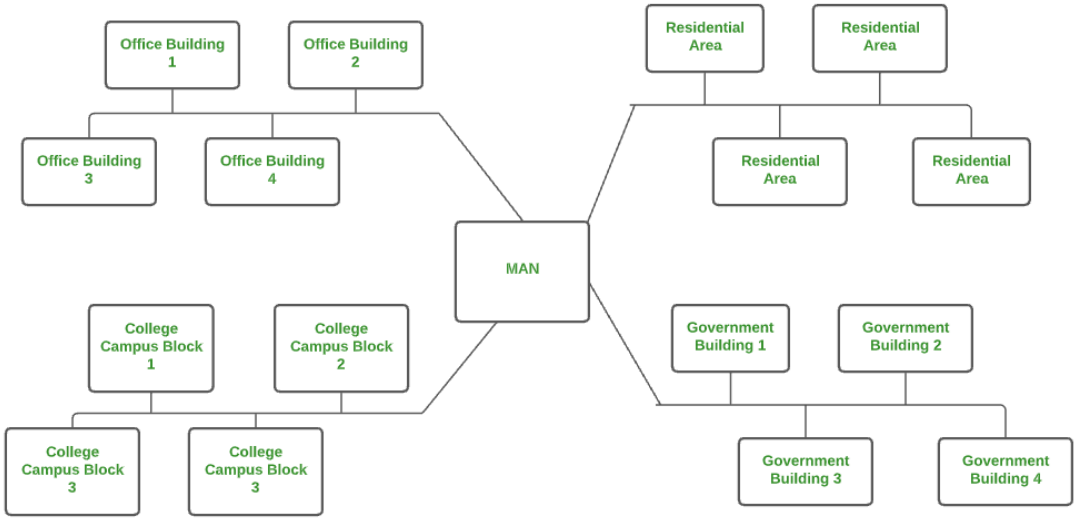
Advantages of CAN

- **Speed:** Communication within a CAN takes place over Local Area Network (LAN) so data transfer rate between systems is little bit fast than Internet.

- **Security:** Network administrators of campus take care of network by continuous monitoring, tracking and limiting access. To protect network from unauthorized access firewall is placed between network and internet.
- **Cost effective:** With a little effort and maintenance, network works well by providing fast data transfer rate with multi-departmental network access. It can be enabled wirelessly, where wiring and cabling costs can be managed. So to work with in a campus using CAN is cost-effective in view of performance

4. Metropolitan Area Network (MAN)

A MAN is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area. This network mainly uses FDDI, CDDI, and ATM as the technology with a range from 5km to 50km. Its transmission speed is average. It is difficult to maintain and it comes with a high cost. Examples of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.



Metropolitan Area Network (MAN)

Advantages of MAN

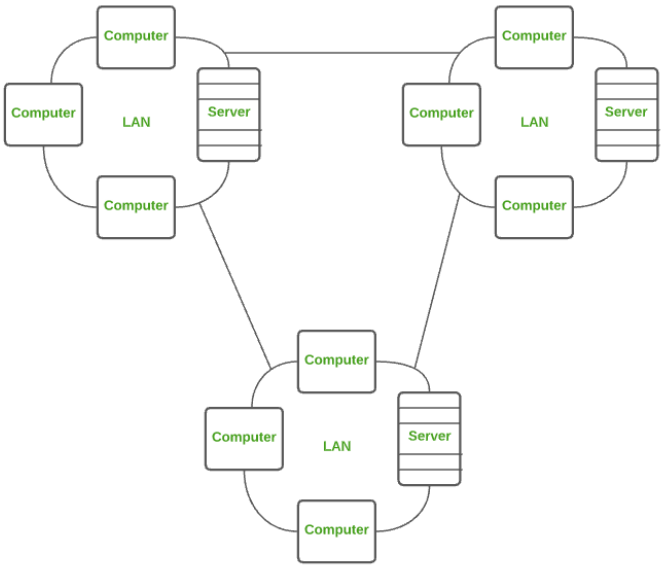
- MAN offers high-speed connectivity in which the speed ranges from 10-100 Mbps.
- The security level in MAN is high and strict as compared to WAN.
- It support to transmit data in both directions concurrently because of dual bus architecture.
- MAN can serve multiple users at a time with the same high-speed internet to all the users.
- MAN allows for centralized management and control of the network, making it easier to monitor and manage network resources and security.

Disadvantages of MAN

- The architecture of MAN is quite complicated hence, it is hard to design and maintain.
- This network is highly expensive because it required the high cost to set up fiber optics.
- It provides less fault tolerance.
- The Data transfer rate in MAN is low when compare to LANs.

5. Wide Area Network (WAN)

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. **WAN** can also be defined as a group of local area networks that communicate with each other with a range above 50km. Here we use Leased-Line & Dial-up technology. Its transmission speed is very low and it comes with very high maintenance and very high cost. The most common example of WAN is the Internet.



Wide Area Network (WAN)

Advantages of WAN

- It covers large geographical area which enhances the reach of organisation to transmit data quickly and cheaply.
- The data can be stored in centralised manner because of remote access to data provided by WAN.
- The travel charges that are needed to cover the geographical area of work can be minimised.
- WAN enables a user or organisation to connect with the world very easily and allows to exchange data and do business at global level.

Disadvantages of WAN

- Traffic congestion in Wide Area Network is very high.
- The fault tolerance ability of WAN is very less.
- Noise and error are present in large amount due to multiple connection point.
- The data transfer rate is slow in comparison to LAN because of large distances and high number of connected system within the network.

Comparison between Different Computer Networks

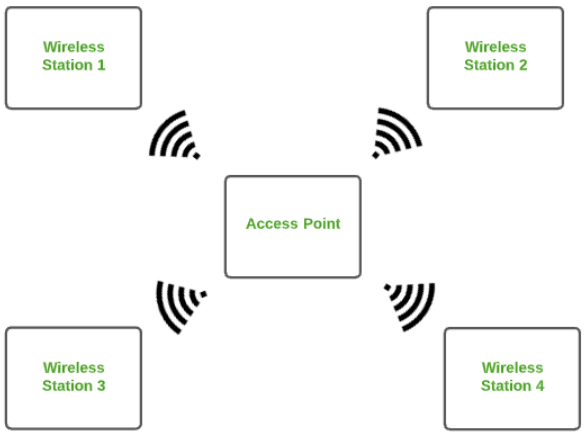
Parameters	PAN	LAN	CAN	MAN	WAN
Full Name	Personal Area Network	Local Area Network	Campus Area Network	Metropolitan Area Network	Wid Are Netw
Technology	Bluetooth, IrDA,Zigbee	Ethernet & Wifi	Ethernet	FDDI, CDDi. ATM	Leas Line Dial-U
Range	1-100 m	Upto 2km	1 – 5 km	5-50 km	Abov 50 k
Transmission Speed	Very High	Very High	High	Average	Lov
Ownership	Private	Private	Private	Private or Public	Priva or Publ
Maintenance	Very Easy	Easy	Moderate	Difficult	Ver Diffic
Cost	Very Low	Low	Moderate	High	Ver Hig

Other Types of Computer Networks

- Wireless Local Area Network (WLAN)
- Storage Area Network (SAN)
- System-Area Network (SAN)
- Passive Optical Local Area Network (POLAN)
- Enterprise Private Network (EPN)
- Virtual Private Network (VPN)
- Home Area Network (HAN)

1. Wireless Local Area Network (WLAN)

WLAN is a type of computer network that acts as a local area network but makes use of wireless network technology like Wi-Fi. This network doesn't allow devices to communicate over physical cables like in LAN but allows devices to communicate wirelessly. The most common example of WLAN is Wi-Fi.

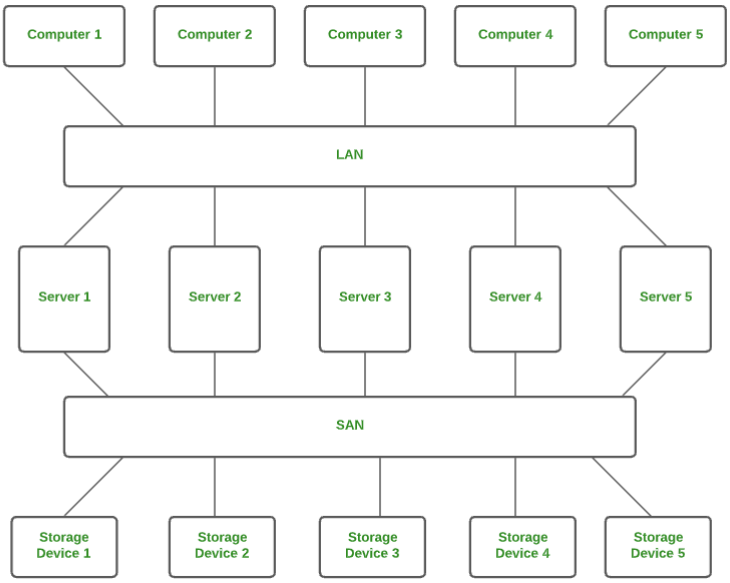


Wireless Local Area Network (WLAN)

There are several computer networks available; more information is provided below.

2. Storage Area Network (SAN)

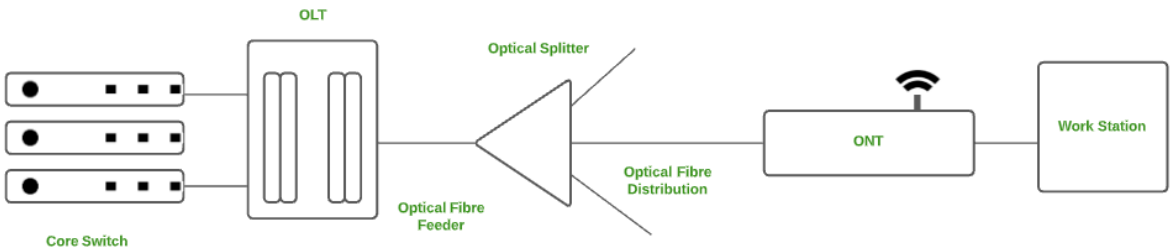
SAN is a type of computer network that is high-speed and connects groups of storage devices to several servers. This network does not depend on LAN or WAN. Instead, a SAN moves the storage resources from the network to its high-powered network. A SAN provides access to block-level data storage. Examples of SAN are a network of disks accessed by a network of servers.



Storage Area Network (SAN)

3. Passive Optical Local Area Network (POLAN)

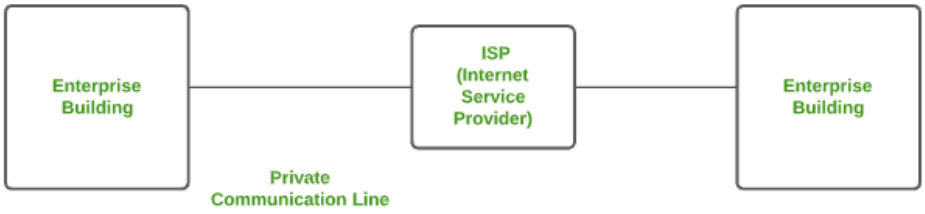
A POLAN is a type of computer network that is an alternative to a LAN. POLAN uses optical splitters to split an optical signal from a single strand of single-mode optical fiber to multiple signals to distribute users and devices. In short, POLAN is a point to multipoint LAN architecture.



Passive Optical Local Area Network (POLAN)

4. Enterprise Private Network (EPN)

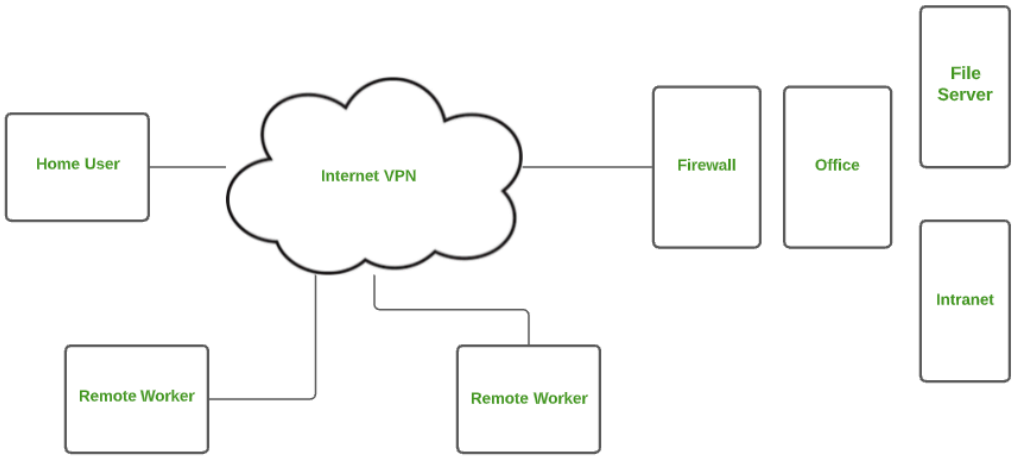
EPN is a type of computer network mostly used by businesses that want a secure connection over various locations to share computer resources.



Enterprise Private Network (EPN)

5. Virtual Private Network (VPN)

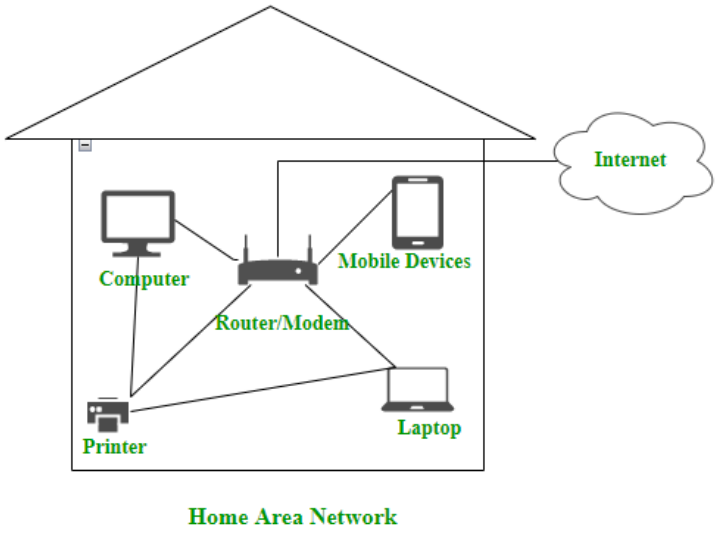
A VPN is a type of computer network that extends a private network across the internet and lets the user send and receive data as if they were connected to a private network even though they are not. Through a virtual point-to-point connection users can access a private network remotely. VPN protects you from malicious sources by operating as a medium that gives you a protected network connection.



Virtual Private Network (VPN)

6. Home Area Network (HAN)

Many of the houses might have more than a computer. To interconnect those computers and with other peripheral devices, a network should be established similar to the local area network (LAN) within that home. Such a type of network that allows a user to interconnect multiple computers and other digital devices within the home is referred to as Home Area Network (HAN). HAN encourages sharing of resources, files, and programs within the network. It supports both wired and wireless communication.



Home Area Network (HAN)

Internetwork

An internet network is defined as two or more computer network LANs, WANs, or computer network segments that are connected by devices and configured with a local addressing system. The method is known as internetworking. There are two types of Internetwork.

- **Intranet**: An internal network within an organization that enables employees to share data, collaborate, and access resources. Intranets are not accessible to the public and use private IP addresses.
- **Extranet**: Extranets extend the intranet to authorized external users, such as business partners or clients. They provide controlled access to specific resources while maintaining security.

Advantages of Computer Network

- **Central Storage of Data:** Files are stored on a central storage database which helps to easily access and available to everyone.
- **Connectivity:** A single connection can be routed to connect multiple computing devices.
- **Sharing of Files:** Files and data can be easily shared among multiple devices which helps in easily communicating among the organization.
- **Security through Authorization:** Computer Networking provides additional security and protection of information in the system.

Disadvantages of Computer Network

- **Virus and Malware:** A virus is a program that can infect other programs by modifying them. Viruses and Malware can corrupt the whole network.
- **High Cost of Setup:** The initial setup of Computer Networking is expensive because it consists of a lot of wires and cables along with the device.
- **loss of Information:** In case of a System Failure, might lead to some loss of data.
- **Management of Network:** Management of a Network is somehow complex for a person, it requires training for its proper use.

Conclusion

In conclusion, computer networks are essential components that connect various computer devices in order to efficiently share data and resources. PAN, LAN, CAN, MAN, and WAN networks serve a wide range of applications and purposes, each with its own set of advantages and drawbacks. Understanding these networks and their applications improves connectivity, data exchange, and resource utilization in a variety of applications from personal use to global communications.

Frequently Asked Questions on Types of Computer Network – FAQs

Types of Multiplexing in Data Communications

Last Updated : 07 Feb, 2025

Imagine you have several friends who all want to send letters to the same person at the same time. Instead of sending each letter individually, which would take a lot of time and effort, you put all the letters into one big envelope and send that. When the big envelope arrives, the letters are taken out and delivered to the person one by one.

Multiplexing in data communications works in a similar way. It's a method that combines multiple signals or data streams into one signal over a shared medium. This process allows for efficient use of resources and can significantly increase the amount of data that can be sent over a network.

What is Multiplexing?

Multiplexing is the sharing of a medium or bandwidth. It is the process in which multiple signals coming from multiple sources are combined and transmitted over a single communication/physical line.

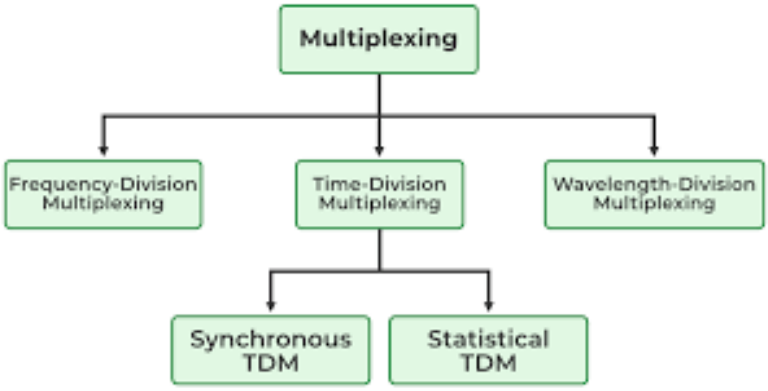
Uses of Multiplexing

Multiplexing is used for a variety of purposes in data communications to enhance the efficiency and capacity of networks. Here are some of the main uses:

- **Efficient Utilization of Resources**: Multiplexing allows multiple signals to share the same communication channel, making the most of the available bandwidth. This is especially important in environments where bandwidth is limited.
- **Telecommunications**: In telephone networks, multiplexing enables the simultaneous transmission of multiple telephone calls over a single line, enhancing the capacity of the network.
- **Internet and Data Networks**: Multiplexing is used in internet communications to transmit data from multiple users over a single network line, improving the efficiency and speed of data transfer.
- **Satellite Communications**: Multiplexing helps in efficiently utilizing the available bandwidth on satellite transponders, allowing multiple signals to be transmitted and received simultaneously.

Types of Multiplexing

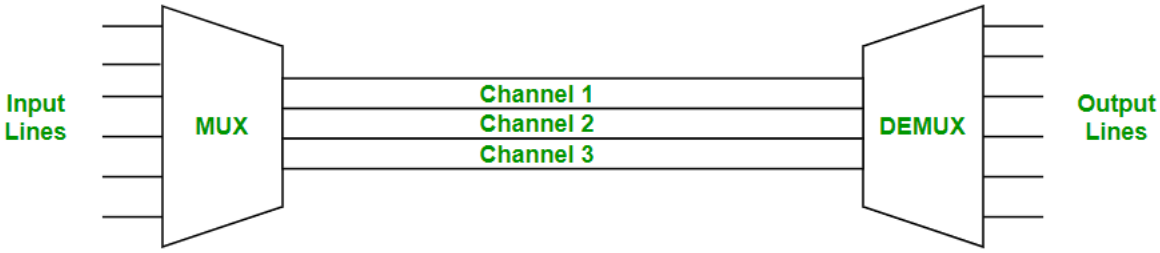
There are five different types of multiplexing techniques, each designed to handle various types of data and communication needs.



Types of Multiplexing

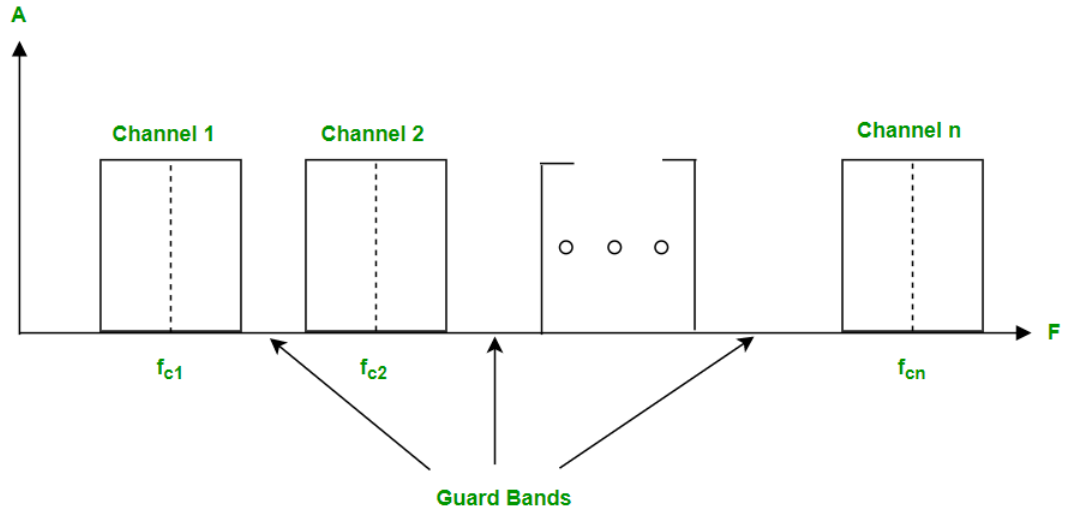
1. Frequency Division Multiplexing

Frequency division multiplexing is defined as a type of multiplexing where the bandwidth of a single physical medium is divided into a number of smaller, independent frequency channels.



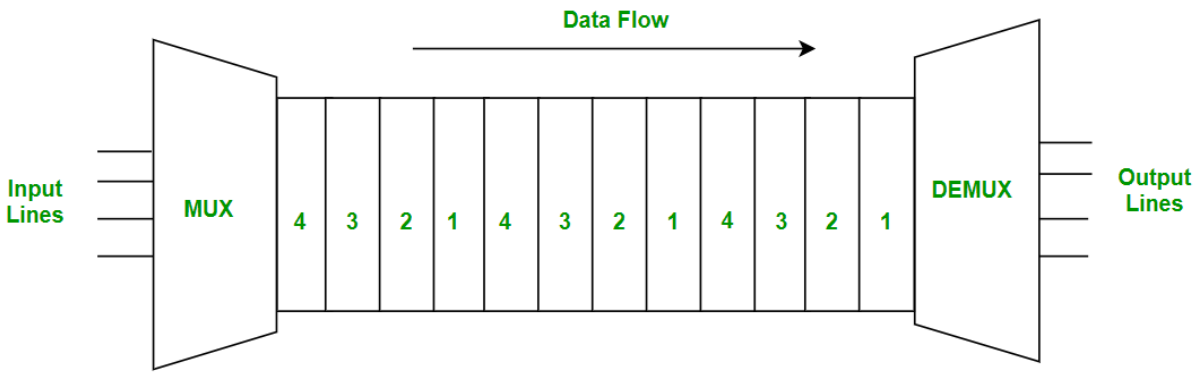
Frequency Division Multiplexing is used in radio and television transmission.

In FDM, we can observe a lot of inter-channel cross-talk because in this type of multiplexing the bandwidth is divided into frequency channels. In order to prevent the inter-channel cross talk, unused strips of bandwidth must be placed between each channel. These unused strips between each channel are known as **guard bands**.



2. Time Division Multiplexing

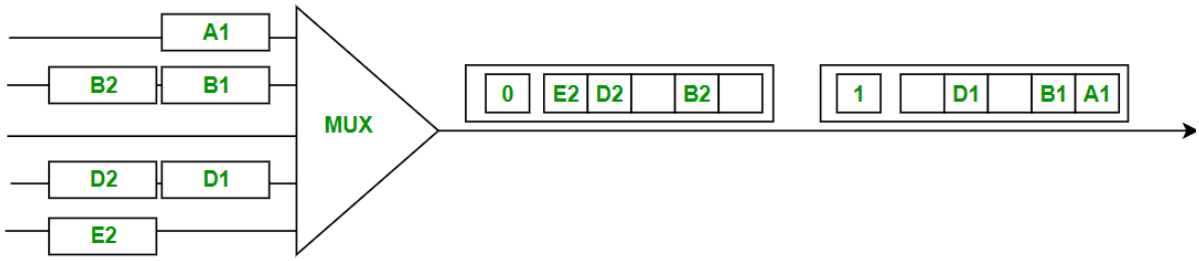
Time-division multiplexing is multiplexing wherein FDM, instead of sharing a portion of the bandwidth in the form of channels, in TDM, time is shared. Each connection occupies a portion of time in the link. In Time Division Multiplexing, all signals operate with the same frequency (bandwidth) at different times.



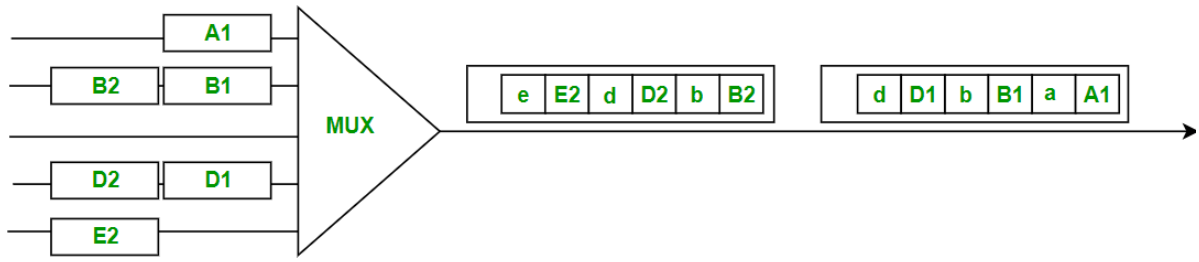
There are two types of Time Division Multiplexing :

- Synchronous Time Division Multiplexing
- Statistical (or Asynchronous) Time Division Multiplexing

Synchronous TDM : Synchronous TDM is a type of Time Division Multiplexing where the input frame already has a slot in the output frame. Time slots are grouped into frames. One frame consists of one cycle of time slots. Synchronous TDM is not efficient because if the input frame has no data to send, a slot remains empty in the output frame. In this, we need to mention the synchronous bit at the beginning of each frame.



Statistical TDM: Statistical TDM is a type of Time Division Multiplexing where the output frame collects data from the input frame till it is full not leaving an empty slot like in Synchronous TDM. In this, we need to include the address of each particular data in the slot that is being sent to the output frame.



Statistical TDM is a more efficient type of time-division multiplexing as the channel capacity is fully utilized and improves the bandwidth efficiency.

Read about Differences between TDM and FDM

3. Wavelength Division Multiplexing

Wavelength Division Multiplexing (WDM) is a multiplexing technology used to increase the capacity of optical fiber by transmitting multiple optical signals simultaneously over a single optical fiber, each with a different wavelength. Each signal is carried on a different wavelength of light, and the resulting signals are combined onto a single optical fiber for transmission. At the receiving end, the signals are separated by their wavelengths, demultiplexed and routed to their respective destinations. It is used in telecommunications, cable TV, ISPs, and data centers for high-speed, long-distance data transmission.

WDM can be divided into two categories:

- Dense Wavelength Division Multiplexing **(DWDM)** is used to multiplex a large number of optical signals onto a single fiber, typically up to 80 channels with a spacing of 0.8 nm or less between the channels.
- Coarse Wavelength Division Multiplexing **(CWDM)** is used for lower-capacity applications, typically up to 18 channels with a spacing of 20 nm between the channels.

Read about Differences between DWDM and CWDM.

Advantages over Time Division Multiplexing (TDM):

- Higher data rates & capacity
- Lower power consumption
- Reduced equipment complexity
- Flexible & easily upgradable

Read about Differences between TDM, FDM and WDM.

Advantages of Multiplexing

- **Efficient Use of Bandwidth:** You can send more than one signal over a single channel. This way, you can use the channel's capacity more efficiently.
- **Increased Data Transmission**: Multiplexing can significantly boost the amount of data that can be sent over a network simultaneously, enhancing overall transmission capacity.
- **Scalability**: Multiplexing allows networks to easily expand and accommodate more data streams without requiring significant changes to the existing infrastructure.
- **Flexibility**: Different types of multiplexing (TDM, FDM, WDM, CDM) can be used based on the specific needs and characteristics of the communication system, providing flexibility in network design.

Disadvantages of Multiplexing

- **Synchronization Issues**: Ensuring that multiple data streams remain properly synchronized can be challenging, leading to potential data loss or errors if not managed correctly.
- **Latency**: Combining multiple signals into one can introduce delays, as each data stream needs to be processed, synchronized, and demultiplexed at the receiving end.
- **Signal Degradation**: Over long distances, multiplexed signals can experience degradation and interference, requiring additional measures such as signal boosters or repeaters to maintain quality.
- **Resource Management**: Allocating and managing resources for multiplexing can be complicated, requiring careful planning and real-time adjustments to avoid congestion and ensure efficient operation.

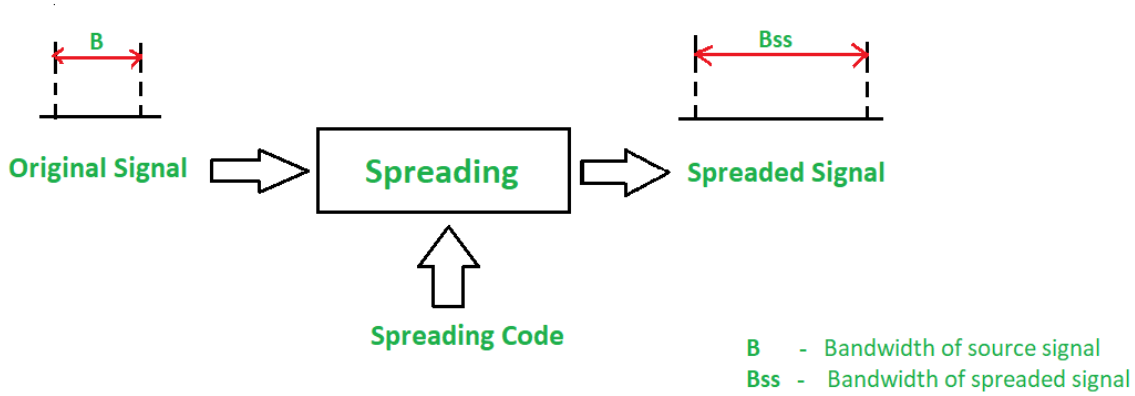
What is Spread Spectrum?

Last Updated : 16 Jul, 2024

Spread Spectrum is a wireless communication technology that distributes the transmitted signal across a larger bandwidth than the original signal. This approach improves communication security and dependability by increasing the signal's resistance to interference, eavesdropping, and jamming. In this article, we will discuss every point about Spread Spectrum and its types.

What is Spread Spectrum?

Spread spectrum is a method of transmitting radio signals over a wide range of frequencies. It spreads the signal over a broader bandwidth than the minimum required to send the information, which provides advantages such as increased resistance to interference, improved security, and enhanced privacy. The excerpt discusses the use of spread-spectrum techniques in communication to ensure secure transmission. This method uses air as a medium and extends bandwidth to create a protective envelope for signals, reducing the risk of interception or jamming. The 'spread code' is a patterned series of numbers that enlarges the original signal's bandwidth. This method is typically used in situations where secure transmission is crucial.



Spread Spectrum

Principles of Spread Spectrum process

- To allow redundancy, it is necessary that the bandwidth allocated to each station should be much larger than needed.
- The spreading process occurs after the signal is created by the source.

Conditions of Spread Spectrum are

- The spread spectrum is a type of modulation where modulated signal BW is much larger than the baseband signal BW i.e. spread spectrum is a wide band scheme.
- A special code (pseudo noise) is used for spectrum spreading and the same code is to be used to despread the signal at the receiver.

Characteristics of Spread Spectrum

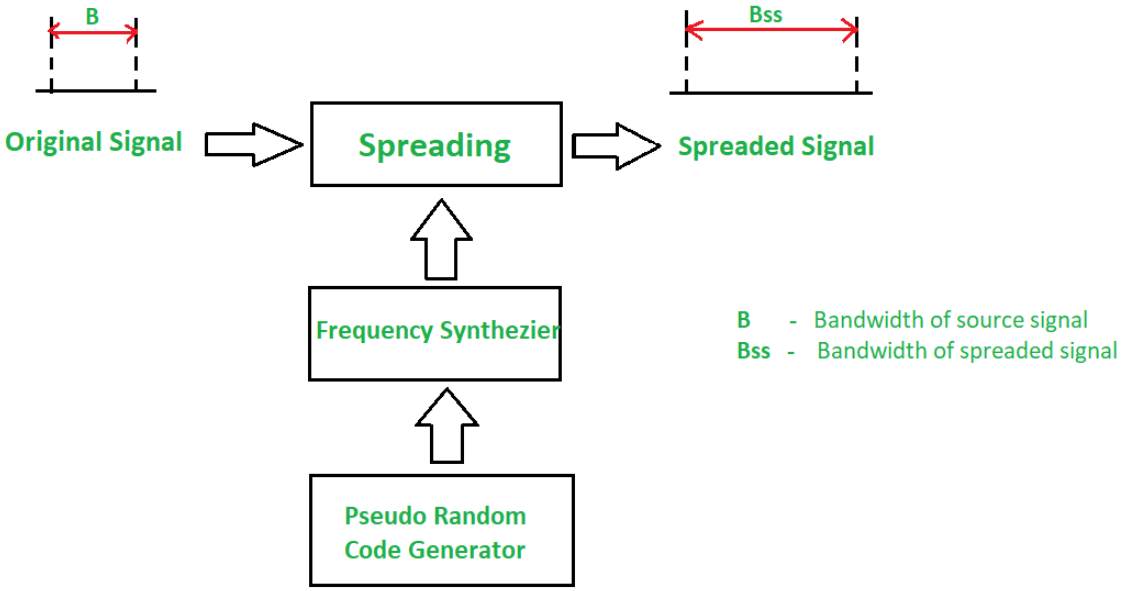
- Higher channel capacity.
- Ability to resist multipath propagation.
- They cannot easily intercept any unauthorized person.
- They are resistant to jamming.
- The spread spectrum provides immunity to distortion due to multipath propagation.
- The spread spectrum offers multiple access capabilities.

Techniques used for Spread Spectrum

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)

Frequency Hopping Spread Spectrum (FHSS)

In Frequency Hopping Spread Spectrum (FHSS), different carrier frequencies are modulated by the source signal i.e. M carrier frequencies are modulated by the signal. At one moment signal modulates one carrier frequency and at the subsequent moments, it modulates other carrier frequencies. The general block diagram of FHSS is shown in the below figure.



Frequency Hopping Spread Spectrum

A pseudorandom code generator generates Pseudo-random Noise of some pattern for each hopping period T_h. The frequency corresponding to the pattern is used for the hopping period and is passed to the frequency synthesizer. The synthesizer generates a carrier signal of that frequency. The figure above shows the spread signal via FHSS.

Advantages of FHSS

- Synchronization is not greatly dependent on distance.
- Processing Gain is higher than DSSS.

Disadvantages of FHSS

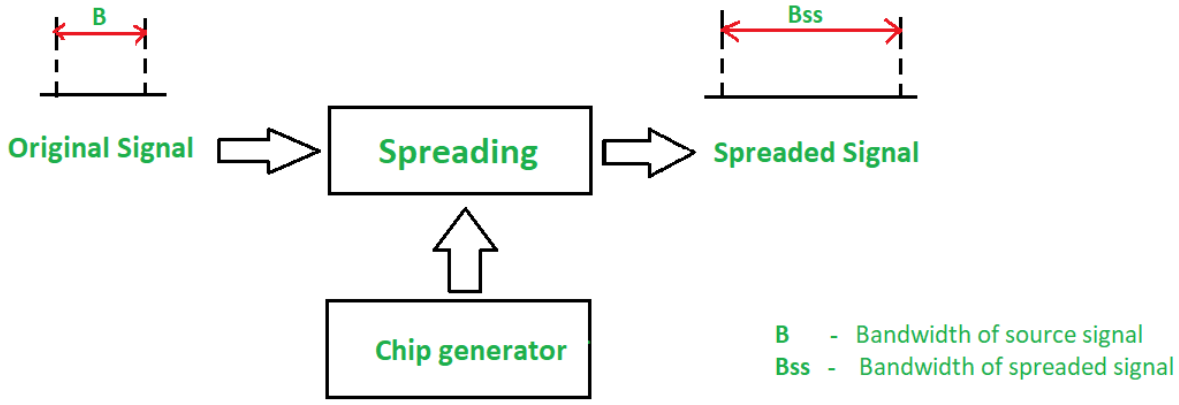
- The bandwidth of the FHSS system is too large (in GHz).
- Complex and expensive Digital frequency synthesizers are required.

Applications of FHSS

- FHSS is used in Bluetooth
- Military Communications
- Walkie-Talkies
- Wireless Local Area Networks (WLANs)
- Remote Controls

Direct Sequence Spread Spectrum (DSSS)

In Direct Sequence Spread Spectrum, the bandwidth of the original signal is also expanded by a different technique. Here, each data bit is replaced with n bits using a spreading code called **chips,** and the bit rate of the chip is called as **chip-rate**. The chip rate is n times the bit rate of the original signal. The below Figure shows the DSSS block diagram.



Direct Sequence Spread Spectrum

In wireless LAN, the sequence with n = 11 is used. The original data is multiplied by **chips** (spreading code) to get the spread signal. The required bandwidth of the spread signal is 11 times larger than the bandwidth of the original signal.

Advantages of DSSS

- The DSSS System combats the jamming most effectively.
- The performance of DSSS in presence of noise is superior to FHSS.
- Interference is minimized against the signals.

Disadvantages of DSSS

- Processing Gain is lower than FHSS.
- Channel Bandwidth is less than FHSS.
- Synchronization is affected by the variable distance between the transmitter and receiver.

Applications of DSSS

- GPS (Global Positioning System)
- CDMA (Code Division Multiple Access) Cellular Networks
- Satellite Communication
- Wireless Sensor Networks

Conclusion

Spread Spectrum is a wireless communication technology that distributes the transmitted signal across a larger bandwidth than the original signal. Frequency-hopping spread spectrum (FHSS) and Direct sequence spread spectrum (DSSS) are both types of spread spectrum techniques that are used in a variety of applications, including wireless communication, radar, and GPS. FHSS involves rapid frequency switching of the transmitted signal among a set of specific frequencies, while DSSS involves spreading the spectrum of the original signal over a wider bandwidth by multiplying it with a pseudo-random sequence of bits.

Frequently Asked Questions on Spread Spectrum – FAQs

How does Spread Spectrum work?

- *A special code (pseudo-noise) is used for spectrum spreading and despread at the receiver.*
- *The spread code enlarges the original signal's bandwidth, creating a protective envelope for signals.*
- *It reduces the risk of interception or jamming, making it crucial for secure transmission.*

Why DSSS is better than FHSS?

The DSSS modulation method transmits data at a higher rate than the FHSS method.