What is Session in php?

Session in PHP is a way of temporarily storing and making data accessible across all the website pages.

PHP session is used to store and pass information from one page to another temporarily (until user close the website).

A session is a way to store information (in variables) to be used across multiple pages.

So; Session variables hold information about one single user, and are available to all pages in one application.

Tip: If you need a permanent storage, you may want to store the data in a database.

Start a PHP Session

A session is started with the session_start() function.

Session variables are set with the PHP global variable: $_SESSION.

Now, let's create a new page called "demo_session1.php". In this page, we start a new PHP session and set some session variables:

Example

```
<?php
// Start the session
session_start();
?>
<!DOCTYPE html>
<html>
<body>

<?php
// Set session variables
$_SESSION["favcolor"] = "green";
$_SESSION["favanimal"] = "cat";
echo "Session variables are set.";
?>

</body>
</html>
```

Destroy a PHP Session

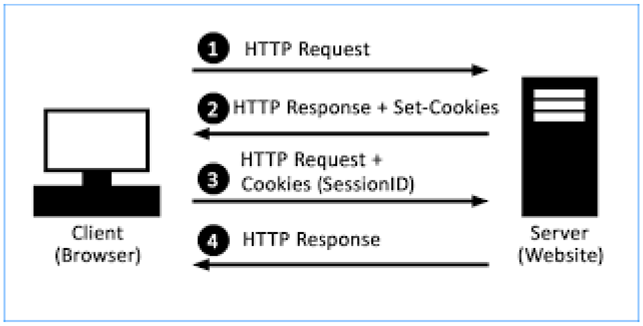
To remove all global session variables and destroy the session, use session_unset() and session_destroy():

Example

```
<?php
session_start();
?>
<!DOCTYPE html>
<html>
<body>

<?php
// remove all session variables
session_unset();

// destroy the session
session_destroy();
?>

</body>
</html>
```

what is cookies?

Cookies are small files of information that a web server generates and sends to a web browser. Web browsers store the cookies they receive for a predetermined period of time, or for the length of a user's session on a website. They attach the relevant cookies to any future requests the user makes of the web server.

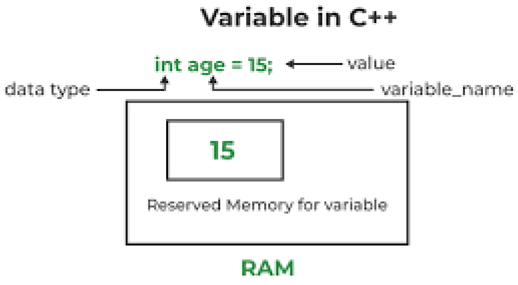


1 HTTP Request
2 HTTP Response + Set-Cookies
3 HTTP Request + Cookies (SessionID)
4 HTTP Response
Client (Browser)
Server (Website)

Variable in c?

In C programming language, a variable is a user-defined or a user-readable custom name assigned to a memory location. Variables hold a value that can be modified and reused many times during the program execution.

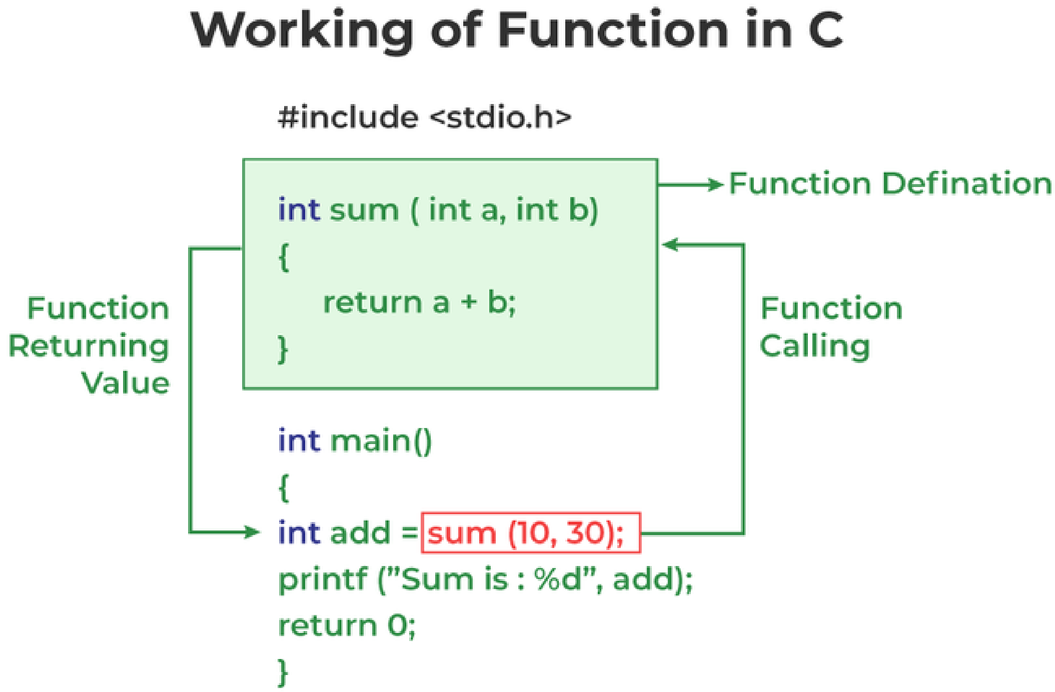
Variables **are containers for storing data values, like** numbers and characters.


Variable in C++

what is built-in function with example in c?

Built-in(Library) Functions:The system provided these functions and stored them in the library. Therefore it is also called Library Functions. e.g. scanf() , printf() , strcpy , strlwr , strcmp , strlen , strcat , etc. You must include the appropriate C header files to use these functions.

A built-in function is a function that is already available in a programming language, application, or another tool that can be accessed by end users


Working of Function in C

```
#include <stdio.h>

int sum ( int a, int b)
{
    return a + b;
}

int main()
{
int add = sum (10, 30);
printf ("Sum is : %d", add);
return 0;
}
```

static and dynamic variable difference in c with example?

Static variables are those whose memory allocation is known at compile time (or it is defined in declaration) as in the example above. Dynamic variables are those memory allocation is not known. It will be known only at the execution time (when the user prints)

Static Variables in C?

Static variables have the property of preserving their value even after they are out of their scope! Hence, a static variable preserves its previous value in its previous scope and is not initialized again in the new scope.

1) A static int variable remains in memory while the program is running. A normal or auto variable is destroyed when a function call where the variable was declared is over.
   For example, we can use static int to count the number of times a function is called, but an auto variable can't be used for this purpos.
2) The below program prints 1 2 because static variables are only initialized once and live till the end of the program. That is why they can retain their value between multiple function calls.

```
// C Program to illustrate the static variable lifetime
#include <stdio.h>

// function with static variable
int fun()
{
    static int count = 0;
    count++;
    return count;
}

int main()
{
    printf("%d ", fun());
    printf("%d ", fun());
    return 0;
}
```

Difference between var, let and const keywords in JavaScript

In JavaScript, users can declare a variable using three keywords that are var, let, and const. The behavior and the scope of a variable are also based on the keyword used to define it.

JavaScript var keyword

The **var** is the oldest keyword to declare a variable in JavaScript. It has the Global scoped or function scoped which means variables defined outside the function can be accessed globally, and variables defined inside a particular function can be accessed within the function.

Example 1: The below code example explains the use of the var keyword to declare the variables in JavaScript.

```
var a = 10
function f() {
    var b = 20
    console.log(a, b)
}
f();
console.log(a)
```

```
10 20

10
```

Example 2: The below example explains the behaviour of var variables when declared inside a function and accessed outside of it.

```
function f() {

    // It can be accessible any
    // where within this function
    var a = 10;
if(true){
    console.log(a)

}
}
f();
```

```
// A cannot be accessible outside of  this function

console.log(a);

Output:
10 10
ReferenceError: a is not defined
```

Example 3: The below code re-declare a variable with same name in the same scope using the var keyword, which gives no error in the case of var keyword.

```
var a = 10

// User can re-declare
// variable using var
var a = 8

// User can update var variable
a = 7
console.log(a);
```

Output

```
7
```

Example 4: The below code explains the hoisting concept with the var keyword variables.

```
  console.log(a);
var a = 10;
```

JavaScript let keyword

The let keyword is an improved version of the var keyword. It is introduced in the ES6 or EcmaScript 2015. These variables has the block scope. It can't be accessible outside the particular code block ({block}).

Example 1: The below code declares the variable using the let keyword.

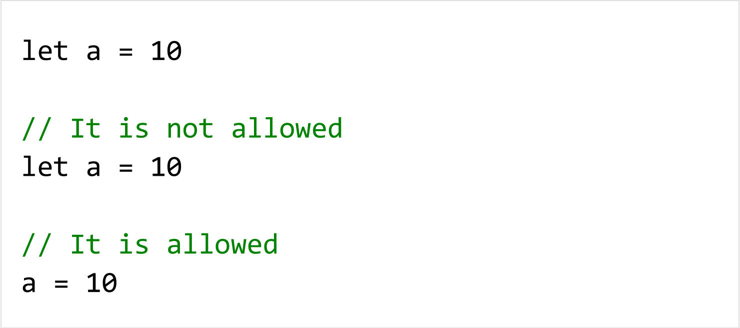
```
let a = 10;
function f() {
    let b = 9
    console.log(b);
    console.log(a);
}
```

```
f()
```

Example 2: The below code explains the block scope of the variables declared using the let keyword.

```
let a = 10;
function f() {
       if (true) {
              let b = 9

              // It prints 9
              console.log(b);
       }

       // It gives error as it
       // defined in if block
       console.log(b);
}
f()

// It prints 10
console.log(a)
```

Example 3: The below code explains the behaviour of let variables when they are re-declared in the same scope.



```
let a = 10

// It is not allowed
let a = 10

// It is allowed
a = 10
```

```
SyntaxError: Identifier 'a' has already been
declared
```

JavaScript const

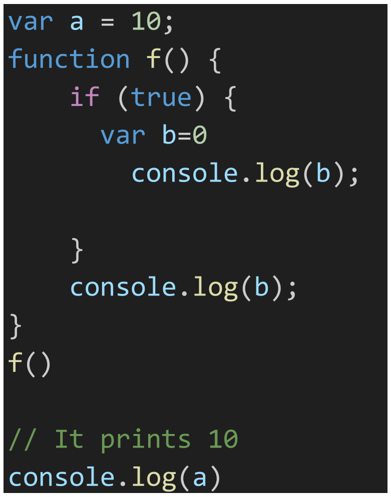
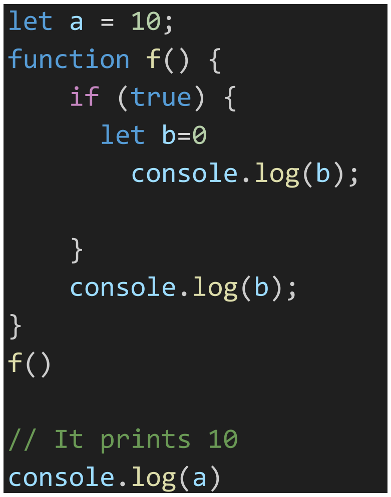
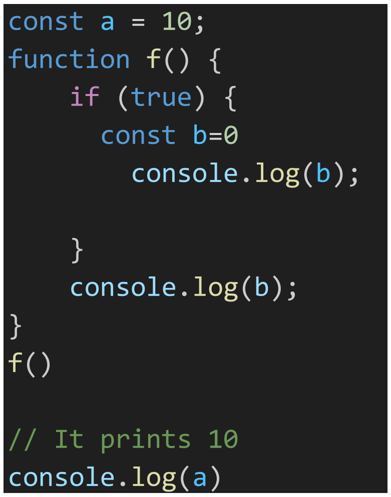
The const keyword has all the properties that are the same as the let keyword, except the user cannot update it and have to assign it with a value at the time of declaration. These variables also have the block scope. It is mainly used to create constant variables whose values can not be changed once they are initialized with a value.

Example 1: This code tries to change the value of the const variable.

```
const a = 10;
 function f() { a = 9 console.log(a) }
 f();
TypeError:Assignment to constant variable.
```

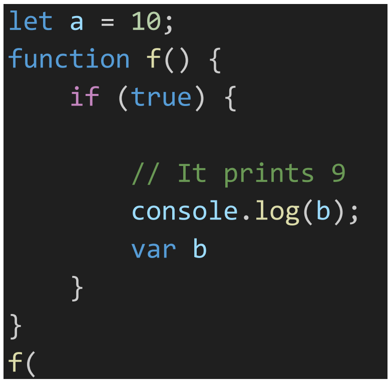
Differences between var, let, and const

var	let	const

The scope of a *var* variable is functional or global scope.

`var a = 10;`
`function f() {`
`    if (true) {`
`      var b=0`
`        console.log(b);`
 	
`    }`
`    console.log(b);`
`}`
`f()`
 	
`// It prints 10`
`console.log(a)`
	The scope of a *let* variable is block scope.
	
	`let a = 10;`
	`function f() {`
	`    if (true) {`
	`      let b=0`
	`        console.log(b);`
	
	`    }`
	`    console.log(b);`
	`}`
	`f()`
	
	`// It prints 10`
	`console.log(a)`
	console.log(b);
	^
	ReferenceError: b is not defined
		The scope of a *const* variable is block scope.
		
		`const a = 10;`
		`function f() {`
		`    if (true) {`
		`      const b=0`
		`        console.log(b);`
		
		`    }`
		`    console.log(b);`
		`}`
		`f()`
		
		`// It prints 10`
		`console.log(a)`
		console.log(b);
		^
		ReferenceError: b is not defined

<table>
<tr><th>var</th><th>let</th><th>const</th></tr>
<tr><td>It can be updated and re-declared in the same scope.</td><td>It can be updated but cannot be re-declared in the same scope.</td><td>It can neither be updated or re-declared in any scope.</td></tr>
<tr><td>It can be declared without initialization.</td><td>It can be declared without initialization.</td><td>It cannot be declared without initialization.</td></tr>
<tr><td>It can be accessed without initialization as its default value is “undefined”.</td><td>It cannot be accessed without initialization otherwise it will give ‘referenceError’.</td><td>It cannot be accessed without initialization, as it cannot be declared without initialization.</td></tr>
<tr><td>

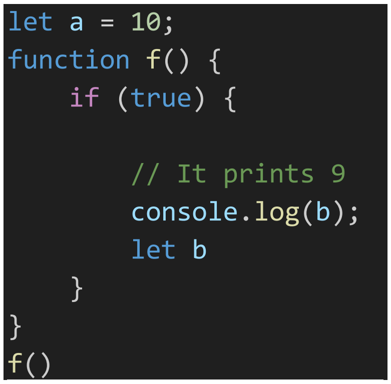
These variables are hoisted(উওলোন) means access variable before declare



```
let a = 10;
function f() {
    if (true) {

        // It prints 9
        console.log(b);
        var b
    }
}
f(
```

</td><td>

These variables are hoisted but stay in the temporal dead zone untill the initialization.

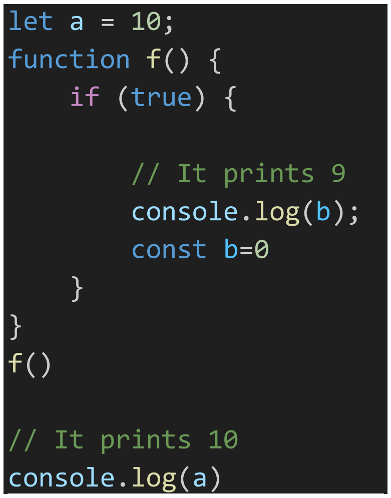


```
let a = 10;
function f() {
    if (true) {

        // It prints 9
        console.log(b);
        let b
    }
}
f()
```

ReferenceError: Cannot access 'b' before initialization

</td><td>

These variables are hoisted but stays in the temporal dead zone until the initialization.



```
let a = 10;
function f() {
    if (true) {

        // It prints 9
        console.log(b);
        const b=0
    }
}
f()

// It prints 10
console.log(a)
```

ReferenceError: Cannot access 'b' before initialization

</td></tr>
</table>

SQL Injection?

SQL injection is a code injection technique that might destroy your database. SQL injection is one of the most common web hacking techniques.

SQL injection is the placement of malicious code in SQL statements, via web page input.

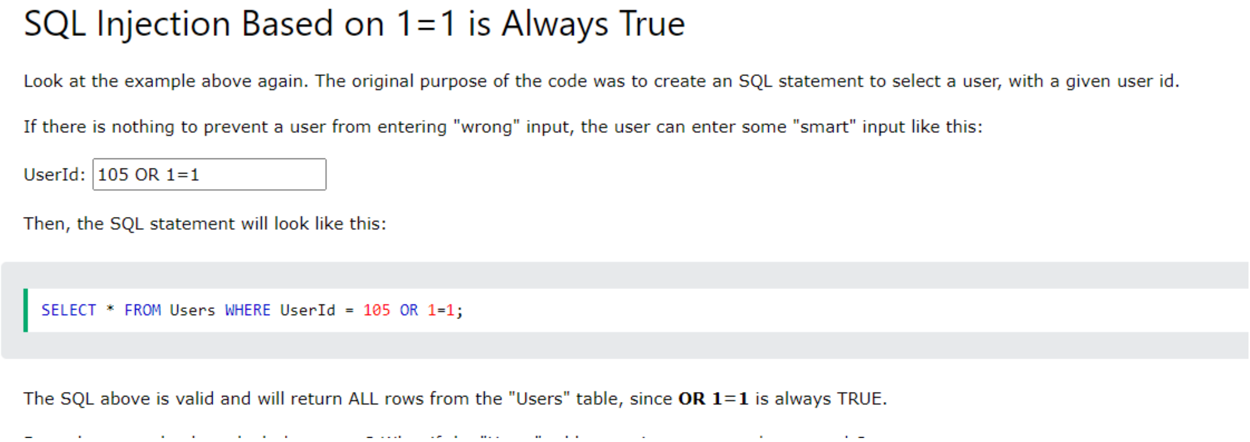
SQL in Web Pages

SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will **unknowingly** run on your database.

Look at the following example which creates a `SELECT` statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):

SQL Injection Based on 1=1 is Always True

```
txtUserId = getRequestString("UserId");
```



SQL Injection Based on 1=1 is Always True

Look at the example above again. The original purpose of the code was to create an SQL statement to select a user, with a given user id.

If there is nothing to prevent a user from entering "wrong" input, the user can enter some "smart" input like this:

UserId: 105 OR 1=1

Then, the SQL statement will look like this:

```
SELECT * FROM Users WHERE UserId = 105 OR 1=1;
```

The SQL above is valid and will return ALL rows from the "Users" table, since **OR 1=1** is always TRUE.

A hacker might get access to all the user names and passwords in a database, by simply inserting 105 OR 1=1 into the input field.

Communication and networking

A network is the combination of two or more computers and their connecting links. A *physical* network is the hardware (equipment such as adapter cards, cables, and telephone lines) that makes up the network. The software and the conceptual model make up the *logical* network. Different types of networks and emulators provide different functions.

A computer network is a collection of computers or devices connected to share resources. Any device which can share or receive the data is called a Node. Through which the information or data propagate is known as channels, It can be guided or unguided.

In general, Computer Network is a collection of two or more computers.

Basics of Computer Networking

Computer Networking is the practice of connecting computers together to enable communication and data exchange between them. In general, Computer Network is a collection of two or more computers. It helps users to communicate more easily. In this article, we are going to discuss the basics which everyone must know before going deep into Computer Networking.

Data Communication – Definition, Components, Types, Channels

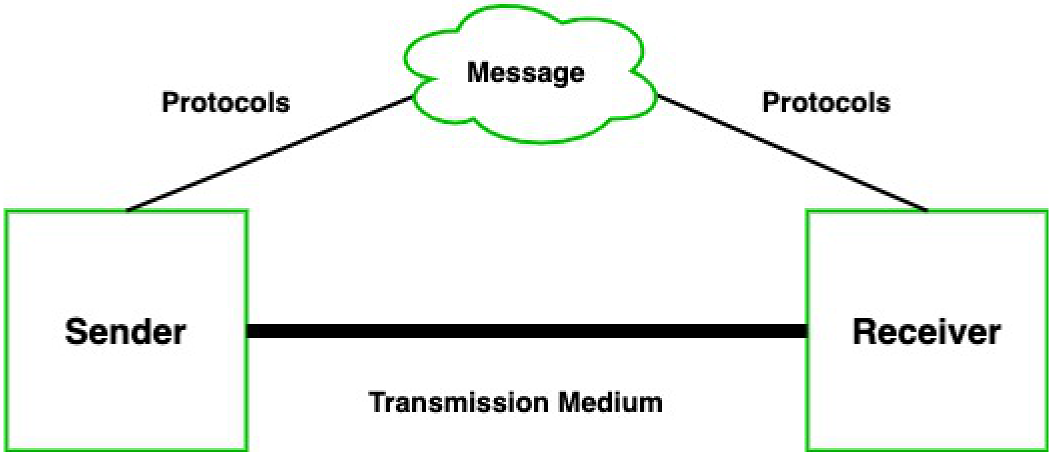
Communication is defined as a process in which more than one computer transfers information, instructions to each other and for sharing resources. Or in other words, communication is a process or act in which we can send or receive data. A network of computers is defined as an interconnected collection of autonomous computers. Autonomous means no computer can start, stop or control another computer.

Components of Data Communication

A communication system is made up of the following components:

1. **Message:** A message is a piece of information that is to be transmitted from one person to another. It could be a text file, an audio file, a video file, etc.
2. **Sender:** It is simply a device that sends data messages. It can be a computer, mobile, telephone, laptop, video camera, or workstation, etc.
3. **Receiver:** It is a device that receives messages. It can be a computer, telephone mobile, workstation, etc.
4. **Transmission Medium / Communication Channels:** Communication channels are the medium that connect two or more workstations. Workstations can be connected by either wired media or wireless media.
5. **Set of rules (Protocol):** When someone sends the data (The sender), it should be understandable to the receiver also otherwise it is meaningless.

For example, Sonali sends a message to Chetan. If Sonali writes in Hindi and Chetan cannot understand Hindi, it is a meaningless conversation.



Therefore, there are some set of rules (protocols) that is followed by every computer connected to the internet and they are:

- **TCP(Transmission Control Protocol)**: It is responsible for dividing messages into packets on the source computer and reassembling the received packet at the destination or recipient computer. It also makes sure that the packets have the information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination.
- **IP(Internet Protocol)**: Do You ever wonder how computer determines which packet belongs to which device. What happens if the message you sent to your friend is received by your father? Scary Right. Well! IP is responsible for handling the address of the destination computer so that each packet is sent to its proper destination.

Type of data communication

As we know that data communication is communication in which we can send or receive data from one device to another. The data communication is divided into three types:

1. **Simplex Communication:** It is one-way communication or we can say that unidirectional communication in which one device only receives and another device only sends data and devices uses their entire capacity in transmission. For example, IoT, entering data using a keyboard, listing music using a speaker, etc.

2. **Half Duplex communication:** It is a two-way communication, or we can say that it is a bidirectional communication in which both the devices can send and receive data but not at the same time. When one device is sending data then another device is only receiving and vice-versa. For example, walkie-talkie.
3. **Full-duplex communication:** It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data at the same time. For example, mobile phones, landlines, etc.

Communication Channels

Communication channels are the medium that connects two or more workstations. Workstations can be connected by either wired media or wireless media. It is also known as a transmission medium. The transmission medium or channel is a link that carries messages between two or more devices. We can group the communication media into two categories:

- Guided media transmission
- Unguided media transmission

1. Guided Media: In this transmission medium, the physical link is created using wires or cables between two or more computers or devices, and then the data is transmitted using these cables in terms of signals. Guided media transmission of the following types:

1. Twisted pair cable: It is the most common form of wire used in communication. In a twisted-pair cable, two identical wires are wrapped together in a double helix. The twisting of the wire reduces the crosstalk. It is known as the leaking of a signal from one wire to another due to which signal can corrupt and can cause network errors. The twisting protects the wire from internal crosstalk as well as external forms of signal interference. Types of Twisted Pair Cable :

- **Unshielded Twisted Pair (UTP):** It is used in computers and telephones widely. As the name suggests, there is no external shielding so it does not protects from external interference. It is cheaper than STP.
- **Shielded Twisted Pair (STP):** It offers greater protection from crosstalk due to shield. Due to shielding, it protects from external interference. It is heavier and costlier as compare to UTP.

2. Coaxial Cable: It consists of a solid wire core that is surrounded by one or more foil or wire shields. The inner core of the coaxial cable carries the signal and the outer shield provides the ground. It is widely used for television signals and also used by large corporations in building security systems. Data transmission of this cable is better but expensive as compared to twisted pair.

3. Optical fibers: Optical fiber is an important technology. It transmits large amounts of data at very high speeds due to which it is widely used in internet cables. It carries data as a light that travels inside a thin glass fiber. The fiber optic cable is made up of three pieces:

1. **Core:** Core is the piece through which light travels. It is generally created using glass or plastic.
2. **Cladding:** It is the covering of the core and reflects the light back to the core.
3. **Sheath:** It is the protective covering that protects fiber cable from the environment.

2. Unguided Media: The unguided transmission media is a transmission mode in which the signals are propagated from one device to another device wirelessly. Signals can wave through the air, water, or vacuum. It is generally used to transmit signals in all directions. Unguided Media is further divided into various parts :

1. Microwave: Microwave offers communication without the use of cables. Microwave signals are just like radio and television signals. It is used in long-distance communication. Microwave transmission consists of a transmitter, receiver, and atmosphere. In microwave communication, there are parabolic antennas that are mounted on the towers to send a beam to another antenna. The higher the tower, the greater the range.

2. Radio wave: When communication is carried out by radio frequencies, then it is termed radio waves transmission. It offers mobility. It is consists of the transmitter and the receiver. Both use antennas to radiate and capture the radio signal.

3. Infrared: It is short-distance communication and can pass through any object. It is generally used in TV remotes, wireless mouse, etc.

Types of Computer Networks

Pre-Requisite: Computer Networking

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.

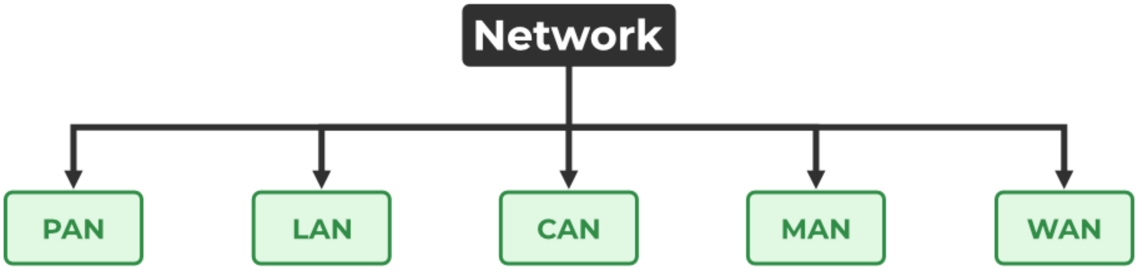
Uses of Computer Networks

- 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

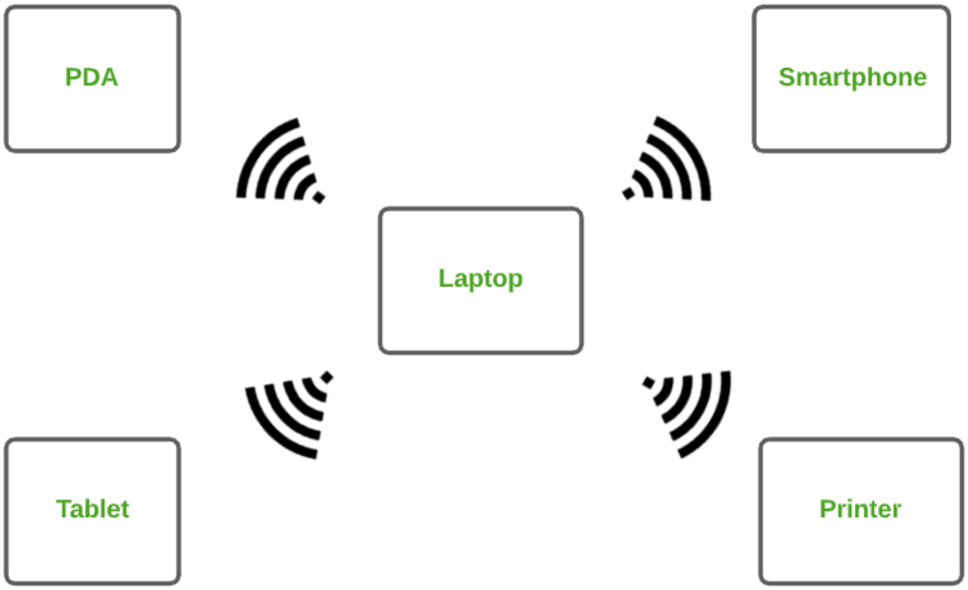
These are explained below.

1. Personal Area Network (PAN)

PAN is the most basic type of computer network. This network is restrained to a single person, that is, communication between the computer devices is centered only on an individual’s workspace. 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.

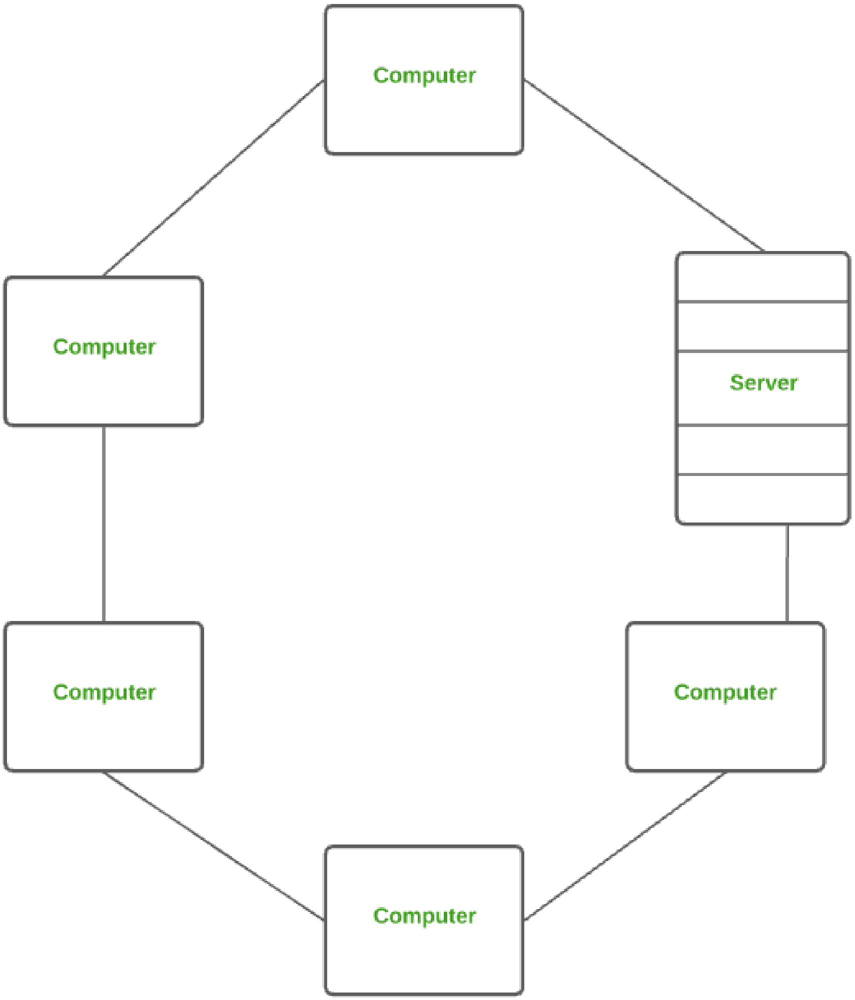


Personal Area Network (PAN)

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.

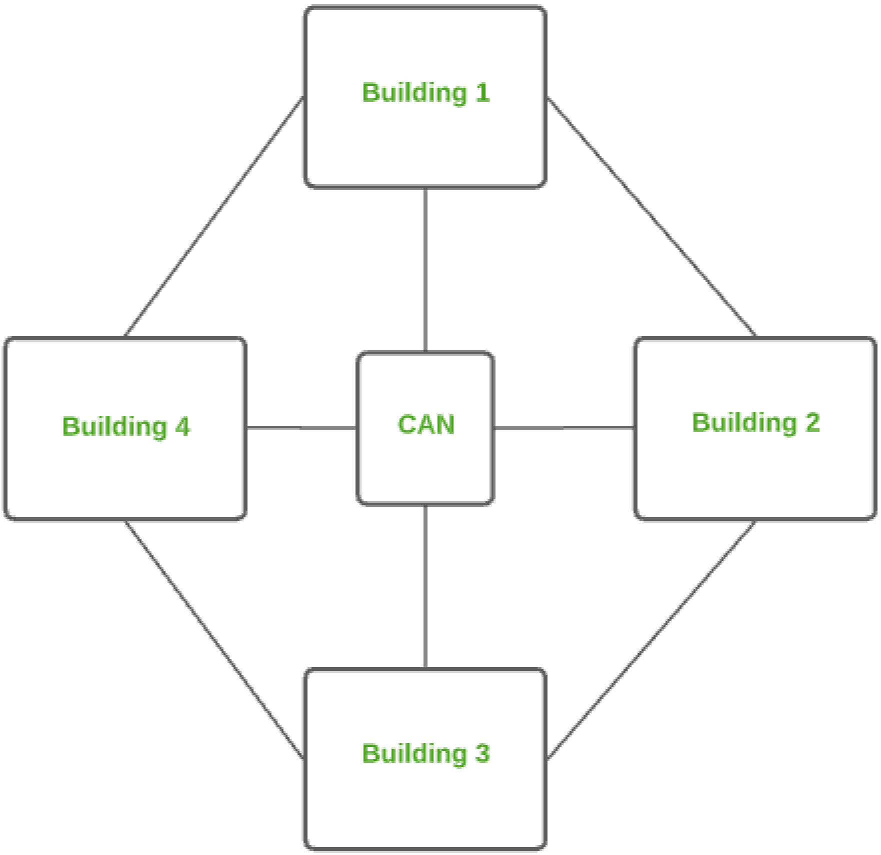


Local Area Network (LAN)

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.

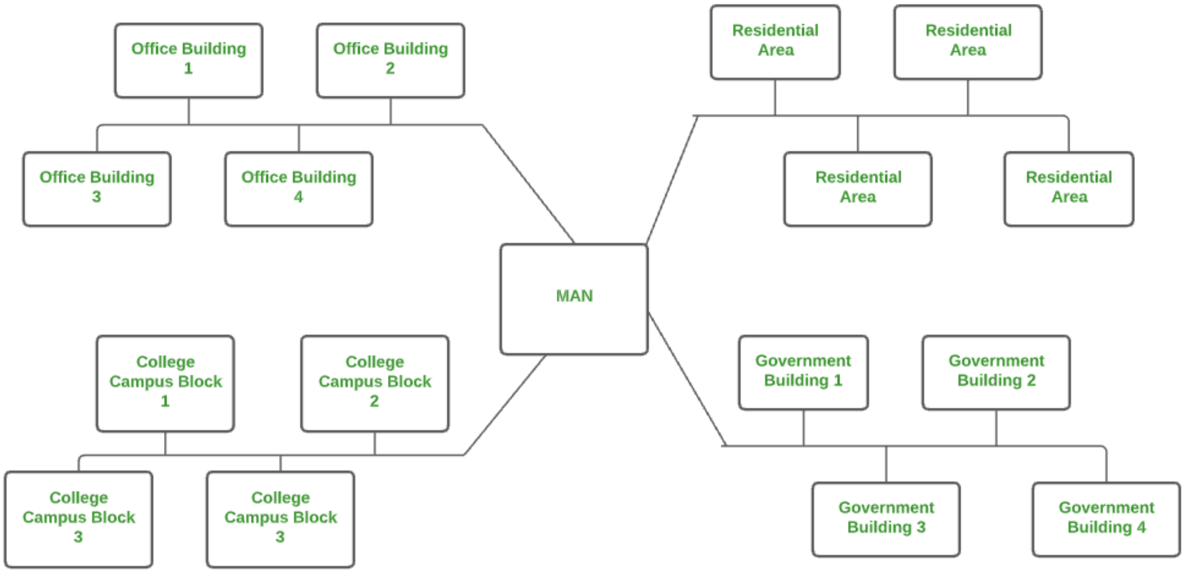
Examples of CAN are networks that cover schools, colleges, buildings, etc.



Campus Area Network (CAN)

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.

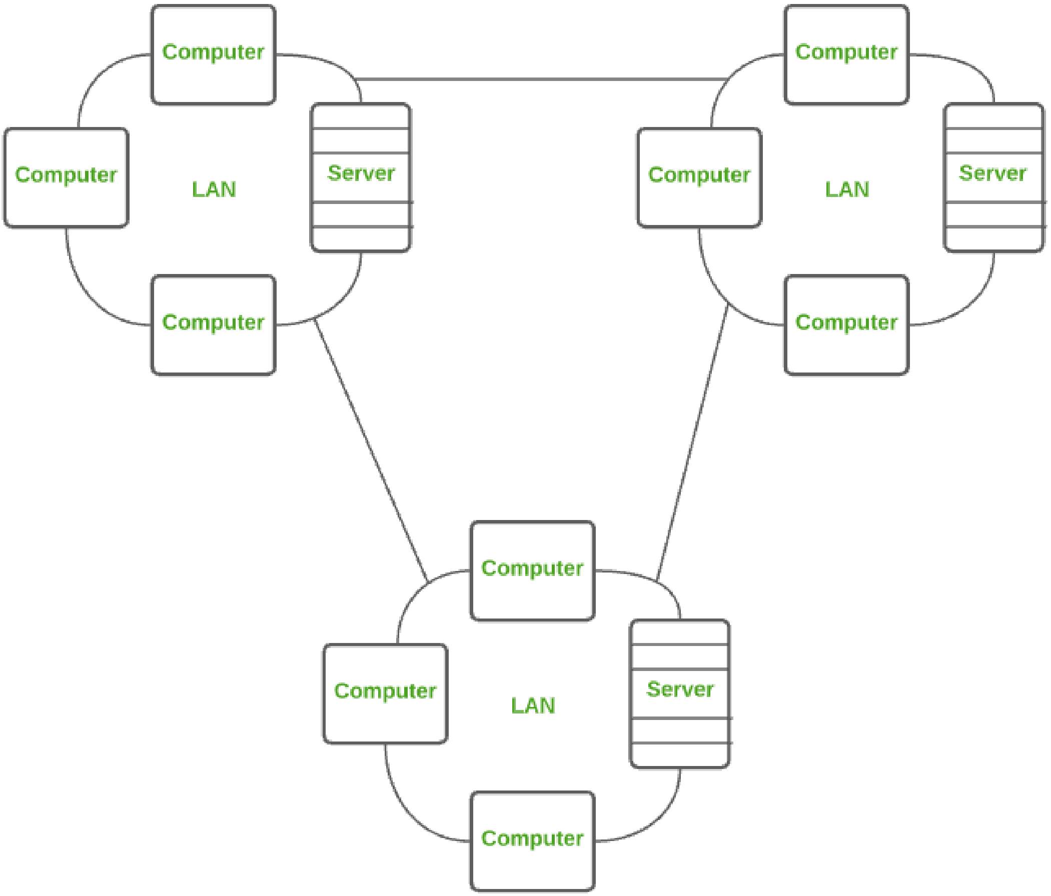


Metropolitan Area Network (MAN)

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)

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	Wide Area Network
Technology	Bluetooth, IrDA,Zigbee	Ethernet & Wifi	Ethernet	FDDI, CDDi. ATM	Leased Line, Dial-Up

Parameters	**PAN**	**LAN**	**CAN**	**MAN**	**WAN**
Range	1-100 m	Upto 2km	1 – 5 km	5-50 km	Above 50 km
Transmission Speed	Very High	Very High	High	Average	Low
Ownership	Private	Private	Private	Private or Public	Private or Public
Maintenance	Very Easy	Easy	Moderate	Difficult	Very Difficult
Cost	Very Low	Low	Moderate	High	Very High

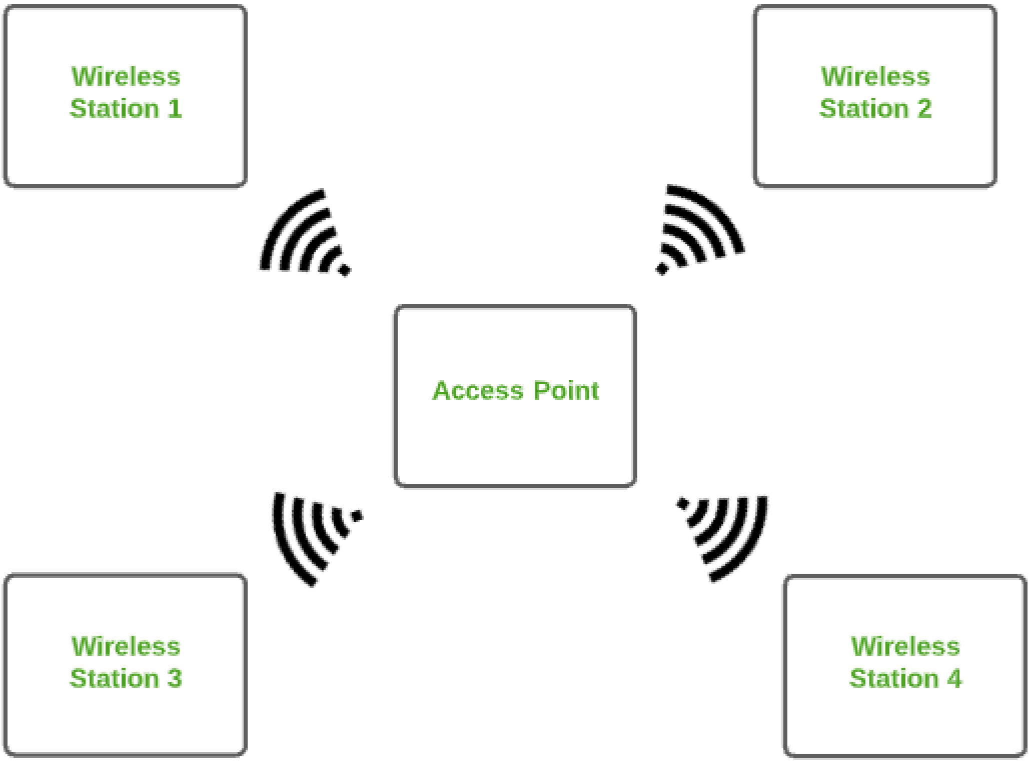
Other Types of Computer Networks

1. Wireless Local Area Network (WLAN)
2. Storage Area Network (SAN)
3. System-Area Network (SAN)
4. Passive Optical Local Area Network (POLAN)
5. Enterprise Private Network (EPN)
6. Virtual Private Network (VPN)
7. 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.



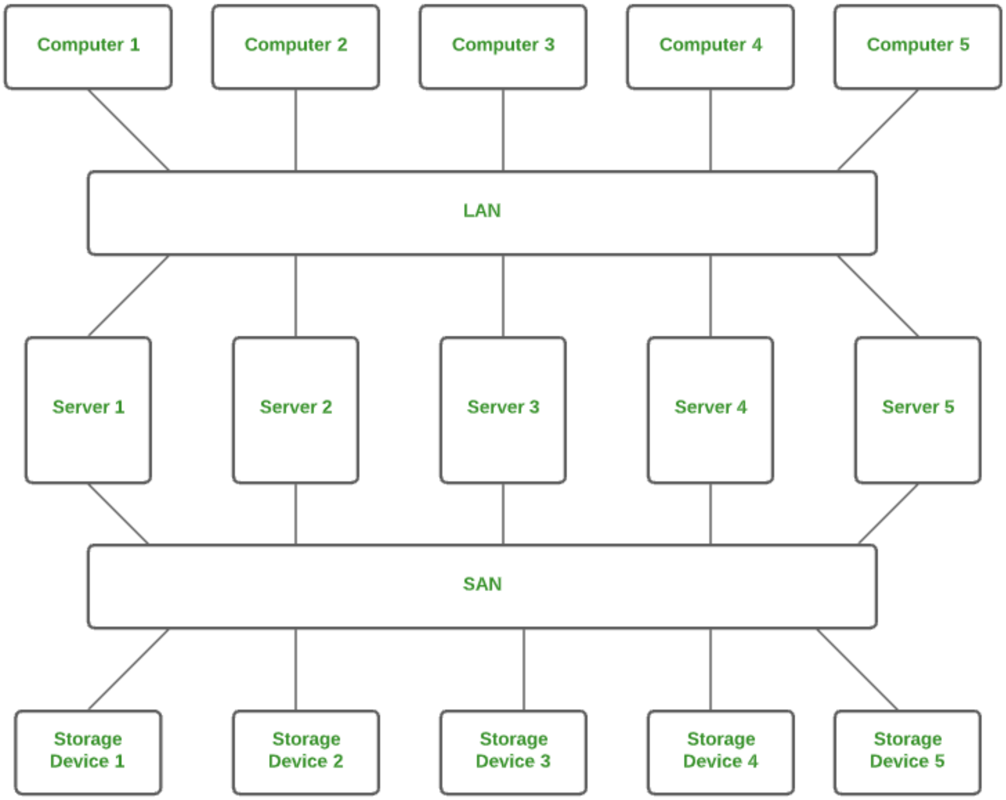
Wireless Local Area Network (WLAN)

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.

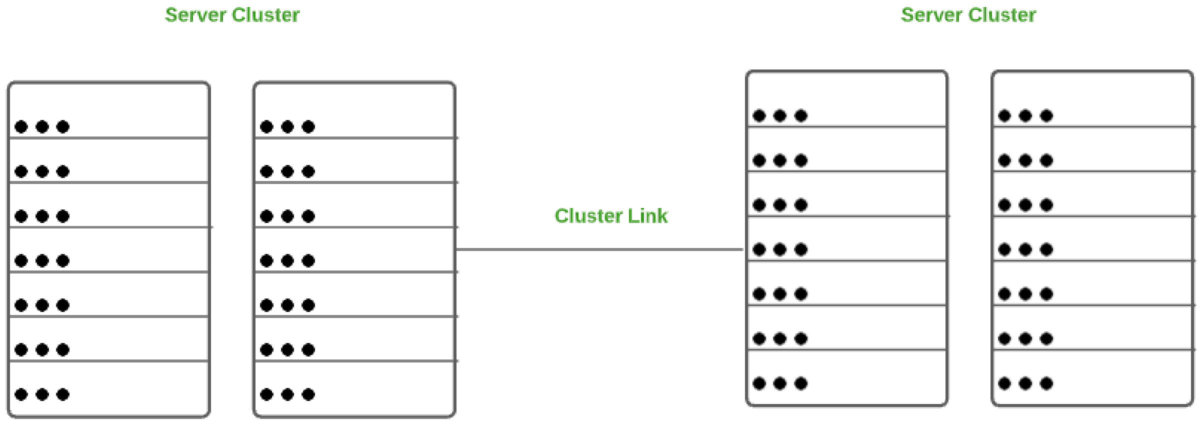


Storage Area Network (SAN)

3. System Area Network (SAN)

A SAN is a type of computer network that connects a cluster of high-performance computers. It is a connection-oriented and high-bandwidth network. A SAN is a type of LAN that handles high amounts of information in large requests. This network is useful for processing applications that require high network performance.

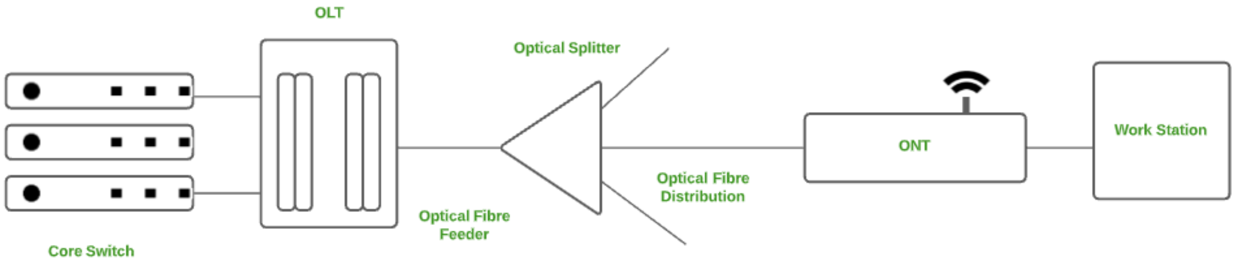
Microsoft SQL Server 2005 uses SAN through a virtual interface adapter.



System Area Network (SAN)

4. Passive Optical Local Area Network (POLAN)

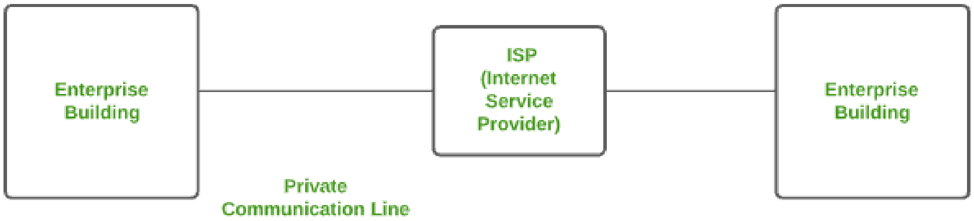
A POLAN is a type of computer network that is an alternative to a LAN. POLAN uses optical splitters to split an optical signal from a single strand of single-mode optical fiber to multiple signals to distribute users and devices. In short, POLAN is a point to multipoint LAN architecture.



Passive Optical Local Area Network (POLAN)

5. Enterprise Private Network (EPN)

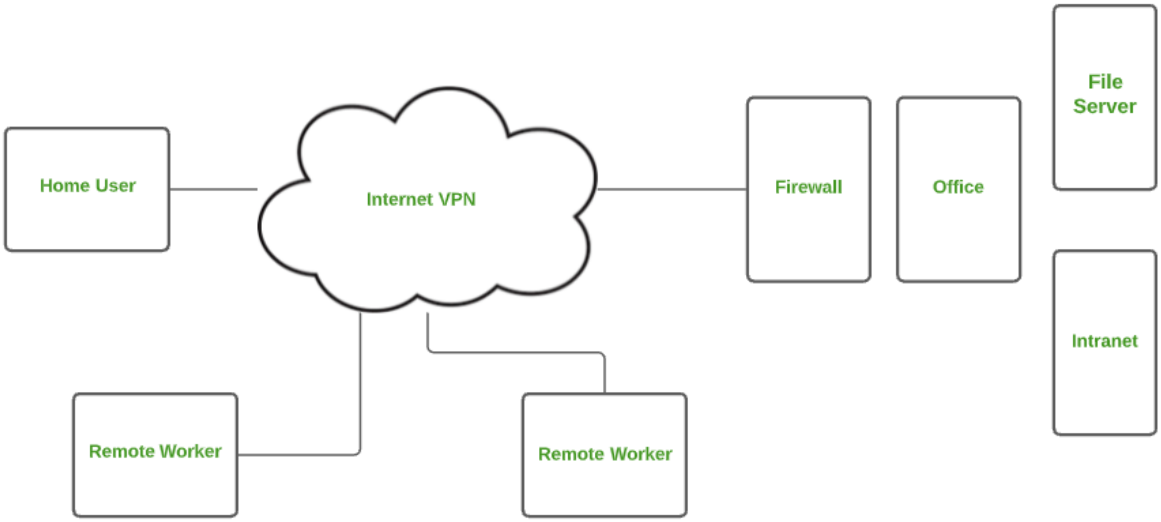
EPN is a type of computer network mostly used by businesses that want a secure connection over various locations to share computer resources.



Enterprise Private Network (EPN)

6. Virtual Private Network (VPN)

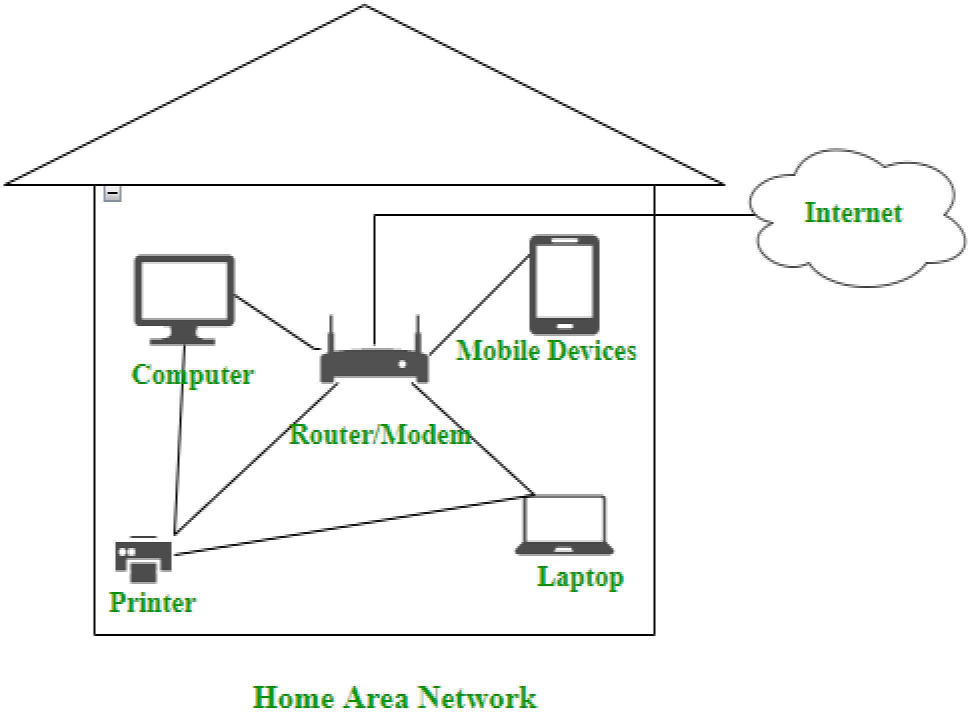
A VPN is a type of computer network that extends a private network across the internet and lets the user send and receive data as if they were connected to a private network even though they are not. Through a virtual point-to-point connection users can access a private network remotely. VPN protects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



Virtual Private Network (VPN)

7. 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)

Advantages of Computer Network

Some of the main advantages of Computer Networks are:

- **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

Some of the main disadvantages of Computer Networks are:

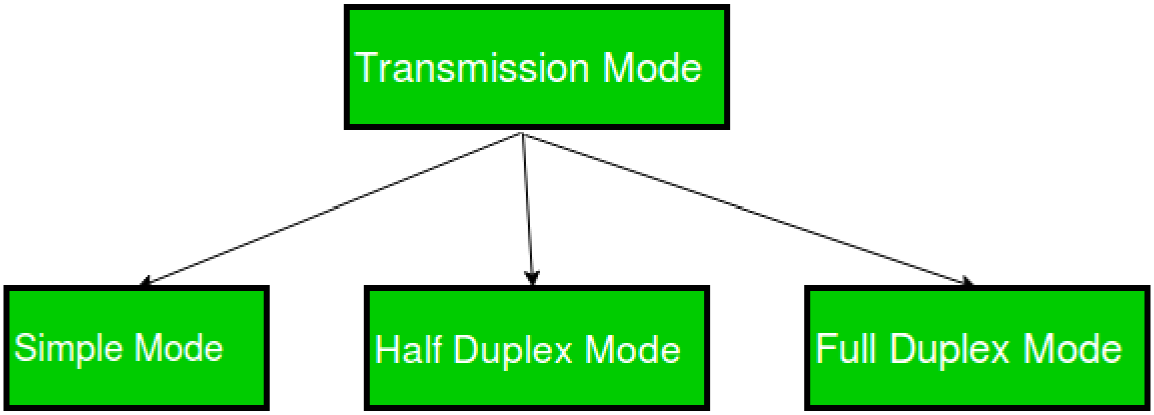
- **Virus and Malware:** A virus is a program that can infect other programs by modifying them. Viruses and Malware can corrupt the whole network.
- **High Cost of Setup:** The initial setup of Computer Networking is expensive because it consists of a lot of wires and cables along with the device.

- **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.

Transmission Modes in Computer Networks (Simplex, Half-Duplex and Full-Duplex)

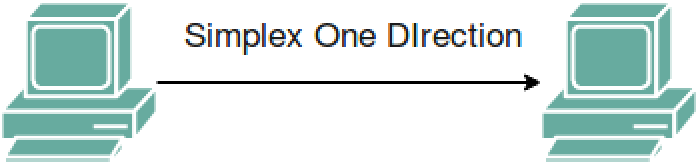
Transmission mode means transferring data between two devices. It is also known as a communication mode. Buses and networks are designed to allow communication to occur between individual devices that are interconnected.

There are three types of transmission mode:-



These are explained as following below.

1. Simplex Mode –
In Simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit, the other can only receive. The simplex mode can use the entire capacity of the channel to send data in one direction.
Example: Keyboard and traditional monitors. The keyboard can only introduce input, the monitor can only give the output.



Advantages:

- Simplex mode is the easiest and most reliable mode of communication.
- It is the most cost-effective mode, as it only requires one communication channel.
- There is no need for coordination between the transmitting and receiving devices, which simplifies the communication process.
- Simplex mode is particularly useful in situations where feedback or response is not required, such as broadcasting or surveillance.

Disadvantages:

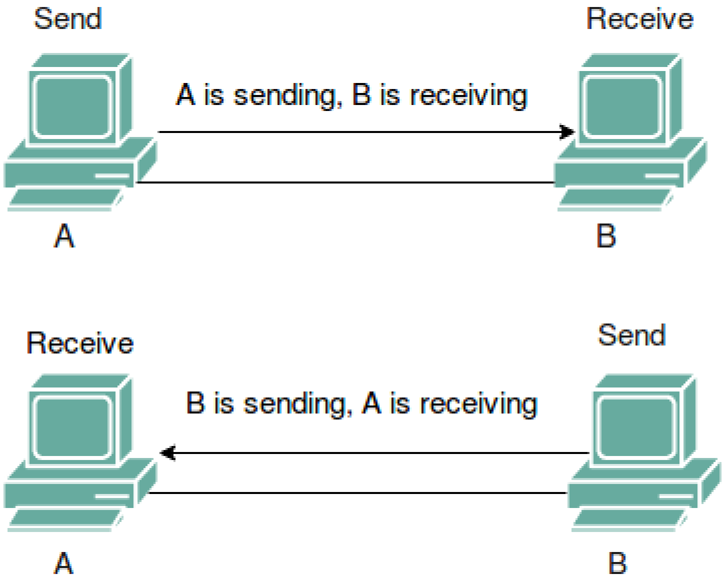
- Only one-way communication is possible.
- There is no way to verify if the transmitted data has been received correctly.
- Simplex mode is not suitable for applications that require bidirectional communication.

2. Half-Duplex Mode –

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is used in cases where there is no need for communication in both directions at the same time. The entire capacity of the channel can be utilized for each direction.

Example: Walkie-talkie in which message is sent one at a time and messages are sent in both directions.

```
Channel capacity=Bandwidth * Propagation Delay
```



Advantages:

- Half-duplex mode allows for bidirectional communication, which is useful in situations where devices need to send and receive data.

- It is a more efficient mode of communication than simplex mode, as the channel can be used for both transmission and reception.
- Half-duplex mode is less expensive than full-duplex mode, as it only requires one communication channel.

Disadvantages:

- Half-duplex mode is less reliable than Full-Duplex mode, as both devices cannot transmit at the same time.
- There is a delay between transmission and reception, which can cause problems in some applications.
- There is a need for coordination between the transmitting and receiving devices, which can complicate the communication process.

3. Full-Duplex Mode –

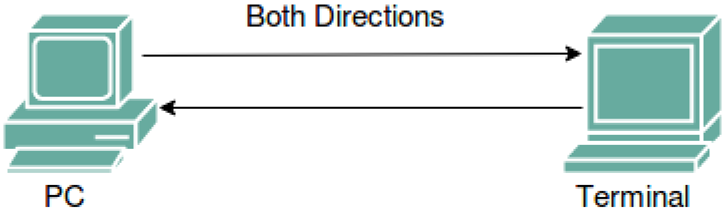
In full-duplex mode, both stations can transmit and receive simultaneously. In full_duplex mode, signals going in one direction share the capacity of the link with signals going in another direction, this sharing can occur in two ways:

- Either the link must contain two physically separate transmission paths, one for sending and the other for receiving.
- Or the capacity is divided between signals traveling in both directions.

Full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

Example: Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.

```
Channel Capacity=2* Bandwidth*propagation Delay
```



Advantages:

- Full-duplex mode allows for simultaneous bidirectional communication, which is ideal for real-time applications such as video conferencing or online gaming.
- It is the most efficient mode of communication, as both devices can transmit and receive data simultaneously.
- Full-duplex mode provides a high level of reliability and accuracy, as there is no need for error correction mechanisms.

Disadvantages:

- Full-duplex mode is the most expensive mode, as it requires two communication channels.
- It is more complex than simplex and half-duplex modes, as it requires two physically separate transmission paths or a division of channel capacity.
- Full-duplex mode may not be suitable for all applications, as it requires a high level of bandwidth and may not be necessary for some types of communication.

Computer Networking

How Does a Computer Network Work?

Basics building blocks of a Computer network are Nodes and Links. A Network Node can be illustrated as Equipment for Data Communication like a Modem, Router, etc., or Equipment of a Data Terminal like connecting two computers or more. Link in

Computer Networks can be defined as wires or cables or free space of wireless networks.

The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate. Each device has an IP Address, that helps in identifying a device.

Basic Terminologies of Computer Networks

- **Network:** A network is a collection of computers and devices that are connected together to enable communication and data exchange.
- **Nodes:** Nodes are devices that are connected to a network. These can include computers, Servers, Printers, Routers, Switches, and other devices.
- **Protocol:** A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include TCP/IP, HTTP, and FTP.
- **Topology:** Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree.
- **Service Provider Networks:** These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.
- **IP Address**: An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.
- **DNS:** The Domain Name System (DNS) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.
- **Firewall:** A firewall is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

Types of Enterprise Computer Networks

- **LAN:** A Local Area Network (LAN) is a network that covers a small area, such as an office or a home. LANs are typically used to connect computers and other devices within a building or a campus.
- **WAN:** A Wide Area Network (WAN) is a network that covers a large geographic area, such as a city, country, or even the entire world. WANs are used to connect LANs together and are typically used for long-distance communication.
- **Cloud Networks:** Cloud Networks can be visualized with a Wide Area Network (WAN) as they can be hosted on public or private cloud service providers and cloud networks are available if there is a demand. Cloud Networks consist of Virtual Routers, Firewalls, etc.

These are just a few basic concepts of computer networking. Networking is a vast and complex field, and there are many more concepts and technologies involved in building and maintaining networks. Now we are going to discuss some more concepts on Computer Networking.

- **Open system:** A system that is connected to the network and is ready for communication.
- **Closed system:** A system that is not connected to the network and can't be communicated with.

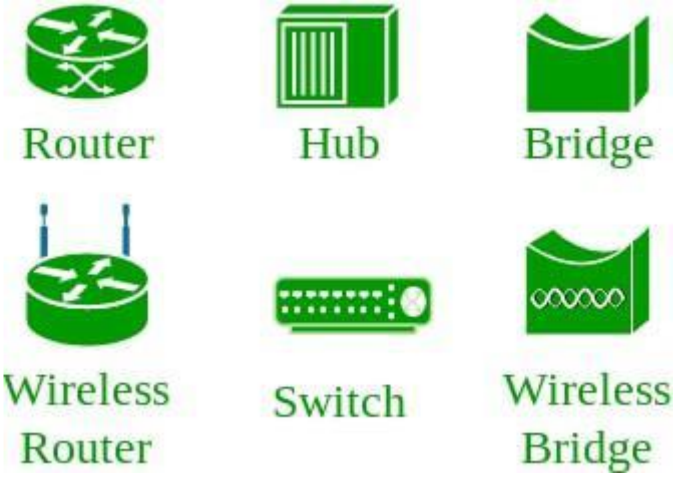
Types of Computer Network Architecture

Computer Network falls under these broad Categories:

- **Client-Server Architecture:** Client-Server Architecture is a type of Computer Network Architecture in which Nodes can be Servers or Clients. Here, the server node can manage the Client Node Behaviour.
- **Peer-to-Peer Architecture:** In P2P (Peer-to-Peer) Architecture, there is not any concept of a Central Server. Each device is free for working as either client or server.

Network Devices

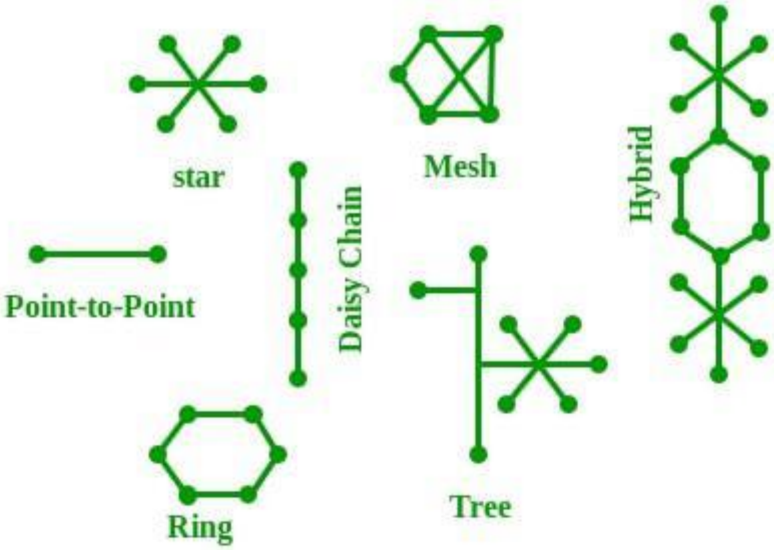
An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as Network devices and include things such as routers, switches, hubs, and bridges.



Network Devices

Network Topology

The Network Topology is the layout arrangement of the different devices in a network. Common examples include Bus, Star, Mesh, Ring, and Daisy chain.



Network Topology

OSI Model

OSI stands for Open Systems Interconnection. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer. The OSI has been developed by the International Organization For Standardization and it is 7 layer architecture. Each layer of OSI has different functions and each layer has to follow different protocols. The 7 layers are as follows:

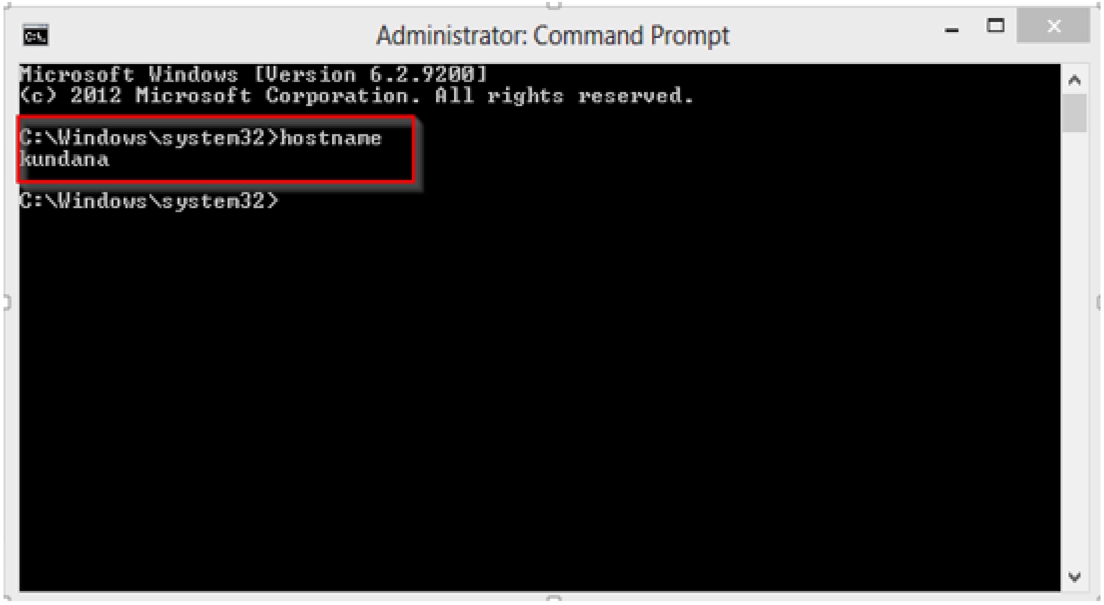
- Physical Layer
- Data link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Protocol

A protocol is a set of rules or algorithms which define the way how two entities can communicate across the network and there exists a different protocol defined at each layer of the OSI model. A few such protocols are TCP, IP, UDP, ARP, DHCP, FTP, and so on.

Unique Identifiers of Network

Hostname: Each device in the network is associated with a unique device name known as Hostname. Type "hostname" in the command prompt(Administrator Mode) and press ‘Enter’, this displays the hostname of your machine.



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
kundana

C:\Windows\system32>
```

HostName

IP Address (Internet Protocol address): Also known as the Logical Address, the IP Address is the network address of the system across the network. To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet. The length of an IPv4 address is 32 bits, hence, we have 2^{32} IP addresses available. The length of an IPv6 address is 128 bits. Type “ipconfig” in the command prompt and press ‘Enter’, this gives us the IP address of the device.

MAC Address (Media Access Control address): Also known as physical address, the MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card). A MAC address is assigned to the NIC at the time of manufacturing. The length of the MAC address is: 12-nibble/ 6 bytes/ 48 bits Type “ipconfig/all” in the command prompt and press ‘Enter’, this gives us the MAC address.

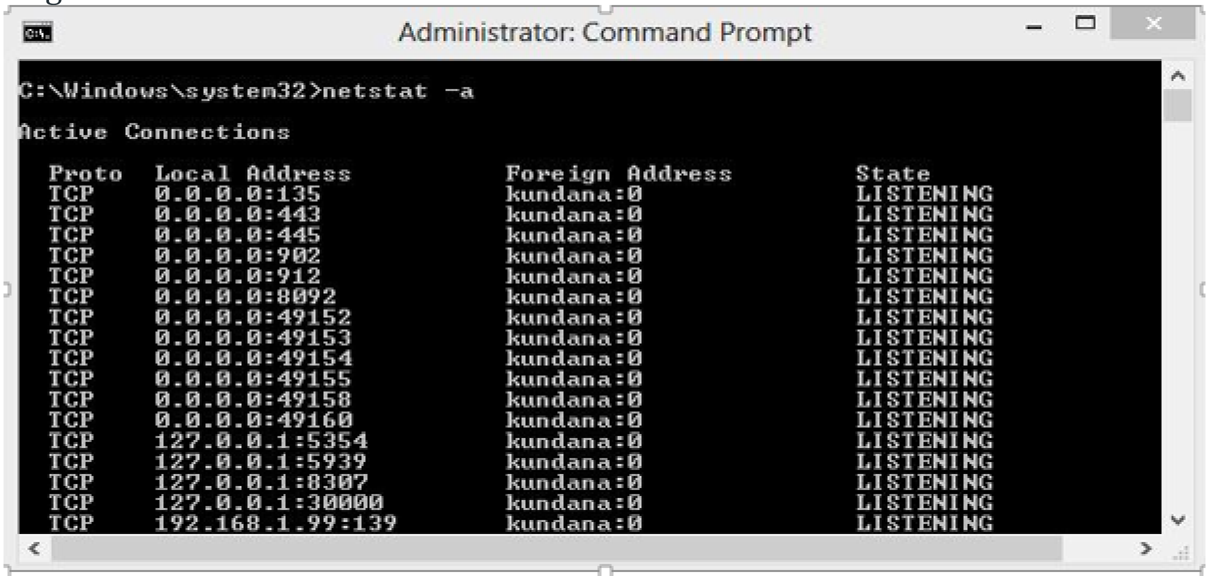
Port: A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

A port number is a 16-bit integer, hence, we have 2^{16} ports available which are categorized as shown below:

Port Types	Range
Well known Ports	0 – 1023
Registered Ports	1024 – 49151
Ephemeral Ports	49152 – 65535

Number of ports: 65,536
Range: 0 – 65535

Type “**netstat -a**” in the command prompt and press ‘Enter’, this lists all the ports being used.



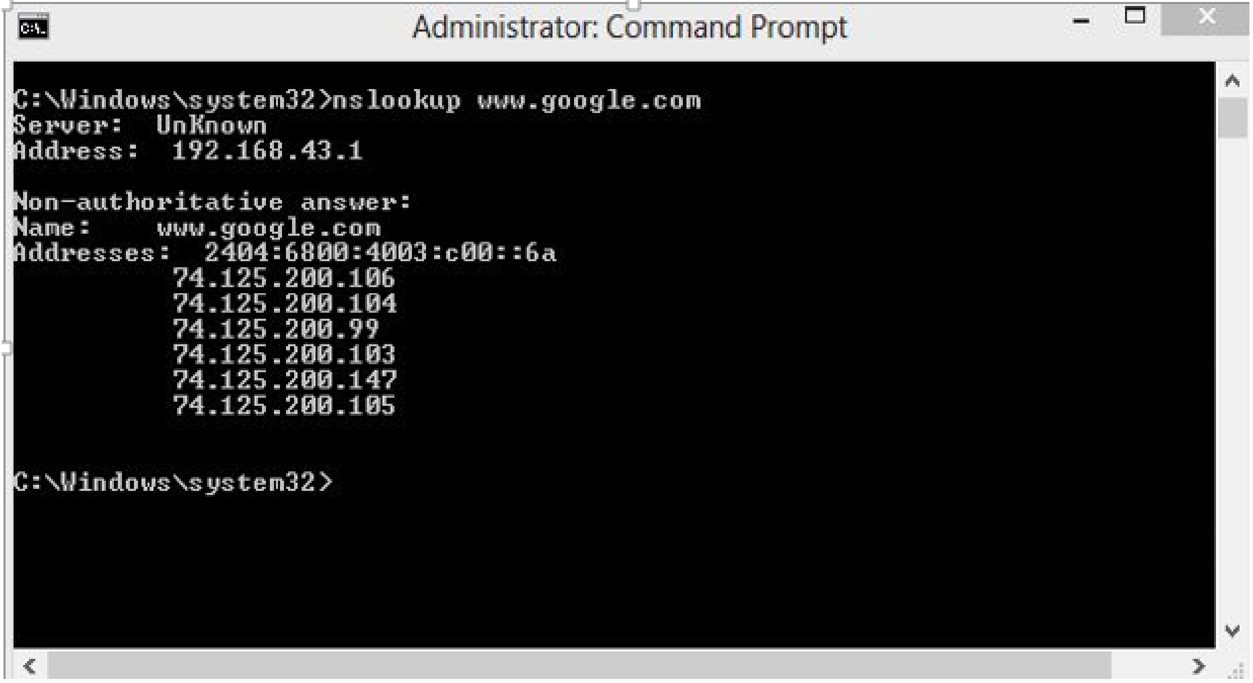
```
C:\Windows\system32>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            kundana:0              LISTENING
  TCP    0.0.0.0:443            kundana:0              LISTENING
  TCP    0.0.0.0:445            kundana:0              LISTENING
  TCP    0.0.0.0:902            kundana:0              LISTENING
  TCP    0.0.0.0:912            kundana:0              LISTENING
  TCP    0.0.0.0:8092           kundana:0              LISTENING
  TCP    0.0.0.0:49152          kundana:0              LISTENING
  TCP    0.0.0.0:49153          kundana:0              LISTENING
  TCP    0.0.0.0:49154          kundana:0              LISTENING
  TCP    0.0.0.0:49155          kundana:0              LISTENING
  TCP    0.0.0.0:49158          kundana:0              LISTENING
  TCP    0.0.0.0:49160          kundana:0              LISTENING
  TCP    127.0.0.1:5354         kundana:0              LISTENING
  TCP    127.0.0.1:5939         kundana:0              LISTENING
  TCP    127.0.0.1:8307         kundana:0              LISTENING
  TCP    127.0.0.1:30000        kundana:0              LISTENING
  TCP    192.168.1.99:139       kundana:0              LISTENING
```

List of Ports

Socket: The unique combination of IP address and Port number together is termed a Socket.

Other Related Concepts

DNS Server: DNS stands for **Domain Name System**. DNS is basically a server that translates web addresses or URLs (ex: www.google.com) into their corresponding IP addresses. We don’t have to remember all the IP addresses of each and every website. The command ‘**nslookup**’ gives you the IP address of the domain you are looking for. This also provides information on our DNS Server. \



```
C:\Windows\system32>nslookup www.google.com
Server:  UnKnown
Address:  192.168.43.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4003:c00::6a
          74.125.200.106
          74.125.200.104
          74.125.200.99
          74.125.200.103
          74.125.200.147
          74.125.200.105


C:\Windows\system32>
```

Domain IP Address

ARP: ARP stands for **Address Resolution Protocol.** It is used to convert an IP address to its corresponding physical address(i.e., MAC Address). ARP is used by the Data Link Layer to identify the MAC address of the Receiver’s machine.
RARP: RARP stands for **Reverse Address Resolution Protocol**. As the name suggests, it provides the IP address of the device given a physical address as input. But RARP has become obsolete since the time DHCP has come into the picture.

Types of Network Topology

In Computer Network ,there are various ways through which different components are connected to one another. **Network Topology** is the way that defines the structure, and how these components are connected to each other.

Types of Network Topology

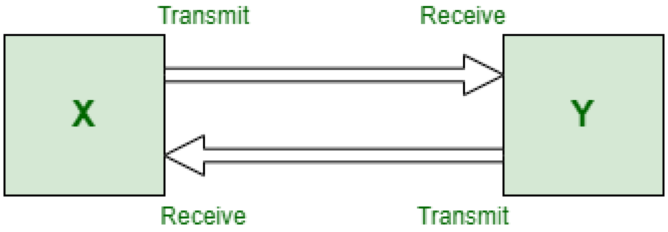
The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**. The various network topologies are:

- Point to Point Topology
- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology

- Tree Topology
- Hybrid Topology

Point to Point Topology

Point-to-Point Topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.

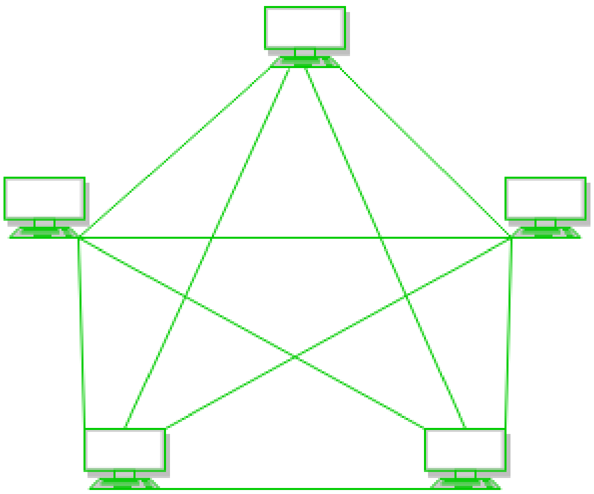


Point to Point Topology

Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.

-
-
-
-
-
-
-
-
-



Mesh Topology

Figure 1: Every device is connected to another via dedicated channels. These channels are known as links.

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N * (N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them

is $^{N}C_{2}$ i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.

Advantages of Mesh Topology

- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Drawbacks of Mesh Topology

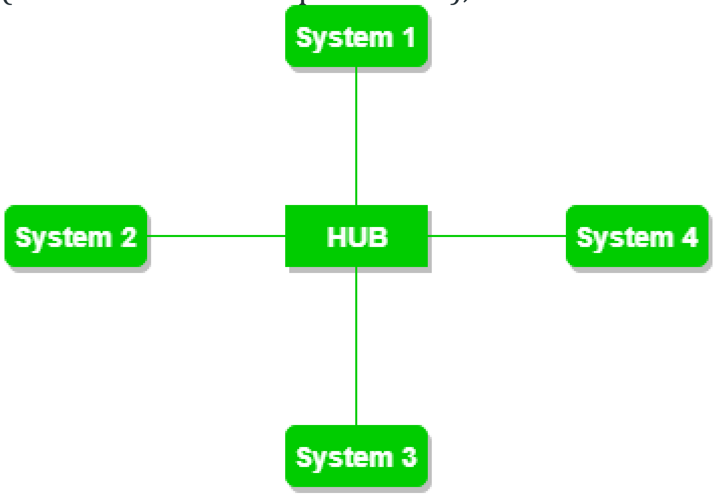
- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication systems and aircraft navigation systems.

For more, refer to the Advantages and Disadvantages of Mesh Topology.

Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



Star Topology

Figure 2: A star topology having four systems connected to a single point of connection i.e. hub.

Advantages of Star Topology

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Drawbacks of Star Topology

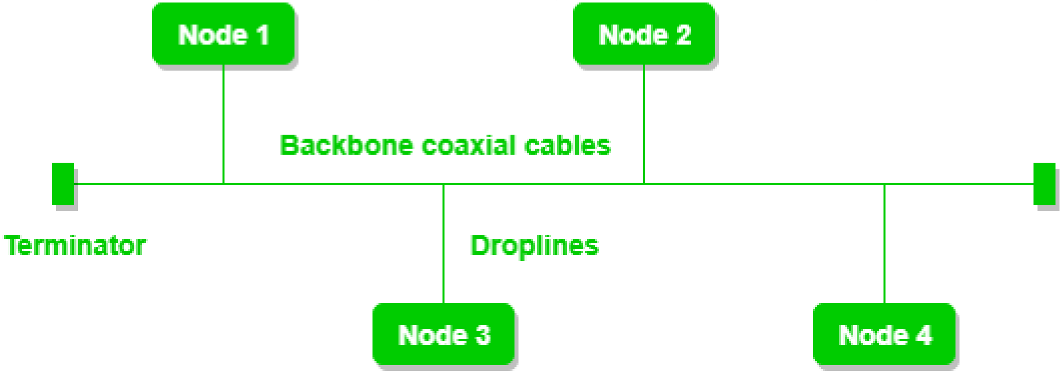
- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

A common example of star topology is a local area network (LAN) in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

For more, refer to the Advantages and Disadvantages of Star Topology.

Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



Bus Topology

Figure 3: A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

Drawbacks of Bus Topology

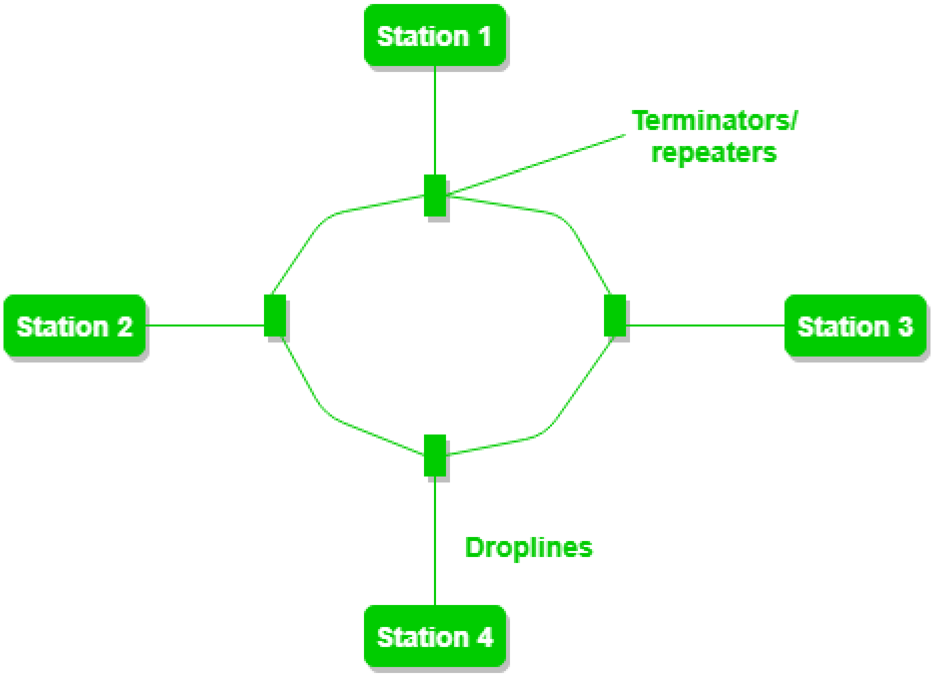
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks. For more, refer to the Advantages and Disadvantages of Bus Topology.

Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



Ring Topology

Figure 4: A ring topology comprises 4 stations connected with each forming a ring. The most common access method of ring topology is token passing.

- **Token passing:** It is a network access method in which a token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

Operations of Ring Topology

1. One station is known as a **monitor** station which takes all the responsibility for performing the operations.
2. To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delayed token release** releases the token after the acknowledgment is received from the receiver.

Advantages of Ring Topology

- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

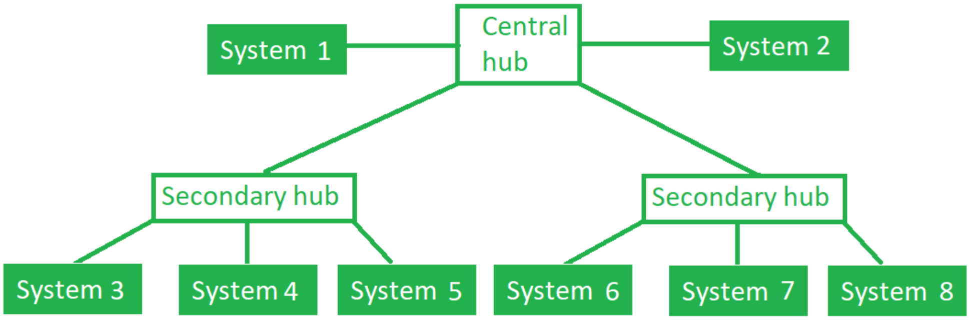
Drawbacks of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

For more, refer to the Advantages and Disadvantages of Ring Topology.

Tree Topology

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration) are used.



Tree Topology

Figure 5: In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.
- We can add **new devices to the existing network.**
- **Error detection** and **error correction** are very easy in a tree topology.

Drawbacks of Tree Topology

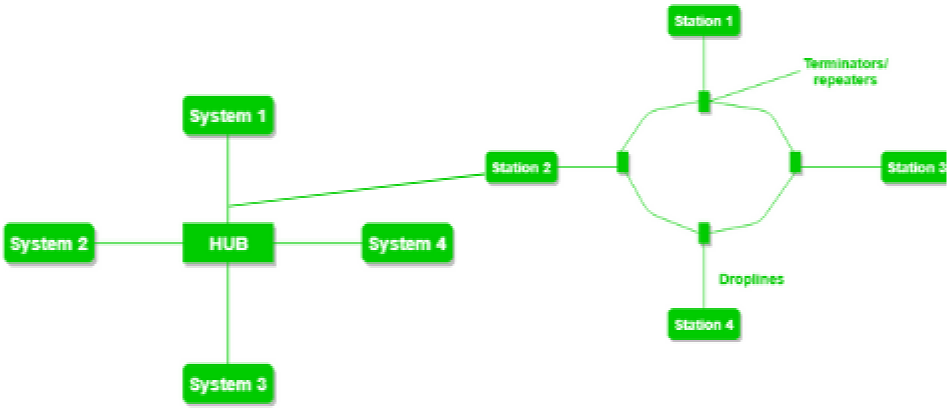
- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

A common example of a tree topology is the hierarchy in a large organization. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.

For more, refer to the Advantages and Disadvantages of Tree Topology.

Hybrid Topology

This topological technology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



Hybrid Topology

Figure 6: The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

Advantages of Hybrid Topology

- This topology is **very flexible**.
- The size of the network can be easily expanded by **adding new devices.**

Drawbacks of Hybrid Topology

- It is challenging **to design the architecture** of the Hybrid Network.
- **Hubs** used in this topology are **very expensive.**

- The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices**.

A common example of a hybrid topology is a university campus network. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices. The wireless access points also create a mesh topology for wireless devices. This hybrid topology allows for efficient communication between different buildings while providing flexibility and redundancy within each building.

MAC Full Form

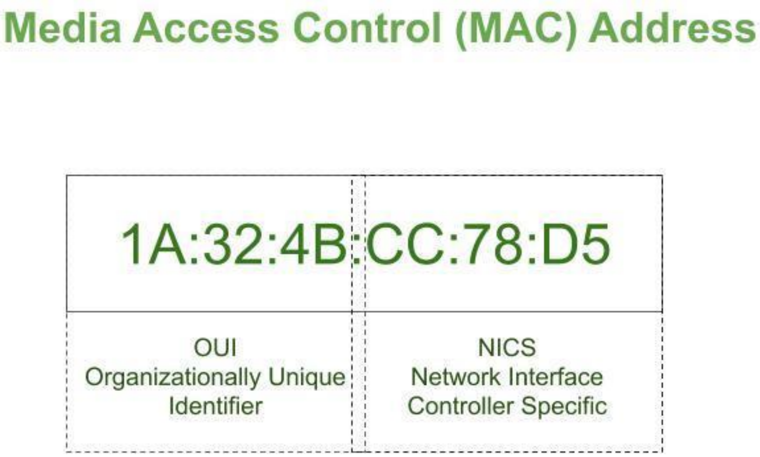
MAC stands for **Media Access Control.**

MAC address is defined as the **identification number for the hardware**. In general, the network interface cards (NIC) of each computer such as Wi-Fi Card, Bluetooth or Ethernet Card has unchangeable MAC address embedded by the vendor at the time of manufacturing. Dell, Nortel, Belkin, and Cisco are some of the well known NIC manufacturers. One can change the given default address of the device by replacing the NIC cards.

History of MAC

As far as history, we can say that **Xerox PARC scientists** have created the existence of **Media Access Control** addresses. There are many similar terms that are used in place of MAC address such as hardware address, physical address, ethernet hardware address of a network device. Even burned-in address (BIA especially for

Cisco Router Switches) also referred to as the same.



Media Access Control (MAC) Address

1A:32:4B	CC:78:D5
OUI Organizationally Unique Identifier	NICS Network Interface Controller Specific

-
-
-
-
-
-
-
-
-
-
-
-
-

Characteristics of MAC

- The MAC address that is considered to be the distinguishing number of the hardware is **globally unique.** This lets us identify each device within a connected network.
- The total length MAC address in **byte is 6 (or 48 bits)**. According to the IEEE 802 standards, this address is written in three commonly used formats:
    - Six two-digits hexadecimals separated by hyphens (-) like 45-67-89-AB-12-CD .
    - Six two-digits hexadecimals separated by colons (:) like 45:67:89:AB:DE:23 .
    - Three four-digits hexadecimals separated by dots (.) like ABCD.4567.1238 .
- The left 24 bits (3 bytes) of the address is termed as **Organizationally Unique Identifier (OUI) number.** This OUI number is assigned by **Internet Assigned Number Authority** (IANA). This globally unique OUI number will always remain the same for NICs manufactured by the same company. The right 24 bits (3 bytes) of the address is termed as **Network Interface Controller Specific (NICS),** which is responsible for communication either by using cables or wirelessly over a computer network.
- Some devices that exist on this second layer are NIC cards, bridges and switches. This layer is also responsible for error free data transmission over the Physical layer under LAN transmissions. If we refer to our Open Systems Interconnection (OSI) network model, we will find that MAC addresses in the medium access control protocol sub-layer **uses data link layer**.

Advantages of MAC

- The devices that connect to the network have no **free attachment cost** associated with it.

- The router or switch has policy set on them. Either it has permitted equipment attached or non-permitted equipment attached irrespective of the person attaching it.
- The MAC addresses for all the devices on the same network subnet are different. Hence, **Diagnosing Network issues** relating to IP address, etc. are easy because of the usefulness of MAC Addresses.
- A network administrator feels **reliability** in identifying senders and receivers of data on the network with the help of MAC address. The only reason behind is that unlike dynamic IP addresses, the MAC addresses doesn't change from time to time.

Disadvantages of MAC

- Due to the reason that the first three bytes (OUI) for a MAC address reserved for the manufacturer, therefore it is limited for having only be **2^24 unique addresses** per OUI by the same manufacturer.
- We can say **spoofing is easy** for MAC address filtering. One can act in disguise and just listen to and from permitted MAC addresses because of the broadcast nature of ethernet.
- In most cases an **intruder can obtain access** to the network by constantly changing his MAC Address to a one that is permitted.

Introduction of Internetworking

Internetworking is combined of 2 words, inter and networking which implies an association between totally different nodes or segments. This connection area unit is established through intercessor devices akin to routers or gateway. The first term for associate degree internetwork was catenet. This interconnection is often among or between public, private, commercial, industrial, or governmental networks. Thus, associate degree internetwork could be an assortment of individual networks, connected by intermediate networking devices, that function as one giant network. Internetworking refers to the trade, products, and procedures that meet the challenge of making and administering internet works.

To enable communication, every individual network node or phase is designed with a similar protocol or communication logic, that is Transfer Control Protocol (TCP) or Internet Protocol (IP). Once a network communicates with another network having constant communication procedures, it's called Internetworking. Internetworking was designed to resolve the matter of delivering a packet of information through many links.

There is a minute difference between extending the network and Internetworking. Merely exploitation of either a switch or a hub to attach 2 local area networks is an extension of LAN whereas connecting them via the router is an associate degree example of Internetworking. Internetworking is enforced in Layer three (Network

Layer) of the OSI-ISO model. The foremost notable example of internetworking is the Internet.

There is chiefly 3 units of Internetworking:

1. Extranet
2. Intranet
3. Internet

Intranets and extranets might or might not have connections to the net. If there is a connection to the net, the computer network or extranet area unit is usually shielded from being accessed from the net if it is not authorized. The net isn't thought-about to be a section of the computer network or extranet, though it should function as a portal for access to parts of the associate degree extranet.

1. **Extranet –** It's a network of the internetwork that's restricted in scope to one organization or entity however that additionally has restricted connections to the networks of one or a lot of different sometimes, however not essential. It's the very lowest level of Internetworking, usually enforced in an exceedingly personal area. Associate degree extranet may additionally be classified as a Man, WAN, or different form of network however it cannot encompass one local area network i.e. it should have a minimum of one reference to associate degree external network.
2. **Intranet –** This associate degree computer network could be a set of interconnected networks, which exploits the Internet Protocol and uses IP-based tools akin to web browsers and FTP tools, that are underneath the management of one body entity. That body entity closes the computer network to the remainder of the planet and permits solely specific users. Most typically, this network is the internal network of a corporation or different enterprise. An outsized computer network can usually have its own internet server to supply users with browsable data.
3. **Internet –** A selected Internetworking, consisting of a worldwide interconnection of governmental, academic, public, and personal networks based mostly upon the Advanced analysis comes Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense additionally home to the World Wide Web (WWW) and cited as the 'Internet' to differentiate from all different generic Internetworks. Participants within the web, or their service suppliers, use IP Addresses obtained from address registries that manage assignments.

Internetworking has evolved as an answer to a few key problems: isolated LANs, duplication of resources, and an absence of network management. Isolated LANs created transmission problems between totally different offices or departments. Duplication of resources meant that constant hardware and code had to be provided to every workplace or department, as did a separate support employee. This lack of network management meant that no centralized methodology of managing and troubleshooting networks existed.

One more form of the interconnection of networks usually happens among enterprises at the Link Layer of the networking model, i.e. at the hardware-centric layer below the amount of the TCP/IP logical interfaces. Such interconnection is accomplished through network bridges and network switches. This can be typically incorrectly termed internetworking, however, the ensuing system is just a bigger, single subnetwork, and no internetworking protocol, akin to web Protocol, is needed to traverse these devices.

However, one electronic network is also reborn into associate degree internetwork by dividing the network into phases and logically dividing the segment traffic with routers. The Internet Protocol is meant to supply an associate degree unreliable packet service across the network. The design avoids intermediate network components maintaining any state of the network. Instead, this task is allotted to the endpoints of every communication session. To transfer information correctly, applications should utilize associate degree applicable Transport Layer protocol, akin to Transmission management Protocol (TCP), that provides a reliable stream. Some applications use a less complicated, connection-less transport protocol, User Datagram Protocol (UDP), for tasks that don’t need reliable delivery of information or that need period of time service, akin to video streaming or voice chat.

Internetwork Addressing –

Internetwork addresses establish devices severally or as members of a bunch. Addressing schemes differ based on the protocol family and therefore the OSI layer. Three kinds of internetwork addresses area units are ordinarily used: data-link layer addresses, Media Access control (MAC) addresses, and network-layer addresses.

1. **Data Link Layer addresses:** A data-link layer address unambiguously identifies every physical network association of a network device. Data-link addresses typically area units cited as physical or hardware addresses. Data-link addresses sometimes exist among a flat address area and have a pre-established and usually fastened relationship to a selected device. End systems usually have just one physical network association, and therefore have just one data-link address. Routers and different internetworking devices usually have multiple physical network connections and so eventually have multiple data-link addresses.
2. **MAC Addresses:** Media Access management (MAC) addresses encompass a set of data-link layer addresses. MAC addresses establish network

entities in LANs that implement the IEEE MAC addresses of the data-link layer. MAC addresses different area units distinctively for every local area network interface. MAC addresses are forty-eight bits long and are expressed in form of twelve hexadecimal digits. The primary half dozen hexadecimal digits, which are usually administered by the IEEE, establish the manufacturer or merchant and therefore comprise the Organizational Unique Identifier (OUI). The last half dozen positional notation digits comprise the interface serial variety or another price administered by the particular merchant. MAC addresses are typically area units referred to as burned-in addresses (BIAs) as a result of being burned into read-only memory(ROM) and are traced into random-access memory (RAM) once the interface card initializes.

3. **Network-Layer Addresses:** Network addresses sometimes exist among a gradable address area and typically area units referred to as virtual or logical addresses. the connection between a network address and a tool is logical and unfixed, it usually relies either on physical network characteristics or on groupings that don't have any physical basis. finish systems need one network-layer address for every network-layer protocol they support. Routers and different Internetworking devices need one network-layer address per physical network association for every network-layer protocol supported.

Challenges to Internetworking –

Implementing useful internetwork isn't at any certainty. There are several challenging fields, particularly in the areas of dependableness, connectivity, network management, and adaptability, and each and every space is essential in establishing associate degree economical and effective internetwork. A few of them are:-

- The initial challenge lies when we are trying to connect numerous systems to support communication between disparate technologies. For example, Totally different sites might use different kinds of media, or they could operate at variable speeds.
- Another essential thought is reliable service that should be maintained in an internetwork. Individual users and whole organizations depend upon consistent, reliable access to network resources.
- Network management should give centralized support associate degree troubleshooting capabilities on the internetwork. Configuration, security, performance, and different problems should be adequately addressed for the internetwork to perform swimmingly.
- Flexibility, the ultimate concern, is important for network enlargement and new applications and services, among different factors.

Advantages:

Increased connectivity: Internetworking enables devices on different networks to communicate with each other, which increases connectivity and enables new applications and services.

Resource sharing: Internetworking allows devices to share resources across networks, such as printers, servers, and storage devices. This can reduce costs and improve efficiency by allowing multiple devices to share resources.

Improved scalability: Internetworking allows networks to be expanded and scaled as needed to accommodate growing numbers of devices and users.

Improved collaboration: Internetworking enables teams and individuals to collaborate and work together more effectively, regardless of their physical location.

Access to remote resources: Internetworking allows users to access resources and services that are physically located on remote networks, improving accessibility and flexibility.

Disadvantages:

Security risks: Internetworking can create security vulnerabilities and increase the risk of cyberattacks and data breaches. Connecting multiple networks together increases the number of entry points for attackers, making it more difficult to secure the entire system.

Complexity: Internetworking can be complex and requires specialized knowledge and expertise to set up and maintain. This can increase costs and create additional maintenance overhead.

Performance issues: Internetworking can lead to performance issues, particularly if networks are not properly optimized and configured. This can result in slow response times and poor network performance.

Compatibility issues: Internetworking can lead to compatibility issues, particularly if different networks are using different protocols or technologies. This can make it difficult to integrate different systems and may require additional resources to resolve.

Management overhead: Internetworking can create additional management overhead, particularly if multiple networks are involved. This can increase costs and require additional resources to manage effectively.

Difference between Internet, Intranet and Extranet

1. Internet :

The network formed by the co-operative interconnection of millions of computers, linked together is called Internet. Internet comprises of :

- **People :** People use and develop the network.
- **Resources :** A collection of resources that can be reached from those networks.
- **A setup for collaboration :** It includes the member of the research and educational committees worldwide.

2. Intranet :

It is an internal private network built within an organization using Internet and World Wide Web standards and products that allows employees of an organization to gain access to corporate information.

3. Extranet :

It is the type of network that allows users from outside to access the Intranet of an organization.

Difference between Internet, Intranet and Extranet :

Point of difference	**Internet**	**Intranet**	**Extranet**
Accessibility of network	Public	Private	Private
Availability	Global system.	Specific to an organization.	To share information with suppliers and vendors it makes the use of public network.
Coverage	All over the world.	Restricted area upto an organization.	Restricted area upto an organization and some of its stakeholders or so.
Accessibility of content	It is accessible to everyone connected.	It is accessible only to the members of organization.	Accessible only to the members of organization and external members with logins.
No. of computers connected	It is largest in number of connected devices.	The minimal number of devices are connected.	The connected devices are more comparable with Intranet.

Point of difference	**Internet**	**Intranet**	**Extranet**
Owner	No one.	Single organization.	Single/ Multiple organization.
Purpose of the network	It's purpose is to share information throughout the world.	It's purpose is to share information throughout the organization.	It's purpose is to share information between members and external, members.
Security	It is dependent on the user of the device connected to network.	It is enforced via firewall.	It is enforced via firewall that separates internet and extranet.
Users	General public.	Employees of the organization.	Employees of the organization which are connected.
Policies behind setup	There is no hard and fast rule for policies.	Policies of the organization are imposed.	Policies of the organization are imposed.
Maintenance	It is maintained by ISP.	It is maintained by CIO. HR or communication department of an organization.	It is maintained by CIO. HR or communication department of an organization.

Point of difference	Internet	Intranet	Extranet
Economical	It is more economical to use.	It is less economical.	It is also less economical.
Relation	It is the network of networks.	It is derived from Internet.	It is derived from Intranet.
Example	What we are normally using is internet.	WIPRO using internal network for its business operations.	DELL and Intel using network for its business operations.

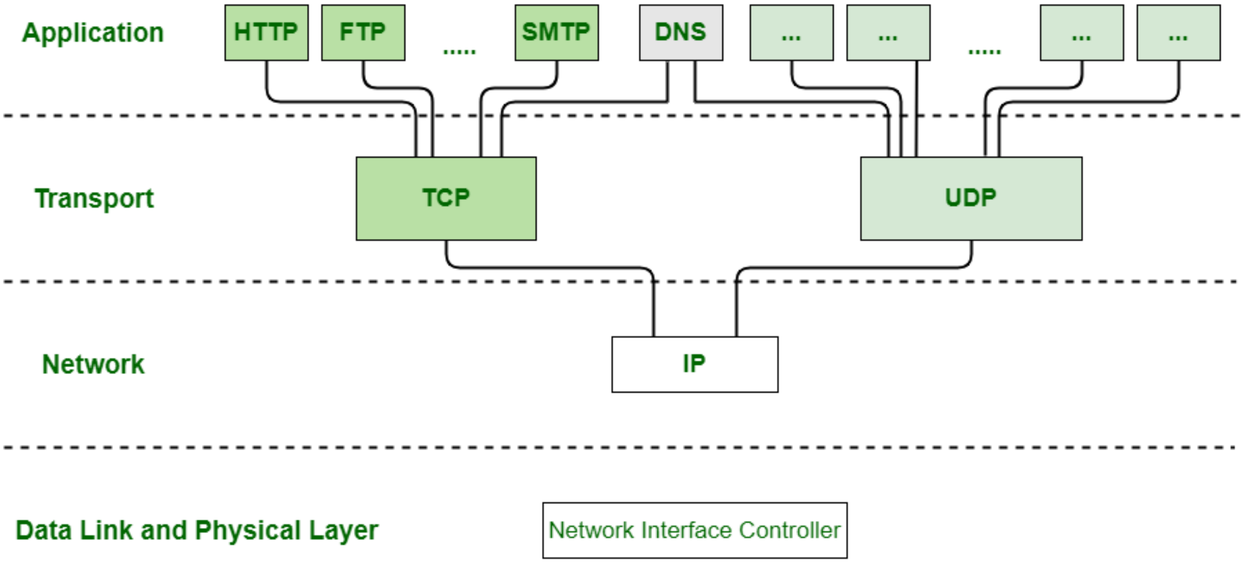
What is Protocol?

A protocol is simply defined as a set of rules and regulations for data communication. Rules are defined for every step and process at the time of communication among two or more computers. Networks are needed to follow these protocols to transmit the data successfully. All protocols might be implemented using hardware, software, or a combination of both of them. There are three aspects of protocols given below :

- **Syntax** – It is used to explain the data format that is needed to be sent or received.
- **Semantics** – It is used to explain the exact meaning of each of the sections of bits that are usually transferred.
- **Timings** – This is used to explain the exact time at which data is generally transferred along with the speed at which it is transferred.

Protocol Hierarchies

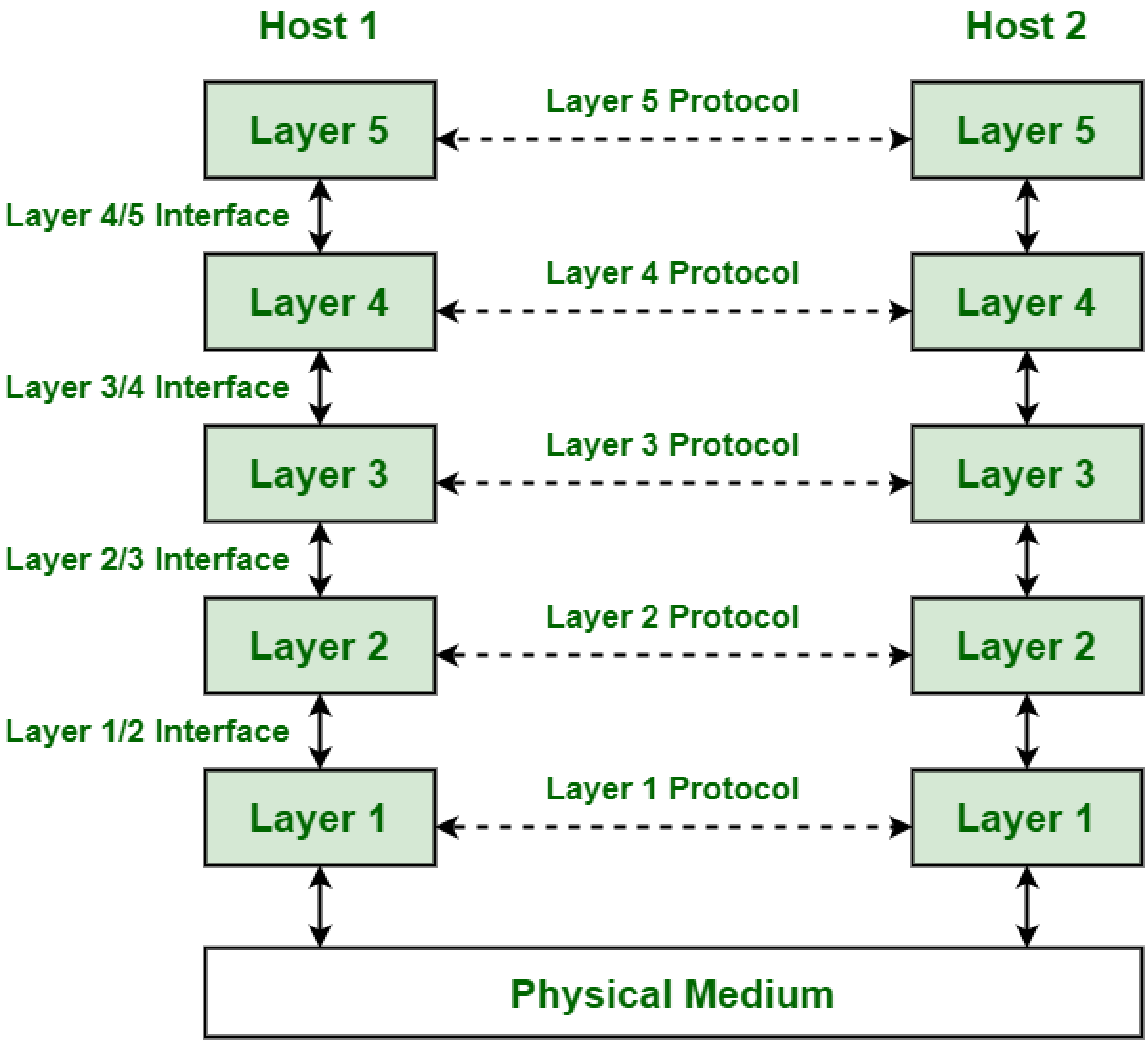
Generally, Computer networks are comprised of or contain a large number of hardware and software. For network design, various networks are organized and arranged as a stack of layers of hardware and software, one on top of another. The number, name, content, and function of each layer might vary and can be different from one network to another. The main purpose of each layer is to provide services to higher layers that are present. Every layer has some particular task or function. The networks are organized and arranged as different layers or levels simply to reduce and minimize the complexity of the design of network software.



Protocol Hierarchy

Example of Protocol Hierarchy

Below is diagram representing a five-layer network. The diagram shows communication between Host 1 and Host 2. The data stream is passed through a number of layers from one host to other. Virtual communication is represented using dotted lines between peer layers. Physical communication is represented using solid arrows between adjacent layers. Through physical medium, actual communication occurs. The layers at same level are commonly known as peers. The peer basically has a set of communication protocols. An interface is present between each of layers that are used to explain services provided by lower layer to higher layer.



Physical Hierarchies

Advantages of Protocol Hierarchy

- The layers generally reduce complexity of communication between networks
- It increases network lifetime.
- It also uses energy efficiently.
- It does not require overall knowledge and understanding of network.

Disadvantages of Protocol Hierarchy

- Protocol Hierarchy require a deep understanding of each layers of OSI model.
- Implementation of protocol hierarchy is very costly.
- Every layer in protocol hierarchy introduce overheading in terms of memory, bandwidth and processing.
- Protocol Hierarchy is not scalable for complex networks.

Network Devices: Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

1. Repeater – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

2. Hub – A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub:-** These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub:-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
- **Intelligent Hub:-** It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

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

Types of Bridges

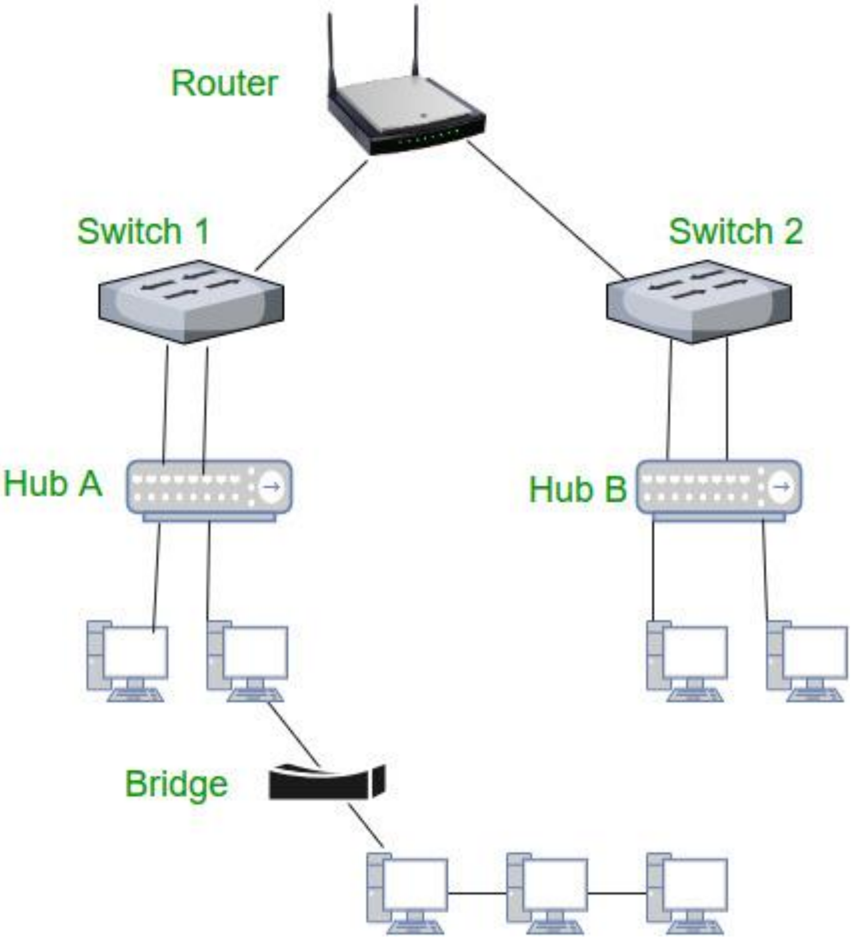
- **Transparent Bridges:-** These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and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

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

Types of Switch

1. Unmanaged switches: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
2. Managed switches: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
3. Smart switches: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.
4. Layer 2 switches: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.
5. Layer 3 switches: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.
6. PoE switches: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.
7. Gigabit switches: These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
8. Rack-mounted switches: These switches are designed to be mounted in a server rack and are suitable for use in data centers or other large networks.
9. Desktop switches: These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.
10. Modular switches: These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centers.

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



6. Gateway – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

7. Brouter – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks and working as the bridge, it is capable of filtering local area network traffic.

8. NIC – NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

What is Ethernet?

A local Area Network (LAN) is a data communication network connecting various terminals or computers within a building or limited geographical area. The connection between the devices could be wired or wireless. Ethernet, Token rings, and Wireless LAN using IEEE 802.11 are examples of standard LAN technologies.

What is Ethernet?

Ethernet is the most widely used LAN technology and is defined under IEEE standards 802.3. The reason behind its wide usability is that Ethernet is easy to understand, implement, and maintain, and allows low-cost network implementation. Also, Ethernet offers flexibility in terms of the topologies that are allowed. Ethernet generally uses a bus topology. Ethernet operates in two layers of the OSI model, the physical layer and the data link layer. For Ethernet, the protocol data unit is a frame since we mainly deal with DLLs. In order to handle collisions, the Access control mechanism used in Ethernet is CSMA/CD.

Although Ethernet has been largely replaced by wireless networks, wired networking still uses Ethernet more frequently. Wi-Fi eliminates the need for cables by enabling users to connect their smartphones or laptops to a network wirelessly. The 802.11ac Wi-Fi standard offers faster maximum data transfer rates when compared to Gigabit Ethernet. However, wired connections are more secure and less susceptible to interference than wireless networks. This is the main justification for why so many companies and organizations continue to use Ethernet.

Error Detection in Computer Networks

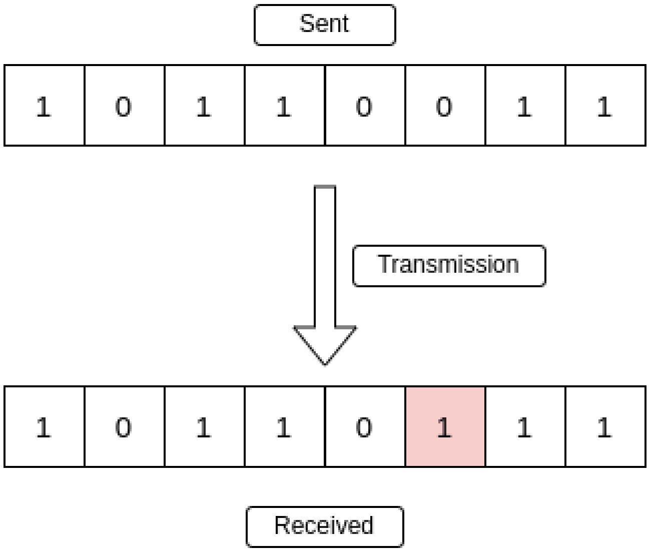
Error is a condition when the receiver's information does not match the sender's information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits traveling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

Data (Implemented either at the Data link layer or Transport Layer of the OSI Model) may get scrambled by noise or get corrupted whenever a message is transmitted. To prevent such errors, error-detection codes are added as extra data to digital messages. This helps in detecting any errors that may have occurred during message transmission.

Types of Errors

Single-Bit Error

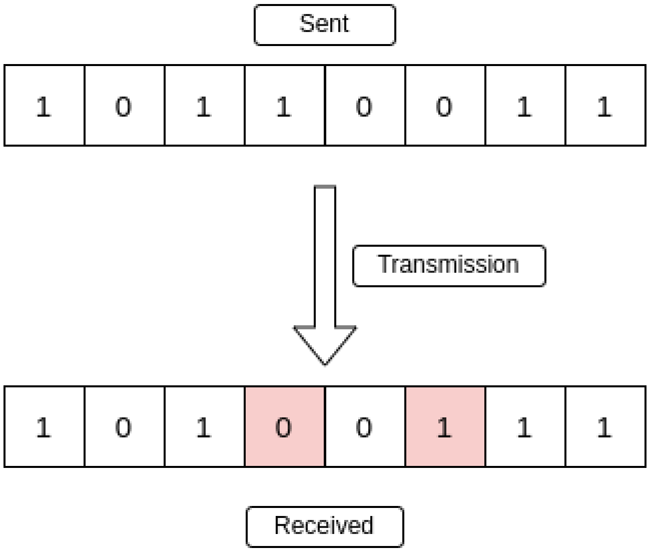
A single-bit error refers to a type of data transmission error that occurs when one bit (i.e., a single binary digit) of a transmitted data unit is altered during transmission, resulting in an incorrect or corrupted data unit.



Single-Bit Error

Multiple-Bit Error

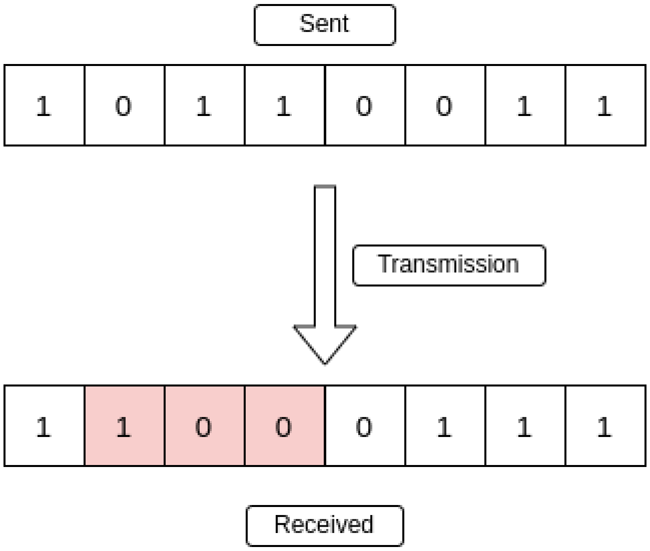
A multiple-bit error is an error type that arises when more than one bit in a data transmission is affected. Although multiple-bit errors are relatively rare when compared to single-bit errors, they can still occur, particularly in high-noise or high-interference digital environments.



Multiple-Bit Error

Burst Error

When several consecutive bits are flipped mistakenly in digital transmission, it creates a burst error. This error causes a sequence of consecutive incorrect values.



Burst Error

To detect errors, a common technique is to introduce redundancy bits that provide additional information. Various techniques for error detection include::

1. Simple Parity Check
2. Two-dimensional Parity Check

3. Checksum
4. Cyclic Redundancy Check (CRC)

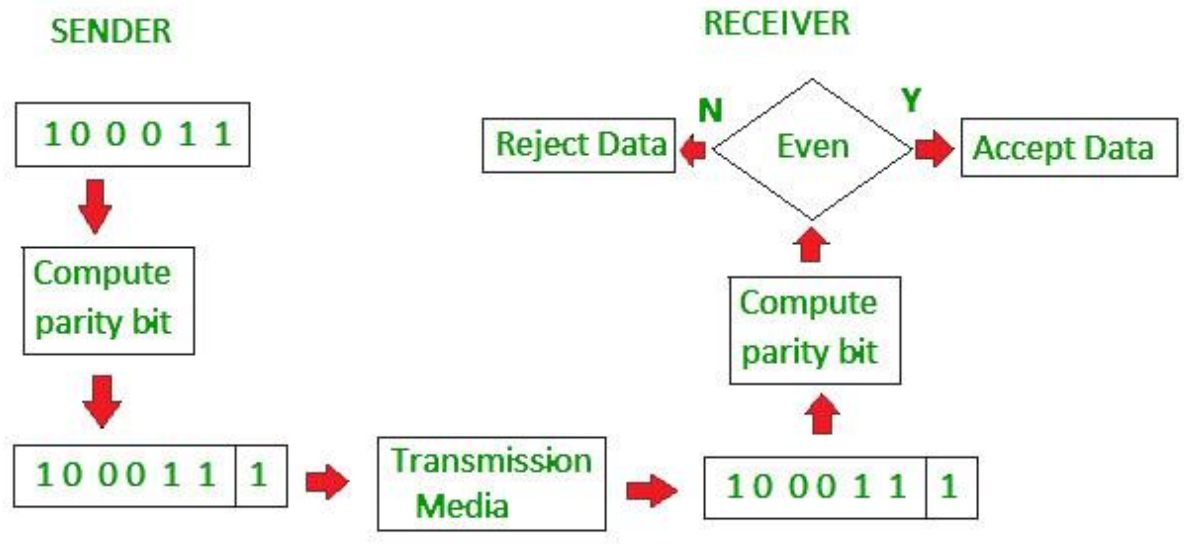
Error Detection Methods

Simple Parity Check

Simple-bit parity is a simple error detection method that involves adding an extra bit to a data transmission. It works as:

- 1 is added to the block if it contains an odd number of 1's, and
- 0 is added if it contains an even number of 1's

This scheme makes the total number of 1's even, that is why it is called even parity checking.

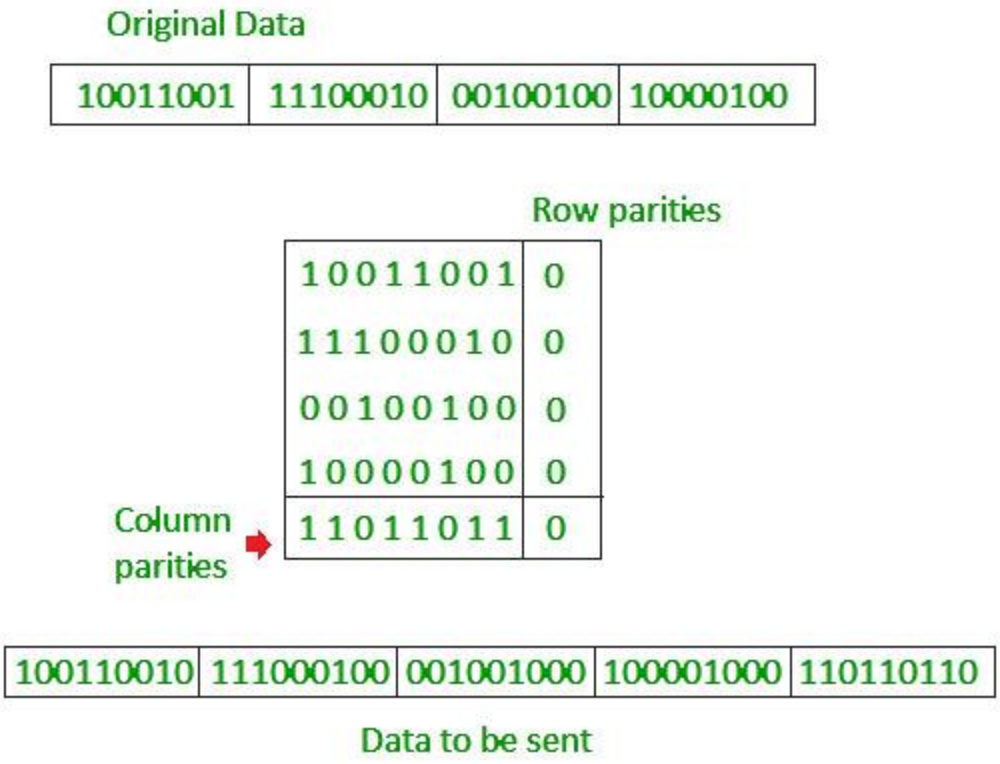


Disadvantages

- Single Parity check is not able to detect even no. of bit error.
- **For example,** the Data to be transmitted is **101010**. Codeword transmitted to the receiver is 1010101 (we have used even parity).
  Let's assume that during transmission, two of the bits of code word flipped to 1111101.
  On receiving the code word, the receiver finds the no. of ones to be even and hence **no error,** *which is a wrong assumption.*

Two-dimensional Parity Check

Two-dimensional Parity check bits are calculated for each row, which is equivalent to a simple parity check bit. Parity check bits are also calculated for all columns, then both are sent along with the data. At the receiving end, these are compared with the parity bits calculated on the received data.



Checksum

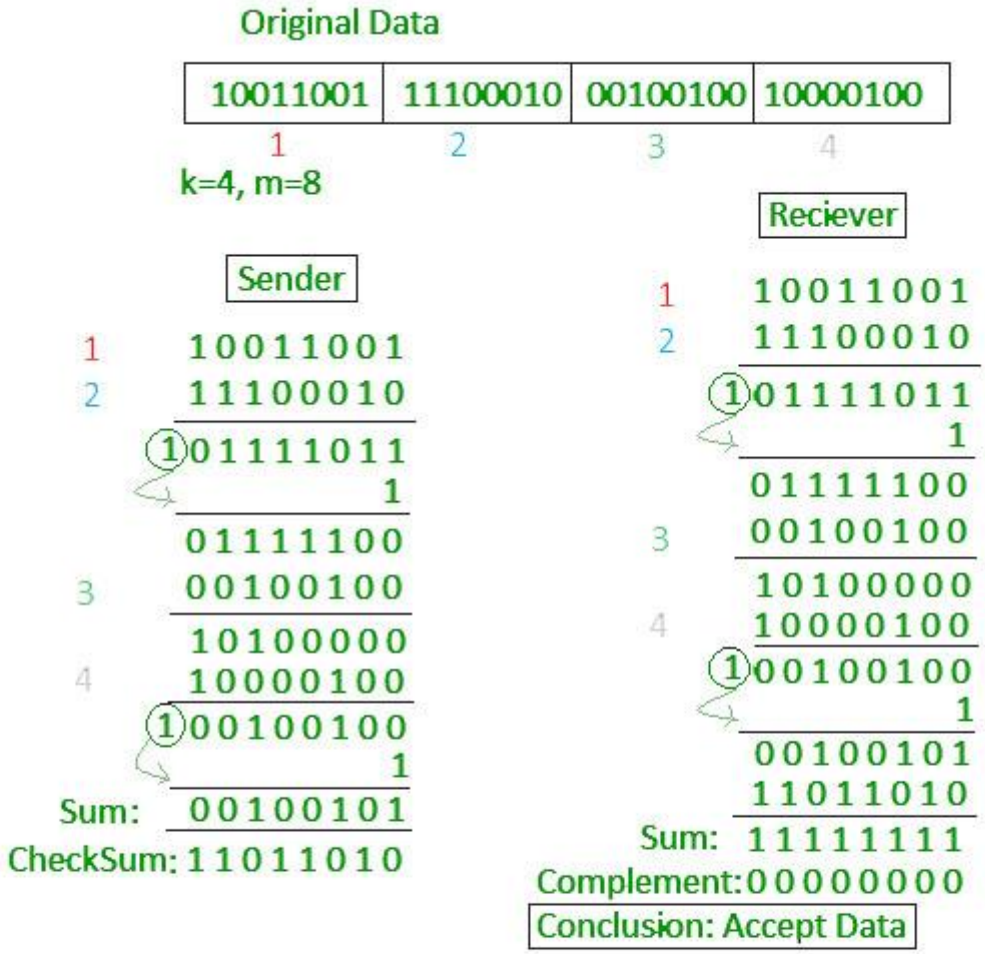
Checksum error detection is a method used to identify errors in transmitted data. The process involves dividing the data into equally sized segments and using a 1's complement to calculate the sum of these segments. The calculated sum is then sent along with the data to the receiver. At the receiver's end, the same process is repeated and if all zeroes are obtained in the sum, it means that the data is correct.

Checksum – Operation at Sender's Side

- Firstly, the data is divided into k segments each of m bits.
- On the sender's end, the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
- The checksum segment is sent along with the data segments.

Checksum – Operation at Receiver's Side

- At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
- If the result is zero, the received data is accepted; otherwise discarded.



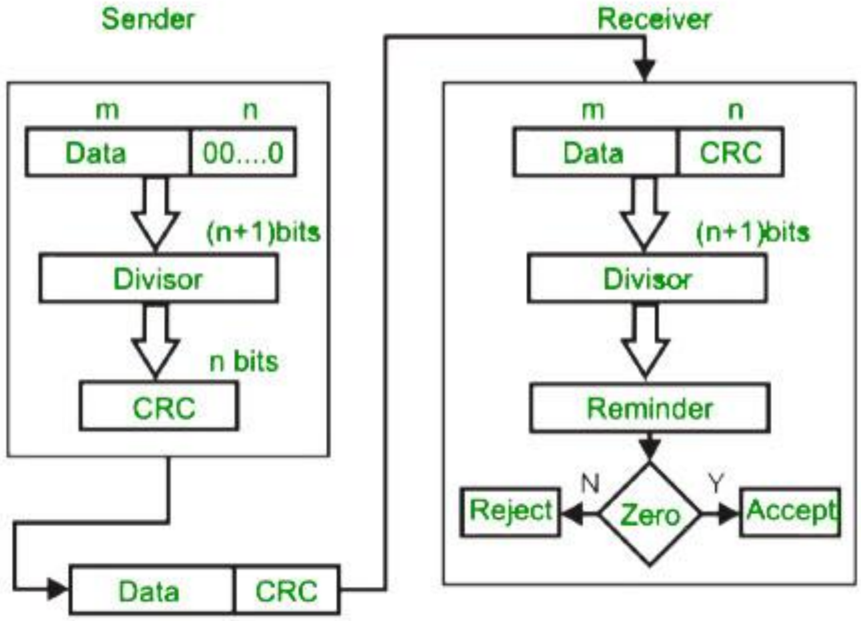
Disadvantages

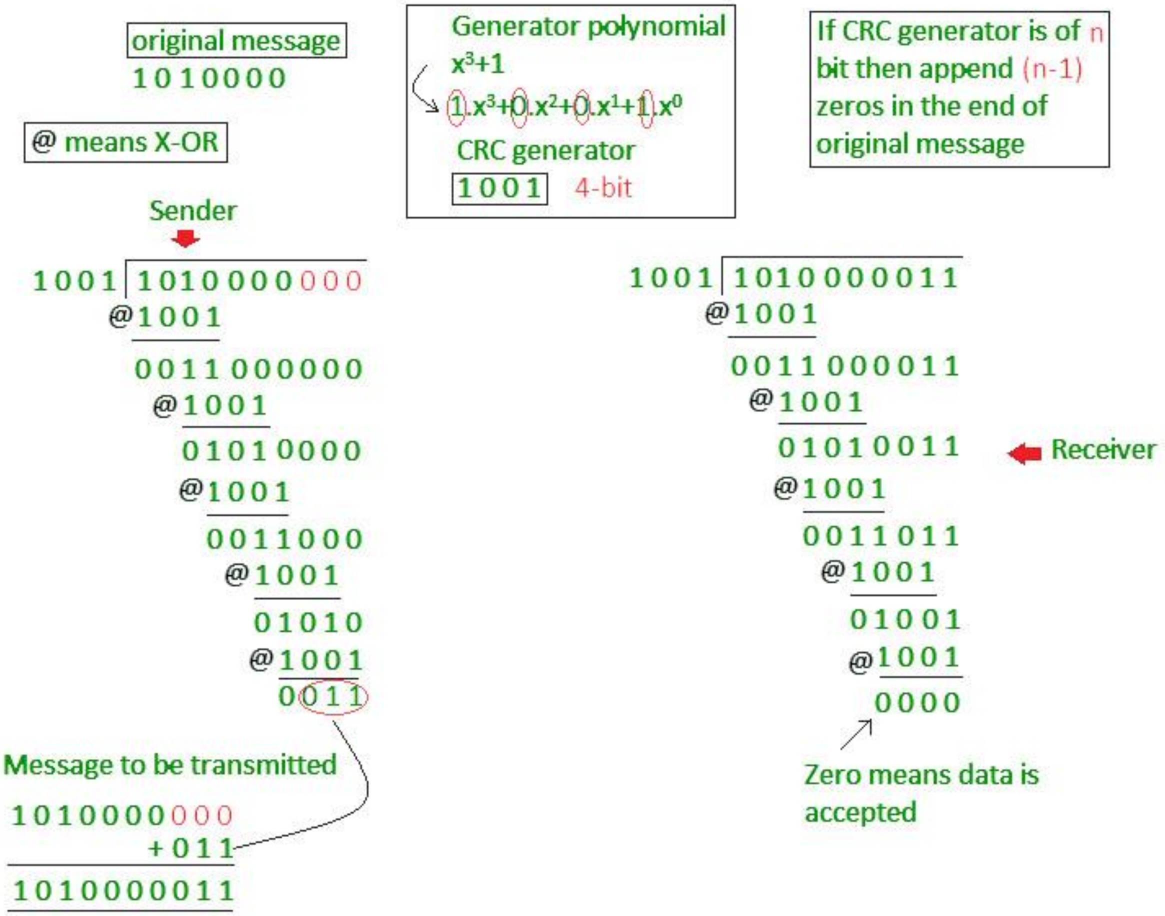
- If one or more bits of a segment are damaged and the corresponding bit or bits of opposite value in a second segment are also damaged.

Cyclic Redundancy Check (CRC)

- Unlike the checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of the data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.

- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.





Example: Previous year GATE questions based on error detection: GATE CS 2009 Question 48 GATE CS 2007 Question 68. This article has been contributed by Vikash Kumar.

Advantages:

Increased Data Reliability: Error detection ensures that the data transmitted over the network is reliable, accurate, and free from errors. This ensures that the recipient receives the same data that was transmitted by the sender.

Improved Network Performance: Error detection mechanisms can help to identify and isolate network issues that are causing errors. This can help to improve the overall performance of the network and reduce downtime.

Enhanced Data Security: Error detection can also help to ensure that the data transmitted over the network is secure and has not been tampered with.

Disadvantages:

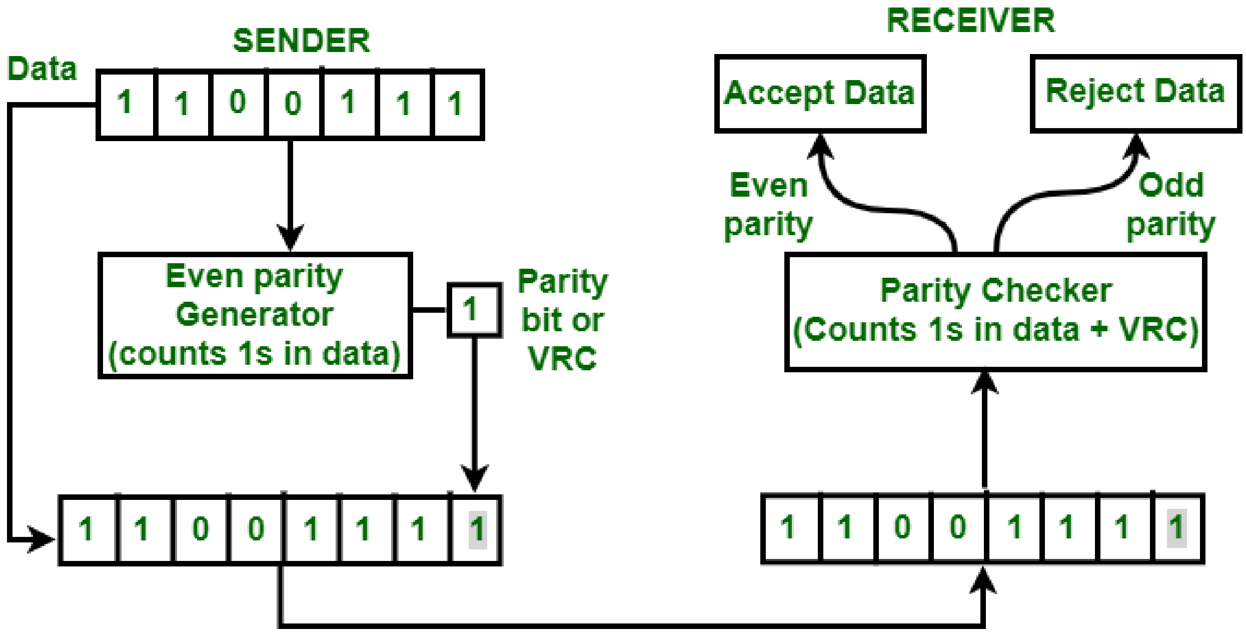
Overhead: Error detection requires additional resources and processing power, which can lead to increased overhead on the network. This can result in slower network performance and increased latency.

False Positives**:** Error detection mechanisms can sometimes generate false positives, which can result in unnecessary retransmission of data. This can further increase the overhead on the network.

Limited Error Correction**:** Error detection can only identify errors but cannot correct them. This means that the recipient must rely on the sender to retransmit the data, which can lead to further delays and increased network overhead.

Vertical Redundancy Check (VRC) or Parity Check

Vertical Redundancy Check is also known as Parity Check. In this method, a redundant bit also called parity bit is added to each data unit. This method includes even parity and odd parity. Even parity means the total number of 1s in data is to be even and odd parity means the total number of 1s in data is to be odd. **Example –** If the source wants to transmit data unit 1100111 using even parity to the destination. The source will have to pass through Even Parity Generator.



Even parity VRC

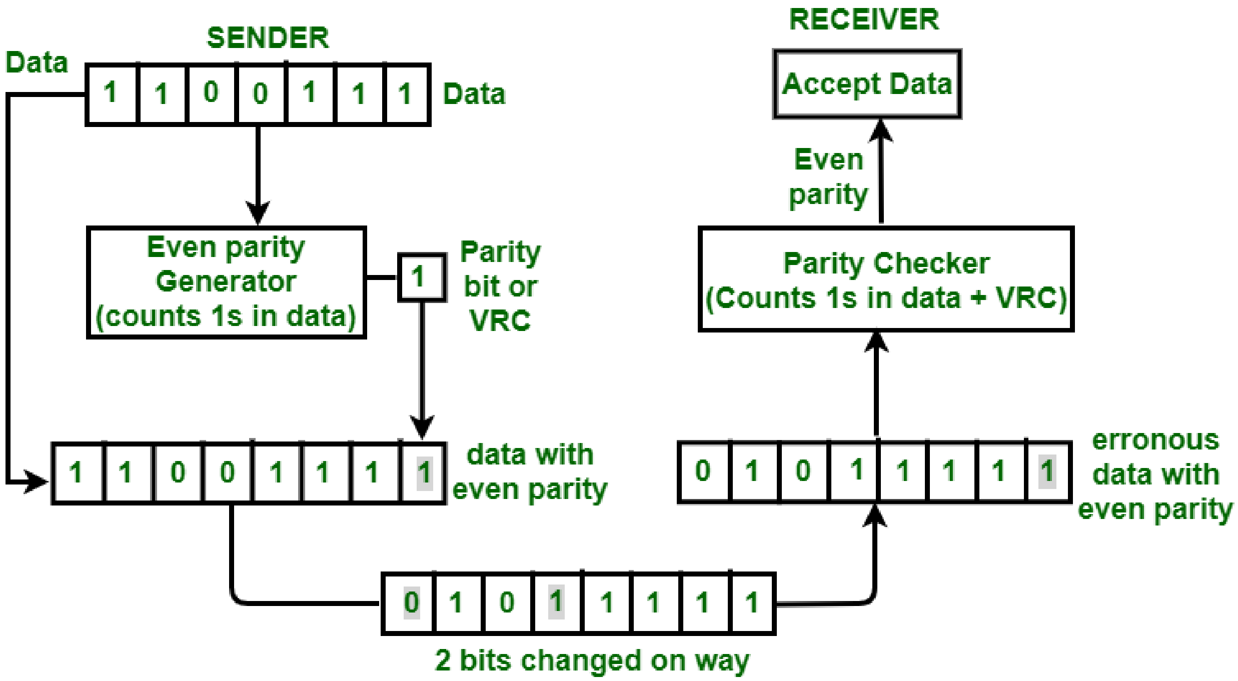
Parity generator will count number of 1s in data unit and will add parity bit. In the above example, number of 1s in data unit is 5, parity generator appends a parity bit 1 to this data unit making the total number of 1s even i.e 6 which is clear from above figure. Data along with parity bit is then transmitted across the network. In this case, 11001111 will be transmitted. At the destination, This data is passed to parity checker at the destination. The number of 1s in data is counted by parity checker. If the number of 1s count out to be odd, e.g. 5 or 7 then destination will come to know that there is some error in the data. The receiver then rejects such an erroneous data unit.

Advantages :

- VRC can detect all single bit error.
- It can also detect burst errors but only in those cases where number of bits changed is odd, i.e. 1, 3, 5, 7, …….etc.
- VRC is simple to implement and can be easily incorporated into different communication protocols and systems.
- It is efficient in terms of computational complexity and memory requirements.
- VRC can help improve the reliability of data transmission and reduce the likelihood of data corruption or loss due to errors.
- VRC can be combined with other error detection and correction techniques to improve the overall error handling capabilities of a system.

Disadvantages :

- The major disadvantage of using this method for error detection is that it is not able to detect burst error if the number of bits changed is even, i.e. 2, 4, 6, 8, …….etc.
- **Example –** If the original data is 1100111. After adding VRC, data unit that will be transmitted is 11001111. Suppose on the way 2 bits are 01011111. When this data will reach the destination, parity checker will count number of 1s in data and that comes out to be even i.e. 8. So, in this case, parity is not changed, it is still even. Destination will assume that there is no error in data even though data is erroneous.
- VRC is not capable of correcting errors, only detecting them. This means that it can identify errors, but it cannot fix them.
- VRC is not suitable for applications that require high levels of error detection and correction, such as mission-critical systems or safety-critical applications.
- VRC is limited in its ability to detect and correct errors in large blocks of data, as the probability of errors increases with the size of the data block.
- VRC requires additional overhead bits to be added to the data stream, which can increase the bandwidth and storage requirements of the system.



Longitudinal Redundancy Check (LRC)/2-D Parity Check

Longitudinal Redundancy Check (LRC) is also known as 2-D parity check. In this method, data which the user want to send is organised into tables of rows and columns. A block of bit is divided into table or matrix of rows and columns. In order to detect an error, a redundant bit is added to the whole block and this block is transmitted to receiver. The receiver uses this redundant row to detect error. After checking the data for errors, receiver accepts the data and discards the redundant row of bits.

Example :

If a block of 32 bits is to be transmitted, it is divided into matrix of four rows and eight columns which as shown in the following figure :

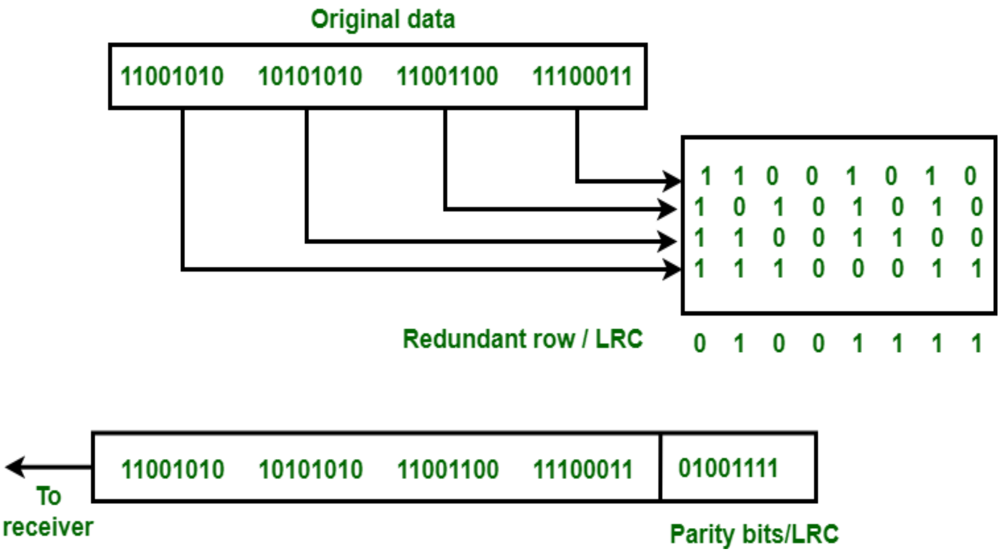


Figure: *LRC*

In this matrix of bits, a parity bit (odd or even) is calculated for each column. It means 32 bits data plus 8 redundant bits are transmitted to receiver. Whenever data reaches at the destination, receiver uses LRC to detect error in data.

Advantage :
LRC is used to detect burst errors.

Example : Suppose 32 bit data plus LRC that was being transmitted is hit by a burst error of length 5 and some bits are corrupted as shown in the following figure :

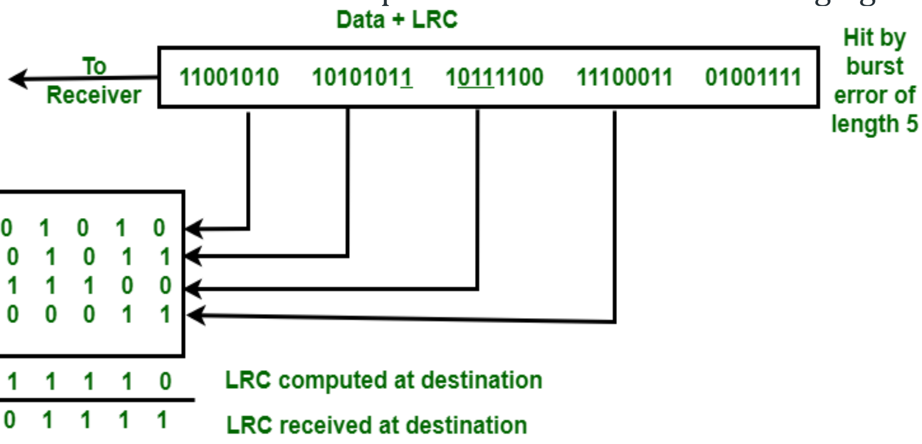


Figure : *Burst error & LRC*

The LRC received by the destination does not match with newly corrupted LRC. The destination comes to know that the data is erroneous, so it discards the data.

Disadvantage :
The main problem with LRC is that, it is not able to detect error if two bits in a data unit are damaged and two bits in exactly the same position in other data unit are also damaged.
Example : If data 110011 010101 is changed to 010010110100.

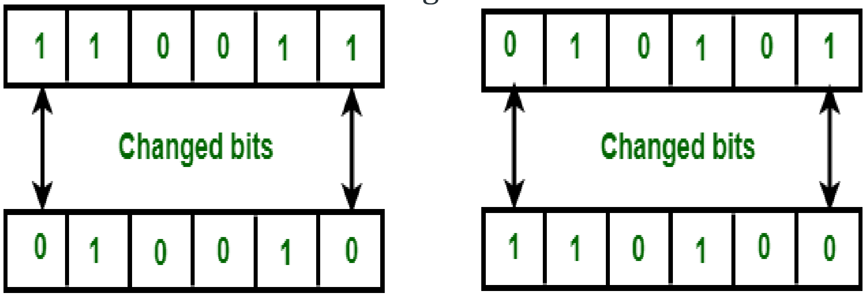


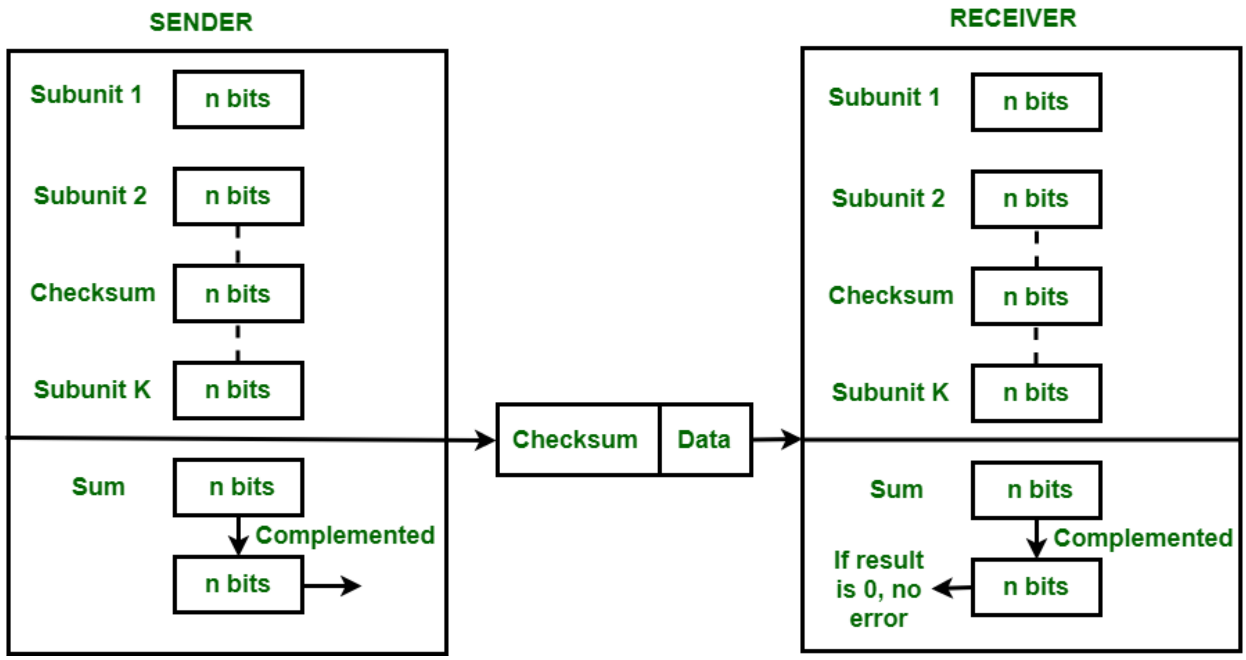
Figure : *Two bits at same bit position damaged in 2 data units*

In this example 1st and 6th bit in one data unit is changed . Also the 1st and 6th bit in second unit is changed.

Error Detection Code – Checksum

Prerequisite – Error Detection in Computer Networks
Checksum is the error detection method used by upper layer protocols and is considered to be more reliable than LRC, VRC and CRC. This method makes the use of **Checksum Generator** on Sender side and **Checksum Checker** on Receiver side.
At the Sender side, the data is divided into equal subunits of n bit length by the checksum generator. This bit is generally of 16-bit length. These subunits are then added together using one's complement method. This sum is of n bits. The resultant bit is then complemented. This complemented sum which is called checksum is appended to the end of original data unit and is then transmitted to Receiver.

-
-
-
-
-
-

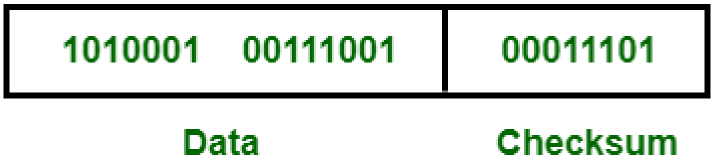


The Receiver after receiving data + checksum passes it to checksum checker. Checksum checker divides this data unit into various subunits of equal length and adds all these subunits. These subunits also contain checksum as one of the subunits. The resultant bit is then complemented. If the complemented result is zero, it means the data is error-free. If the result is non-zero it means the data contains an error and Receiver rejects it.

Example –
If the data unit to be transmitted is 10101001 00111001, the following procedure is used at Sender site and Receiver site.
Sender Site :

```
10101001        subunit 1
00111001        subunit 2
11100010        sum (using 1s complement)
00011101        checksum (complement of sum)
```

Data transmitted to Receiver is –



Receiver Site :

```
10101001        subunit 1
00111001        subunit 2
00011101        checksum
11111111        sum
00000000        sum's complement

Result is zero, it means no error.
```

Advantage :
The checksum detects all the errors involving an odd number of bits as well as the error involving an even number of bits.
Disadvantage :
The main problem is that the error goes undetected if one or more bits of a subunit is damaged and the corresponding bit or bits of a subunit are damaged and the corresponding bit or bits of opposite value in second subunit are also damaged. This is because the sum of those columns remains unchanged.
Example –
If the data transmitted along with checksum is 10101001 00111001 00011101. But the data received at destination is **0**0101001 **1**0111001 00011101.

Receiver Site :

```
00101001            1st bit of subunit 1 is damaged
10111001            1st bit of subunit 2 is damaged
00011101            checksum
11111111            sum
00000000            Ok 1's complement
```

Although data is corrupted, the error is undetected.

Network Address Translation (NAT)

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

Network Address Translation (NAT) working –

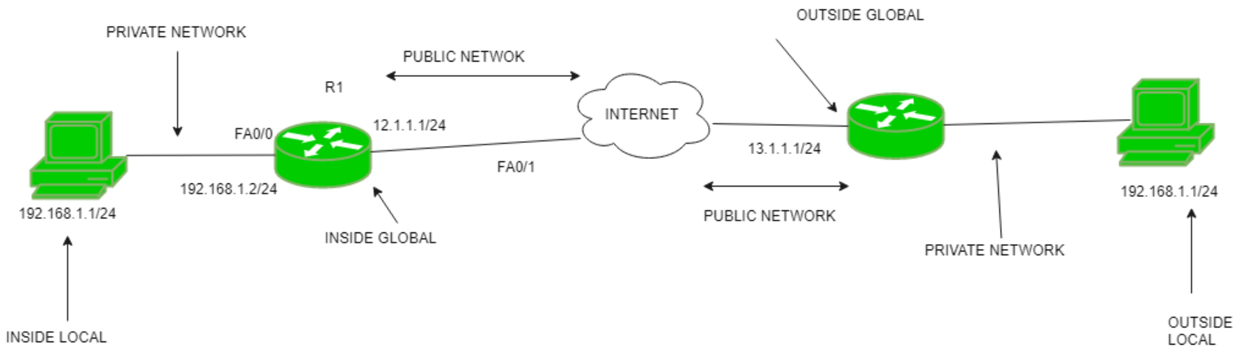
Generally, the border router is configured for NAT i.e the router which has one interface in the local (inside) network and one interface in the global (outside) network. When a packet traverse outside the local (inside) network, then NAT converts that local (private) IP address to a global (public) IP address. When a packet enters the local network, the global (public) IP address is converted to a local (private) IP address.

If NAT runs out of addresses, i.e., no address is left in the pool configured then the packets will be dropped and an Internet Control Message Protocol (ICMP) host unreachable packet to the destination is sent.

Why mask port numbers ?

Suppose, in a network, two hosts A and B are connected. Now, both of them request for the same destination, on the same port number, say 1000, on the host side, at the same time. If NAT does only translation of IP addresses, then when their packets will arrive at the NAT, both of their IP addresses would be masked by the public IP address of the network and sent to the destination. Destination will send replies to the public IP address of the router. Thus, on receiving a reply, it will be unclear to NAT as to which reply belongs to which host (because source port numbers for both A and B are the same). Hence, to avoid such a problem, NAT masks the source port number as well and makes an entry in the NAT table.

NAT inside and outside addresses –
Inside refers to the addresses which must be translated. Outside refers to the addresses which are not in control of an organization. These are the network Addresses in which the translation of the addresses will be done.



- **Inside local address –** An IP address that is assigned to a host on the Inside (local) network. The address is probably not an IP address assigned by the service provider i.e., these are private IP addresses. This is the inside host seen from the inside network.

- **Inside global address –** IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.

- **Outside local address –** This is the actual IP address of the destination host in the local network after translation.

- **Outside global address –** This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

Network Address Translation (NAT) Types –
There are 3 ways to configure NAT:

1. **Static NAT –** In this, a single unregistered (Private) IP address is mapped with a legally registered (Public) IP address i.e one-to-one mapping between local and global addresses. This is generally used for Web hosting. These are not used in organizations as there are many devices that will need Internet access and to provide Internet access, a public IP address is needed.
   Suppose, if there are 3000 devices that need access to the Internet, the organization has to buy 3000 public addresses that will be very costly.

2. **Dynamic NAT –** In this type of NAT, an unregistered IP address is translated into a registered (Public) IP address from a pool of public IP addresses. If the IP address of the pool is not free, then the packet will be

dropped as only a fixed number of private IP addresses can be translated to public addresses.
Suppose, if there is a pool of 2 public IP addresses then only 2 private IP addresses can be translated at a given time. If 3rd private IP address wants to access the Internet then the packet will be dropped therefore many private IP addresses are mapped to a pool of public IP addresses. NAT is used when the number of users who want to access the Internet is fixed. This is also very costly as the organization has to buy many global IP addresses to make a pool.

3. **Port Address Translation (PAT) –** This is also known as NAT overload. In this, many local (private) IP addresses can be translated to a single registered IP address. Port numbers are used to distinguish the traffic i.e., which traffic belongs to which IP address. This is most frequently used as it is cost-effective as thousands of users can be connected to the Internet by using only one real global (public) IP address.

Advantages of NAT –

- NAT conserves legally registered IP addresses.
- It provides privacy as the device's IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT –

- Translation results in switching path delays.
- Certain applications will not function while NAT is enabled.
- Complicates tunneling protocols such as IPsec.
- Also, the router being a network layer device, should not tamper with port numbers(transport layer) but it has to do so because of NAT.

Difference between Unicast, Broadcast and Multicast in Computer Network

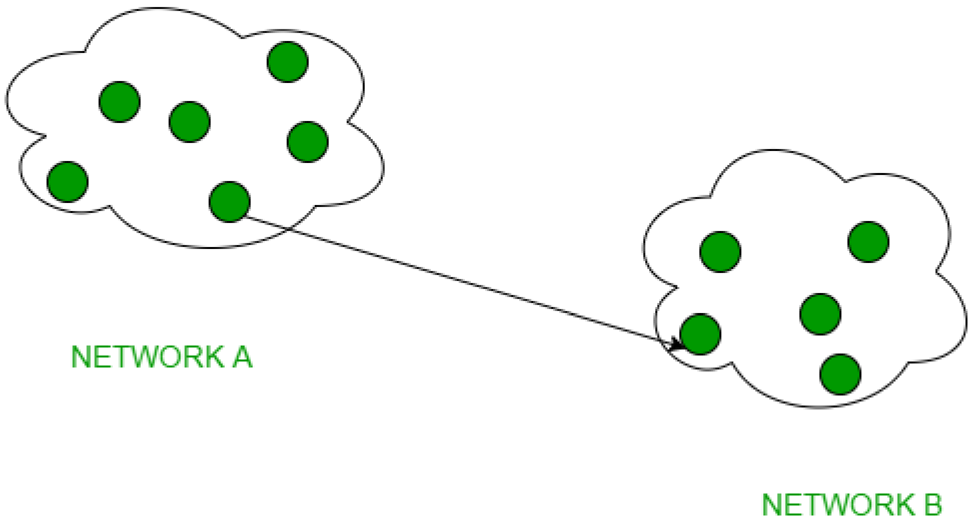
The **cast** term here signifies some data(stream of packets) is being transmitted to the recipient(s) from the client(s) side over the communication channel that helps them to communicate. Let’s see some of the “cast” concepts that are prevailing in the computer networks field.

Feature	Unicast	Broadcast	Multicast
Definition	A communication where a message is sent from one sender to one receiver.	A communication where a message is sent from one sender to all receivers.	A communication where a message is sent from one sender to a group of receivers
Transmission	Data is sent to a single recipient	Data is sent to all recipients in a network	Data is sent to a group of recipients
Addressing	Uses a unique destination address	Uses a special broadcast address	Uses a special multicast address
Delivery	Guaranteed delivery	Not all devices may be interested in the data	Not all devices may be interested in the data
Network Traffic	Generates the least amount of network traffic	Generates the most amount of network traffic	Generates moderate network traffic
Security	More secure because data is sent to a specific recipient	Less secure because data is sent to all devices in the network	Moderately secure because data is sent to a specific group of devices
Examples	Email, file transfer	DHCP requests, ARP requests	Video streaming, online gaming

Destination	Single receiver	All receivers	Grop of receivers
Bandwidth usage	Moderate	High	Moderate
Latency	Low	High	Moderate

1. Unicast:

This type of information transfer is useful when there is a participation of a single sender and a single recipient. So, in short, you can term it a one-to-one transmission. For example, if a device having IP address 10.1.2.0 in a network wants to send the traffic stream(data packets) to the device with IP address 20.12.4.2 in the other network, then unicast comes into the picture. This is the most common form of data transfer over networks.

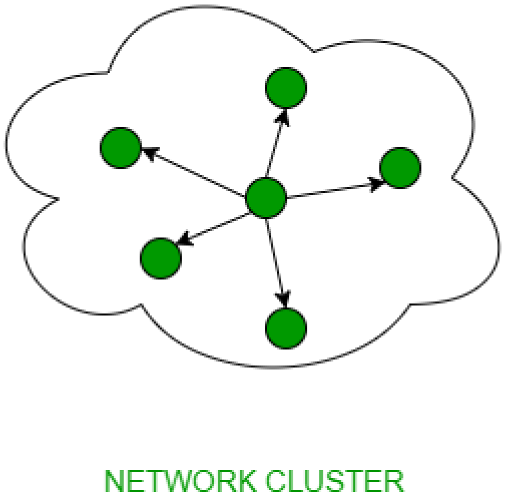


UNICAST EXAMPLE

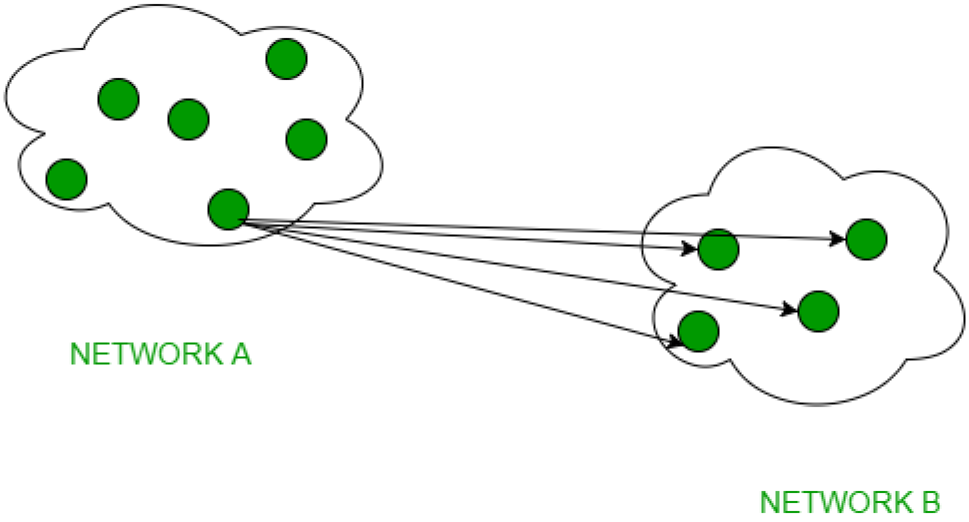
2. Broadcast:

Broadcasting transfer (one-to-all) techniques can be classified into two types:

Limited Broadcasting: Suppose you have to send a stream of packets to all the devices over the network that your reside, this broadcasting comes in handy. For this to achieve, it will append 255.255.255.255 (all the 32 bits of IP address set to 1) called **Limited Broadcast Address** in the destination address of the datagram (packet) header which is reserved for information transfer to all the recipients from a single client (sender) over the network.



Direct Broadcasting: This is useful when a device in one network wants to transfer packet stream to all the devices over the other network. This is achieved by translating all the Host ID part bits of the destination address to 1, referred to as **Direct Broadcast Address** in the datagram header for information transfer.



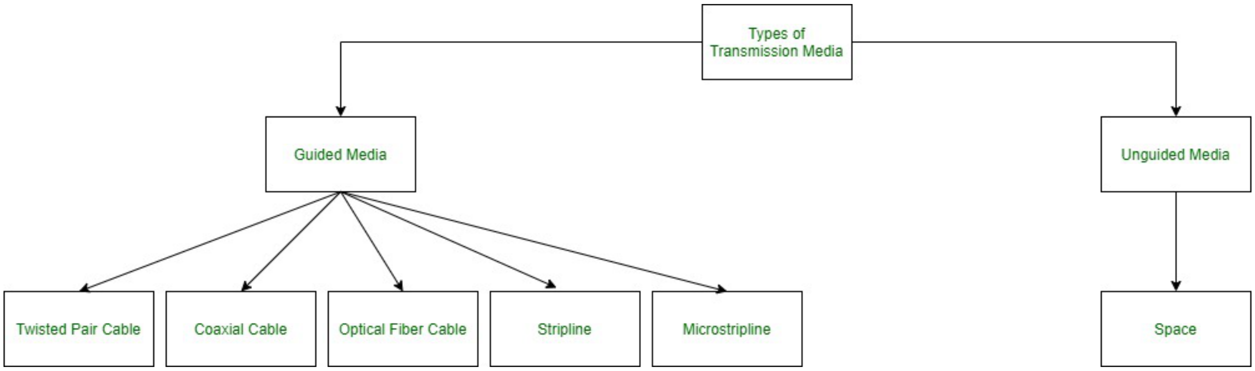
This mode is mainly utilized by television networks for video and audio distribution. One important protocol of this class in Computer Networks is Address Resolution Protocol (ARP) which is used for resolving an IP address into a physical address which is necessary for underlying communication.

3. Multicast:

In multicasting, one/more senders and one/more recipients participate in data transfer traffic. In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets servers direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires the support of some other protocols like **IGMP (Internet Group Management Protocol), Multicast routing** for its work. Also in Classful IP addressing **Class D** is reserved for multicast groups.

Types of Transmission Media

In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:



1. Guided Media: It 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

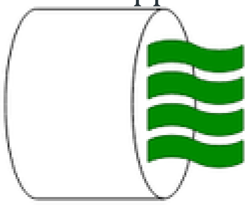
There are 3 major types of Guided Media:

-
-
-
-
-
-
-
-
-
-
-
-
-

(i) 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:

⇢ Least expensive

⇢ Easy to install

⇢ High-speed capacity

Disadvantages:

⇢ Susceptible to external interference

⇢ Lower capacity and performance in comparison to STP

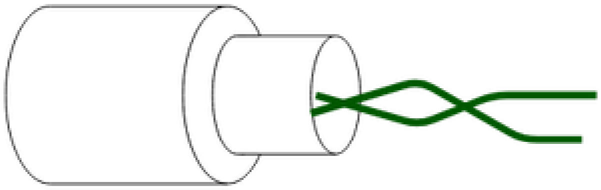
⇢ Short distance transmission due to attenuation

Applications:

Used in telephone connections and LAN networks

- **Shielded Twisted Pair (STP):**
  This type of 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.



Shielded Twisted Pair

Advantages:

⇢ Better performance at a higher data rate in comparison to UTP

⇢ Eliminates crosstalk

⇢ Comparatively faster

Disadvantages:

⇢ Comparatively difficult to install and manufacture

⇢ More expensive

⇢ Bulky

Applications:

The shielded twisted pair type of cable is most frequently used in extremely cold climates, where the additional layer of outer covering makes it perfect for withstanding such temperatures or for shielding the interior components.

(ii) Coaxial Cable –

It 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.

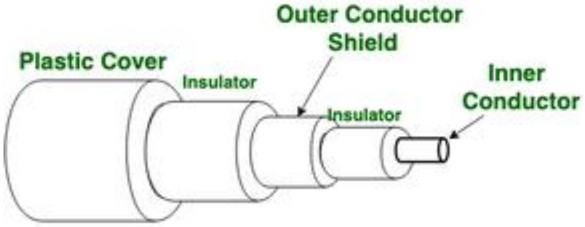


Figure of Coaxial Cable

Advantages:

- High Bandwidth
- Better noise Immunity

- Easy to install and expand
- Inexpensive

Disadvantages:

- Single cable failure can disrupt the entire network

Applications:

Radio frequency signals are sent over coaxial wire. It can be used for cable television signal distribution, digital audio (S/PDIF), computer network connections (like Ethernet), and feedlines that connect radio transmitters and receivers to their antennas.

(iii) Optical Fiber Cable –

It uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. 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.

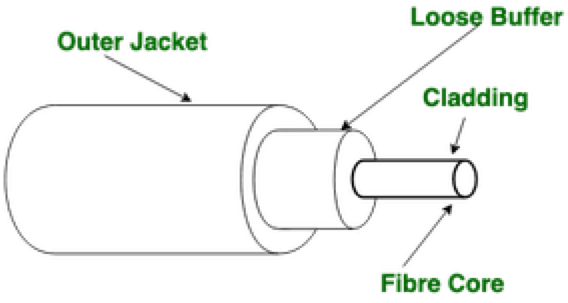


Figure of Optical Fibre Cable

Advantages:

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

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile

Applications:

- 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.

(iv) 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.

(v) Microstripline

In this, the conducting material is separated from the ground plane by a layer of dielectric.

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.

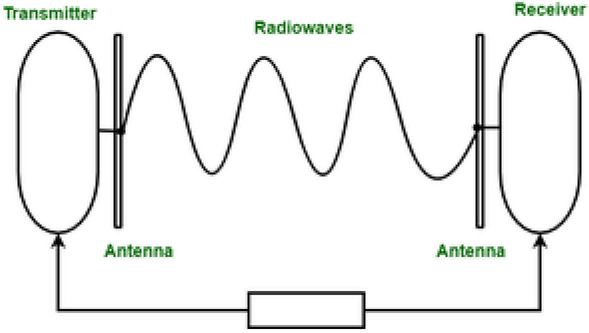
Features:

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

There are 3 types of Signals transmitted through unguided media:

(i) Radio waves –

These 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.



Further Categorized as (i) Terrestrial and (ii) Satellite.

(ii) 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. These are majorly used for mobile phone communication and television distribution.

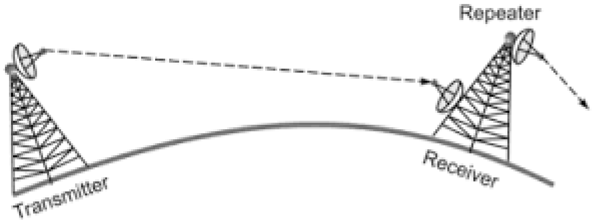
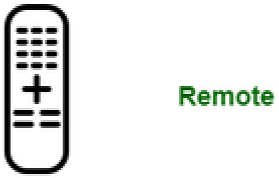


Fig: Microwave Transmission

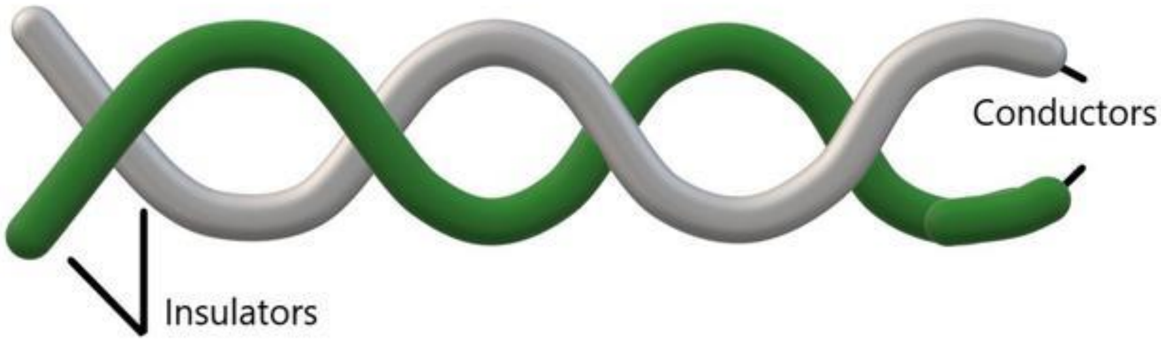
Microwave Transmission

(iii) 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.



Twisted-pair Cable

Prerequisite : Types of Transmission Media
Introduction :
Transmission media can be divided into two parts Guided Media and Unguided Media. In guided media, the signal is contained within the physical limits of the transmission medium and is directed along with it.
Twisted Pair Cables :
These are a type of guided media. It was invented by Alexander Graham Bell. Twisted pair cables have two conductors that are generally made up of copper and each conductor has insulation. These two conductors are twisted together, thus giving the name twisted pair cables.


Conductors
Insulators

-
-
-
-
-
-
-
-
-
-
-
-
-

•

•

•

•

•

×

One of the conductors is used to carry the signal and the other is used as a ground reference only. The receiver uses the difference of signals between these two conductors. The noise or crosstalk in the two parallel conductors is high but this is greatly reduced in twisted pair cables due to the twisting characteristic. In the first twist, one conductor is near to noise source and the other is far from the source but in the next twist the reverse happens and the resultant noise is very less and hence the balance in signal quality is maintained and the receiver receives very less or no noise. The quality of signal in twisted pair cables greatly depends upon the number of twists per unit length of the cable.

Twisted Pair Cables are further of two types :
1. Unshielded Twisted Pair Cables (UTP) :
These are a pair of two insulated copper wires twisted together without any other insulation or shielding and hence are called unshielded twisted pair cables. They reduce the external interference due to the presence of insulation. Unshielded twisted pair cables are arranged in pairs so that we can add a new connection whenever required. The DSL or telephone lines in our houses have one extra pair in them. When UTP are arranged in pairs, each pair is coded with a different color as defined by the 25-pair color code developed by AT&T Corporation. The Electronic Industries Association divides UTP into 7 categories based on some standards. Categories are based upon cable quality where 1 is the highest quality and 7 is the lowest quality. Each cable in a category is put to a different use as needed.

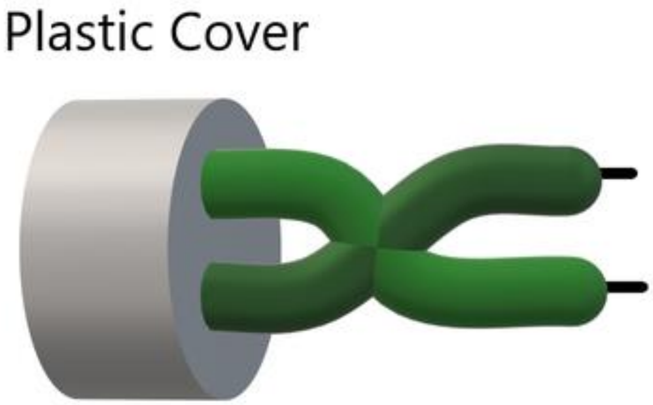
Advantages –

1. These cables are cost-effective and easy to install owing to their compact size.
2. They are generally used for short-distance transmission of both voice and data.
3. It is less costly as compared to other types of cables.

Disadvantages –

1. The connection established using UTP is not secure.
2. They are efficient only for a distance up to 100 meters and have to be installed in pieces of up to 100 meters.

3. These cables have limited bandwidth.



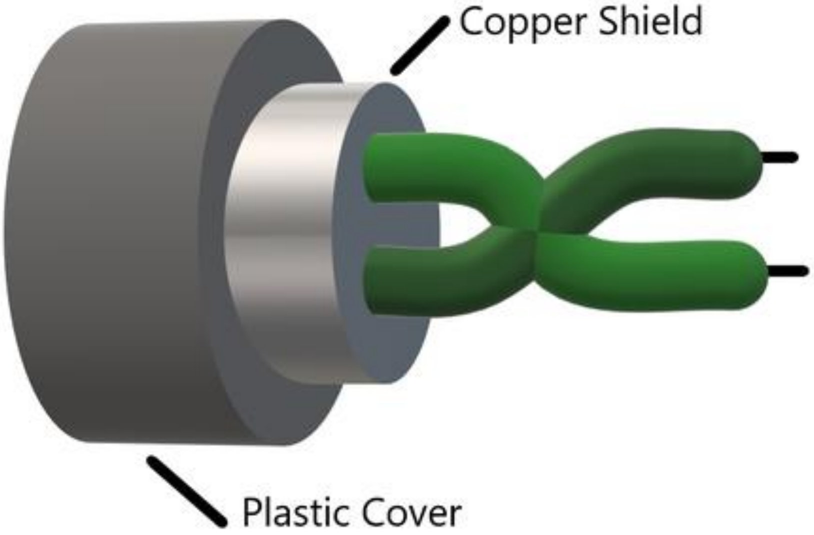
Unshielded Twisted Pair Cable (UTP)

2. Shielded Twisted Pair Cables (STP) :

These types of cables have extra insulation or protective covering over the conductors in the form of a copper braid covering. This covering provides strength to the overall structure of the cable. It also reduces noise and signal interference in the cable. The shielding ensures that the induced signal can be returned to the source via ground and only circulate around the shield without affecting the main propagating signal. The STP cables are also color-coded like the UTP cables as different color pairs are required for analog and digital transmission. These cables are costly and difficult to install.

Advantages –

1. They are generally used for long-distance communication and transmission and are installed underground.
2. The protective shield prevents external electromagnetic noise penetration into the cable.
3. They have a higher bandwidth as compared to UTP.



Shielded Twisted Pair Cable (STP)

Disadvantages –

1. These cables are very expensive.
2. They require a lot of maintenance which increases the cost more.
3. These can be installed underground only.
4. The length of the segment is similar to UTP for these cables.

Applications of Twisted pair cables :

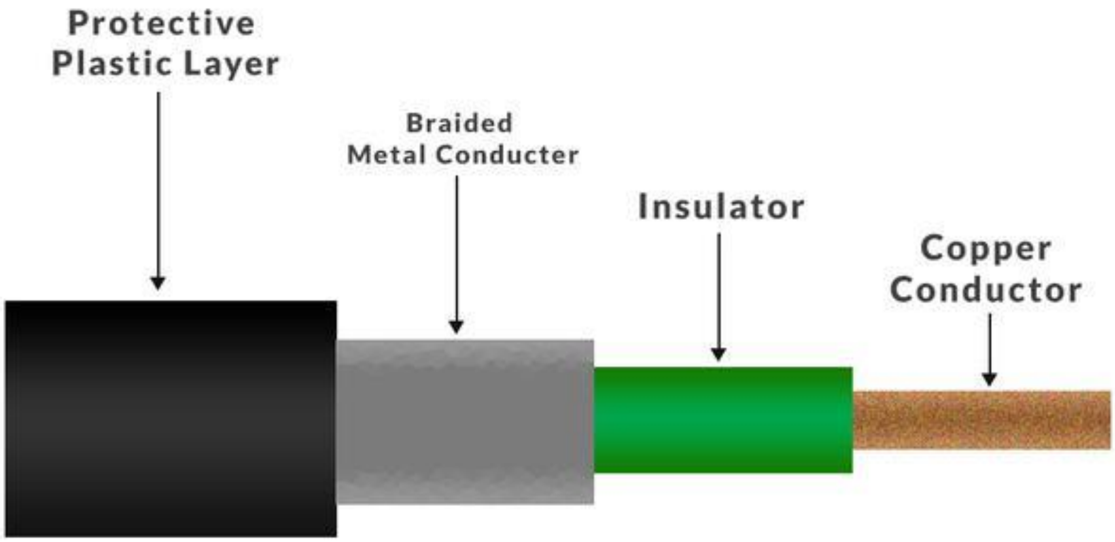
- Twisted Pair cables are used in telephone lines to provide data and voice channels.
- The DSL lines make use of these cables.
- Local Area Networks (LAN) also make use of twisted pair cables.
- They can be used for both analog and digital transmission.
- RJ-45 is a very common application of twisted pair cables.

What is Coaxial Cable ?

A coaxial cable is an electrical cable with a copper conductor and an insulator shielding around it and a braided metal mesh that prevents signal interference and cross talk. Coaxial cable is also known as **coax.**

The core copper conductor is used for the transmission of signals and the insulator is used to provide insulation to the copper conductor and the insulator is surrounded by a braided metal conductor which helps to prevent the interference of electrical signals and prevent cross talk. This entire setup is again covered with a protective plastic layer to provide extra safety to the cable.

Structure of Coaxial Cable



Coaxial Cable

Copper conductor: A central conductor, which consists of copper. The conductor is the point at which data transmits.
Insulator: Dielectric plastic insulation around the copper conductor. it is used to maintain the spacing between the center conductor and shield.

Braided mesh: A braided mesh of copper helps to shield from electromagnetic interference, The braid provides a barrier against EMI moving into and out of the coaxial cable.
Protective plastic layer: An external polymer layer, which has a plastic coating. It is used to protect internal layers from damages.

Types of Coaxial cables

1. **Hardline coaxial cable:** Hardline coaxial cable's center conductor is made of copper, silver and has a larger diameter when compared to other coaxial cables.
2. **Flexible coaxial cable:** The flexible coaxial cables are very flexible and the inner conductor is surrounded by a flexible polymer.
3. **Semi-rigid coaxial cable:** Semi-rigid coaxial cable uses a solid copper outer sheath with a dielectric of Polytetrafluoroethylene.
4. **Formable coaxial cable:** It is an alternative to semi-rigid cable, instead of a rigid copper outer sheath a flexible metal sheath is utilized.
5. **Twinaxial cable:** It has two central conductors in the core and a single outer core and dielectric. these cables are best for low-frequency digital and video transmission.
6. **Triaxial cable:** It is also known as Triax. It is very much similar to a coaxial cable but with an additional copper braid added to it, the braid works as a shield and protects from noise. Triaxial cables offer more bandwidth.
7. **Rigid coaxial cable:** Rigid coaxial cable is made up of two copper tubes supported at cable ends and fixed intervals across the length of the cable using PTFE supports or disk insulators. The rigid coaxial cable cannot be bent. It is mainly used in TV and FM broadcasting systems.

Applications of Coaxial cable

The coaxial cables are used in Ethernet LANs and also used in MANs

1. **Television:** Coaxial cable used for television would be 75 Ohm and RG-6 coaxial cable.
2. **Internet:** Coaxial cables are also used for carrying internet signals, RG-6 cables are used for this.
3. **CCTV:** The coaxial cables are also used in CCTV systems and both RG-59 AND RG-6 cables can be used.

4. **Video:** The coaxial cables are also used in video Transmission the RG-6 is used for better digital signals and RG-59 for lossless transmission of video signals.
5. **HDTV**: The HDTV uses RG-11 as it provides more space for signals to transfer.

Advantages

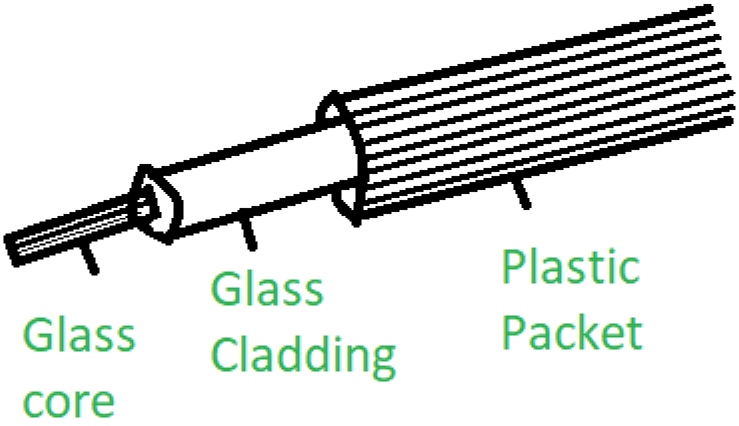
1. Coaxial cables support high bandwidth.
2. It is easy to install coaxial cables.
3. coaxial cables have better cut-through resistance so they are more reliable and durable.
4. Less affected by noise or cross-talk or electromagnetic inference.
5. Coaxial cables support multiple channels

Disadvantages

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

Fiber Optics and Types

An Optical Fiber is a cylindrical fiber of glass which is hair thin size or any transparent dielectric medium. The fiber which is used for optical communication is waveguides made of transparent dielectrics.



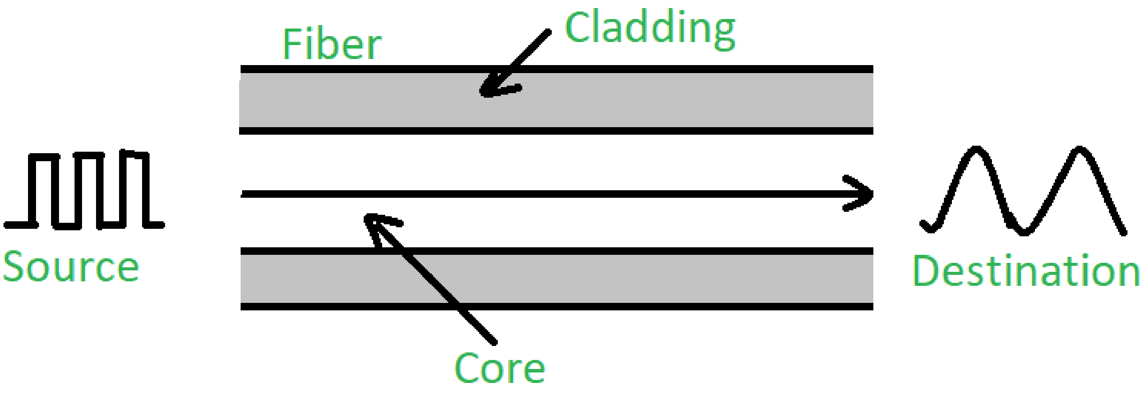
Main element of Fiber Optics

- **Core:** It is the central tube of very thin size made of optically transparent dielectric medium and carries the light transmitter to receiver and the core diameter may vary from about 5um to 100 um.
- **Cladding:** It is outer optical material surrounding the core having reflecting index lower than core and cladding helps to keep the light within the core throughout the phenomena of total internal reflection.
- **Buffer Coating:** It is a plastic coating that protects the fiber made of silicon rubber. The typical diameter of the fiber after the coating is 250-300 um.

Types of Fiber optics

On the basis of the Number of Modes:

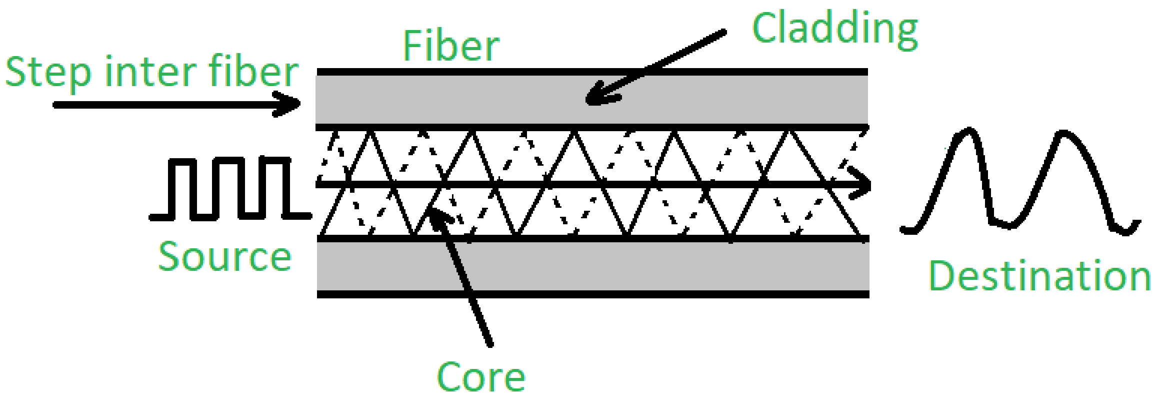
- **Single-mode fiber:** In single-mode fiber, only one type of ray of light can propagate through the fiber. This type of fiber has a small core diameter (5um) and high cladding diameter (70um) and the difference between the refractive index of core and cladding is very small. There is no dispersion i.e. no degradation of the signal during traveling through the fiber. The light is passed through it through a laser diode.



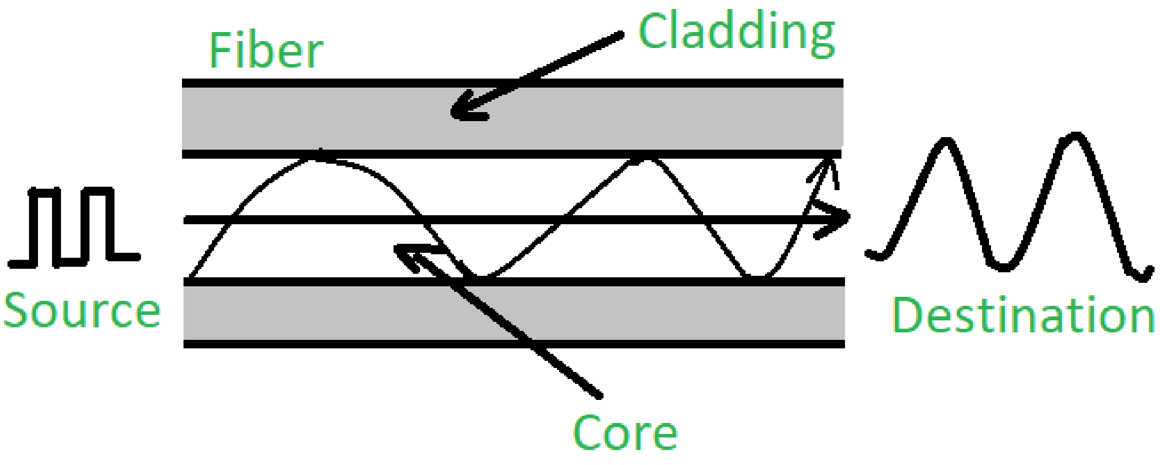
- **Multi-mode fiber:** Multimode fiber allows a large number of modes for the light ray traveling through it. The core diameter is generally (40um) and that of cladding is (70um). The relative refractive index difference is also greater than single mode fiber. There is signal degradation due to multimode dispersion. It is not suitable for long-distance communication due to large dispersion and attenuation of the signal. There are two categories on the basis of Multi-mode fiber i.e. **Step Index Fiber** and **Graded Index Fiber**. Basically these are categories under the types of optical fiber on the basis of Refractive Index

On the basis of Refractive Index:

- **Step-index optical fiber:** The refractive index of core is constant. The refractive index of the cladding is also constant. The rays of light propagate through it in the form of meridional rays which cross the fiber axis during every reflection at the core-cladding boundary.



- **Graded index optical fiber:** In this type of fiber, the core has a non-uniform refractive index that gradually decreases from the centre towards the core-cladding interface. The cladding has a uniform refractive index. The light rays propagate through it in the form of skew rays or helical rays. it is not cross the fiber axis at any time.



On the basis of Material Used:

- **Plastic Optical Fibres**: For transmission of light, polymethylmethacrylate is used as core material

- **Glass Fibres:** It is an extremely fine glass fibres, core and cladding of the optical fibre is made of plastic.

Difference between Twisted pair cable, Co-axial cable and Optical fiber cable

Twisted Pair Cable:
Wires are twisted together in pairs. Each pair would consist of a wire used for the positive data signal and a wire used for the negative data signal. Any noise that appears on the positive/negative wire of the pair would occur on the other wire. Because the wires are opposite polarities, these are 180 degrees out of phase (180 degrees or definition of opposite polarities). When the noise appears on both wires, it cancels or nulls itself out at the receiving end.

There are two types of twisted pair cable –

1. **Shielded Twisted Pair Cable –**
   Twisted pair cables are most effectively used in a system that uses a balanced line method of transmission. Cables with shields are called Shielded twisted pair cables and commonly abbreviated STP.
2. **Unshielded Twisted Pair Cable –**
   Cables without shields are called unshielded twisted pair cables or UTP. Twisting the wires together results in characteristics impedance for the cable. UTP cable is used on Ethernet.

Advantages

Unmute

-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-

×

- Cost-effective: Twisted pair cables are the most cost-effective option for communication and networking.
- Easy to install: They are easy to install and terminate, making them ideal for small to medium-sized networks.
- Flexibility: Twisted pair cables come in different categories, including Cat5, Cat6, and Cat7, offering different levels of performance and flexibility.
- Suitable for short distances: Twisted pair cables are suitable for communication over short distances, making them ideal for use in homes and small businesses.

Disadvantages:

- Limited bandwidth: Twisted pair cables have limited bandwidth, which can restrict data transfer rates and performance.
- Susceptible to interference: Twisted pair cables are susceptible to interference from other electrical equipment, leading to data errors and loss.
- Limited distance: Twisted pair cables are limited in terms of distance, making them less suitable for larger networks.

Co-axial Cable:

It consists of two conductors. The inner conductor of the coaxial cable is contained inside the insulator with the other conductor weaves around it providing a shield. An insulating protective coating called a jacket covers the outer conductor. The outer shield protects the inner conductor from outside electrical signals. Distance between the outer conductor and inner conductor plus the type of material used for insulating the inner conductor determine the cable properties.

Advantages:

- Better bandwidth: Co-axial cables offer better bandwidth than twisted pair cables, allowing for faster data transfer rates and improved performance.
- Longer distance transmission: Co-axial cables can transmit data over longer distances than twisted pair cables.
- Resistance to interference: Co-axial cables are resistant to electromagnetic interference, improving signal quality and reducing data loss.

Disadvantages:

- More expensive: Co-axial cables are more expensive than twisted pair cables, making them less cost-effective for some applications.
- Difficult to install: Co-axial cables are more difficult to install than twisted pair cables, requiring specialized equipment and expertise.
- Limited flexibility: Co-axial cables are less flexible than twisted pair cables, limiting their use in some applications.

Optical Fiber Cable:

It consists of thin glass fiber that can carry information at frequencies in the visible light spectrum. Typical optical fiber consists of a very narrow strand of glass called cladding. The typical core diameter is 62.5 microns.

Typically cladding has a diameter of 125 minors. Coating the cladding is a protective coating consisting of plastic, it is called the jacket. The device generating the message has it in electromagnetic form (electrical signal). This has to be converted into light to send it on an optical fiber cable.

Advantages:

- High-speed data transmission: Optical fiber cables can transmit data at very high speeds, up to several gigabits per second. This makes them ideal for applications that require fast and reliable data transmission, such as video conferencing, online gaming, and cloud computing.
- Immunity to electromagnetic interference: Optical fiber cables are immune to electromagnetic interference, making them ideal for use in environments where electromagnetic interference is a concern. This includes industrial settings and medical applications, where sensitive electronic equipment must be shielded from electromagnetic interference.
- Lower power consumption: Optical fiber cables use less power than traditional copper cables, which means they are more energy-efficient and cost-effective to operate over the long term.

Disadvantages:

- Cost: Optical fiber cables are more expensive to install than traditional copper cables. This can make them less attractive to companies and organizations that are looking for cost-effective solutions.
- Fragility: Optical fiber cables are fragile and can be damaged easily if they are bent or twisted too much. This makes them less suitable for applications that require cables to be frequently moved or repositioned.

- Difficult to splice: Optical fiber cables are more difficult to splice than traditional copper cables, which can make them more challenging to install and maintain.

Difference Between Twisted pair cable, Co-axial cable, and Optical fiber

Characteristics	**Twisted pair cable**	**Co-axial cable**	**Optical fiber cable**
Signal transmission	Takes place in the electrical form over the metallic conducting wires.	Takes place in the electrical form over the inner conductor of the cable.	Takes place in an optical form over glass fiber.
Consists of	Pair of insulated copper wires	Requires 4 components from inner to outer- • Solid conductor wire • Layer of insulation • Grounding conductor • Layer of exterior insulation.	Bundling of very thin optical fibers made up of glass or plastic in a single cable.
Installation and Implementation	Simple and easy	Relatively difficult	Difficult
External magnetic field	Affected due to external magnetic field.	The external magnetic field is less affected.	The external magnetic field is not affected.

Characteristics	**Twisted pair cable**	**Co-axial cable**	**Optical fiber cable**
Cause of power	Power loss due to conduction and radiation.	Power loss due to conduction.	power loss due to absorption, scattering, and bending.
Diameter	Large diameter than Optical fiber cable.	Large diameter than Optical fiber cable.	Small diameter
Bandwidth	The twisted-pair cable has low bandwidth.	Co-axial cable has moderately high bandwidth.	Optical fiber cable has a very high bandwidth.
Electromagnetic interference(EMI)	EMI can take place.	EMI is reduced to shielding.	EMI is not present.
Installation	Easy installation.	Fairly easy installation.	Difficult to install.
Attenuation	In twisted pair cable has very high attenuation.	In coaxial cable has low attenuation.	In optical fiber cable has very low attenuation.
Data rate	Twisted pair cable supports a low data rate.	Moderately high data rate.	Very high data rate.

Characteristics	Twisted pair cable	Co-axial cable	Optical fiber cable
Noise immunity	Twisted pair cable has low noise immunity.	Co-axial cable has higher noise immunity.	Optical fiber cable has the highest noise immunity.
Cost	The cost is very low.	Cost is moderate	Cost is expensive.
Repeater Spacing	Repeater spacing is 2-10 km.	Repeater spacing is 1-10 km.	Repeater spacing is 10-100 km.
Security	Security is not guaranteed of the transmitted signal.	Security is not guaranteed of the transmitted signal.	Security is guaranteed of the transmitted signal.
Types	• Unshielded Twisted Pair (UTP) • Shielded Twisted Pair (STP)	• RG59 • RG6	• Single mode fiber (SMF) • Multimode fiber (MMF)
Power loss	Reasons-conduction and radiation	Reasons- absorption, scattering dispersion and bending	Reasons-conduction

Conclusion:

each type of cable has its own unique features and is used for different purposes. Twisted Pair Cable is the most common and cheapest option, Co-axial Cable has a higher bandwidth and is used for high-speed connections, and Optical Fiber Cable is immune to electromagnetic interference and has a very high bandwidth. Choosing the right type of cable depends on the application, distance, and budget.

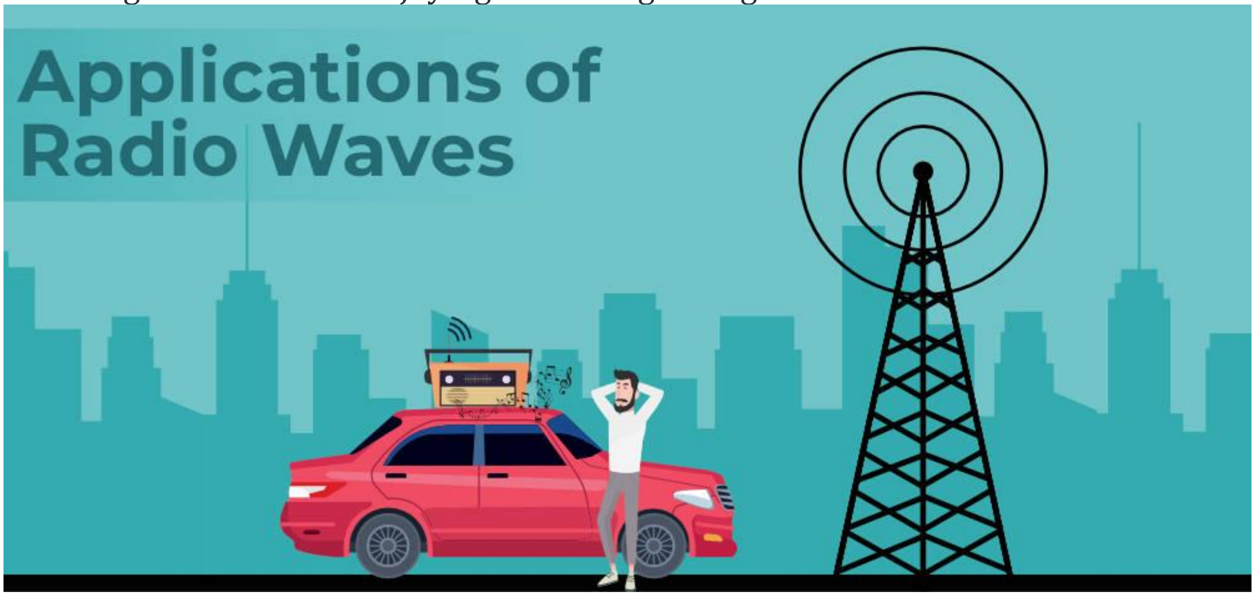
Radio Waves

Radio waves are part of the electromagnetic spectrum and waves with one of the largest wavelengths. These waves are used for long-range communication as they are capable of propagating along the curvature of the earth. They are sent using the transmitter and are received using the antenna called the receiver. Radio waves are widely used for long-range communication and they operate in the range of 300 GHz to 3 kHz.

What are Radio Waves?

Radio waves are wave which is generated at the furthest end of the electromagnetic spectrum where the wavelength is highest they are transmitted using a radio transmitter and are received using a radio receiver. These waves can easily bend along the Earth's curvature and are best suited for long-range communication. They do not get diffracted while travelling along the earth's atmosphere. Similar to other electromagnetic waves radio waves also travel at the speed of light. They are generated by fast-accelerating electrons.

The image shows a man enjoying radio songs using radio waves.



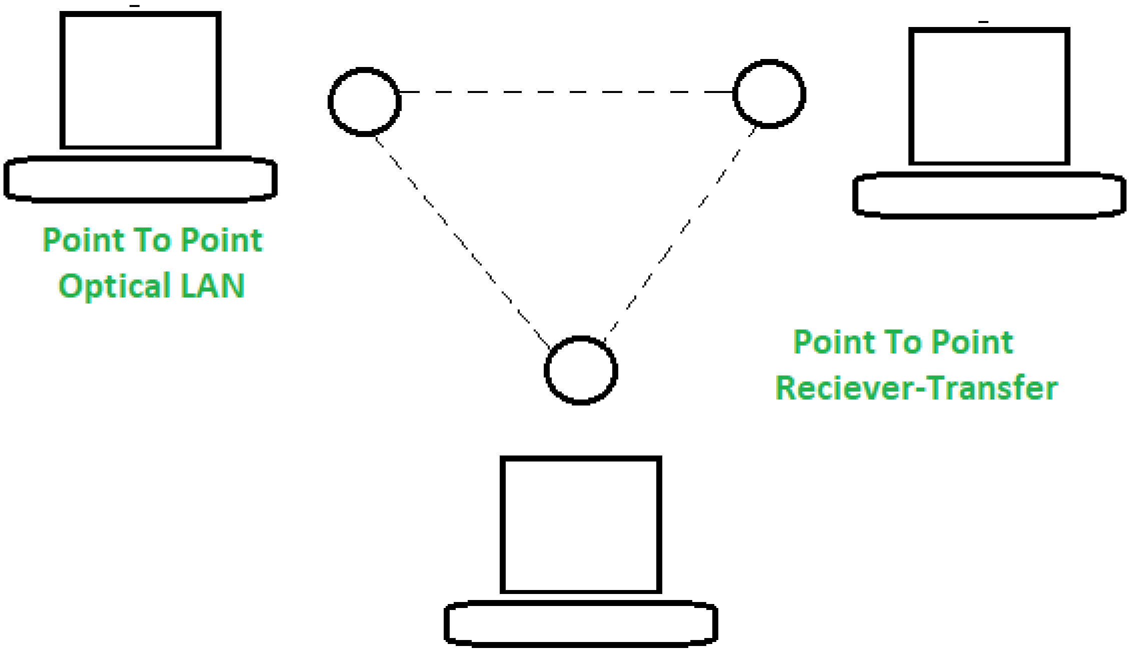
Infrared light for Transmission

Infrared light for Transmission :

Infrared is the frequency of light that is not visible to the eyes .The frequency of the waves lies between three hundred gigacycles to four hundred THz. In this, the radiation is in the region of the electromagnetic spectrum . Infrared could be a communication medium whose properties are considerably totally different from those of radio frequencies. The necessary property of the infrared is that it cannot penetrate through walls. Which suggests that it is often simply contained inside a space. Because of this property, the infrared is often used in a way that reduces interference and the chance of reprocessing of a similar band in numerous rooms. Its wavelength is longer than visible light but shorter than radio waves. The wavelength of the infrared ranges from 850 nm to 900 nm. Another advantage of infrared communication is that the massive information measure that is offered to be used, however has not been exploited to its full extent. The foremost disadvantage is that the sun generates radiation within the infrared band. This may cause tons of interference with IR communication. The infrared band is often utilized in the development of terribly high-speed wireless LANs in the future.

Applications and Standards :

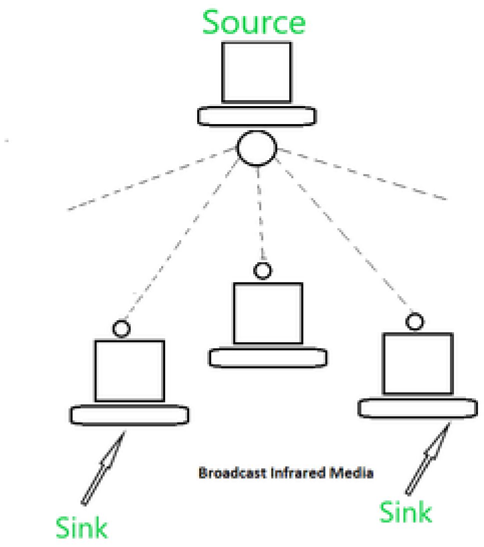
Several standards are developed for associate degree infrared electrical circuit (IRDA). The IRDA-C commonplace provides the standards for the bidirectional communications utilized in conductor devices like mice; keyboards, joysticks, and hand-held computers. The IRDA-C commonplace operates at a touch rate of seventy-five Kbits/sec and therefore the distance varies, is up to eight meters. Another commonplace referred to as IRDA-D commonplace provides information rates from one hundred fifteen kb/s to 4Mb/s with a distance vary up to one meter. The IR electrical circuit was designed as a wireless different to connecting devices like laptop computers to a pointer. Purpose to purpose transmission permits for higher information rates. However, devices should stay in their locations. Broadcast permits for additional flexibility, however, with lower information rates. One advantage of infrared is that an associate degree independent agency license isn’t needed to use it. The sole disadvantage of infrared signals is that they can not penetrate walls or alternative objects and that they are units diluted by robust lightweight sources.



Point -To-Point infrared media in a network

Characteristics Point to Point Infrared System :

- The frequency range is 100 GHz to 1000 terahertz.
- Data rates between 100 kbps to 16 mbps.
- Attenuation depends on the quality of emitted light, its purity, atmospheric conditions and signal obstructions.
- EMI is affected by intense light.
- Installation requires precise alignment.



Characteristics Broadcast Infrared System :

- The frequency range is 100 GHz to 1000 terahertz.
- Bandwidth capacity is less than 1 mbps.
- Attenuation depends on the quality of emitted light, its purity, atmospheric conditions .
- EMI is affected by intense light.
- Installation is fairly simple.

Applications of Infrared :

1. With these devices, we can talk via short range wireless signals.
2. With infrared transmission, computers can transfer files and other digital data bidirectional.
3. Very high data rates can be supported, due to very high bandwidth (approximately 400THz).
4. For communication between keyboard, mouse PCs and printers.
5. It is used in medical, scientific and industrial applications.

Unlock the Power of Placement Preparation!

Difference between Guided and Unguided Media

Prerequisite – Types of Transmission Media

Guided Media:

In this type of media, signal energy is enclosed and guided within a solid medium. The guided media is used either for point-to-point links or a shared link with various connections. In guided media, interference is generated by emissions in the adjacent cables. Proper shielding of guided media is required to reduce the interference issue.

Unguided Media:

In the unguided media, the signal energy propagates through a wireless medium. Wireless media is used for radio broadcasting in all directions. Microwave links are chosen for long-distance broadcasting transmission unguided media. Interference is also a problem in unguided media, overlapping frequency bands from competing signals can alter or eliminate a signal. Let's see the difference between the Guided Media and Unguided Media:

S. No.	Guided Media	Unguided Media
1.	The guided media is also called wired communication or bounded transmission media.	The unguided media is also called wireless communication or unbounded transmission media.
2.	The signal energy propagates through wires in guided media.	The signal energy propagates through the air in unguided media.
3.	Guided media is used for point-to-point communication.	Unguided media is generally suited for radio broadcasting in all directions.
4.	It is cost-effective.	It is expensive.
5.	Discrete network topologies are formed by the guided media.	Continuous network topologies are formed by the unguided media.
6.	Signals are in the form of voltage, current, or photons in the guided media.	Signals are in the form of electromagnetic waves in unguided media.
7.	Examples of guided media are twisted pair wires, coaxial cables, and optical fiber cables.	Examples of unguided media are microwave or radio links and infrared light.

S. No.	Guided Media	Unguided Media
8.	By adding more wires, the transmission capacity can be increased in guided media.	It is not possible to obtain additional capacity in unguided media.
9.	It sends out a signal that indicates which way to go.	It does not indicate which way to travel.
10.	For a shorter distance, this is the best option.	For longer distances, this method is used.
11.	It is unable to pass through walls.	It can pass through walls.

What are Ping and Latency ?

Ping (Packet Internet Groper) is a method for determining communication latency between two networks. Simply put, ping is a method of determining latency or the amount of time it takes for data to travel between two devices or across a network. As communication latency decreases, communication effectiveness improves.

A ping is a Command Prompt command that can be used to test a connection between one computer and another. A ping is **used to verify connectivity at an IP-level to a second TCP/IP device**