*Department of Information Technology*

*Faculty of Engineering and technology, UoS Jamshoro*

**Computer Communication and Networks ITEC-428**

**Semester Assignment**

1. **Discuss various guided transmission media (e.g. twisted Pair, Coaxial, Fiber optics) along with their types categories , connectors, and applications.**

Guided transmission media are cables like **twisted pair** cables, **coaxial cables**, and **fiber optic cables**. Unguided transmission media are **wireless**, such as infrared, radio waves, and microwaves. Connectors are used to connect the media with networking devices, and they are specific for each transmission medium.

There are **three types of guided media** which are Twisted-Pair Cable, Coaxial Cable and Fiber-Optic Cable are explained below.

**Twisted-Pair Cable:**

**wisted pair cabling** is a type of **wiring** in which two conductors of a single circuit are **twisted** together for the purposes of improving electromagnetic compatibility.

**TYPES:**

There are two main **types** of **twisted pair cables**, unshielded **twisted pair** (UTP), and shielded **twisted pair** (STP), which contains each **pair** of wires within an aluminium foil shield for further isolation.

**Speed:**1 Mbps

|  |  |
| --- | --- |
| Speed | 1 Mbps |
| Maximum nodes with/without repeaters | 256/64 |
| Maximum distance with/without repeaters | Greater than 10 km/2 km |
| Arbitration | bus arbiter |
| Cable type | twisted-pair |
| Header/Data size | 1 to 128 bytes |
| Major benefits | distributed data base/very deterministic |
| Primary applications | Real-time control/process/machine |

**Applications:**

**Twisted**-**pair cable** is a type of **cabling** that is used for telephone communications and most modern Ethernet networks. A **pair** of wires forms a circuit that can transmit data. The **pairs** are **twisted** to provide protection against crosstalk, the noise generated by adjacent **pairs**.

**Coaxial cable:**

Coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference. It is primarily used by cable TV companies to connect their satellite antenna facilities to customer homes and businesses. It is also sometimes used by telephone companies to connect central offices to telephone poles near customers. Some homes and offices use coaxial cable, too, but its widespread use as an [Ethernet](https://searchnetworking.techtarget.com/definition/Ethernet) connectivity medium in enterprises and data centers has been supplanted by the deployment of twisted pair cabling.

**Coaxial cable Types:**

The three most commonly used coaxial cable types for video applications are RG59/U, RG6/U and RG11/U.

[](https://www.accesscomms.com.au/products/y8058.htm)

[**RG59/U**](https://www.accesscomms.com.au/products/y8058.htm) is available with either solid copper or copper-clad-steel centre conductor. It's suitable for basic analog TV antenna feeds in residential applications and for basic CCTV systems over short cable runs. The copper-clad-steel type has high tensile strength and should be used when terminating the cable with F-Type connectors.

[](https://www.accesscomms.com.au/products/y8041.htm)

[**RG6/U Quad-shield**](https://www.accesscomms.com.au/products/y8041.htm) is the minimum requirement under the latest Australian Standard for [digital TV antenna cabling](http://www.dba.org.au/uploads/documents/Consumer_D.I.Y._140802_amend.pdf) and for all TV antenna cabling for apartments/units (MATV). It is also used for the distribution of Cable TV (CATV) and Satellite TV (SATV) in residential or commercial premises. It features a copper-clad-steel inner conductor. Single-shield, [dual-shield](https://www.accesscomms.com.au/products/y8021.htm) and tri-shield versions of RG6/U are available but do not provide adequate EMI shielding.



**RG11/U Quad-shield** is used for the same applications as RG6/U for either backbone cabling or for long distribution runs. It features a copper-clad-steel inner conductor.

**Applications**:

**Applications**. **Coaxial cable** is used as a transmission line for radio frequency signals. Its **applications** include feedlines connecting radio transmitters and receivers to their antennas, computer network (e.g., Ethernet) connections, digital audio (S/PDIF), and distribution of **cable** television signals.

**Fiber optic cable:**

1. a cable consisting of one or more thin flexible fibres with a glass core through which light signals can be sent with very little loss of strength.

digital cable TV is delivered via a network of high-speed fibre-optic cables.

**Fiber Optic Cable Types**

Typically customers will ask for either multimode or single mode fiber cable. They may be able to give you some specifics but not always. They may rely on you to decide the exact type of fiber they need. Every now and then you may have a more technical customer that asks for Fiber cable but gives you a specific type like OM3 fiber. Well what does that mean? What is OM3 or OM4 Fiber?

This section will review the more technical naming conventions and specifications for both Multimode and Single Mode Fiber.

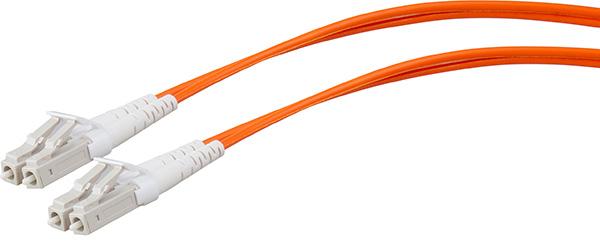
**Multimode Fibers – OM1, OM2, OM3, OM4 and OM5**

Multimode fibers are identified by the OM (optical mode) designation and their specifications are outlined by the ISO/IEC 11801 standard. Multimode cable disperses the light into multiple paths as it travels down the core. This allows for higher bandwidth over short to medium distances. However, on longer cable runs, multiple paths of light can cause distortion at the receiving end, resulting in an unclear and incomplete data transmission. For this reason, Multimode is generally only used for short distance applications like data centers.

**Types of Multimode Fiber Cable and Specifications**

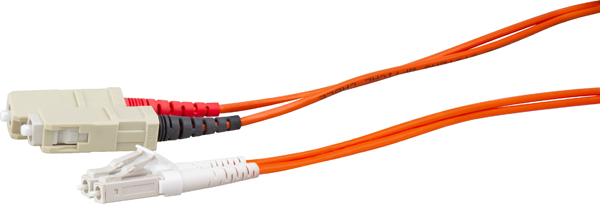
**OM1**

* Jacket Color – Orange
* Core Size – 62.5um
* Data Rate – 1Gb @ 850nm wavelength
* Distance – Up to 300 meters
* **Application** – Short-haul networks, Local Area Networks(LANs) & private networks



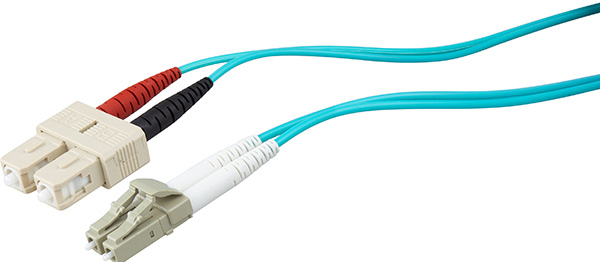
**OM2**

* Jacket Color – Orange
* Core Size – 50um
* Data Rate – 1Gb @ 850nm wavelength
* Distance – Up to 600 meters
* **Application** – Short-haul networks, Local Area Networks(LANs) & private networks
* Generally used for shorter distances. Has twice the distance capacity has OM1



**OM3 – Laser-Optimized Multimode**

* Jacket Color – Aqua
* Core Size – 50um
* Data Rate – 10Gb @ 850nm wavelength
* Distance – Up to 300 meters
* Uses fewer modes of light, enabling increased speeds
* Able to run 40GB or 100GB up to 100 meters utilizing an MPO connector
* **Application** – Larger Private Networks



**OM4 – Laser Optimized Multimode**

* Jacket Color – Aqua
* Core Size – 50um
* Data Rate – 10G @ 850nm wavelength
* Distance – Up to 550 meters
* Able to run 100GB up to 150 meters utilizing an MPO connector
* **Application** – High-Speed Networks, Data Centers, Financial Centers and Corporate Campuses



**OM5 – The latest and greatest in Multimode Fiber**

* Jacket Color – Lime Green
* Fully compatible and can mate with OM3 and OM4 cabling
* Utilizes a wider range of wavelengths between 850nm and 953nm
* Designed to support Short Wavelength Division Multiplexing (SWDM)
* Can Transmit 40 Gb/s and 100 Gb/s
* **Application** – High-speed Networks and Data Centers that require greater link distances and higher speeds.



**Multimode Fiber Summary**

Multimode fiber has come a long way in 30 years. It has evolved with the growing demand for more speed. Since OM1 and OM2 fiber could not support the higher speeds, OM3 and OM4 became the main choice for multimode fiber to support 25G, 40G and 100G Ethernet. With even greater demands on the horizon, OM5 was developed to extend the benefits of multimode fiber in data centers.

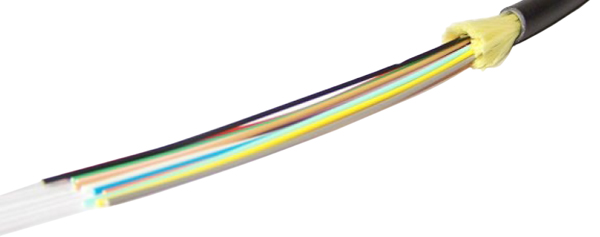
**Single Mode Fibers – OS1 and OS2**

Single Mode fibers are identified by the designation OS or Optical Single-mode Fiber. Single Mode cable has a much smaller core (8-9um) than multimode cable and uses a single path (mode) to carry the light. The main difference between single mode OS1 and OS2 is cable construction rather than optical specifications. OS1 type cable uses a tight buffered construction while OS2 is a loose tube or blown cable construction.

**OS1 Single Mode Tight Buffered Cable**

Each fiber has its own protective two-layer coating (color-coded for identification). One layer is plastic and the other is waterproof acrylate. The tight buffer allows for a smaller, lighter weight cable that is more flexible and crush resistant than Loose Tube. Installation is easier as there is no gel to clean up and no fan out kit required for connector termination.

**Application:** (Indoor Use) – moderate distance telco local loops, LANs and point-to-point links in cities, buildings, factories, office parks or campuses. OS1 can support speeds up to 10G and distances up to about 10km (6 miles).

Tight Buffered 12 Core

**OS2 Single Mode Loose Tube Cable**

All fibers are essentially bare other than their outer coating. Each fiber has a colored coating for identification. Other than this coating the fiber “floats” within a rugged, abrasion resistant, oversized tube usually filled with optical gel which protects the fibers from moisture. Connector termination requires a fan out kit.

**Application:** (Outdoor Use) high fiber count, long distance telco backbone and backhaul lines, direct bury applications along streets and railroads. OS2 can support speeds up to 100G and distances up to 200km (124 miles).

Loose Tube 12 Core

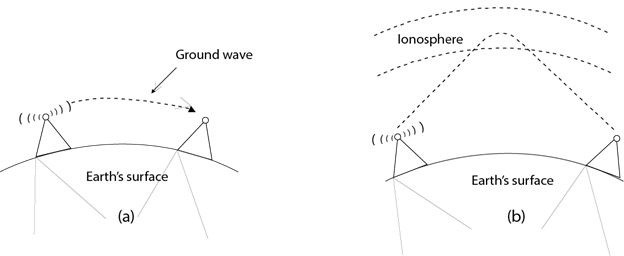
1. **Discuss various unguided transmission media (e.g. Radio, infrared, microwave) along with their coverage and applications.**

* An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
* In unguided media, air is the media through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

## **Radio waves**

* Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
* Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
* The range in frequencies of radio waves is from 3Khz to 1 khz.
* In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
* An example of the radio wave is **FM radio**.



**Applications Of Radio waves:**

* A Radio wave is useful for multicasting when there is one sender and many receivers.
* An FM radio, television, cordless phones are examples of a radio wave.

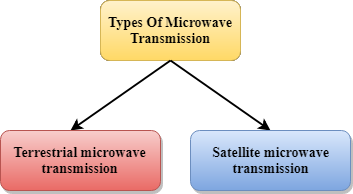
## **Infrared**

* An infrared transmission is a wireless technology used for communication over short ranges.
* The frequency of the infrared in the range from 300 GHz to 400 THz.
* It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

**Characteristics Of Infrared:**

* It supports high bandwidth, and hence the data rate will be very high.
* Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
* An infrared communication provides better security with minimum interference.
* Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

## **Microwaves**



Microwaves are of two types:

* Terrestrial microwave
* Satellite microwave communication.

**Characteristics of Microwave:**

* **Frequency range:** The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
* **Bandwidth:** It supports the bandwidth from 1 to 10 Mbps.
* **Short distance:** It is inexpensive for short distance.
* **Long distance:** It is expensive as it requires a higher tower for a longer distance.
* **Attenuation:** Attenuation means loss of signal. It is affected by environmental conditions and antenna size.
  1. **What signals are used in Wifi, Bluetooth, NFC, Zigbee communication protocols.**

Other surfaces of attack that threaten mobile data security are wireless communication protocols. Whether it is WiFi, Zigbee, Bluetooth, radio, or NFC, wireless communication media pose threats to the safety of mobile data. Zigbee exploitations were illustrated in several studies, including the recent findings depicted in Refs. [72,73], which depicted the pitfalls in Zibgee implementations in some smart-home devices. The main issue with the Zigbee protocol pertained to insecure key exchange, which rendered critical data accessible in almost-plain format to eavesdroppers within the communication range of the designated devices. Weakly secured key-exchange processes allowed the researchers to jam wireless signals, identify target devices, and reset them to factory settings. To achieve their goal of breaking the Zigbee protocol in the examined devices, researchers did not even need prior knowledge of any secret keys. Vulnerabilities in Zigbee have been identified years before such recent studies. For example, the work in Ref. [74] depicts a Zigbee exploitation framework that capitalizes on Zigbee's killer vulnerability of plaintext key-exchange as well as its susceptibility to replay attacks. The work in Ref. [74] also shows that the Zigbee protocol implementation where plaintext key-exchange was replaced with hard-coding critical keys in devices' memories was not anymore secure, as breaking into the device's memories to extract the plain keys was easy, relatively speaking.

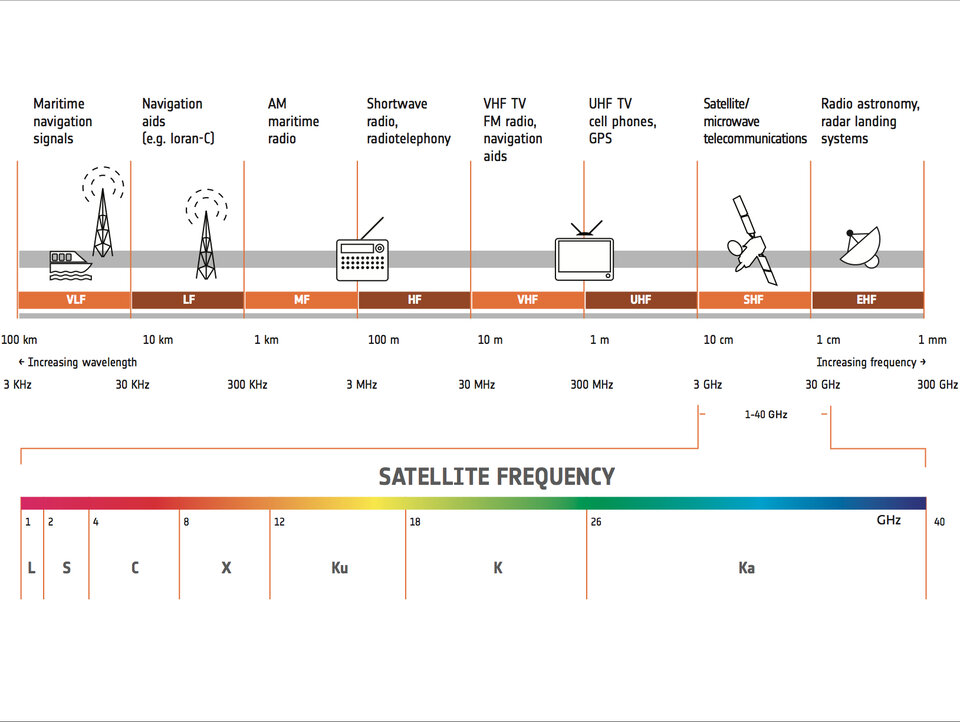
* 1. **Write down frequency bands used by Wifi, Bluetooth, NFC, Zigbee communication protocols.**

2.4GHz

* Zigbee uses the global standard 2.4**GHz** ISM frequency band, whereas Z- Wave uses the 915 **MHz** ISM band (in the U.S.) and the 868 **MHz** RFID band (in Europe).
  1. **What signals are used by satellites, walkie talkie and cell phones.** 
     + Satellites communicate by using **radio waves** to send signals to the antennas on the Earth. The antennas then capture those signals and process the information coming from those signals.
     + **Walkie talkies** are handheld portable radios that **use radio** waves to communicate wirelessly on a single frequency band.
     + Cell phones use **radio waves** to communicate. **Radio waves** transport digitized **voice** or data in the form of oscillating electric and magnetic fields, called the electromagnetic field (EMF). The rate of oscillation is called **frequency**. **Radio waves** carry the information and travel in air at the **speed** of light.
  2. **Write down frequency bands used by satellites, walkie talkie and cell phones.**

**Satellites:**

Satellite technology is developing fast, and the applications for satellite technology are increasing all the time. Not only can satellites be used for radio communications, but they are also used for astronomy, weather forecasting, broadcasting, mapping and many more applications.

****

Walkie Talkie:

The Family Radio Service (FRS) is an improved walkie-talkie radio system authorized in the United States since 1996. This personal radio service uses channelized frequencies around 462 and 467 **MHz** in the ultra high frequency (UHF) band.

**Cell Phones:**

### 5G and 4G LTE Frequency Bands

|  |  |  |
| --- | --- | --- |
| **Carriers:** | **5G Bands and Frequencies:** | **4G LTE Bands and Frequencies:** |
|  |  |  |
| **AT&T** | 850 MHz: Band n5 39GHz: Band n260 | 700 MHz: Bands 12/17/29 850 MHz: Band 5 1900 MHz: Band 2 1700 MHz /2100 MHz: Bands 4/66 2300 MHz: Band 30 |
| **Verizon Wireless** | 28 GHz: Band n261 39 GHz: Band n260 | 700 MHz: Band 13 850 MHz: Band 5 1700/2100 MHz: Bands 4/66 1900 MHz: Band 2 |
| **T-Mobile** | 600 MHz: Band n71 2.5 GHz: Band n41 39 GHz: Band n260 28 GHz: Band n261 | 600 MHz: Band 71 700 MHz: Band 12 850 MHz: Band 5 1700/2100 MHz: Bands 4/66 1900 MHz: Band 2 |
| **Sprint** | 2.5 GHz: Band n41 | 800 MHz: Band 26 1900 MHz: Band 25 2500 MHz: Band 41 |
| **U.S. Cellular** | 600 MHz: Band n71 | 700 MHz: Band 12 850 MHz: Band 5 1700/2100: Band 4 1900: Band 2 |
| **Cricket Wireless** | 850 MHz: Band n5 | 700 MHz: Bands 17 1900 MHz: Band 2 1700 MHz /2100 MHz: Band 4 2300 MHz: Band 30 |
| **Boost Mobile** | 2.5 GHz: Band n41 | 800 MHz: Band 26 1900 MHz: Band 25 2500 MHz: Band 41 |
| **Metro by T-Mobile** | 600 MHz: Band n71 | 600 MHz: Band 71 700 MHz: Band 12 850 MHz: Band 5 1700/2100 MHz: Bands 4/66 1900 MHz: Band 2 |

### 3G Frequency Bands

|  |  |  |
| --- | --- | --- |
| **Carriers:** | **Network:** | **3G Bands and Frequencies:** |
| **AT&T** | GSM/UMTS/HSPA+ | 850 MHz: Band 5 1900 MHz: Band 2 |
| **Verizon Wireless** | CDMA | 850 MHz: Band 0 1900 MHz: Band 1 |
| **T-Mobile** | GSM/UMTS/HSPA+ | 1900 MHz: Band 2 1700/2100 MHz: Band 4 |
| **Sprint** | CDMA | 800 MHz: Band 10 1900 MHz: Band 2 |
| **U.S. Cellular** | CDMA | 850 MHz: Band 5 1900 MHz: Band 2 |
| **Cricket Wireless** | GSM/UMTS/HSPA+ | 850 MHz: Band 5 1900 MHz: Band 2 |
| **Boost Mobile** | CDMA | 800 MHz: Band 10 1900 MHz: Band 2 |
| **Metro by T-Mobile** | GSM/UMTS/HSPA+ | 1900 MHz: Band 2 1700/2100 MHz: Band 4 |

1. **Discuss significance of Multiple Access Control (MAC) Protocols.**

A media access control is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable. The media access control policy involves sub-layers of the data link layer 2 in the OSI reference model.

The essence of the MAC protocol is to ensure non-collision and eases the transfer of data packets between two computer terminals. A collision takes place when two or more terminals transmit data/information simultaneously. This leads to a breakdown of communication, which can prove costly for organizations that lean heavily on[data transmission](https://www.getkisi.com/blog/robust-physical-security-access-control-for-the-one-percent-cases).

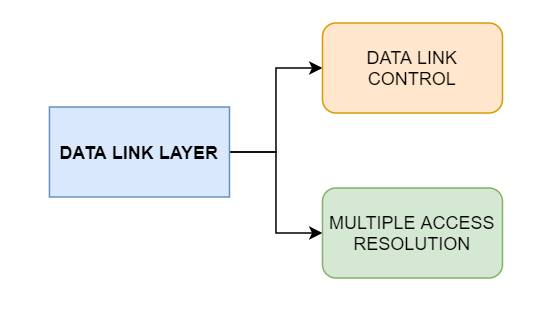
1. **Discuss various types of Random Acess Control (e.g Pure ALOHA, Slotted ALLOHA, CSMA/CD) protocols.**

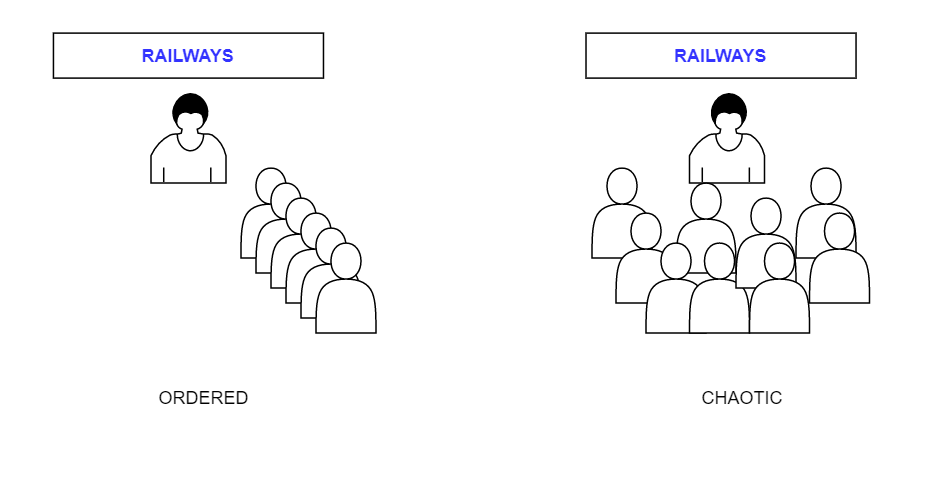
Random Access Protocols is a Multiple access protocol that is divided into four categories which are ALOHA, CSMA, CSMA/CD, and CSMA/CA. In this article, we will cover all of these Random Access Protocols in detail.

Have you ever been to a railway station? And noticed the ticket counter over there?

Above are the scenarios for approaching a ticket counter. Which one do you think is more productive? The ordered one, right? And we all know the reason why. Just to get things working and avoid problems we have some rules or protocols, like "please stand in the queue", "do not push each other", "wait for your turn", etc. in the same way computer network channels also have protocols like **multiple access protocols**, **random access protocols**, etc.

Let's say you are talking to your friend using a mobile phone. This means there is a link established between you and him. But the point to be remembered is that the communication channel between you and him (the sender & the receiver or vice-versa) is not always a dedicated link, which means the channels are not only providing service to you at that time but to others as well. This means multiple users might be communicating through the same channel.





The random access protocols consist of the following characteristics:

1. There is **no time restriction for sending the data** (you can talk to your friend without a time restriction).
2. There is a **fixed sequence of stations** which are transmitting the data.

As in the above diagram you might have observed that the random-access protocol is further divided into four categories, which are:

1. ALOHA
2. CSMA
3. CSMA/CD
4. CSMA/CA
5. **Discuss various types of controlled Access Control (e.g. Reservation, Polling, Token Passing) Protocols**
   1. **Which access method is used in Ethernet LANs?**
   2. **Which access method is used in Token Ring LANs?**
   3. **Which access method is used in Fiber Distributed Data Interface (FDDI) LANs?**
   4. **Which access methods is used in wireless LANs?**

Can two people speak at the same time and still understand each other's statements? Well, not. The same goes for **data-frames in a computer network**. If we transmit two frames at a time, they'll collide with each other, and data will get lost.

Before discussing Controlled access protocols, please do refer to [Random access protocols](https://www.studytonight.com/post/random-access-protocols-aloha-csma-csmaca-and-csmacd).

So **how are controlled access protocols different from random access protocols?**

The difference is, only that station can transmit the data which is approved by all other stations in that network. And we saw that in random access protocols the transmission is based on the availability of the transmission channel.

So, here in controlled access protocols only one station can transmit the data-frames at a time, which leads us to a collision-free transmission through the communication channel.

Let us now discuss the types of controlled access protocols. There are three types of Controlled access protocols:

1. Reservation
2. Polling
3. Token Passing

Let's learn about them one by one.

## **Reservation**

Whenever we travel from a train or an airplane, the first thing we do is to reserve our seats, similarly here a station must make a reservation first before transmitting any data-frames.

This reservation timeline consists of two kinds of periods:

1. Reservation interval of a fixed time duration
2. Data transmission period of variable frames

Consider there are 4 stations then the reservation intervals are divided into 4 slots so that each station has a slot. Means if n number of stations are there then n slot will be allotted.

## **Polling**

Recall your school or college classroom, what was the first thing the teacher does after entering the class? The answer is roll call or attendance. Let's compare the scenario. The teacher calls roll number 1 and gets a response if he/she is present then switches to the next roll number, say roll number two and roll number 2 is absent, so the teacher gets no response in return or say a negative response. Similarly, in a computer network there is a primary station or controller (teacher) and all other stations are secondary (students), the primary station sends a message to each station. The message which is sent by the primary station consists of the address of the station which is selected for granting access.

We calculate the efficiency of this method in terms of time for polling & time required for transmission of data.

*Tpoll = time for polling*

*Tt = time required for transmission of data*

So, **efficiency = Tt / (Tt + Tpoll)**

## **Token Passing**

Now, say 4 people are sitting on a round table and only that person can speak who has the token. In computer networks a token is a special bit pattern that allows the token possessing system to send data or we can say that a token represents permission to transmit data. The token circulation around the table (or a network ring) is in a predefined order. A station can only pass the token to its adjacent station and not to any other station in the network. If a station has some data queued for transmission it can not transmit the data until it receives the token and makes sure it has transmitted all the data before passing on the received token.

This method has some drawbacks like duplication of token or sometimes the token is damaged or lost during the circulation, or some times if we introduce a new station or remove an existing station from the network, this leads to a huge disturbance, which should be taken care of so that the efficiency of the method is not affected.

The performance of a token ring is governed by 2 parameters, which are delay and throughput.

**Delay**is a measure of the time; it is the time difference between a packet ready for transmission and when it is transmitted. Hence, the average time required to send a token to the next station is a/N.

**Throughput**is a measure of the successful traffic in the communication channel.

**Throughput, S = 1/ (1 + a/N) for a<1**

**S = 1/[a(1+1/N)] for a>1, here N = number of stations & a = Tp/Tt**

**Tp = propagation delay &Tt = transmission delay**

* 1. **Which access method is used in Ethernet LANs?**

IEEE 802.11 wireless LANs use a media access control protocol called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). While the name is similar to Ethernet's Carrier Sense Multiple Access with Collision Detection (CSMA/CD), the operating concept is totally different.

WiFi systems are the half duplex shared media configurations, where all stations transmit and receive on the same radio channel. The fundamental problem of a radio system is that a station cannot *hear* while it is sending, and hence it is impossible to detect a collision. Because of this, the developers of the 802.11 specifications came up with a collision avoidance mechanism called the **Distributed Control Function** (DCF).

According to DCF, a WiFi station will transmit only when the channel is clear. All transmissions are acknowledged, so if a station does not receive an acknowledgement, it assumes a collision occurred and retries after a random waiting interval.

The incidence of collisions will increase as the traffic increases or in situations where mobile stations cannot hear each other.

* 1. **Which access method is used in Token Ring LANs?**

**Token Ring** is a [computer networking](https://en.wikipedia.org/wiki/Computer_network) technology used to build [local area networks](https://en.wikipedia.org/wiki/Local_area_network). It was introduced by [IBM](https://en.wikipedia.org/wiki/IBM) in 1984, and standardized in 1989 as [**IEEE**](https://en.wikipedia.org/wiki/IEEE_Standards_Association)**802.5**.

It uses a special three-byte [frame](https://en.wikipedia.org/wiki/Frame_(networking)) called a *token* that travels around a logical *ring* of workstations or [servers](https://en.wikipedia.org/wiki/Server_(computing)). This [token passing](https://en.wikipedia.org/wiki/Token_passing) is a [channel access method](https://en.wikipedia.org/wiki/Channel_access_method) providing fair access for all stations, and eliminating the [collisions](https://en.wikipedia.org/wiki/Collision_(telecommunications)) of [contention](https://en.wikipedia.org/wiki/Contention_(telecommunications))-based access methods.

* 1. **Which access method is used in Fiber Distributed Data Interface (FDDI) LANs?**

Fiber Distributed Data Interface (FDDI) is a set of ANSI and ISO standards for transmission of data in local area network (LAN) over fiber optic cables. It is applicable in large LANs that can extend up to 200 kilometers in diameter

* 1. **Which access methods is used in wireless LANs?**

IEEE 802.11 wireless LANs use a media access control protocol called Carrier Sense Multiple Access with Collision **Avoidance** (CSMA/CA). While the name is similar to Ethernet's Carrier Sense Multiple Access with Collision Detection (CSMA/CD), the operating concept is totally different.

1. **Discuss the significance of private IPV4 address** .

In IPv4, link-local addresses are codified in [RFC 6890](https://tools.ietf.org/html/rfc6890) and [RFC 3927](https://tools.ietf.org/html/rfc3927). Their utility is in [zero configuration networking](https://en.wikipedia.org/wiki/Zero_configuration_networking) when [Dynamic Host Configuration Protocol](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol) (DHCP) services are not available and manual configuration by a network administrator is not desirable. The block *169.254.0.0/16* was allocated for this purpose. If a host on an IEEE 802 ([Ethernet](https://en.wikipedia.org/wiki/Ethernet)) network cannot obtain a network address via DHCP, an address from *169.254.1.0* to *169.254.254.255*[[Note 2]](https://en.wikipedia.org/wiki/Private_network#cite_note-7) may be assigned [pseudorandomly](https://en.wikipedia.org/wiki/Pseudorandom). The standard prescribes that address collisions must be handled gracefully.