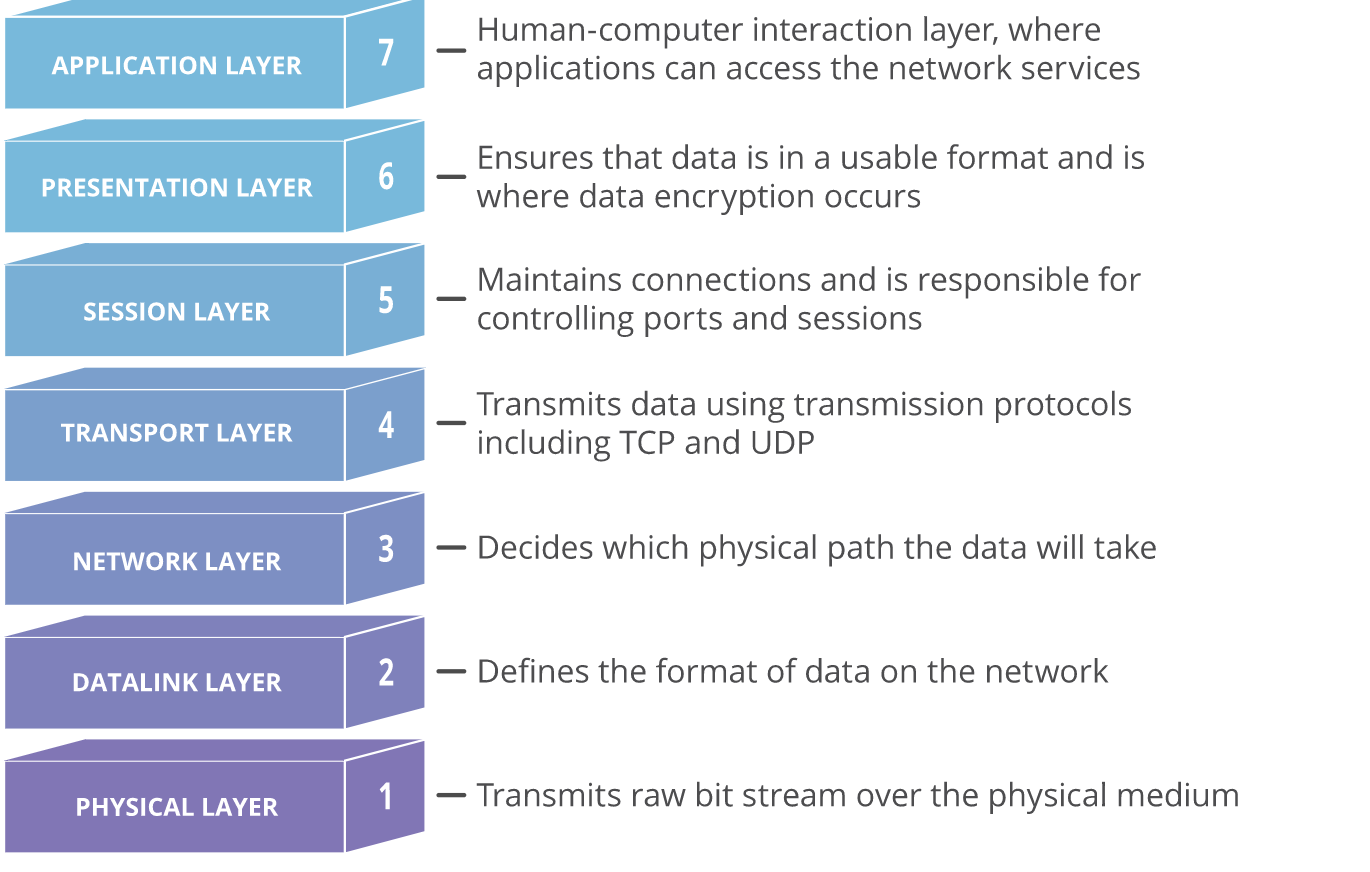
**Data Communication and Computer Networks Lab**

**Study of different types of physical layer wired/wireless connections**

* **The Open System Interconnection (OSI) model:**
* The Open Systems Interconnection (OSI) model is a conceptual model created by the **International Organization for Standardization (ISO)** which enables diverse communication systems to communicate using standard protocols. In plain English, the OSI provides a standard for different computer systems to be able to communicate with each other.[1]
* The OSI model can be seen as a universal language for computer networking. It’s based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.[1]



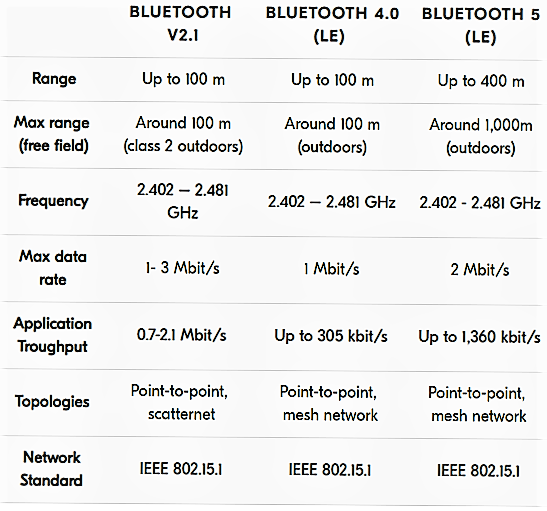
* Each layer of the OSI model handles a specific job and communicates with the layers above and below itself. But in this experiment, we will talk about the lowest layer of the OSI model i.e. **Physical Layer**
* **Physical Layer – OSI Model:**
* This layer includes the physical equipment involved in the data transfer, such as the cables and switches. This can include everything from the cable type, radio frequency link (as in an 802.11 wireless systems), as well as the layout of pins, voltages and other physical requirements. This is also the layer where the data gets converted into a bit stream, which is a string of 1s and 0s. The physical layer of both devices must also agree on a signal convention so that the 1s can be distinguished from the 0s on both devices.
* In the further discussion, we divide the Physical Layer into two depending upon the medium of transmission, discus their various parameters and show their scalability and applicability in different architectures such as LAN, WAN, MAN, PAN etc.
* **Wireless Transmission Media**
* Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.
* When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range. The receptor on the other end receives these signals and converts them back to digital data.
* A little part of electromagnetic spectrum can be used for wireless transmission.[3]



* **Range and Specification of Some wireless media:**

1. **Bluetooth**

* Bluetooth wireless technology is a short-range communications technology intended to replace the cables connecting portable unit and maintaining high levels of security. Bluetooth technology is based on Ad-hoc technology also known as Ad-hoc Pico nets, which is a local area network with a very limited coverage.[2]
* Bluetooth employs Radio Frequency (RF) for communication. It makes use of **frequency modulation** to generate radio waves in the **ISM** band.
* Bluetooth technology operates in **the unlicensed industrial, scientific and medical** (ISM) band at **2.4 to 2.485 GHZ**, using a spread spectrum hopping, full-duplex signal at a nominal rate of 1600 hops/sec. the 2.4 GHZ ISM band is available and unlicensed in most countries.
* Bluetooth supports **1Mbps data rate for version 1.2** and **3Mbps data rate for Version 2.0** combined with Error Data Rate**.**
* Bluetooth operating range depends on the device Class 3 radios have a range of up to 1 meter or 3 feet Class 2 radios are most commonly found in mobile devices have a range of 10 meters or 30 feet Class 1 radios are used primarily in industrial use cases have a range of 100 meters or 300 feet.[2]



* **Scalability**
* Bluetooth uses short-range radio waves. Uses in a WPAN include, for example, Bluetooth devices such as keyboards, pointing devices, audio headsets, printers may connect to smartwatches, cell phones, or computers.
* A Bluetooth WPAN is also called a piconet, and is composed of up to 8 active devices in a master-slave relationship (a very large number of additional devices can be connected in parked mode).).
* the first Bluetooth device in the piconet is the master, and all other devices are slaves that communicate with the master.
* A piconet typically has a range of 10 meters (33 ft), although ranges of up to 100 meters (330 ft) can be reached under ideal circumstances. Long-range Bluetooth routers with augmented antenna arrays connect Bluetooth devices up to 1,000 feet.

1. **Infrared Technology**

* Infrared (IR) is a wireless mobile technology used for device communication over short ranges. Infrared wave lies in between visible light spectrum and microwaves. It has wavelength of **700-nm to 1-mm and frequency ranges from 300-GHz to 430-THz.[4]**
* **Infrared Data Association** (IrDA) device communication is usually exchanged on a one-to-one basis. Thus, data transmitted between IrDA devices is normally unencrypted.
* IR-enabled devices are known as IrDA devices because they conform to standards set by the Infrared Data Association (IrDA). IR light-emitting diodes (LED) are used to transmit IR signals, which pass through a lens and focus into a beam of IR data. The beam source is rapidly switched on and off for data encoding.
* Infrared wave is used for very short-range communication purposes such as television and it’s remote. Infrared travels in a straight line hence it is directional by nature. Because of high frequency range, Infrared cannot cross wall-like obstacles.[4]

1. **ZigBee**

* Zigbee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless IoT networks. The Zigbee standard operates on the **IEEE 802.15.4** physical radio specification and operates in unlicensed bands including **2.4 GHz, 900 MHz and 868 MHz**
* Zigbee is low-cost and low-powered mesh network widely deployed for controlling and monitoring applications where it covers **10-100 meters** within the range. This communication system is less expensive and simpler than the other proprietary short-range wireless sensor networks as Bluetooth and Wi-Fi.
* The Zigbee 3.0 protocol is designed to communicate data through noisy RF environments that are common in commercial and industrial applications. The date rate of **250 kbps** is best suited for periodic as well as intermediate two-way transmission of data between sensors and controllers. **Version 3.0** builds on the existing ZigBee standard but unifies the market-specific application profiles to allow all devices to be wirelessly connected in the same network, irrespective of their market designation and function.
* Zigbee enables broad-based deployment of wireless networks with low-cost, low-power solutions. It provides the ability to run for years on inexpensive batteries for a host of monitoring and control applications. Smart energy/smart grid, AMR (Automatic Meter Reading), lighting controls, building automation systems, tank monitoring, HVAC control, medical devices and fleet applications are just some of the many spaces where Zigbee technology is making significant advancements.[5]
* **Scalability**:
* The technology defined by the Zigbee specification is intended to be simpler and less expensive than other wireless personal area networks (WPANs), such as Bluetooth or more general wireless networking such as Wi-Fi.
* Applications include wireless light switches, home energy monitors, traffic management systems, and other consumer and industrial equipment that require short-range low-rate wireless data transfer.

1. **Near Field Communication (NFC)**

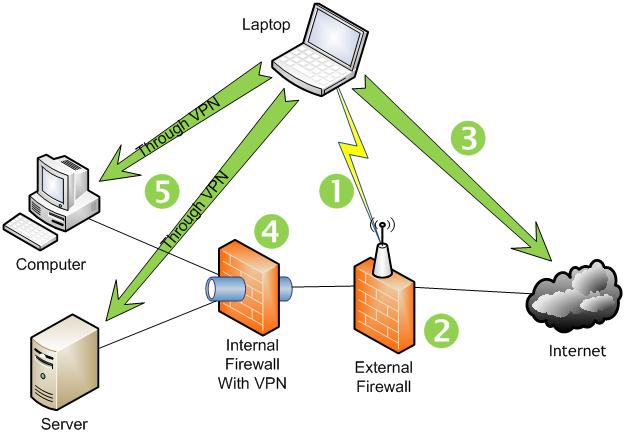
* Near-field communication (NFC) allows data to be exchanged between devices via short-range, high-frequency wireless communication technology by combining the interface of a smartcard and reader into a single device.
* NFC is a standards-based technology used to provide short range wireless connectivity technology that carry secure two-way interactions between electronic devices. Communications are established in a simple way, not requiring set-up by users as in the case of many other wireless communications. As such NFC enables users to perform contactless transactions, access digital content and connect electronic devices by touching devices together.
* NFC near field communication provides contactless communication up to **distances of about 4 or 5 centimeters**. In this way their communications are inherently more secure because devices normally only come into contact and hence communication when the user intends this.
* NFC is a form of **RFID**, but it has a specific set of standards governing its operation, interface, etc. This means that NFC equipment, and elements from a variety of manufacturers can be used together. The NFC standards determine not only the contactless operating environment, but also the data formats and data transfer rates.
* NFC utilizes inductive-coupling, at a frequency of **13.56 MHz** - a license free allocation in the **HF portion of the radio spectrum** and using the **ISO/IEC 18000-3** air interface standard at data rates ranging from **106 to 424 Kbit/s. [6]**

1. **Wireless Fidelity (Wi-Fi)**

* Wi-Fi is a family of wireless network protocols, based on the **IEEE 802.11** family of standards, which are commonly used for local area networking of devices and Internet access. Wi-Fi uses

multiple parts of the **IEEE 802** protocol family and is designed to interwork seamlessly with its wired sibling Ethernet. Compatible devices can network through wireless access points to each other as well as to wired devices and the Internet.

* Wi-Fi allows local area networks to operate without cable and wiring. It is making popular choice for home and business networks. A computer’s wireless adaptor transfers the data into a radio signal and transfers the data into antenna for users.
* The radio signals are transmitted from antennas and routers that signals are picked up by Wi-Fi receivers, such has computers and cell phones that are ready with Wi-Fi cards. Whenever the computer receives the signals within the range **of 100-150 feet** for router it connects the device immediately. The range of the Wi-Fi is depending upon the environment, indoor or outdoor ranges. The Wi-Fi cards will read the signals and create an internet connection between user and network. The speed of the device using Wi-Fi connection increases as the computer gets closer to the main source and speed is decreases computer gets further away.
* An access point (or hotspot) often has a range of about **20 meters indoors** while some modern access points claim up to a **150-metre range outdoors**. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers using many overlapping access points with roaming permitted between them. Over time the speed and spectral efficiency of Wi-Fi have increased. As of 2019, at close range, some versions of Wi-Fi, running on suitable hardware, can achieve speeds of over 1 Gbit/s.[7]
* Scalability
* Compared to cell phones and similar technology, Wi-Fi transmitters are low power devices. In general, the maximum amount of power that a Wi-Fi device can transmit is limited by local regulations, such as FCC Part 15 in the US.
* Equivalent isotropically radiated power (EIRP) in the European Union is limited to 20 dBm (100 mW). To reach requirements for wireless LAN applications, Wi-Fi has higher power consumption compared to some other standards designed to support wireless personal area network (PAN) applications.
* For example, Bluetooth provides a much shorter propagation range between 1 and 100m[74] and so in general have a lower power consumption. Other low-power technologies such as ZigBee have fairly long range, but much lower data rate.
* The high power consumption of Wi-Fi makes battery life in some mobile devices a concern.[7]



1. **Cellular Network**

* Cellular network is an underlying technology for mobile phones, personal communication systems, wireless networking etc. The technology is developed for mobile radio telephone to replace high power transmitter/receiver systems. Cellular networks use lower power, shorter range and more transmitters for data transmission.
* The coverage area of cellular networks are divided into cells, each cell having its own antenna for transmitting the signals. Each cell has its own frequencies. Data communication in cellular networks is served by its base station transmitter, receiver and its control unit.
* The shape of cells can be either square or hexagon.
* When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.[8]

**Specifications:**

* ● Range: A cellular network is used by the mobile phone operator to achieve both coverage and capacity for their subscribers. Large geographic areas are split into smaller cells to avoid line of-sight signal loss and to support a large number of active phones in that area.
* In cities, each cell site may have a range of up to approximately 1 ⁄2 mile (0.80 km), while in rural areas, the range could be as much as 5 miles (8.0km). It is possible that in clear open areas, a user may receive signals from a cell site 25 miles (40 km) away.

**LTE (Long-Term Evolution) (Type of Cellular Network)**:

* Long-Term Evolution (LTE) is a standard for wireless broadband communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA technologies. It increases the capacity

and speed using a different radio interface together with core network improvements.

* LTE offers high peak data transfer rates -- up to 100 Mbps downstream and 30 Mbps upstream. It also provides reduced latency, scalable bandwidth capacity and backward-compatibility with existing GSM

and UMTS technology. Future developments could yield peak throughput on the order of 300 Mbps.

* LTE devices use QPSK, 16QAM and 64QAM to modulate data and control information.
* LTE bandwidths range from 15MHz to 200MHz
* LTE is used for high speed Internet connections for mobile devices and it is also used in communication with VoLTE(Voice over LTE). [23]

1. **Li-fi**

* LiFi is a wireless technology holds the key to solving challenges faced by 5G. LiFi can transmit at multiple gigabits, is more reliable, virtually interference free and uniquely more secure than radio technology such as Wi-Fi or cellular. LiFi is a mobile wireless technology that uses light rather than radio frequencies to transmit data. The technology is supported by a global ecosystem of companies driving the adoption of LiFi, the next generation of wireless that is ready for seamless integration into the 5G core. Li-Fi is a derivative of optical wireless communications (OWC) technology, which uses light from light-emitting diodes (LEDs) as a medium to deliver network, mobile, high-speed communication in a similar manner to Wi-Fi. The Li-Fi market was projected to have a compound annual growth rate of 82% from 2013 to 2018 and to be worth over $6 billion per year by 2018. However, the market has not developed as such and Li-Fi remains with a niche market, mainly for technology evaluation.[24]
* **Specifications:**
* **Security**: Radio waves can be intercepted by people outside your network since they can pass through walls compromising the security of your data. But light is stopped by opaque objects making LiFi significantly more secure than other wireless technologies. You wont have to worry about leaking your connection to public spaces potentially giving other people access to your network. Some rooms could even be designated as high- security areas with their own LiFi networks, isolating them from other areas of the building where vulnerable IoT devices might be connected.
* **Range:** The fact that light cant penetrate through walls might be a good thing when it comes to security but this also means that LiFi has a very limited range. That means you can only use it effectively in closed spaces. In establishments, lights must be tactically placed in rooms, and halls to expand the scope of the LiFi network. In open spaces, Wi-Fis coverage can go up to 32 meters but LiFi can only go up to 10 meters.
* **Scalability**:

The technology defined by the LiFi specification is intended to be used as a wireless personal area networks (WPANs), such as WiFi or more general wireless networking.[24]



1. **WiMax**

* WiMAX is one of the hottest broadband wireless technologies around today. WiMAX systems are expected to deliver broadband access services to residential and enterprise customers in an economical way. Loosely, WiMax is a standardized wireless version of Ethernet intended primarily as an alternative to wire technologies (such as Cable Modems, DSL and T1/E1 links) to provide broadband access to customer premises.
* More strictly, WiMAX is an industry trade organization formed by leading communications, component, and equipment companies to promote and certify compatibility and interoperability of broadband wireless access equipment that conforms to the IEEE 802.16 and ETSI HIPERMAN standards. WiMAX would operate similar to WiFi, but at higher speeds over greater distances and for a greater number of users. WiMAX has the ability to provide service even in areas that are difficult for wired infrastructure to reach and the ability to overcome the physical limitations of traditional wired infrastructure. WiMAX was formed in April 2001, in anticipation of the publication of the original 10-66 GHz IEEE 802.16 specifications. WiMAX is to 802.16 as the WiFi Alliance is to 802.11.

WiMAX can provide two forms of wireless service −

* Non-line-of-sight − service is a WiFi sort of service. Here a small antenna on your computer connects to the WiMAX tower. In this mode, WiMAX uses a lower frequency range -- 2 GHz to 11 GHz (similar to WiFi).
* Line-of-sight − service, where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. The line-of-sight connection is stronger and more stable, so it’s able to send a lot of data with fewer errors. Line-of sight transmissions use higher frequencies, with ranges reaching a possible 66 GHz.
* **Use of Wireless Media in different Network Architecture:**

1. **Wireless PAN (Personal Area Network)**

* The main characteristic of the WPAN:
* Short-Range Communication
* Low Power Consumption
* Low Cost
* Small Personal Networks
* Communication of devices with personal space
* While providing these features, a WPAN has to achieve two main goals: broad market applicability and device interoperability. It is important that the WPAN specification addresses the leading device categories that require wireless connectivity in a way that is both easy to implement and affordable
* Three wireless standards are leading the way for WPANs: IrDA, Bluetooth, and IEEE 802.15. Each of these standards enables users to connect a variety of devices without having to buy, carry, or connect cables. They also provide a way to establish ad hoc networks among the abundance of mobile devices on the market.
* WiMAX can provide two forms of wireless service −
* Non-line-of-sight − service is a WiFi sort of service. Here a small antenna on your computer connects to the WiMAX tower. In this mode, WiMAX uses a lower frequency range -- 2 GHz to 11 GHz (similar to WiFi).
* Line-of-sight − service, where a fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. The line-of-sight connection is stronger and more stable, so it39;s able to send a lot of data with fewer errors. Line-ofsight transmissions use higher frequencies, withranges reaching a possible 66 GHz. [9]

1. **Wireless LAN (Local Area Network)**

* Wireless LAN stands for Wireless Local Area Network. It is also called LAWN (Local Area Wireless Network). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.
* The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm.
* Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.[10]

1. **Wireless MAN (Metropolitan Area Network)**

* Wireless MANs offer connections between buildings and users within a city or campus area through several system configurations. In most cases, the wireless MAN beams RF or infrared light from one point to another using directive antennae.
* Wireless Metropolitan Area Network (WMAN), like WLAN and WPAN, is a generic term for networking confined to a geographical area and a set of specific networking technologies that provide wireless communications in metropolitan areas. WMAN is a new technology that will be a supplement to well-known wired technologies such as Resilient Packet Ring (RPR), Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH), SONET over IP, Gigabit Ethernet, and Wavelength Division Multiplexing (WDM).
* The area of coverage of WMAN falls between WLAN/WPAN, which are customer premises networks, and Wireless Wide Area Networks (WWAN), which are associated with cellular radio mobile networks. Methods of access to WMANs have some resemblance to those of broadband wired access technologies such as Digital Subscriber Line (DSL) and Data over Cable Service Interface Specifications (DOCSIS).[11]

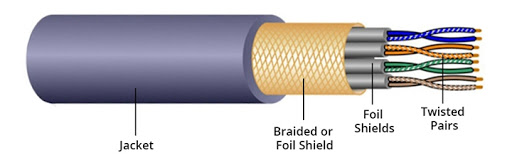
1. **Wireless WAN (Wide Area Network)**

* Wireless wide area networks are wireless networks that typically cover large areas, such as between neighboring towns and cities, or city and suburb. These networks can be used to connect branch offices of business or as a public Internet access system. The wireless connections between access points are usually point to point microwave links using parabolic dishes on **the 2.4 GHz and 5.8Ghz band**, rather than omnidirectional antennas used with smaller networks. A typical system contains base station gateways, access points and wireless bridging relays. Other configurations are mesh systems where each access point acts as / a relay also. When combined with renewable energy systems such as photovoltaic solar panels or wind systems they can be standalone systems.

1. **Global Area Network**

* A global area network (GAN) refers to a network composed of different interconnected networks that cover an unlimited geographical area. The term is loosely synonymous with Internet, which is considered a global area network.
* Global area network (GAN)refers to any network that is composed of different interconnected computer networks (WANs) and also covers an unlimited geographical area.
* Unlike local area networks (LAN) and wide area networks (WAN), GANs cover a large geographical area. Because a GAN is used to support mobile communication across a number of wireless LANs, the key challenge for any GAN is transferring user communications from one local coverage area to the next.
* The most sought-after GAN type is a broadband GAN. The broadband GAN is a global satellite Internet network that uses portable terminals for telephony. The terminals connect laptop computers located in remote areas to broadband Internet.[12]
* **Wired Transmission Media**
* Transmission media is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
* In Wired Transmission Media, **medium characteristics** are more important where as in wireless transmission media, **signal characteristics** are important.
* In general, wired communications are considered to be the most stable of all types of communications services. They are relatively impervious to adverse weather conditions in comparison to wireless communication solutions. These characteristics have allowed wired communications to remain popular even as wireless solutions have continued to advance.[13]
* **Range and Specification of Some Wired Media:**

1. **Twisted Pair Cable**

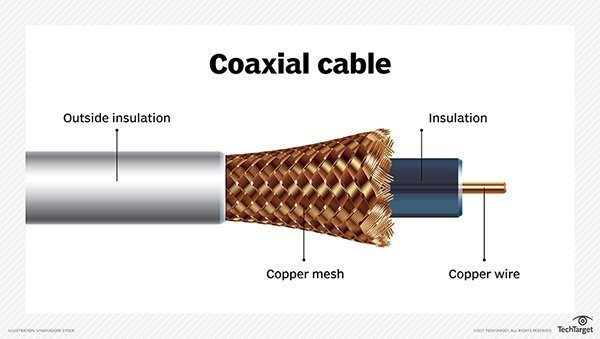


* A twisted pair cable comprises of two separate insulated copper wires, which are twisted together and run in parallel. The copper wires are typically 1mm in diameter. One of the wires is used to transmit data and the other is the ground reference.
* All transmissions are prone to noise, interferences, and crosstalk. When the wires are twisted, some part of the noise signals is in the direction of data signals while the other parts are in the opposite directions. Thus, the external waves cancel out due to the different twists. The receiver calculates the difference in the voltages of the two wires for retrieving data. Thus, a much better immunity against noise is obtained.
* There are two types of twisted pair cables –
* **Unshielded Twisted Pair** (UTP): These generally comprise of wires and insulators.
* **Shielded Twisted Pair** (STP): They have a braided wired mesh that encases each pair of insulated wires.
* EIA has classified twisted pair cables into seven categories −
* Category 1 − UTP used in telephone lines with data rate < 0.1 Mbps
* Category 2 − UTP used in transmission lines with a data rate of 2 Mbps
* Category 3 − UTP used in LANs with a data rate of 10 Mbps
* Category 4 − UTP used in Token Ring networks with a data rate of 20 Mbps
* Category 5 − UTP used in LANs with a data rate of 100 Mbps
* Category 6 − UTP used in LANs with a data rate of 200 Mbps
* Category 7 − STP used in LANs with a data rate of 10 Mbps.[14]

**Scalability:**

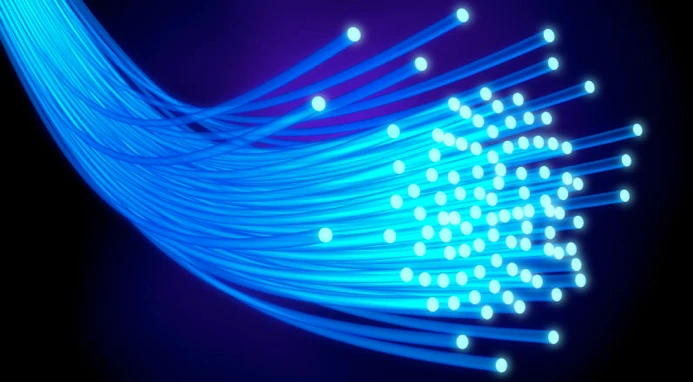
Higher grades of UTP are used in LAN technologies like Ethernet.

1. **Coaxial Cable**



* Coaxial cable, sometimes known as coax cable, is an electrical cable which transmits **radio frequency (RF)** signals from one point to another. Coaxial cable is a type of copper cable specially built with a metal shield and other components engineered to block signal interference
* Coaxial cable is commonly used by cable operators, telephone companies, and internet providers around the world to convey data, video, and voice communications to customers. It has also been used extensively within homes.
* Coaxial cable received its name because it includes one physical channel that carries the signal surrounded -- after a layer of insulation -- by another concentric physical channel, both running along the same axis. The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance.
* The key to the coaxial cable's success has been its shielded design, which allows the cable's copper core to transmit data quickly, without succumbing to interference or damage from environment factors.
* Coaxial cables provide high bandwidth rates of up to **450 mbps** and are used in ethernet systems, namely the **RG-58 (Thick Ethernet) and RG-11 (Thick Ethernet)[15]**
* **It also has limitations that will cause it to be replaced in some cases by  fiber optic cable , category cable or, sometimes, by wireless signals.[15]**

1. **Fiber Optic Cable**



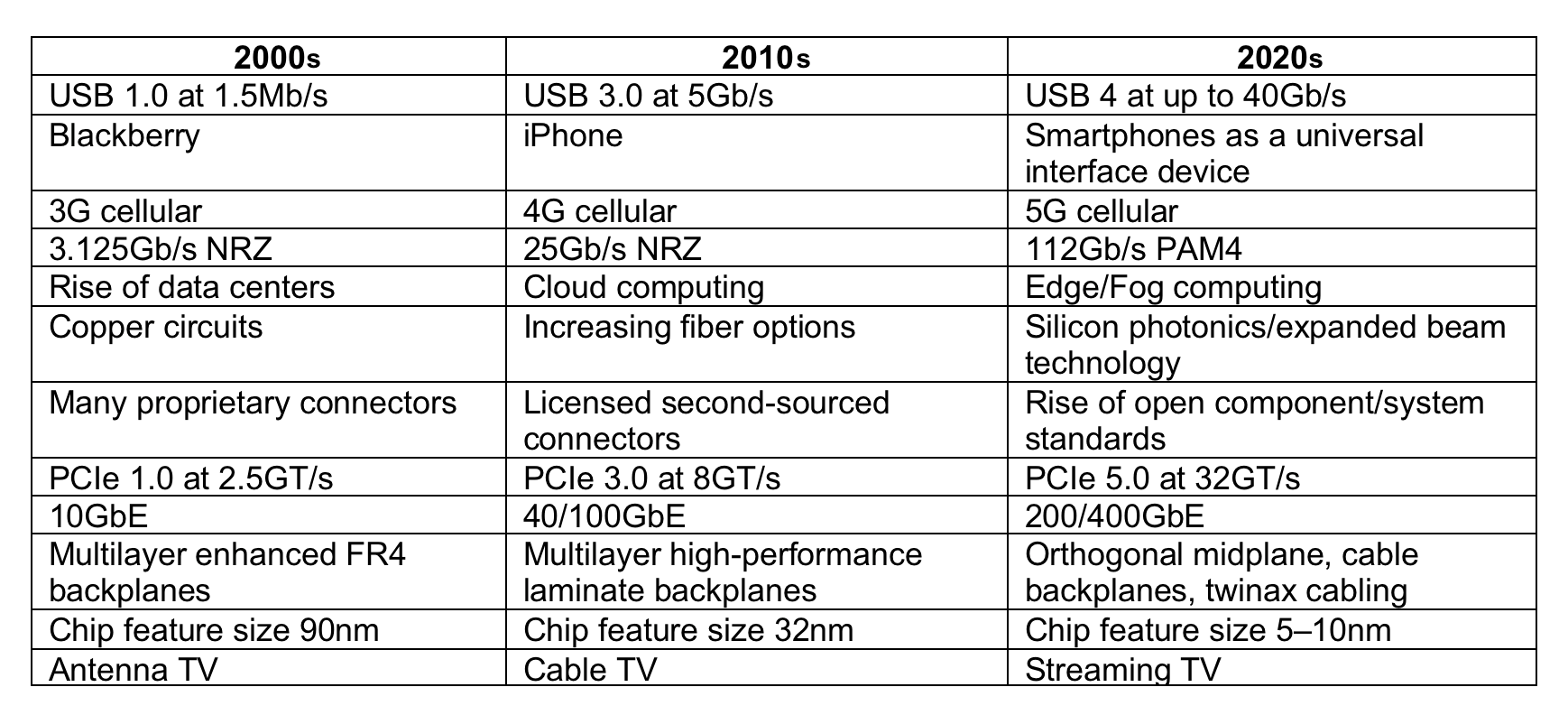
* Optical fiber is a very thin strand of pure glass which acts as a waveguide for light over long distances. It uses a principle known as total internal reflection. Fiber optic cable is actually composed of two layers of glass: The core, which carries the actual light signal, and the cladding, which is a layer of glass surrounding the core. The cladding has a lower refractive index than the core. This causes Total Internal Reflection within the core.
* here are two main types of fiber optic cables: S**ingle Mode Fiber** (SMF) and **Multi-Mode Fiber** (MMF).
* Fiber optics support a **higher capacity**. The amount of network bandwidth a fiber cable can carry easily exceeds that of a copper cable with similar thickness. Fiber cables rated at **10 Gbps, 40 Gbps, and 100 Gbps** are standard.
* A fiber optic cable is less susceptible to interference. A copper network cable requires shielding to protect it from electromagnetic interference. While this shielding helps, it is not sufficient to prevent interference when many cables are strung together in proximity to one another. The physical properties of fiber optic cables avoid most of these problems.[16,17]
* **Scalability**:

Used in CAN networks.

* **Some Technologies used in Wired Media**

1. **Universal Serial Bus (USB)**

* A Universal Serial Bus (USB) is a common interface that enables communication between devices and a host controller such as a personal computer (PC) or smartphone. It connects peripheral devices such as digital cameras, mice, keyboards, printers, scanners, media devices, external hard drives and flash drives. Because of its wide variety of uses, including support for electrical power, the USB has replaced a wide range of interfaces like the parallel and serial port.
* **USB** **Version 1** allowed for two speeds: 1.5 Mb/s (megabits per second) and 12 Mb/s, which work well for slow I/O devices. **USB** **Version 2** allows up to 480 Mb/s and is backward compatible with slower USB devices. The first **USB version 3** (USB 3.0 or SuperSpeed USB) was released in 2008, and allowed for a speed of 500 Mb/s. In 2013 and 2017, two new USB version 3 were released: **USB 3.1** and **USB 3.2**, which allowed for 1.21 Gb/s and 2.42 Gb/s, respectively.[18]
* **Scalability:** USB’s are used mostly in Wired Personal Area Networks (WPAN).



1. **Ethernet**

* Ethernet is a widely deployed LAN technology. This technology was invented by Bob Metcalfe and D.R. Boggs in the year 1970. It was standardized in **IEEE 802.3** in 1980.
* Ethernet shares media. Network which uses shared media has high probability of data collision. Ethernet uses Carrier Sense Multi Access/Collision Detection (CSMA/CD) technology to detect collisions. On the occurrence of collision in Ethernet, all its hosts roll back, wait for some random amount of time, and then re-transmit the data.
* Ethernet connector is, network interface card equipped with 48-bits MAC address. This helps other Ethernet devices to identify and communicate with remote devices in Ethernet.
* Ethernet uses 10BASE-T specifications. The number 10 depicts 10MBPS speed, BASE stands for baseband, and T stands for Thick Ethernet. 10BASE-T Ethernet provides transmission speed up to 10MBPS and uses coaxial cable or Cat-5 twisted pair cable with RJ-45 connector. Ethernet follows star topology with segment length up to 100 meters. All devices are connected to a hub/switch in a star fashion.
* **Fast-Ethernet:** To encompass need of fast emerging software and hardware technologies, Ethernet extends itself as Fast-Ethernet. It can run on UTP, Optical Fiber, and wirelessly too. It can provide speed up to 100 MBPS. This standard is named as 100BASE-T in IEEE 803.2 using Cat-5 twisted pair cable.
* There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.
* **Giga-Ethernet:** After being introduced in 1995, Fast-Ethernet could enjoy its high-speed status only for 3 years till Giga-Ethernet introduced. Giga-Ethernet provides speed up to 1000 Mbits/seconds. IEEE802.3ab standardize Giga-Ethernet over UTP using Cat-5, Cat-5e and Cat-6 cables. IEEE802.3ah defines Giga-Ethernet over Fiber.
* Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections. This developing standard is moving away from a LAN design that broadcasts to all nodes, toward a system which includes some elements of wide area routing. As it is still very new, which of the standards will gain commercial acceptance has yet to be determined. [19,20]

**Scalability**

* Ethernet is a family of computer networking technologies commonly used in local area networks (LAN), metropolitan area networks (MAN), and wide area networks (WAN).
* Ethernet is currently the most widely used technology in enterprise networking. Unfortunately, it is widely acknowledged that Ethernet does not have the scalability to meet the emerging networking needs of large enterprises.
* Ethernet does not scale well to large networks. The flat MAC address space, whilst having obvious benefits for the user and administrator, is the primary cause of this poor scalability.
* Ethernet exhibits scalability issues on networks of more than a few thousand devices, such as costly and energy-dense address table logic and storms of broadcast traffic. Ethernet’s inability to handle networks containing loops also presents a scalability problem.
* **Use of Wired Media in different Network Architecture:**

1. **Wired Personal Area Network**

* Wired PAN provide short connections between peripherals. It mainly uses the USB cables to set up a small Personal network between the wired devices.

1. **Wired LAN**

* A standard wired LAN uses Ethernet to connect devices together. Wireless LANs are typically created using a Wi-Fi signal. If a router supports both Ethernet and Wi-Fi connections, it can be used to create a LAN with both wired and wireless devices.
* The common implementations of lO-Mbps Ethernet are lOBase5 (thick Ethernet), 10Base2 (thin Ethernet), lOBase-T (twisted-pair Ethernet), and lOBase-F (fiber Ethernet). The 10Base5 implementation of Ethernet uses thick coaxial cable. lOBase2 uses thin coaxial cable. lOBase-T uses four twisted-pair cables that connect each station to a common hub. lOBase-F uses fiber-optic cable.

1. **Campus Area Network (CAN)**

* Campus Area Network (CAN) is a computer network which provides wireless access to the Internet or LAN for the users located in two or more buildings on the limited geographical area, or in the open space surrounding these buildings.
* Most CANs are comprised of several LANs connected via switches and routers that combine to create a single network. They operate similar to LANs, in that users with access to the network (wired or wireless) can communicate directly with other systems within the network.
* Unlike a wide area network (WAN), a CAN is managed and maintained by a single entity, such as the campus IT team. The network administrators can monitor, allow, and limit access to the network. Firewalls are typically placed between the CAN and the Internet to protect the network from unauthorized access.
* Since communication within a CAN takes place over a local network, data transfer speeds between systems within the network are often higher than typical Internet speeds. This makes it easy to share large files with other users on the network. For example, it may take several hours to upload a long video to a colleague over the Internet, but the transfer may only take a few minutes over a CAN.
* Corporate CANs connect several buildings like Googleplex and Microsoft's campus. Campus networks are normally interconnected with high speed Ethernet links operating over optical fiber such as gigabit Ethernet and 10 Gigabit Ethernet.[21,22]

1. **Metropolitan Area Network (MAN)**

* A Metropolitan Area Network (MAN) is a great computer network located on the large geographical area or region. It is a network bigger than Local Area Network (LAN), but territorially smaller than Wide Area Network (WAN), its diameter usually ranges from 5 to 50 kilometers.
* It is based on high data rate compounds using the fiber channels and other digital data transmission channels. MAN includes a lot of communicating devices, for its construction are used multiple routers, switches and hubs.
* Distributed Queue Dual Bus (DQDB) is the MAN standard specified by the Institute Of Electrical And Electronics Engineers (IEEE) as IEEE 802.6. Using this standard, a MAN extends up to 30-40 km, or 20-25 miles.[21]

1. **Storage Area Network (SAN)**

* A Storage Area Network (SAN) is a specialized, high-speed network that provides block-level network access to storage. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols. SANs may also span multiple sites.
* When SANs were first built, hubs were the only devices that were Fibre Channel capable, but **Fibre Channel switches** were developed and hubs are now rarely found in SANs. Switches have the advantage over hubs that they allow all attached devices to communicate simultaneously, as a switch provides a dedicated link to connect all its ports with one another. When SANs were first built Fibre Channel had to be implemented over copper cables, these days **multimode optical fibre cables** are used in SANs.

1. **Global Area Network (GAN)**

* Interconnected IP networks (principally the Internet, with estimated 2.5 billion users worldwide in 2014), and the GSM mobile communication network (with over 6 billion worldwide users in 2014) form the largest global networks of all.
* Many applications run on several networks, such as VoIP (voice over IP). Mobile communication (voice and data) networks are also intimately intertwined, because the majority of 21st century cell phones have both voice and data (internet navigation and emailing) capabilities. Digital global networks require huge carrying capacity in the main backbones. This is currently achieved by fiber optic cables.[12]

**References:** 1.https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

2.https://www.tutorialspoint.com/wireless\_communication/wireless\_communication\_bluetooth.html

3.https://www.tutorialspoint.com/data\_communication\_computer\_network/wireless\_transmission.htm

4.https://www.techopedia.com/definition/630/infraredir#:~:text=Infrared%20(IR)%20is%20a%20wireless,is%20unable%20to%20penetrate%20walls.

5.https://www.digi.com/solutions/by-technology/zigbee-wireless standard#:~:text=Zigbee%20is%20a%20wireless%20technology,operates%20on%20the%20IEEE%20802.15.&text=The%20protocol%20allows%20devices%20to,battery%20life%20lasting%20several%20years.

6.https://www.electronics-notes.com/articles/connectivity/nfc-near-field-communication/what-is-nfc-tutorial.php

7.https://www.elprocus.com/how-does-wifi-work/

8. https://danielmiessler.com/study/cellular/

9.http://etutorials.org/Mobile+devices/mobile+wireless+design/Part+One+Introduction+to+the+Mobile+and+Wireless+Landscape/Chapter+3+Wireless+Networks/Wireless+Personal+Area+Networks+WPANs/

10. https://www.javatpoint.com/wireless-lan-introduction

11.https://www.cambridge.org/core/books/fixedmobile-wireless-networks-convergence/wireless-metropolitan-area-networking/C0E94B28910E11DEE51AB2F3D01B52CF

12. https://www.techopedia.com/definition/7368/global-area-network-gan

13. https://www.javatpoint.com/transmission-media

14. https://www.tutorialspoint.com/Twisted-Pair-Cable

15. https://searchnetworking.techtarget.com/definition/coaxial-cable-illustrated

16. https://www.firefold.com/blogs/news/what-is-fiber-optic-cable

17.https://www.lifewire.com/fiber-optic-cable-817874

18. https://www.techopedia.com/definition/2320/universal-serial-bus-usb

19.https://www.tutorialspoint.com/data\_communication\_computer\_network/network\_lan\_technologies.htm

20. http://examradar.com/wired-lans-ethernet-short-notes/

21. https://www.conceptdraw.com/examples/wired-personal-area-network

22. <https://techterms.com/definition/can>

23. <https://en.wikipedia.org/wiki/LTE_(telecommunication)>

24. <https://en.wikipedia.org/wiki/Li-Fi>

25. https://www.tutorialspoint.com/wimax/wimax\_salient\_features.htm