CHAPTER 1

**Frequency translation**

It is the process of moving a signal from one part of the **frequency** axis, to another part of the axis. **Frequency translation** is often done in wireless communications systems to move a pass band signal to base band before demodulation.

Electromagnetic spectrum

The **electromagnetic spectrum** is the range of [frequencies](https://en.wikipedia.org/wiki/Frequency) (the [spectrum](https://en.wikipedia.org/wiki/Spectrum)) of [electromagnetic radiation](https://en.wikipedia.org/wiki/Electromagnetic_radiation) and their respective [wavelengths](https://en.wikipedia.org/wiki/Wavelength) and [photon energies](https://en.wikipedia.org/wiki/Photon_energy).

CHAPTER 2

NETWORK FUNDAMENTALS

A network is simply a group of two or more Personal Computers linked together. Many types of networks exist, but the most common types of networks are Local-Area Networks (LANs), and Wide-Area Networks (WANs).

In a LAN, computers are connected together within a "local" area (for example, an office or home). In a WAN, computers are further apart and are connected via telephone/communication lines, radio waves or other means of connection.

HOW ARE NETWORKS CATEGORIZED?

Networks are usually classified using three properties: Topology, Protocols and Architecture.

**Topology** specifies the geometric arrangement of the network. Common topologies are a bus, ring and star.You can check out a figure showing the three common types of network topologies here.

**Protocol** specifies a common set of rules and signals the computers on the network use to communicate. Most networks use Ethernet, but some networks may use IBM's Token Ring protocol. We recommend Ethernet for both home and office networking. For more information, please select the Ethernet link on the left.

**Architecture** refers to one of the two major types of network architecture: Peer-to-peer or client/server. In a Peer-to-Peer networking configuration, there is no server, and computers simply connect with each other in a workgroup to share files, printers and Internet access.

This is most commonly found in home configurations and is only practical for workgroups of a dozen or less computers. In a client/server network there is usually an NT Domain Controller, to which all of the computers log on. This server can provide various services, including centrally routed Internet Access, mail (including e-mail), file sharing and printer access, as well as ensuring security across the network. This is most commonly found in corporate configurations, where network security is essential.

**Hardware LAN**

The hardware components of a LAN consist of:

* PCs/workstations and servers
* Network Interface Card (NIC)
* Cabling and connectors, for example, coaxial cable and BNC connector, Unshielded Twisted Pair (UTP) and RJ-45 connector
* Hub, concentrator, and more complicated network devices such as Bridge, LAN Switch and Router

**What is a Hub?**

A Hub is a central device used on star network topology that repeats or amplifies signals, allowing the network to be lengthened or expanded with additional stations. For example, an Ethernet hub normally has 8 or 12 or 16 RJ-45 ports, each port can be connected to a PC or workstation or server. Also, the hub’s BNC port can be connected to a coaxial cable to lengthen the network.

**What is a Bridge?**

A Bridge is a device used to connect two or more LANs. It operates at the Media Access Control Layer (layer 2), checking and forwarding data packets between different LANs.

**What is a LAN Switch?**

A LAN Switch is a device using switching hardware to speed-up the checking and forwarding of data packets between LANs. LAN Switch is functionally like a bridge, but its speed and performance is faster and better than a bridge.

**What is a Router?**

A Router is a device that operates at the network layer (layer 3), routing data between similar or dissimilar networks. A router is more powerful than a bridge or LAN Switch because the router checks the network protocols and addresses (for example, IP or IPX).

**ETHERNET LAN**

An Ethernet LAN is the combination of components that allows users to access applications and data, share resources and connect with other networks.

Common components of an Ethernet LAN are; User devices (such as Computers, PCs, Servers and Network printers), Network devices (LAN switches, hubs, firewalls, so on) and different types of media (such as Coaxial, UTP, and STP). Usually, these components are owned by the same company or organization which builds the Ethernet LAN.

Based on scalability, an Ethernet LAN can be categorized in two types; SOHO LAN and the Enterprise LAN

# **Token Ring**

**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.

Token Ring was a successful technology, particularly in corporate environments, but was gradually eclipsed by the later versions of [Ethernet](https://en.wikipedia.org/wiki/Ethernet)

CHAPTER 4

Cellular telephone systems

A **cellular network** or **mobile network** is a communication network where the last link is [wireless](https://en.wikipedia.org/wiki/Wireless). The network is distributed over land areas called "**cells**", each served by at least one fixed-location [transceiver](https://en.wikipedia.org/wiki/Transceiver), but more normally, three [cell sites](https://en.wikipedia.org/wiki/Cell_site) or [base transceiver stations](https://en.wikipedia.org/wiki/Base_transceiver_station). These base stations provide the cell with the network coverage which can be used for transmission of voice, data, and other types of content. A cell typically uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed service quality within each cell.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)][[1]](https://en.wikipedia.org/wiki/Cellular_network#cite_note-Zander-1)

When joined together, these cells provide radio coverage over a wide geographic area. This enables numerous portable transceivers (e.g., [mobile phones](https://en.wikipedia.org/wiki/Mobile_phone), [tablets](https://en.wikipedia.org/wiki/Tablet_computer) and [laptops](https://en.wikipedia.org/wiki/Laptop) equipped with [mobile broadband modems](https://en.wikipedia.org/wiki/Mobile_broadband_modem), [pagers](https://en.wikipedia.org/wiki/Pager), 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.

Cellular networks offer a number of desirable features:[[1]](https://en.wikipedia.org/wiki/Cellular_network#cite_note-Zander-1)

* More capacity than a single large transmitter, since the same frequency can be used for multiple links as long as they are in different cells
* Mobile devices use less power than with a single transmitter or satellite since the cell towers are closer
* Larger coverage area than a single terrestrial transmitter, since additional cell towers can be added indefinitely and are not limited by the horizon

Major telecommunications providers have deployed voice and data cellular networks over most of the inhabited land area of Earth. This allows mobile phones and [mobile computing](https://en.wikipedia.org/wiki/Mobile_computing) devices to be connected to the [public switched telephone network](https://en.wikipedia.org/wiki/Public_switched_telephone_network) and public [Internet](https://en.wikipedia.org/wiki/Internet). Private cellular networks can be used for research[[2]](https://en.wikipedia.org/wiki/Cellular_network#cite_note-2) or for large organizations and fleets, such as dispatch for local public safety agencies or a taxicab company

## GSM (Global System For Mobile Communications).

GSM is a standard set developed by European Telecommunications Standards Institute (ETSI) to describe technologies for second generation (2G) digital cellular networks. The GSM standard is more improved after the development of third generation (3G) UMTS standard developed by the 3GPP.

## CDMA (Code Division Multiple Access).

CDMA is a channel access method used by various radio communication technologies. It should not be confused with the mobile phone standards called cdma One, CDMA2000 (the 3G evolution of cdmaOne) and WCDMA (the 3G standard used by GSM carriers), which are often referred to as simply CDMA, and use CDMA as an underlying channel access method

## AMPS (Advance Mobile Phone Service).

AMPS Advanced Mobile Phone Service (**AMPS**) is a standard system for analog signal cellular telephone service in the United States and is also used in other countries. It is based on the initial electromagnetic radiation spectrum allocation for cellular service by the Federal Communications Commission (FCC) in 1970.

**WCDMA**(Wideband Code Division Multiple Access) –

Wideband CDMA is a third-generation (3G) wireless standard which allows use of both voice and data and offers data speeds of up to 384 Kbps. The frequency bands for **WCDMA** are as follows: Europe and Asia - 2100MHz, North America - 1900MHz and 850MHz.

# **Wireless LAN**

A **wireless LAN** (**WLAN**) is a [wireless computer network](https://en.wikipedia.org/wiki/Wireless_network) that links two or more devices using [wireless communication](https://en.wikipedia.org/wiki/Wireless_communication) to form a [local area network](https://en.wikipedia.org/wiki/Local_area_network) (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building. This gives users the ability to move around within the area and remain connected to the network. Through a [gateway](https://en.wikipedia.org/wiki/Gateway_(telecommunications)), a WLAN can also provide a connection to the wider [Internet](https://en.wikipedia.org/wiki/Internet)

**PAN**

A **personal area network** (**PAN**) is a [computer network](https://en.wikipedia.org/wiki/Computer_network) for interconnecting [electronic devices](https://en.wikipedia.org/wiki/Electronic_devices) centered on an individual person's workspace.[[1]](https://en.wikipedia.org/wiki/Personal_area_network#cite_note-Gratton2013-1) A PAN provides [data transmission](https://en.wikipedia.org/wiki/Data_transmission) among devices such as [computers](https://en.wikipedia.org/wiki/Computer), [smartphones](https://en.wikipedia.org/wiki/Smartphone), [tablets](https://en.wikipedia.org/wiki/Tablet_computer) and [personal digital assistants](https://en.wikipedia.org/wiki/Personal_digital_assistant). PANs can be used for communication among the personal devices themselves, or for connecting to a higher level network and the Internet where one master device takes up the role as [gateway](https://en.wikipedia.org/wiki/Gateway_(telecommunications)). A PAN may be wireless or carried over wired interfaces such as [USB](https://en.wikipedia.org/wiki/USB).

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.

## History of Bluetooth

WLAN technology enables device connectivity to infrastructure based services through a wireless carrier provider. The need for personal devices to communicate wirelessly with one another without an established infrastructure has led to the emergence of **Personal Area Networks (PANs)**.

* Ericsson's Bluetooth project in 1994 defines the standard for PANs to enable communication between mobile phones using low power and low cost radio interfaces.
* In May 1988, Companies such as IBM, Intel, Nokia and Toshiba joined Ericsson to form the Bluetooth Special Interest Group (SIG) whose aim was to develop a defacto standard for PANs.
* IEEE has approved a Bluetooth based standard named IEEE 802.15.1 for Wireless Personal Area Networks (WPANs). IEEE standard covers MAC and Physical layer applications.

**Bluetooth** specification details the entire protocol stack. Bluetooth employs Radio Frequency (RF) for communication. It makes use of **frequency modulation** to generate radio waves in the **ISM** band.



The usage of Bluetooth has widely increased for its special features.

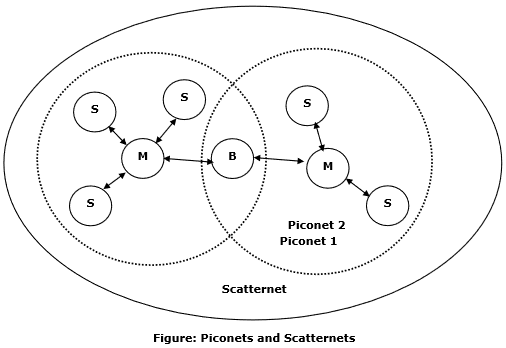
* Bluetooth offers a uniform structure for a wide range of devices to connect and communicate with each other.
* Bluetooth technology has achieved global acceptance such that any Bluetooth enabled device, almost everywhere in the world, can be connected with Bluetooth enabled devices.
* Low power consumption of Bluetooth technology and an offered range of up to ten meters has paved the way for several usage models.
* Bluetooth offers interactive conference by establishing an adhoc network of laptops.
* Bluetooth usage model includes cordless computer, intercom, cordless phone and mobile phones.

## Piconets and Scatternets

Bluetooth enabled electronic devices connect and communicate wirelessly through shortrange devices known as **Piconets**. Bluetooth devices exist in small ad-hoc configurations with the ability to act either as master or slave the specification allows a mechanism for **master** and **slave** to switch their roles. Point to point configuration with one master and one slave is the simplest configuration.

When more than two Bluetooth devices communicate with one another, this is called a **PICONET**. A Piconet can contain up to seven slaves clustered around a single master. The device that initializes establishment of the Piconet becomes the **master**.

The master is responsible for transmission control by dividing the network into a series of time slots amongst the network members, as a part of **time division multiplexing** scheme which is shown below.



The features of Piconets are as follows −

* Within a Piconet, the timing of various devices and the frequency hopping sequence of individual devices is determined by the clock and unique **48-bit address** of master.
* Each device can communicate simultaneously with up to seven other devices within a single Piconet.
* Each device can communicate with several piconets simultaneously.
* Piconets are established dynamically and automatically as Bluetooth enabled devices enter and leave piconets.
* There is no direct connection between the slaves and all the connections are essentially master-to-slave or slave-to-master.
* Slaves are allowed to transmit once these have been polled by the master.
* Transmission starts in the slave-to-master time slot immediately following a polling packet from the master.
* A device can be a member of two or more piconets, jumping from one piconet to another by adjusting the transmission regime-timing and frequency hopping sequence dictated by the master device of the second piconet.
* It can be a slave in one piconet and master in another. It however cannot be a master in more than once piconet.
* Devices resident in adjacent piconets provide a bridge to support inner-piconet connections, allowing assemblies of linked piconets to form a physically extensible communication infrastructure known as **Scatternet**.

### **Spectrum**

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.

### **Range**

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.

### **Data rate**

Bluetooth supports 1Mbps data rate for version 1.2 and 3Mbps data rate for Version 2.0 combined with Error Data Rate

### **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.

The 802.15.4 specification upon which the Zigbee stack operates gained ratification by the [Institute of Electrical and Electronics Engineers](http://www.ieee.org/portal/site) (IEEE) in 2003. The specification is a packet-based radio protocol intended for low-cost, battery-operated devices. The protocol allows devices to communicate in a variety of network topologies and can have battery life lasting several years.

### The Zigbee 3.0 Protocol

The Zigbee protocol has been created and ratified by member companies of the [Zigbee Alliance](http://www.zigbee.org/).Over 300 leading semiconductor manufacturers, technology firms, OEMs and service companies comprise the Zigbee Alliance membership. The Zigbee protocol was designed to provide an easy-to-use wireless data solution characterized by secure, reliable wireless network architectures.

### THE ZIGBEE ADVANTAGE

The Zigbee 3.0 protocol is designed to communicate data through noisy RF environments that are common in commercial and industrial applications. 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. Furthermore, a Zigbee 3.0 certification scheme ensures the interoperability of products from different manufacturers. Connecting Zigbee 3.0 networks to the IP domain opens up monitoring and control from devices such as smartphones and tablets on a LAN or WAN, including the Internet, and brings the true Internet of Things to fruition.

Zigbee protocol features include:

* Support for multiple network topologies such as point-to-point,  
  point-to-multipoint and mesh networks
* Low duty cycle – provides long battery life
* Low latency
* Direct Sequence Spread Spectrum (DSSS)
* Up to 65,000 nodes per network
* 128-bit AES encryption for secure data connections
* Collision avoidance, retries and acknowledgements

The Zigbee 3.0 software stack incorporates a ‘base device’ that provides consistent behavior for commissioning nodes into a network. A common set of commissioning methods is provided, including Touchlink, a method of proximity commissioning.

Zigbee 3.0 provides enhanced network security. There are two methods of security that give rise to two types of network:

* Centralized security: This method employs a coordinator/trust center that forms the network and manages the allocation of network and link security keys to joining nodes.
* Distributed security: This method has no coordinator/trust center and is formed by a router. Any Zigbee router node can subsequently provide the network key to joining nodes.

Nodes adopt whichever security method is used by the network they join. Zigbee 3.0 supports the increasing scale and complexity of wireless networks, and copes with large local networks of greater than 250 nodes. Zigbee also handles the dynamic behavior of these networks (with nodes appearing, disappearing and re-appearing in the network) and allows orphaned nodes, which result from the loss of a parent, to re-join the network via a different parent. The self-healing nature of Zigbee Mesh networks also allows nodes to drop out of the network without any disruption to internal routing.

The backward compatibility of Zigbee 3.0 means that applications already developed under the Zigbee Light Link 1.0 or Home Automation 1.2 profile are ready for Zigbee 3.0. The Smart Energy profile is also compatible with Zigbee 3.0 at the functional level, but Smart Energy has additional security requirements that are only addressed within the profile.

Zigbee’s Over-The-Air (OTA) upgrade feature for software updates during device operation ensures that applications on devices already deployed in the field can be seamlessly migrated to Zigbee 3.0. OTA upgrade is an optional functionality that manufacturers are encouraged to support in their Zigbee products.

### **Mesh Networks**

A key component of the Zigbee protocol is the ability to support mesh networking. In a mesh network, nodes are interconnected with other nodes so that multiple pathways connect each node. Connections between nodes are dynamically updated and optimized through sophisticated, built-in mesh routing table.

Mesh networks are decentralized in nature; each node is capable of self-discovery on the network. Also, as nodes leave the network, the mesh topology allows the nodes to reconfigure routing paths based on the new network structure. The characteristics of mesh topology and ad-hoc routing provide greater stability in changing conditions or failure at single nodes.

**WIRELESS NETWORK**

**Wireless networks** are computer **networks** that are not connected by cables of any kind. The use of a **wireless network** enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations.

# **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 is

* Acronym for **Worldwide Interoperability for Microwave Access**.
* Based on Wireless MAN technology.
* A wireless technology optimized for the delivery of IP centric services over a wide area.
* A scalable wireless platform for constructing alternative and complementary broadband networks.
* A certification that denotes interoperability of equipment built to the IEEE 802.16 or compatible standard. The IEEE 802.16 Working Group develops standards that address two types of usage models −
  + A fixed usage model (IEEE 802.16-2004).
  + A portable usage model (IEEE 802.16e)

**IR wireless (infrared wireless)**

IR wireless is the use of [wireless](https://searchmobilecomputing.techtarget.com/definition/wireless) technology in devices or systems that convey data through infrared (IR) radiation.  Infrared is electromagnetic energy at a [wavelength](https://searchnetworking.techtarget.com/definition/wavelength) or wavelengths somewhat longer than those of red light.  The shortest-wavelength IR borders visiblered in the [electromagnetic radiation spectrum](https://whatis.techtarget.com/definition/electromagnetic-radiation-spectrum);the longest-wavelength IR borders radio waves.

Some engineers consider IR technology to be a sub-specialty of optical technology.  The hardware is similar, and the two forms of energy behave in much the same way.  But strictly speaking, "optical" refers to visibleelectromagnetic radiation, while "infrared" is invisible to the unaidedeye.  To compound the confusion, IR is sometimes called "infrared light."

IR wireless is used for short- and medium-range communications andcontrol.  Some systems operate in line-of-sight mode; this means that theremust be a visually unobstructed straight line through space between the transmitter(source) and receiver (destination).  Other systems operate in diffuse mode,also called scatter mode.  This type of system can function when the sourceand destination are not directly visible to each other.  An example is a televisionremote-control box.  The box does not have to be pointed directly at the set,although the box must be in the same room as the set, or just outside the room with thedoor open.

IR wireless technology is used in intrusion detectors; home-entertainment control units; robot control systems; medium-range, line-of-sight [laser](https://whatis.techtarget.com/definition/laser) communications; cordless microphones, headsets, modems, and printers and other peripherals.

Unlike radio-frequency (RF) wireless links, IR wireless cannot passthrough walls.  Therefore, IR communications or control is generally not possible between different rooms in a house, or between different houses in a neighborhood (unless they have facing windows).  This might seem like a disadvantage, but IR wireless is more private than RF wireless.  Some IR wireless schemes offer a level of securitycomparable to that of hard-wired systems.   It is difficult, for example, toeavesdrop on a well-engineered, line-of-sight, IR laser communications link.

**RFID Communication**

**RFID** (radio frequency identification) is a form of wireless **communication** that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person

## Ultra Wideband

UWB is a short-range, wireless communication protocol that – like Bluetooth or Wi-Fi – uses radio waves. But it differs substantially in that it operates at a very high frequency. As its name denotes, it also uses a wide spectrum of several GHz. One way to think of it is as a radar that can continuously scan an entire room and precisely lock onto an object like a laser beam to discover its location and communicate data.