GALGOTIAS UNIVERSITY

UNIT – I INTRODUCTION TO WIRELESS COMMUNICATION

Introduction to Wireless Technologies - Wireless LAN - IEEE 802.11 standards - Frequency bands - Sub Standards (a,b,g,n) - Network Topology - Terminology, Client Server Network Management for WLAN

Introduction to Wireless Technologies:

The term wireless communication refers to the transfer of information using electromagnetic (EM) or acoustic waves over the atmosphere rather than using any propagation medium that employs wires. Not requiring an explicit network of wires and permitting communication while on the move. Fortunately, EM waves travel with the speed of light in free space and inside medium (cables) – with a delay-time =length of cable/C . This allows very fast communication. Wireless technologies enable one or more devices to communicate without physical connections. Wireless technologies use radio frequency transmissions as the means for transmitting data, where as wired technologies use cables. Wireless networks are frequently categorized into three groups based on their coverage range: Wireless Wide Area Networks (WWAN), Wireless Local Area Networks (WLAN), and Wireless Personal Area Networks (WPAN). WLAN is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure. The term wireless refers to the communication or transmission of information over a distance without requiring wires, cables or any other electrical conductors. Wireless communication is one of the important mediums of transmission of data or information to other devices. The Communication is set and the information is transmitted through the air, without requiring any cables, by using electromagnetic waves like radio frequencies, infrared, satellite, etc., in a wireless communication technology network. At the end of the 19th century, the first wireless communication systems were introduced and the technology has significantly been developed over the intervening and subsequent years. Today, the term wireless refers to a variety of devices and technologies ranging from smart phones to laptops, tabs, computers, printers, Bluetooth, etc. Types of Wireless Communication Technologies In recent days, the wireless communication technology has become an integral part of several types of communication devices as it allows users to communicate even from remote areas. The devices used for wireless communication are cordless telephones, mobiles, GPS units, ZigBee technology, wireless computer parts, and satellite television, etc.

Figure 1.1 Types of Communication Technologies

Satellite:

Satellite communication is one of the wireless technologies, which is widely spread all over the world allowing users to stay connected virtually anywhere on the Earth. The Satellites used in this mode of communication, communicate directly with the orbiting satellites via radio signals. Portable satellite phones and modems have more powerful broadcasting abilities than the cellular devices as they have high range, apart from being more expensive in terms of cost, than their counterparts. For example, for outfitting a ship through satellite communication, a traditional communication system is linked to a single satellite, which allows multiple users to share the same broadcast equipment.

Wireless Networking:

Wireless Networking technologies connect multiple computers, systems and devices together without requiring wires or cables: a wireless local area network or WLAN comes under Wi-Fi.

WiMAX:

There are wireless broadband systems that offer fast Web surfing without being getting connected through cable or DSL (Example of wireless broadband is WiMAX). Although WiMAX can potentially deliver data rates of more than 30 Megabits per second, yet the providers offer average 0 data rates of 6 Mbps and often deliver less, making the service significantly slower than the hard-wired broadband. The actual cost of the data available using WiMAX widely varies with the distance from the transmitter. WiMAX is also one of the versions of 4G wireless available in phones as Sprint’s 4G technology.

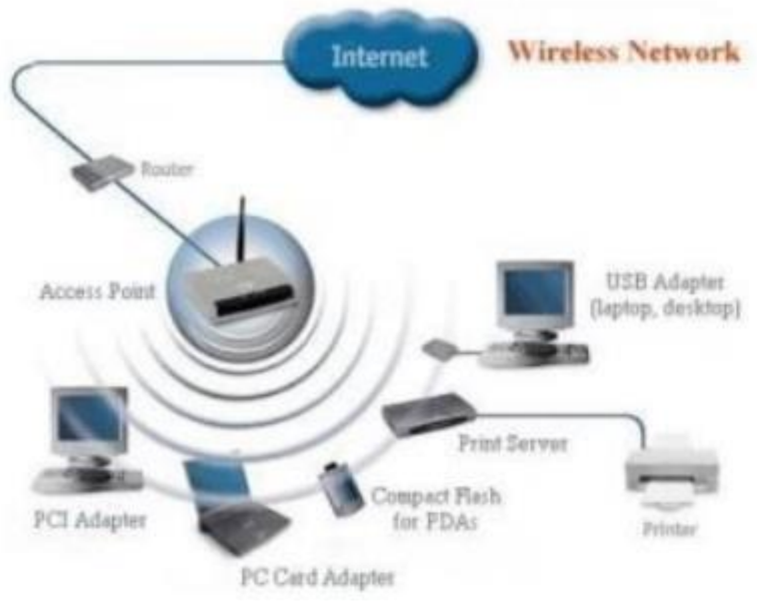


Figure 1.2 Wireless Networking

Wi-Fi:

Wi-Fi is a form of low-power wireless communication used by many electronic devices such as laptops, systems, smart phones, etc. In a Wi-Fi setup, a wireless router serves as the communication hub. These networks are extremely limited in range due to low power of transmissions allowing users to connect only within close proximity to a router or signal repeater. Wi-Fi is common in home networking applications which provides portability without any need of cables. Wi-Fi networks need to be secured with passwords for security purposes in order not to be accessed by others.

Figure 1.3 WIFI

Wireless Networking (Wi-Fi):

Advantages

- Ease of Integration and Convenience – The wireless nature of such networks allows users to access network resources from nearly any convenient location.

- Mobility – With the emergence of public wireless networks, users can access the internet even outside their normal working environment.

- Expandability – Wireless networks are capable of serving a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients require additional wiring.

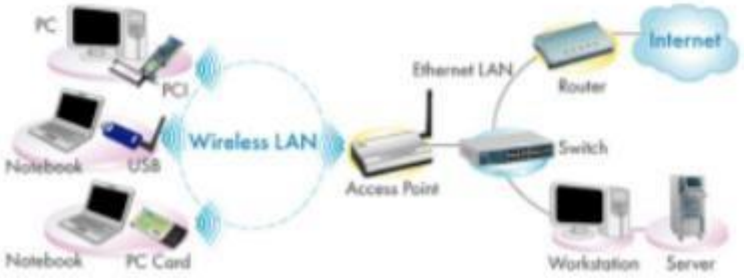


Figure 1.4 Wireless Networking WiFi

Disadvantages:

• Wireless LANs may not be desirable for a number of reasons.

• Radio Frequency transmission and wireless networking signals are subjected to a wide variety of interference including the complex propagation effects that are beyond the control of the network administrator.

• Security Problems – Wireless networks may choose to utilize some of the various encryption technologies.

• Range will be insufficient for a larger structure – and, in order to increase its range, repeaters or additional access points have to be purchased.

• The speed on most wireless networks will be slower than the slowest common wired networks.

• Installation of an infrastructure-based wireless network is a complex to set up.

Bluetooth Technology

Bluetooth technology allows to connect a variety of different electronic devices wirelessly to a system for the transfer and sharing of data and this is the main function of Bluetooth. Cell phones are connected to hands-free earpieces, wireless keyboard, mouse and mike to laptops with the help of Bluetooth as it transmits information from one device to other device. Bluetooth technology has many functions, and it is used most commonly in wireless communications' market.

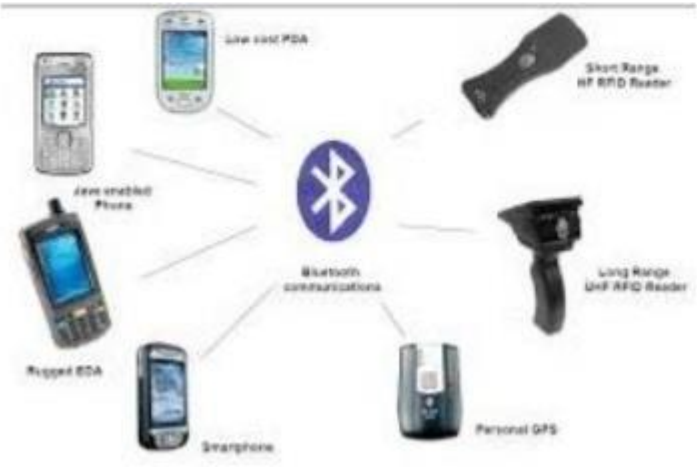


Figure 1.5 Bluetooth Technology

Features:

- Bluetooth technology uses radio waves to communicate between devices. Most of these radio waves have a range of 15-50 feet.
- According to the official Bluetooth website, Bluetooth uses a low-power signal with a maximum range of 50 feet with sufficient speed to enable transmission of data.
- The pairing process identifies and connects any two devices to each other. It also prevents interference from other non-paired Bluetooth devices in the area.
- It uses maximum power only when it is required, thus preserving battery life.

ZigBee

ZigBee is a wireless communication standard designed to address the unique needs of low- power, low-cost wireless sensor, and control networks. ZigBee can be used almost anywhere, as it is easy to implement and requires little power to operate. Zigbee has been developed looking into the needs of the communication of data with a simple structure like the data from the sensors.

Zigbee Technology

Features

- ZigBee devices are designed for low-power consumption.
- ZigBee is used in Commercial Applications like sensing and monitoring applications.
- ZigBee uses very low power and extremely long device battery life.
- ZigBee gives flexibility to do more with the reliable wireless performance and battery operation.

Types of Wireless Data Transmission

Wireless technology defines the electronic devices that communicate in air without cables using radio frequency signals. Wireless technology is used in a variety of modern device and provides greater mobility. Wireless devices play an important role in voice and Internet communications.

Wireless Router

Wireless routers accepts an incoming Internet connection and sends the data as RF signals to other wireless devices that are near to the router. A network set up with a wireless router is called as a Wireless Local Area Network (WLAN).Many routers have built-in security features such as firewalls that help protect devices connected to the router against malicious data such as computer viruses.

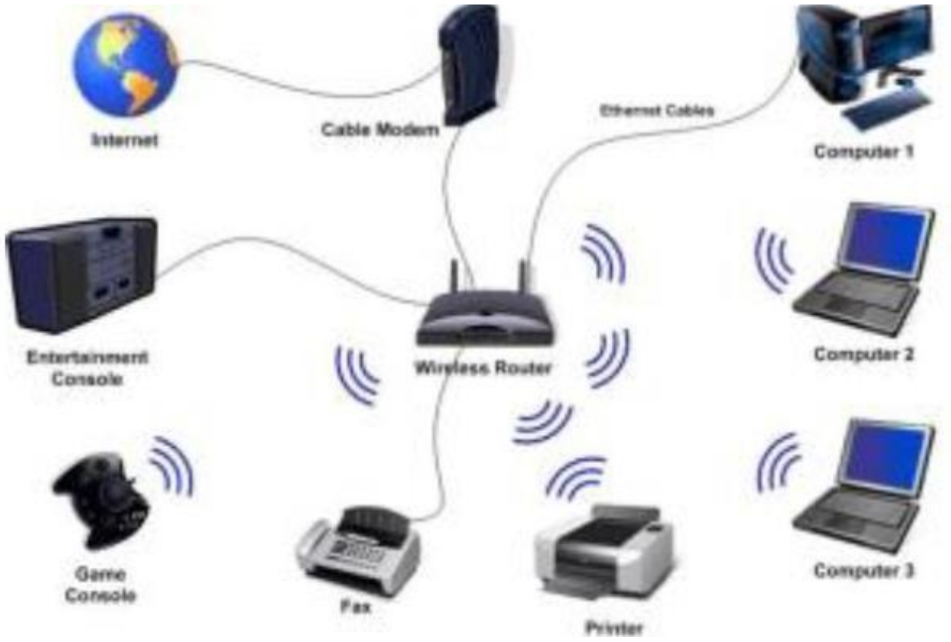


Figure 1.6 Wireless Router

Wireless Router

A wireless router is used in many houses to connect their computers to the Internet.

Wireless Adapters

Wireless adapters are hardware devices that are installed inside computers which enables wireless connectivity. If a computer does not have a wireless adapter, it will not be able to connect to a router in order to access the Internet. Some computers have wireless adapters built directly into the motherboard, while it is also possible to install stand-alone wireless adapters to add wireless capability to a computer that doesn't have a built-in facility.

Wireless Repeater

A wireless repeater is a wireless networking device that is used to extend the range of a wireless router. A repeater receives wireless signals and amplifies the strength of the signals, and then re-emits them. The strength of the signal can be increased by placing a repeater between the router and the computer connected to the router.

Figure 1.7 Wireless Repeater

Microwave

Microwave is an effective type of wireless data transmission that transfers information using two separate methods. One method which is used to transmit data through the wireless media of a microwave is the satellite method that transmits information via a satellite that orbits 22,300 miles above the Earth. Stations on the ground send and receive data signals to and from the satellite with a frequency ranging from 11 GHz to 14 GHz and with a transmission speed of 1 Mbps to 10 Mbps. Another method is a terrestrial method, in which two microwave towers with a clear line of sight between them are used ensuring no obstacles to disrupt that line of sight. For the purpose of privacy, it is used often. The frequency of data transmission for terrestrial systems is typically 4 GHz to 6 GHz or 21 GHz to 23 GHz, and the speed is usually 1 megabit per second (Mbps) to 10 Mbps.

Infrared (IR)

Infrared is a media transmission system that transmits data signals through light emitting diodes (LEDs) or Lasers. Infrared is an electromagnetic energy at a wavelength which is longer than that of the red light. The information cannot be travelled through obstacles in an infrared system, but can be inhibited by light. One type of infrared is the point to point system in which transmission is possible between two points limited to a range and line of sight. The signal frequency to transmit in a point to point system is 100 GHz to 1,000 terahertz (THz), and the speed ranges from 100 Kbps to 16 Mbps.

Another method of transmission of infrared includes the broadcast system – and, in this method, a reflective material or a transmission unit amplifies and retransmits a data signal to several other units. The normal frequency of an infrared broadcast system is 100 GHz to 1,000 THz with a limited speed of 1 Mbps.

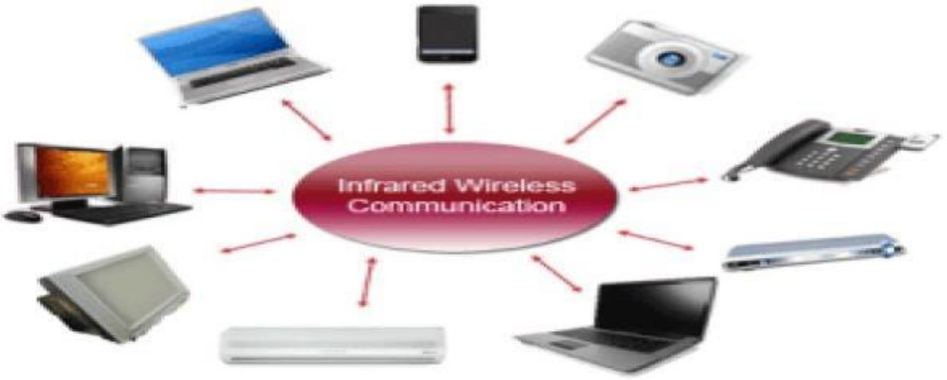


Figure 1.8 Infrared

Types of Wireless Devices

Radio

The radio system is one type of wireless data transmission, and it is a wireless media that transfers data by carrying electromagnetic waves with low frequencies to distant locations through an electrical conductor and an antenna. Ham radio enthusiasts share information and serve as emergency communication aids during disasters with their powerful amateur broadcasting equipment and can even communicate digital data over the radio spectrum.

Citizen’s band and maritime radios provide communication services for truckers and sailors. The transmission frequency for information transmitted through a radio system ranges from 10 kilohertz (kHz) to 1 gigahertz (GHz), and the frequencies are regulated by the Federal Communications Commission (FCC).

Figure 1.9 Radio

Wireless Phones

The evolution of cellular networks is enumerated by generations. Many different users communicate across a single frequency band through Cellular and cordless phones. Cellular and cordless phones are two more examples of devices that make use of wireless signals. Cordless phones have a limited range but cell phones typically have a much larger range than the local wireless networks since cell phone use large telecommunication towers to provide cell phone coverage. Some phones make use of signals from satellites to communicate, similar to Global Positioning System (GSP) devices.

Figure 1.10 Wireless Phones

Other Devices

Anything that uses radio signals to communicate can be considered as a wireless device. Common devices such as garage door openers, baby monitors, certain video game consoles and walkie-talkies make use of wireless technology.

Advantages and Disadvantages of Wireless Communications

Advantages

• Any information can be conveyed or transmitted quickly and with a high speed.

• The Internet can be accessed from anywhere and at anytime without the need to carry cables or wires and it improves easy access and productivity.

• Helpful for Doctors, workers and other professionals working in remote areas as they can be in touch with the medical centers through wireless communication.

• Emergency situations can be alerted through wireless communication. The affected regions can be provided support with the help of these alerts through wireless communication.

• Wireless networks cost less for installation and maintenance.

Disadvantages

• A Hacker can easily capture the wireless signals that spread through the air.

• It is very important to secure the wireless network so that the information cannot be exploited by unauthorized users, and this also increases the risk of losing data or information.

Thus, Wireless networks are one of the fastest growing technologies in telecommunications market. WiMax, Bluetooth, Wi-Fi, Femtocell and 4G are some of the most significant standards of Wireless technology for the next generations. Radio, Mobiles, Internet, etc., all use technological advancements in wireless data transmission systems that carry invisible electromagnetic waves to transmit data over long distances within a short amount of time.

Wireless LAN

wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc. This gives users the ability to move around within the area and yet still be connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet. Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name. Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial properties that offer wireless access to their employees and customers. Norman Abramson, a professor at the University of Hawaii, developed the world's first wireless computer communication network, ALOHA net. The system became operational in 1971 and included seven computers deployed over four islands to communicate with the central computer on the Oahu island without using phone lines. Wireless LAN hardware initially cost so much that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Early development included industry-specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802.11 (in products using the Wi-Fi brand name). Beginning in 1991, a European alternative known as HiperLAN/1 was pursued by the European Telecommunications Standards Institute (ETSI) with a first version approved in 1996. This was followed by a HiperLAN/2 functional specification with ATM influences accomplished February 2000. Neither European standard achieved the commercial success of 802.11, although much of the work on HiperLAN/2 has survived in 15 the physical specification (PHY) for IEEE 802.11a, which is nearly identical to the PHY of HiperLAN/2. In 2009 802.11n was added to 802.11. It operates in both the 2.4 GHz and 5 GHz bands at a maximum data transfer rate of 600 Mbit/s. Most newer routers are able to utilise both wireless bands, known as dualband. This allows data communications to avoid the crowded 2.4 GHz band, which is also shared with Bluetooth devices and microwave ovens. The 5 GHz band is also wider than the 2.4 GHz band, with more channels, which permits a greater number of devices to share the space. Not all channels are available in all regions. A Home RF group formed in 1997 to promote a technology aimed for residential use, but it disbanded at the end of 2002. Architecture Stations All components that can connect into a wireless medium in a network are referred to as stations (STA). All stations are equipped with wireless network interface controllers (WNICs). Wireless stations fall into two categories: wireless access points, and clients. Access points (APs), normally wireless routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with. Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones and other smartphones, or non-portable devices such as desktop computers, printers, and workstations that are equipped with a wireless network interface. Basic service set The basic service set (BSS) is a set of all stations that can communicate with each other at PHY layer. Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS. There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS. An independent BSS (IBSS) is an ad hoc network that contains no access points, which means they cannot connect to any other basic service set. Extended service set An extended service set (ESS) is a set of connected BSSs. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string. Distribution system A distribution system (DS) connects access points in an extended service set. The concept of a DS can be used to increase network coverage through roaming between cells. DS can be wired or wireless. Current wireless distribution systems are mostly based on WDS or MESH protocols, though other systems are in use. Types of wireless LANs The IEEE 802.11 has two basic modes of operation: infrastructure and ad hoc mode. In ad hoc mode, mobile units transmit directly peer-to-peer. In infrastructure mode, mobile units communicate through an access point that serves as a bridge to other networks (such as Internet or LAN). Since wireless communication uses a more open medium for communication in comparison to wired LANs, the

802.11 designers also included encryption mechanisms: Wired Equivalent Privacy (WEP, now insecure), Wi-Fi Protected Access (WPA, WPA2, WPA3), to secure wireless computer networks. Many access points will also offer Wi-Fi Protected Setup, a quick (but now insecure) method of joining a new device to an encrypted network. Infrastructure Most Wi-Fi networks are deployed in infrastructure mode. In infrastructure mode, a base station acts as a wireless access point hub, and nodes communicate through the hub. The hub usually, but not always, has a wired or fiber network connection, and may have permanent wireless connections to other nodes. Wireless access points are usually fixed, and provide service to their client nodes within range. Wireless clients, such as laptops, smartphones etc. connect to the access point to join the network. Sometimes a network will have a multiple access points, with the same 'SSID' and security arrangement. In that case connecting to any access point on that network joins the client to the network. In that case, the client software will try to choose the access point to try to give the best service, such as the access point with the strongest signal. 17 Peer-to-peer An ad hoc network (not the same as a WiFi Direct network is a network where stations communicate only peer to peer (P2P). There is no base and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).

BSS can exist with and without AP. BSS without access point cannot send data to another BSS. So, it is known as a stand alone network or ad hoc architecture. In this type of architecture stations can form a network without using AP.

Extended Service Set (ESS): An extended service set consists of two or more BSSs with access points. The BSS in this system are connected to each other via a distribution system which is generally a wired LAN. The distribution system connects the access points to each other. The distribution system can be any type LAN such as Ethernet, thus ESS contains two types of station:

Mobile Station

Stationary of non-moving stations

Peer-to-Peer or ad hoc wireless LAN A WiFi Direct network is another type of network where stations communicate peer to peer. In a Wi-Fi P2P group, the group owner operates as an access point and all other devices are clients. There are two main methods to establish a group owner in the Wi-Fi Direct group. In one approach, the user sets up a P2P group owner manually. This method is also known as Autonomous Group Owner (autonomous GO). In the second method, also called negotiation based group creation, two devices compete based on the group owner intent value. The device with higher intent value becomes a group owner and the second device becomes a client. Group owner intent value can depend on whether the wireless device performs a cross connection between an infrastructure WLAN service and a P2P group, remaining power in the wireless device, whether the wireless device is already a group owner in another group and/or a received signal strength of the first wireless device. A peer-to-peer network allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network. This can basically occur in devices within a closed range. If a signal strength meter is used in this situation, it may not read the strength accurately and can be misleading, because it registers the strength of the strongest signal, which may be the closest computer. IEEE 802.11 defines the physical layer (PHY) and MAC (Media Access Control) layers based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). This is in contrast to Ethernet which uses CSMA-CD (Carrier Sense Multiple Access with Collision Detection). The 802.11 specification includes provisions designed to minimize collisions, because two mobile units may both be in range of a common access point, but out of range of each other. Bridge A bridge can be used to connect networks, typically of different types. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN. Wireless distribution system A wireless distribution system (WDS) enables the wireless interconnection of access points in an

IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required. The notable advantage of a WDS over other solutions is that it preserves the MAC addresses of client packets across links between access points. An access point can be either a main, relay or remote base station. A main base station is typically connected to the wired Ethernet. A relay base station relays data between remote base stations, wireless clients or other relay stations to either a main or another relay base station. A remote base station accepts connections from wireless clients and passes them to relay or main stations. Connections between clients are made using MAC addresses rather than by specifying IP assignments. All base stations in a WDS must be configured to use the same radio channel, and share WEP keys or WPA keys if they are used. They can be configured to different service set identifiers. 19 WDS also requires that every base station be configured to forward to others in the system as mentioned above. WDS capability may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging). Throughput in this method is halved for all clients connected wirelessly. When it is difficult to connect all of the access points in a network by wires, it is also possible to put up access points as repeaters.

Roaming

Roaming among Wireless Local Area Networks

There are two definitions for wireless LAN roaming:

1. Internal roaming: The Mobile Station (MS) moves from one access point (AP) to another AP within a home network if the signal strength is too weak. An authentication server (RADIUS) performs the re-authentication of MS via 802.1x (e.g. with PEAP). The billing of QoS is in the home network. A Mobile Station roaming from one access point to another often interrupts the flow of data among the Mobile Station and an application connected to the network. The Mobile Station, for instance, periodically monitors the presence of alternative access points (ones that will provide a better connection). At some point, based on proprietary mechanisms, the Mobile Station decides to re-associate with an access point having a stronger wireless signal. The Mobile Station, however, may lose a connection with an access point before associating with another access point. In order to provide reliable connections with applications, the Mobile Station must generally include software that provides session persistence.

2. External roaming: The MS (client) moves into a WLAN of another Wireless Internet Service Provider (WISP) and takes their services (Hotspot). The user can use a foreign network independently from their home network, provided that the foreign network allows 20 visiting users on their network. There must be special authentication and billing systems for mobile services in a foreign network. Applications Wireless LANs have a great deal of applications. Modern implementations of WLANs range from small in-home networks to large, campus-sized ones to completely mobile networks on airplanes and trains. Users can access the Internet from WLAN hotspots in restaurants, hotels, and now with portable devices that connect to 3G or 4G networks. Oftentimes these types of public access points require no registration or password to join the network. Others can be accessed once registration has occurred and/or a fee is paid. Existing Wireless LAN infrastructures can also be used to work as indoor positioning systems with no modification to the existing hardware.

Benefits of WLAN

While the most obvious is mobility, there are advantages also in building and maintaining a wireless network.

Mobility:
Mobility is a significant advantage of WLANs. User can access shared resources without looking for a place to plug in, anywhere in the organization. A wireless network allows users to be truly mobile as long as the mobile terminal is under the network coverage area.
Range of coverage: The distance over which RF and IR waves can communicate depends on product design (including transmitted power and receiver design) and the propagation path, especially in indoor environments. Interactions with typical building objects, such as walls, metal, and even people, can affect the propagation of energy, and thus also the range and coverage of the system. IR is blocked by solid objects, which provides additional limitations. Most wireless LAN systems use RF, because radio waves can penetrate many indoor walls and surfaces. The range of a typical WLAN node is about 100 m. Coverage can be extended, and true freedom of mobility achieved via roaming. This means using access points to cover an area in such a way that their coverages overlap each other. Thereby the user can wander around and move from the coverage area of one access point to another without even knowing he has, and at the same time seamlessy maintain the connection between his node and an access point.
Ease of use:
WLAN is easy to use and the users need very little new information to take advantage of WLANs. Because the WLAN is transparent to a user's network operating system, applications work in the same way as they do in wired LANs.
Installation Speed, Simplicity and Flexibility Installation of a WLAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings. Furthermore, wireless LAN enables networks to be set up where wires might be impossible to install. Scalability Wireless networks can be designed to be extremely simple or complex. Wireless networks can support large numbers of nodes and large physical areas by adding access points to extend coverage.
Cost
Finally, the cost of installing and maintaining a WLAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, WLAN eliminates the direct costs of cabling and the labor associated with installing and repairing it. Second, because WLANs simplify moving, additions, and changes, the indirect costs of user downtime and administrative overhead are reduced.

IEEE 802.11 standards
IEEE is basically used for WLAN i.e wireless local area network. It provides time bounded and asynchronous services for different downloading and uploading speed with time limitation. This is the standard protocol used all over the world. 802.11 comes under the most popular IEEE specification for wireless LAN. It covers the physical and data link layers. This post includes Wireless Communication Notes on IEEE 802.11 Standards for WLAN for the students to provide a help for Communication students to perform well in their exams and interviews.
802.x belongs to different families of IEEE protocol where x denotes types of services. Different protocols used for different services are:

- 802.11 is used for Wi-Fi.
- 802.15 is used for bluetooth.
- 802.16 is used for Wi-Max

IEEE 802.11 Architecture
IEEE 802.11 defines two types of services which are
1) Basic Service Set (BSS) 2) Extended Service Set (ESS)
Basic Service Set (BSS): IEEE 802.11 has defined the BSS as the basic building block of wireless LAN. A BSS is made of stationary or moving wireless stations and a central base station called as the access point (AP).

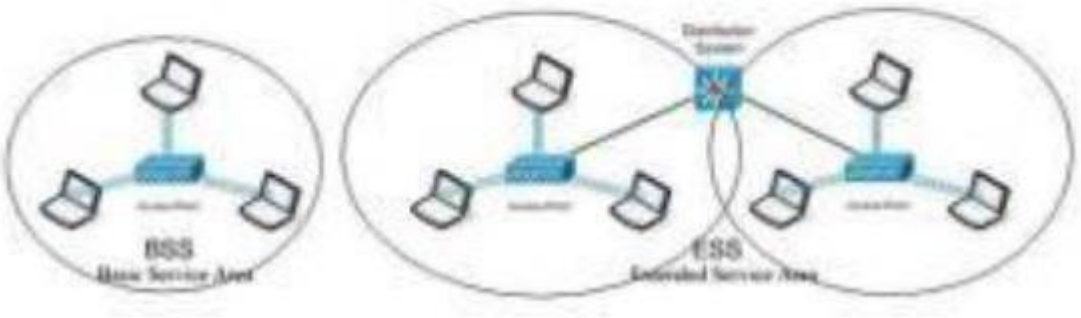


Figure 1.11 Access Point

BSS can exist with and without AP. BSS without access point cannot send data to another BSS. So, it is known as a stand alone network or ad hoc architecture. In this type of architecture stations can form a network without using AP.

Extended Service Set (ESS): An extended service set consists of two or more BSSs with access points. The BSS in these systems are connected to each other via a distribution system which is generally a wired LAN. The distribution system connects the access points to each other. The distribution system can be any type LAN such as Ethernet, thus ESS contains two types of station.

- Mobile Stations
- Stationary of non-moving stations

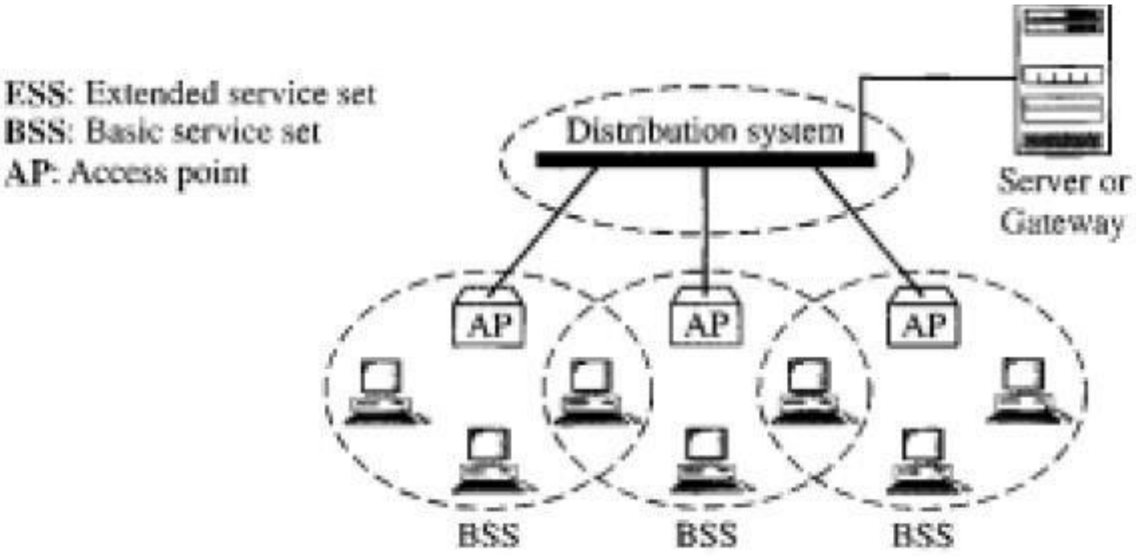


Figure 1.12 Distribution System

Out of these, the non-moving stations are the access points which are a part of the wired LAN whereas the mobile stations are those contained in the BSS. The BSSs are connected to each other to form a network called infrastructure network. In such networks the station close to each other can communicate taking help of access points. But if two stations are located in two different BSS wish to communicate with each other, than they have to do do through access points. This type of communication is very similar to that in the cellular communication. The BSS acts as a cell and AP as base station.

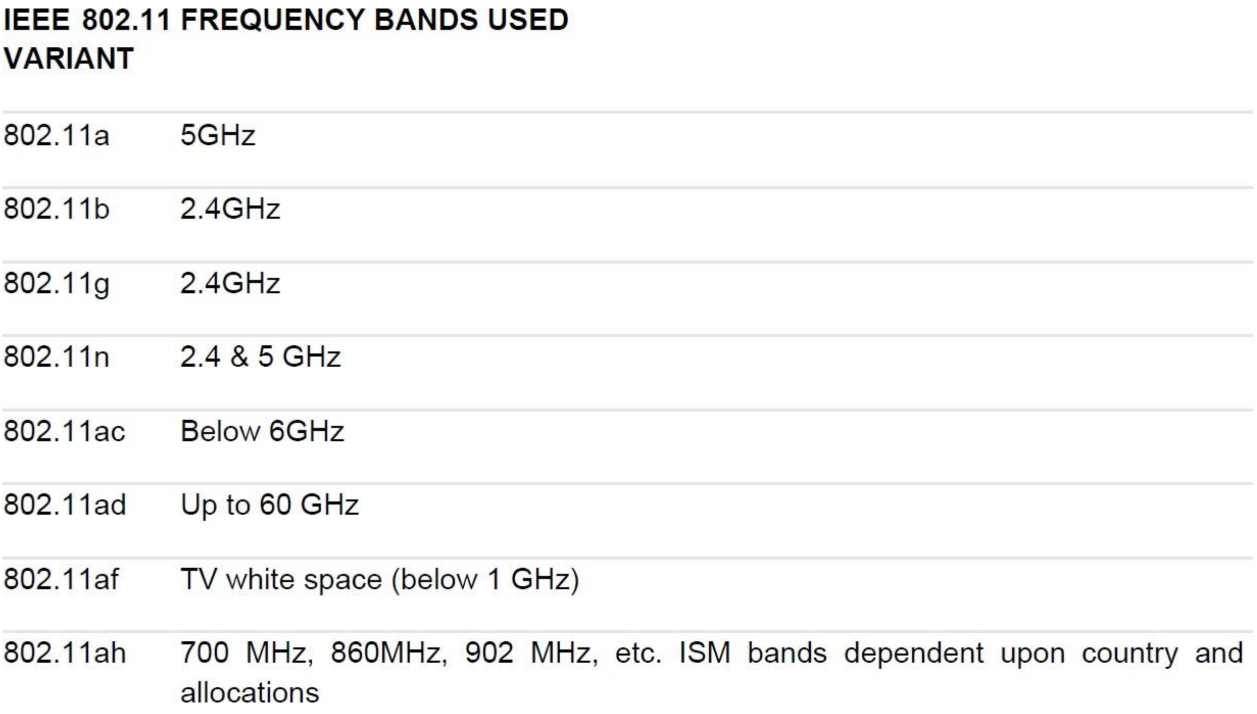
Types of Stations in ESS are as follow:

There are three types of stations are defined by IEEE 802.11 depending on their mobility in the wireless LAN as

1) No transition Mobility: It is defined as a station which is non-moving (stationary) or moving only inside a BSS.
2) BSS Transition Mobility: A station having BSS transition mobility is the one which can move from BSS to another but does not move outside one ESS.
3) ESS transition Mobility: A station having ESS transition mobility is the one which can move from one ESS to another. But IEEE 802.11 does not guarantee communication when the station is moving.

802.11 systems & frequency bands
There are several different 802.11 variants in use. Different 802.11 variants use different bands. A summary of the bands used by the 802.11 systems is given below:

Table 1.1 Frequency Band



IEEE 802.11 VARIANT	FREQUENCY BANDS USED
802.11a	5GHz
802.11b	2.4GHz
802.11g	2.4GHz
802.11n	2.4 & 5 GHz
802.11ac	Below 6GHz
802.11ad	Up to 60 GHz
802.11af	TV white space (below 1 GHz)
802.11ah	700 MHz, 860MHz, 902 MHz, etc. ISM bands dependent upon country and allocations

Sub Standards (a,b,g,n)

IEEE802.11a The IEEE802.11a standard was released on September 1999. Networks using 802.11a operate at radio frequency of 5GHz or 3.7GHz and a bandwidth of 20MHz. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited to use in office settings. In 802.11a, data speeds as high as 54 Mbps are possible. This standard employ the single input, single output (SISO) antenna technologies, and the indoor/outdoor ranges from 35m to 125m for 5GHz operating frequency. The outdoor range goes to 5Km for operating frequency of 3.7G. The IEEE802.11a is less prone to interference compared to with 802.11b due to the high operating frequency of 5GHz.

IEEE 802.11b
IEEE 802.11b standard was released on September 1999 as well. This standard provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz operating frequency and bandwidth of 22MHz. The 802.11b uses only DSSS (Direct Sequence Spread Spectrum) modulation technique. This standard also employs the SISO antenna technology as in the IEEE802.11a standard. The IEEE802.11b standard was ratified on 1999 from the original IEEE802.11 standard which allowed

wireless functionality comparable to Ethernet. The IEEE802.11b standard is prone to higher interference due to the fact that the 2.4GHz frequency range is becoming crowded with carriers, hence increased interference risk. The indoor and outdoor ranges for this standard is 35m to 140m

IEEE 802.11g

The standard 802.11g was ratified in 2003 as an IEEE standard for Wi-Fi wireless networking and it supports maximum network bandwidth of 54 Mbps compared to 11 Mbps for 802.11b. This standard operates at 2.4GHz frequency and bandwidth of 20MHz. This standard uses the OFDM or DSSS modulation schemes. This standard employ the SISO antenna technologies, and its indoor/outdoor range are from 38m to 140m respectively

IEEE 802.11n

The 802.11n standard was ratified in 2009 and it utilizes multiple wireless antennas in tandem to transmit and receive data. The IEEE802.11n standard employs OFDM modulation technique. The antenna technology used with the IEEE802.11n standard is known as Multiple Input, Multiple Output (MIMO). This technology refers to the ability of 802.11n and similar technologies to coordinate multiple simultaneous radio signals. The MIMO increases both the range and throughput of a wireless network. An additional technique employed by 802.11n involves increasing the channel bandwidth from 20MHz to 40MHz. The 802.11n standard support maximum theoretical network bandwidth up to 300 Mbps. The IEEE802.11n indoor/outdoor ranges are 75m, and 250m respectively.

IEEE 802.11ac

IEEE 802.11ac is the fifth generation in Wi-Fi networking standards released December 2013[5-6]. This standard operating frequency is 5GHz, and bandwidth of 20, 40, 80, 160MHz sectors. The stream rates ranges for these bandwidth sectors are 7.2 - 96.3Mbps for 20MHz, and 15 – 200Mbps for 40MHz, 32.5 - 433.3Mbps for 80MHz, and 65 - 866.7Mbps for 160MHz. This standard exhibits better performance, and better coverage compared to IEEE 802.11a,b,g and n standards. The 802.11ac standard uses a wider channel and an improved modulation scheme that also supports more clients. The IEEE 802.11ac standard utilizes a modulation technique known as multi-user MIMO. This technique allows a set of users or wireless terminals, each with one or more antennas, o communicate with each other. The indoor range is 35m, and there is no recorded max for outdoor range.

Network Topology

A network topology is the physical layout of computers, cables, and other components on a network. There are a number of different network topologies, and a network may be built using multiple topologies. The different types of network layouts are Bus topology, Star topology, Mesh topology, Ring topology, Hybrid topology and Wireless topology.

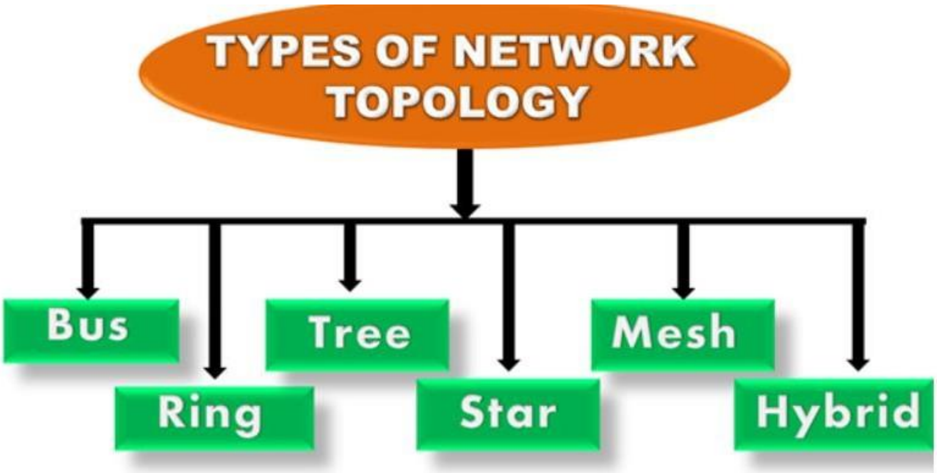


Figure 1.13 Network Topology

Bus Topology

A bus topology consists of a main run of cable with a terminator at each end. All nodes like workstations, printers, laptops, servers etc., are connected to the linear cable. The terminator is used to absorb the signal when the signal reaches the end, preventing signal bounce. When using bus topology, when a computer sends out a signal, the signal travels the cable length in both directions from the sending computer. When the signal reaches the end of the cable length, it bounces back and returns in the direction it came from. This is known as signal bounce. Signal bounce may create problems in the computer network, because if another signal is sent on the cable at the same time, the two signals will collide. Collisions in a computer network can drastically reduce the performance of the computer network.

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).
- **CSMA:** It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

- **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
- **CSMA CA: CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

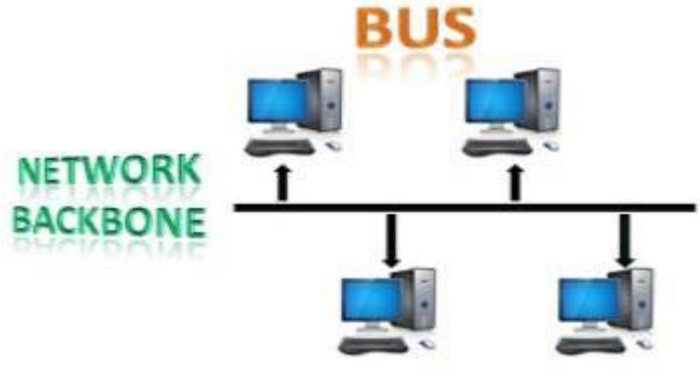


Figure 1.14 Bus Topology

Advantages:

- **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
- **Limited failure:** A failure in one node will not have any effect on other nodes.

Disadvantages:

- **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

Ring Topology

The physical shape of the network need not be in ring or circular shape. A ring topology can be a logical circle that has no start and no end. Terminators are not necessary in a ring topology. Signals travel in one direction on a ring while they pass from one computer to the next. Each device in ring topology can regenerate the data signal, so that the data signal may travel the required distance, without signal quality deterioration.

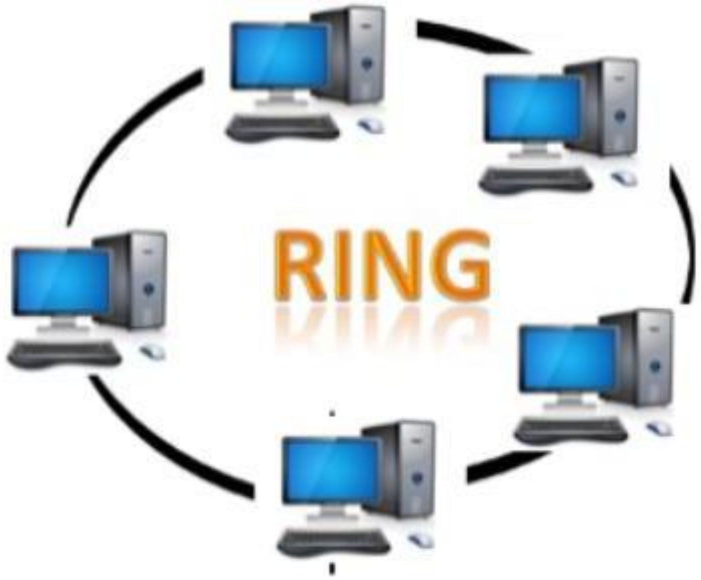


Figure 1.15 Ring Topology

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
  - **Token passing:** It is a network access method in which token is passed from one node to another node.
  - **Token:** It is a frame that circulates around the network.

Working of Token Passing:

- A token moves around the network, and it is passed from computer to computer until it reaches the destination.
- The sender modifies the token by putting the address along with the data.
- The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
- In a ring topology, a token is used as a carrier.

Advantages of Ring Topology:

- **Network Management:** Faulty devices can be removed from the network without bringing the network down.
- **Product availability:** Many hardware and software tools for network operation and monitoring are available.

- **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
- **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

Disadvantages of Ring Topology:

- **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- **Failure:** The breakdown in one station leads to the failure of the overall network.
- **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
- **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

Star Topology

A star topology is designed with each node (like workstations, printers, laptops, servers etc.) connected directly to a central device called as a network switch. Each workstation has a cable that goes from its network interface card (NIC) to a network switch. Most popular and most widely used LAN technology Ethernet operates in Star or Star-Bus topology

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
- The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- Hubs or Switches are mainly used as connection devices in a **physical star topology**.
- Star topology is the most popular topology in network implementation.

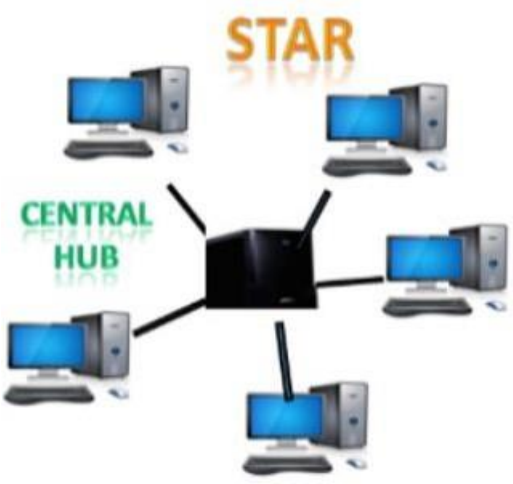


Figure 1.16 Star Topology

Advantages of Star Topology:

- **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.

- **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
- **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
- **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
- **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
- **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

Disadvantages of Star Topology:

- **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
- **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

Tree Topology

In tree topology, the devices are arranged in a tree fashion similar to the branches of a tree. Devices at lower level are connected to devices at next higher level, which resembles a tree like structure. At higher levels of the tree, often point-to-point or point-to-multipoint connections are used

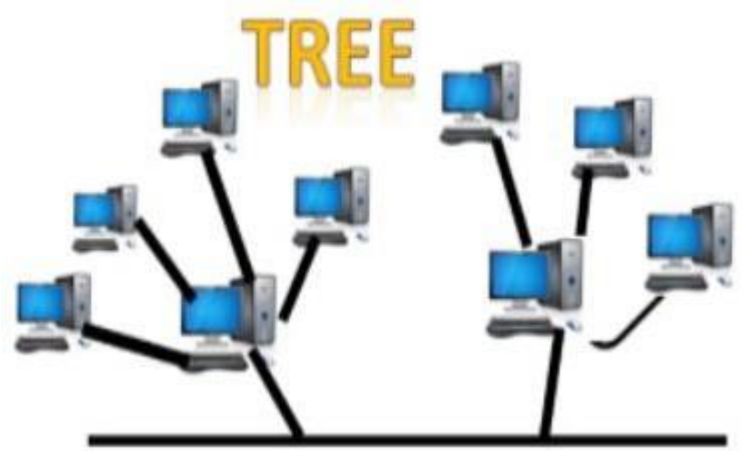


Figure 1.17 Tree Topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
- There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

Advantages of Tree Topology

- **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
- **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
- **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
- **Error detection:** Error detection and error correction are very easy in a tree topology.
- **Limited failure:** The breakdown in one station does not affect the entire network.
- **Point-to-point wiring:** It has point-to-point wiring for individual segments.

Disadvantages of Tree Topology

- **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
- **High cost:** Devices required for broadband transmission are very costly.
- **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
- **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

Mesh Topology:

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.
- Mesh topology is mainly used for wireless networks.
- Mesh topology can be formed by using the formula: **Number of cables = (n*(n-1))/2;** Where n is the number of nodes that represents the network.

In wired full-mesh topology, each device on the network is connected together, creating connections between all device on the network. Full-Mesh topology provide an extreme level of redundancy when compared with other network topologies. The main advantage in full-mesh topology is, if any connection between two devices failed, there is always an alternate path exists to reach the destination.

Full-mesh topology works well in a small network. Example; less than five devices. But as the number of devices in the network increases, Full-Mesh topology based networks become complex. It is not easy to connect 500 computers together in full-mesh topology.

- **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
- **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

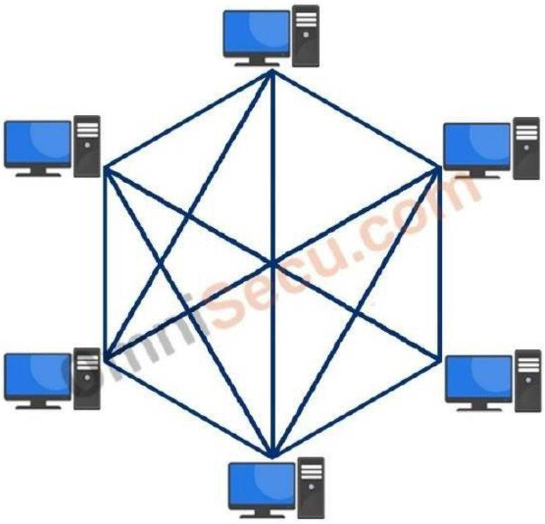


Figure 1.18 Partial Mesh Topology

Advantages of full-mesh topology

Redundancy of paths is the main advantage of full-mesh topology. If a connection between two devices failed, there is always an alternate path available to reach the destination.

Because of the extreme level of redundancy, full-Mesh topology is often used in the core layer and distribution layer of hierarchical network designs. Full-Mesh topology is also used for server connectivity redundancy and site-to-site WAN connectivity redundancy.

- **Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.
- **Fast Communication:** Communication is very fast between the nodes.

Easier Reconfiguration: Adding new devices would not disrupt the communication between other devices

Disadvantages of full-mesh topology

• The cabling costs of full-mesh topology-based network can be very high.

• It is not easy to troubleshoot a large full-Mesh topology based network.

A partial-mesh topology is also a mesh topology similar to full-mesh topology. In partial-mesh topology, all the devices are not connected to each other as in full-mesh topology. In partial-mesh topology, some of the devices are connected to many devices together, but other devices are connected only to one or two devices.

- **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
- **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
- **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

Hybrid Topology

- The combination of various different topologies is known as **Hybrid topology**.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For

example, if there exist a ring topology in one branch of ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

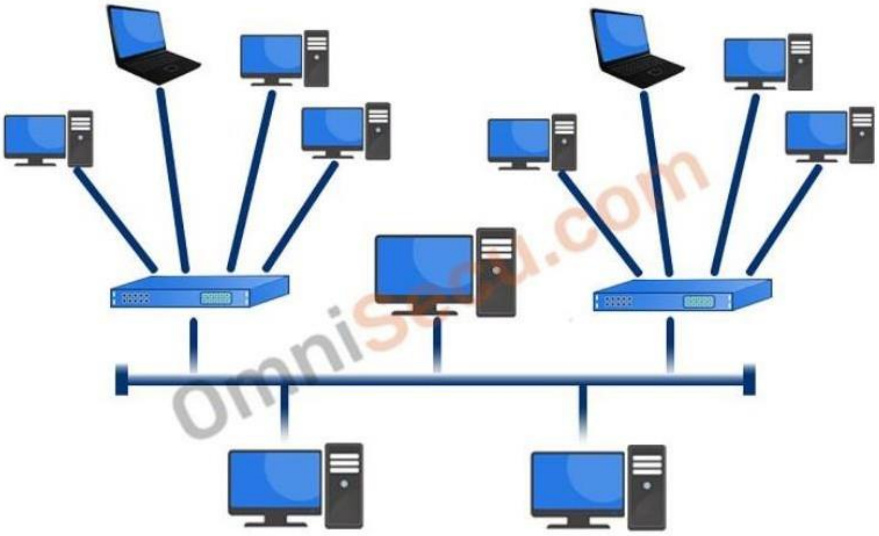


Figure 1.19 Hybrid Topology

Advantages of Hybrid Topology:

- **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
- **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
- **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
- **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized

Disadvantages of Hybrid Topology

- **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
- **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
- **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

Client-Server Network Management for WLAN

Network management Systems have played a great important role in information systems. There are different network management systems such as remote monitoring, desktop sharing, bandwidth management etc. It elaborates the above-mentioned issues i.e., remote desktop sharing, bandwidth management and Remote monitoring which are accumulated in single network management system. Remote desktop sharing is a technology that allows remote access and remote collaboration on a person's computer. Remote desktop sharing provides the capability to technology consultants, administrator or anyone to have full access and control of home computers, office workstations and servers remotely. Another application in network system is Bandwidth management.

- The client server network communication system is implemented by using .Net framework and C# language for application interface and use to detect the network feature and use SQL to store the important data of the system.
- This system uses Wi-Fi to connect various computers in network. This system uses TCP/IP protocol for network transaction.
- Client sends request for desktop sharing and sever responds to client's request and desktop sharing initiates. Similarly in remote monitoring request-Response method is used.
- Network communication system means different things to different people. In some cases, it involves a network consultant monitoring network activity with an outdated protocol analyzer.
- In other cases, network system involves a distributed database, auto polling of network devices, and high-end workstations generating real-time graphical views of network topology changes and traffic. In general, network communication system is a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks

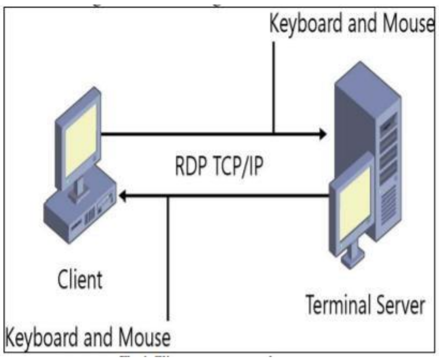


Figure 1.20 Client – Server Network Management

TEXT / REFERENCES BOOKS

1. Jun Zheng, Abbas Jamalipour,"Wireless Sensor Networks: A Networking Perspective", Wiley India, 1st Edition, 2014.

2. Waltenegus Dargie, Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", John Wiley & Sons, 1st Edition, 2010.

3. Edgar H. Callaway, "Wireless Sensor Networks: Architectures and Protocols", CRC Press, 1st Edition, August 2003.

4. Jose A. Gutierrez, Edgar H. Callaway, Raymond Barrett, "IEEE 802.15.4 Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensor Networks", Standards Information Network, 3rd Edition,2011.

5. Kazem Sohraby, Daniel Minoli, TaiebZnati, "Wireless Sensor Networks: Technology, Protocols, and Applications", John Wiley & Sons, 1st Edition, 2007.

PART A

1. Discuss the basic requirements needed in wireless technologies
2. Classify the terms WAN and LAN

3. Tabulate the advantage and disadvantage of star topology
4. Report the different types of wireless networks and explain in detail
5. Discuss the objectives of Adhoc wireless network
6. Explain the term wireless LAN
7. Interpret the concept of Client-Server Network Management for WLAN

PART B

1. Generalize in detail about different network topologies
2. Summarize the application of wireless technologies
3. Outline the wireless network generations
4. Describe in detail about IEEE 802.111 standard
5. Discuss in detail about frequency sub bands a,b,g,n

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – II

WIRELESS SENSOR NETWORKS FOR IOT – SECA5203

UNIT – II FUNDAMENTALS OF BLUETOOTH

Bluetooth Basics, Classic Bluetooth Profiles - L2CAP, RFCOMM, Bluetooth Smart/Low Energy, BLE Profiles-GATT, GAP, BLE Motes, Beacons- Protocols, Implementation support, frame support, Advertising, discovering, data Transmission, Bluetooth 5/ Bluetooth Mesh protocols

Bluetooth Basics:

Now-a-days bluetooth has become part of our lives due to its immense applications from audio devices which include headsets and mobile phones, home stereos, MP3 players, laptop, desktop, tablets and more. With bluetooth one can transfer data (meeting schedules, phone numbers), audio, graphic images and video from one device to the other provided they are bluetooth compliant. IEEE 802.15.1 standard describes detailed bluetooth specifications. 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. Bluetooth is a short-range wireless communications technology.

  - It was taken from the 10th century Danish King Harald Blatand who unified Denmark and Norway.
- The Bluetooth specification was first developed in 1994 by Sven Mattison and Jaap Haartsen, who were working for Ericsson Mobile Platforms in Sweden.
  - 5 companies (Ericsson, Nokia, IBM, Intel & Toshiba) joined to form the Bluetooth Special Interest Group (SIG) in 1998.
  - First specification released in July 1999.
- Bluetooth is a wireless system that uses radio waves for communication. It has the ability to communicate with many different devices at once without interference.
- Bluetooth is an open standard for short-range transmission of digital voice and data that supports point-to-point and multipoint applications.

Bluetooth is based on a low-cost, low power, short range radio link. Bluetooth cuts the cord that used to tie up digital devices. When two bluetooth devices come within 50 meters range of each other, they establish a connection together. It operates at 2.45 Ghz which is available globally, although slight variation of location and width of band apply.

- The range is set at 10 to100 meters to optimize for target market of mobile and business user.
- Gross data rate is 1mbit/s, with second generation plans to increase to 2mbit/sec. One-to-one connections allow maximum data transfer rate of 723 kbit/s. It has low power consumption, drawing only 0.3ma in standby mode. This enables maximum performance longevity for battery powered devices.

- Bluetooth network consists of many bluetooth users. There are two types of network topologies in bluetooth viz. Piconet and scatternet. Piconet is formed by one master and one slave as well as one master and multiple slaves. There will be maximum 7 active slaves in the piconet. Hence there will be about 8 maximum devices communicating in a small network referred as piconet. Slaves can only transmit when they have been requested by the master bluetooth device. There will be about 255 slaves in parking state. Active slaves are polled by the master for transmission. Each station will get 8bit parked address. Total 255 parked slaves are possible in one piconet. The parked station can join in just 2ms. All the other stations can join in more time. About 10 such piconets exist in the bluetooth radio coverage area. Combinations of multiple piconets is known as scatternet. A device can participate in multiple piconets. It will timeshare and need to be synchronized with the master of current piconet. It supports data rate based on different versions from 720 kbps to about 24 Mbps. It will have distance coverage to about 1 to 100 meters based on power class supported on bluetooth devices.

These are the different versions of bluetooth technologies we have since 1999.

- Bluetooth v1.0 and v1.0B (with mandatory bluetooth hardware device address)
- Bluetooth v1.1 (ratified as IEEE standard 802.15.1-2002)
- Bluetooth v1.2 (faster connection and discovery)
- Bluetooth v2.0 + EDR (enhanced data rate)
- Bluetooth v2.1 (secure simple pairing-SSP)
- Bluetooth v3.0 (high speed data transfer)
- Bluetooth v4.0 (low energy consumption – recently used in apple i-phone 4S)

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.

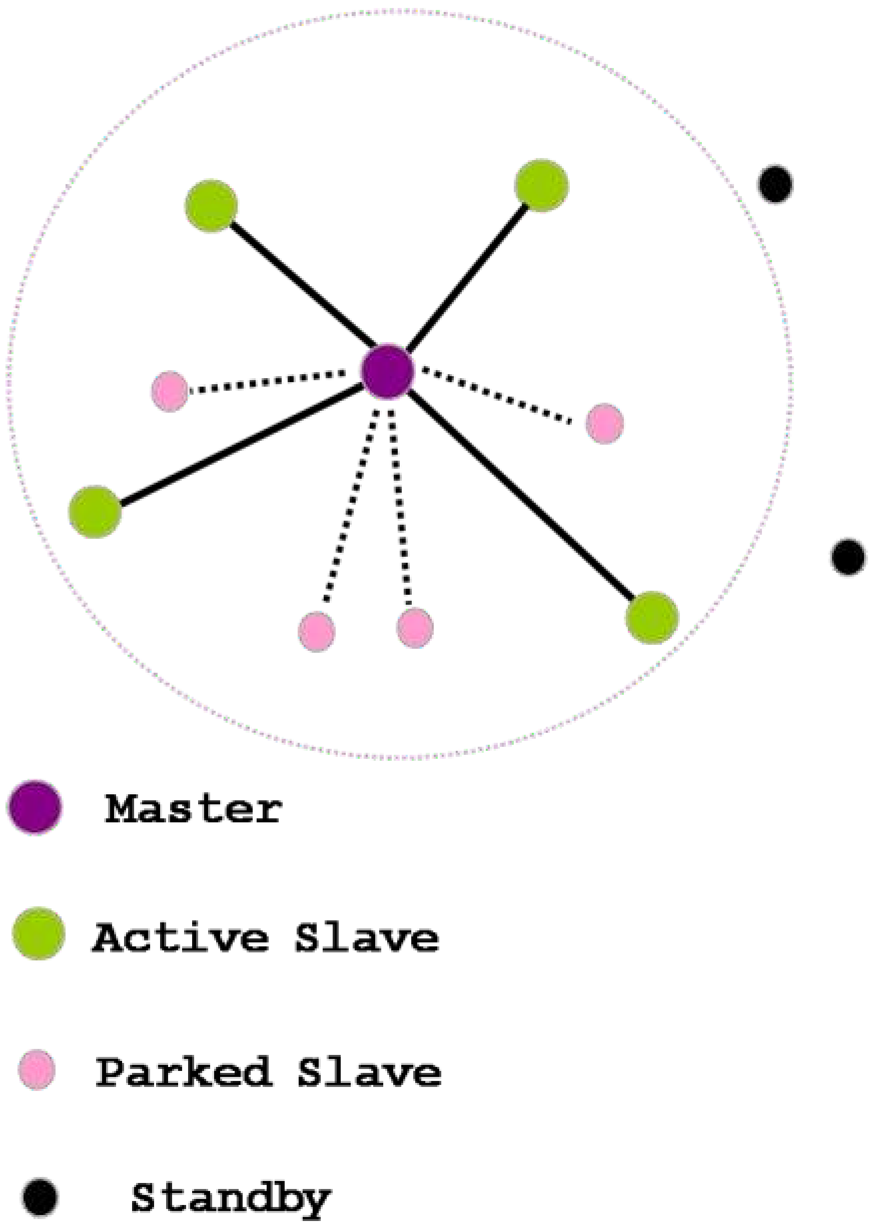


Figure 2.1 Piconet

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.

Classic Bluetooth Profiles
The Bluetooth specification contains several profile specifications. A profile describes how to use and implement a function.
They can depend on each other, here is a basic layout of the most common profile dependencies

All profiles can be found at BT SIG, be aware that different versions might contain different functionality. Also note that some of the profiles contains several categories, these are sometimes optional, so make sure that your device supports the category in question. Here are some of the most common *smartphone Profiles* and their specifications

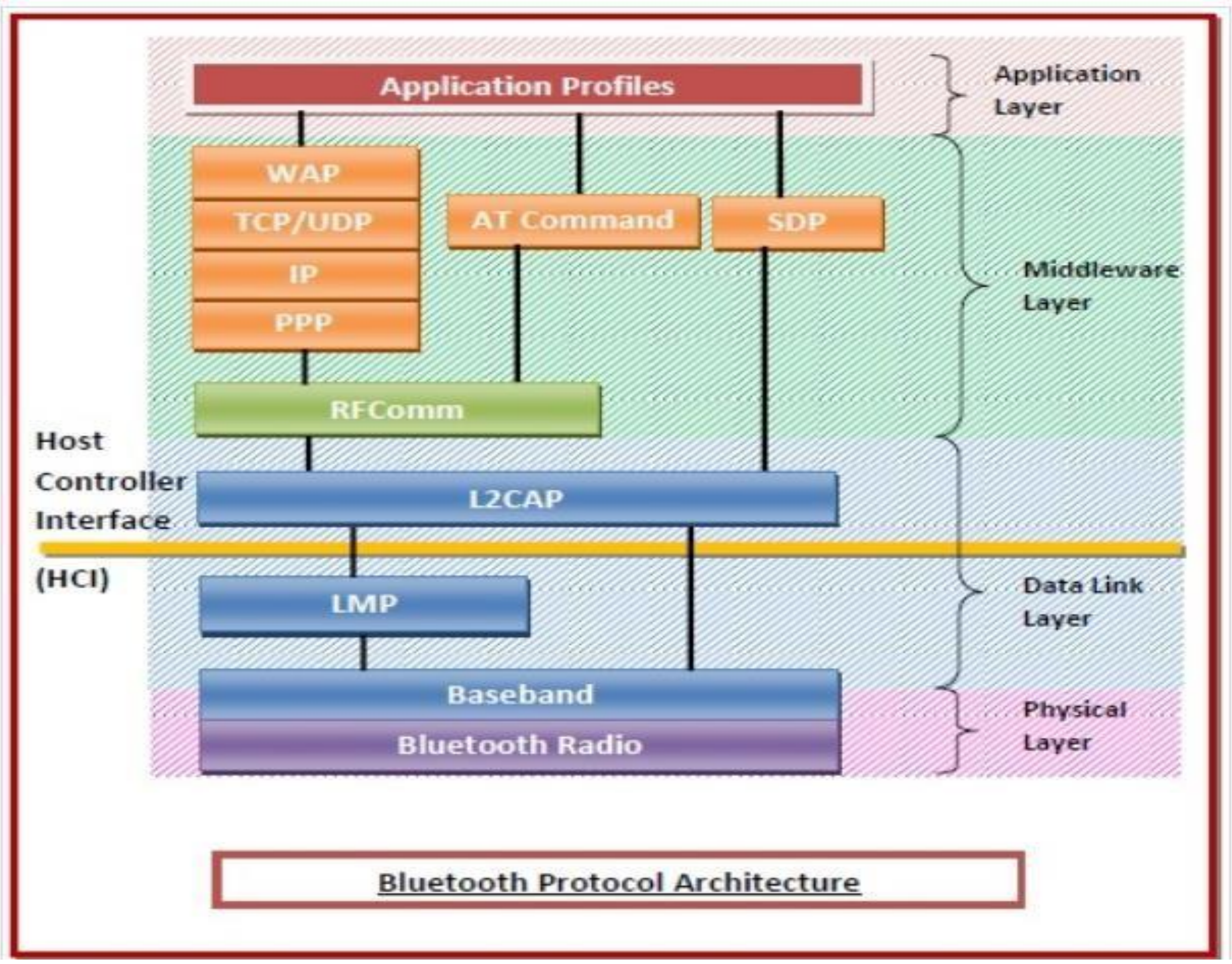


Figure 2.2 Bluetooth Protocol Architecture

Protocols in the Bluetooth Protocol Architecture

Physical Layer − This includes Bluetooth radio and Baseband (also in the data link layer.
Radio − This is a physical layer equivalent protocol that lays down the physical structure and specifications for transmission of radio waves. It defines air interface, frequency bands, frequency hopping specifications, and modulation techniques.
Baseband − This protocol takes the services of radio protocol. It defines the addressing scheme, packet frame format, timing, and power control algorithms.
Data Link Layer − This includes Baseband, Link Manager Protocol (LMP), and Logical Link Control and Adaptation Protocol (L2CAP).

- **Link Manager Protocol (LMP)** − LMP establishes logical links between Bluetooth devices and maintains the links for enabling communications. The other main functions of LMP are device authentication, message encryption, and negotiation of packet sizes.
- **Logical Link Control and Adaptation Protocol (L2CAP)** − L2CAP provides adaption between upper layer frame and baseband layer frame format. L2CAP provides support for both connection-oriented as well as connectionless services.
- **Middleware Layer** − This includes Radio Frequency Communications (RFComm) protocol, adopted protocols, SDP, and AT commands.
    - **RFComm** − It is short for Radio Front end Component. It provides a serial interface with WAP.

- **Adopted Protocols** − These are the protocols that are adopted from standard models. The commonly adopted protocols used in Bluetooth are Point-to-Point Protocol (PPP), Internet Protocol (IP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Wireless Application Protocol (WAP).
- **Service Discovery Protocol (SDP)**− SDP takes care of service-related queries like device information so as to establish a connection between contending Bluetooth devices.
- **AT Commands** − ATtention command set.
- **Applications Layer** − This includes the application profiles that allow the user to interact with the Bluetooth applications.

Bluetooth Protocol Stack

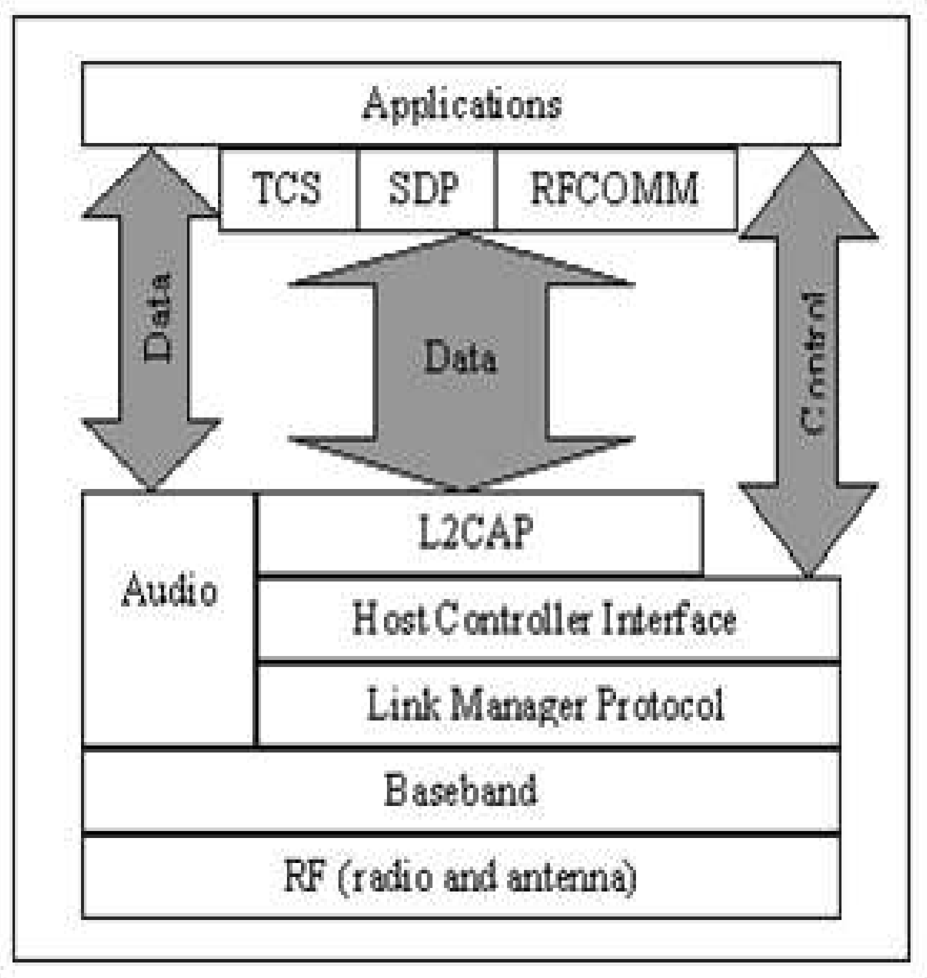


Figure 2.3 Bluetooth Protocol Stack

The heart of the Bluetooth specification is the Bluetooth protocol stack by providing well-defined layers of functionality, the Bluetooth specification ensures interoperability of Bluetooth devices and encourages adoption of Bluetooth technology. Bluetooth is defined as a layered protocol architecture consisting of core protocols, cable replacement and telephony control protocols, and adopted protocols.

Core System Protocols:

- **Radio (RF) protocol :** Specifies details of the air interface, the use of frequency hopping, modulation scheme, and transmit power.

- **Baseband protocol:** Concerned with connection establishment within a Piconet, addressing, packet format, timing, and power control.
- **Link Manager protocol (LMP):** Responsible for link setup between Bluetooth devices and ongoing link management.
- **Logical link control and adaptation protocol (L2CAP)** L2CAP provides both connectionless and connection-oriented services.
- **Service discovery protocol (SDP) :** Device information, services, and the characteristics of the services can be queried to enable the establishment of a connection between two or more Bluetooth devices
- **RFCOMM:** It provides connections to multiple devices by relying on L2CAP to handle multiplexing over single connection
- **Wireless access protocol (WAP):** It supports the limited display size and resolution typically found on mobile devices by providing special formats for Web pages
- **Object exchange protocol (OBEX):** OBEX is a protocol designed to allow a variety of devices to exchange data simply and spontaneously.
- **Telephony control protocol:** Bluetooth's Telephony Control protocol Specification (TCS) defines how telephone calls should be sent across a Bluetooth link
- **Point-to-point protocol (PPP):** The point-to-point protocol is an Internet standard protocol for transporting IP datagram over a point- to-point link

Bluetooth Profiles:

- In order to use Bluetooth wireless technology, a device must be able to interpret certain Bluetooth profiles. The profiles define the possible applications
- Each profile specification contains information on the following topics:
  - ➢ Dependencies on other profiles
  - ➢ Suggested user interface formats
  - ➢ Specific parts of the Bluetooth protocol stack used by

the profile. To perform its task, each profile uses particular options and parameters at each layer of the stack.

- Certain examples: Generic Access Profiles, Telephony Control Protocol Specification, Generic Object Exchange Profiles, Serial Port Profiles

Applications of Bluetooth:

- Wireless control of and communication between a mobile phone and a **hands free headset**. This was one of the earliest applications to become popular.
- **Wireless communication with pc** input and output devices, the most

common being the mouse, keyboard and printer.

- **Transfer of files**, contact details, calendar appointments, and reminders between devices with obex.
- In 2004 released cars like toyota prius & lexus ls 430 have **hands free call system.**
- Sending small advertisementsfrom bluetooth-enabled advertising

hoardings to other, discoverable, bluetooth devices.

- In game consoles like sony's playstation 3 and psp go, use bluetooth for their respective wireless controllers.
- Dial-up internet access on personal computers or PDAs using a data-capable mobile phone as a wireless modem.
- Personal security application on mobile phones for prevention of theft or loss of items.
- In Real-time location systems (RTLS). Digital Pulse Oximetry System Toshiba Washer & Dryer.

Classic Bluetooth:

- Classic Bluetooth is mainly used for audio such as wireless telephone connections, wireless headphones and wireless speakers. Bluetooth Low Energy is more often seen in wearable devices, smart IoT devices, fitness monitoring equipment, and battery-powered accessories such as a keyboard.
- Bluetooth Classic is the wireless protocol that's been ubiquitous for almost 15 years. Bluetooth Headsets, Speakers, Smartphones, Smart watches and many devices use a Bluetooth radio to communicate.
- While in 2010 the standard was updated with Bluetooth Low Energy, we're going to talk about Bluetooth Classic, the original radio protocol that is still widely used for streaming audio and voice.
- The Bluetooth standard was born out of necessity of creating a wireless connection between computers and devices.
- In the late 90's it was clear that computers would require wireless connectivity for a host of devices.
- The basis for Bluetooth (now usually referred to as Bluetooth classic to distinguish it from Bluetooth Low Energy) was developed in the late 90's.
- In 1998, the Bluetooth Special Interest Group (Bluetooth SIG) was formed among a consortium of companies to push the standard. It took several years for the companies to come together and settle on a specification.
- The first official Bluetooth specification adopted was Bluetooth v1.0, but it wasn't really until Bluetooth 2.0 that it began solidifying.
- The 1.0, 1.0b 1.1 and 1.2 Bluetooth specifications contained various bugs, limitations, or lacked features that were needed for users.
- Bluetooth 2.0 resolved significant issues and introduced the Enhanced Data Rate mode which had faster modulation and allowed up to 3Mbps throughput.
- This enabled higher quality audio. The Bluetooth 2.1 + EDR specification is the spec that forms the basis for Bluetooth Classic, and the technology has stayed mostly the same since.
- Bluetooth 2.0 didn't have any real security and 2.1 brought Secure Simple Pairing. You're probably familiar with it by the pairing pin you need to type when pairing a Bluetooth device to another.
- Despite all the changes in the Bluetooth specification - the latest is Bluetooth 5.2 - the Bluetooth Classic has remained the same since Bluetooth 2.1 + EDR was released in 2007. Bluetooth 3.0 introduced the High Speed (HS) mode, which allows a Bluetooth paired device to use Wi-Fi or another medium (PHY) to transfer the data.

- Despite all the changes in the Bluetooth specification - the latest is Bluetooth 5.2 - the Bluetooth Classic has remained the same since Bluetooth 2.1 + EDR was released in 2007. Bluetooth 3.0 introduced the High Speed (HS) mode, which allows a Bluetooth paired device to use Wi-Fi or another medium (PHY) to transfer the data.

- Since the introduction of Bluetooth Low Energy in the Bluetooth 4.0 specification, there are basically two different radios in Bluetooth. Because of this, it's important to understand what the radio supports.
- A Bluetooth 5.0 or 4.0 device could support Bluetooth Classic, Bluetooth Low Energy, or both (called Dual mode devices).

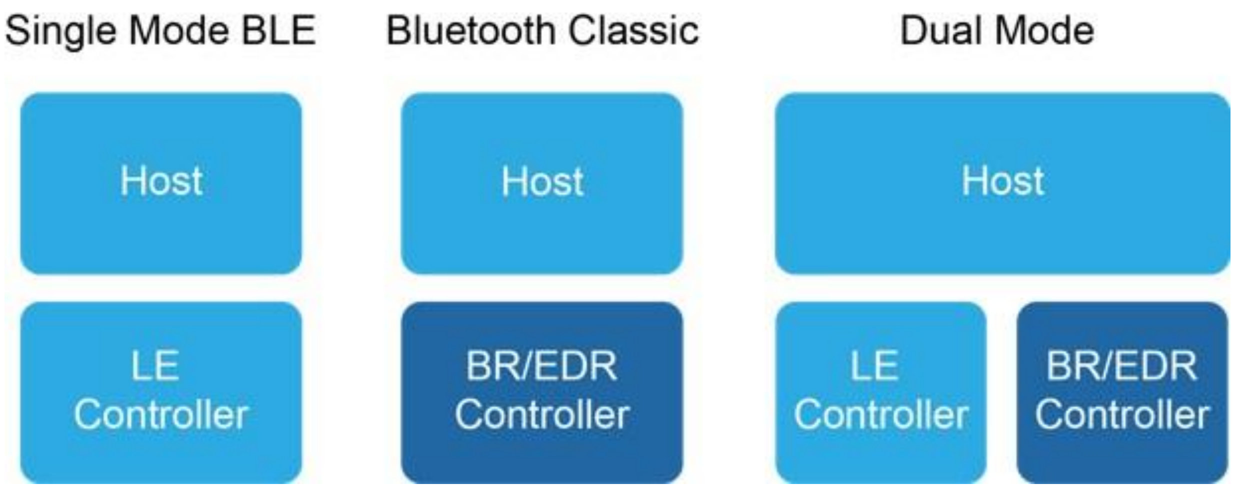


Figure 2.4 Bluetooth Mode

Bluetooth Physical Layer

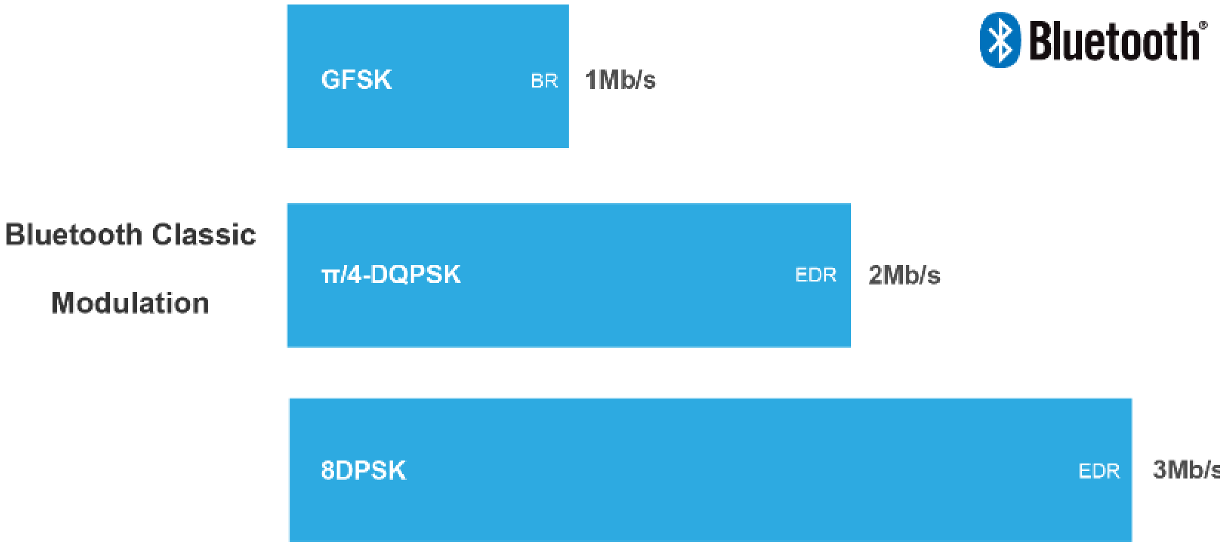


Figure 2.5 Bluetooth Physical Layer

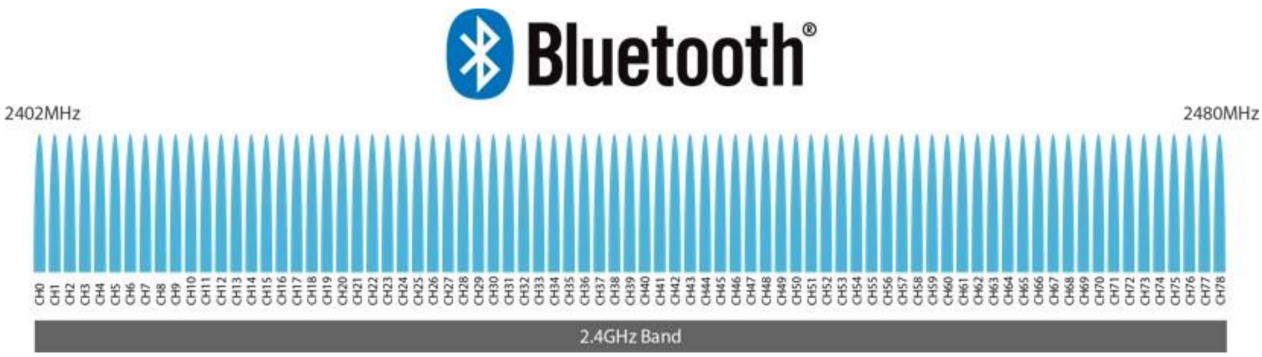


Figure 2.6 channels

- Bluetooth Classic uses the 2.4GHz ISM band. This band is available worldwide, which means that users can use Bluetooth anywhere in the world.
- The 2.4GHz ISM band extends from 2400MHz to 2483.5Mhz, but Bluetooth and many other systems only use 80MHz of the bandwidth.
- This bandwidth is divided by Bluetooth into 79 channels, each spaced 1MHz apart, starting from 2402MHz up to 2480MHz. The channels are numbered 0 to 78.
- One of the goals of Bluetooth is to avoid interference. The number of channels and the adaptive frequency hopping algorithm help prevent interference from many sources. Since the 2.4GHz band is unlicensed, there are many transmitters nearby like baby monitors, Wi-Fi, and Microwave ovens
- Bluetooth creates point-to-point or point-to multipoint connections. In practice though, the Single Slave or Multi-slave approaches dominate.
- For example, an iPhone connected to a Bluetooth Headset. Bluetooth can form complex networks where a slave may be connected to two different masters.
- The main form of the topology in Bluetooth is called a piconet. A piconet has a single master that has a master clock and can have up to seven slaves.
- When piconets share slaves (or masters that act as a slave in another piconet), they form what is called a scatternet. Piconets are not synchronized and each has its own hopping sequence

Bluetooth Packet Format:

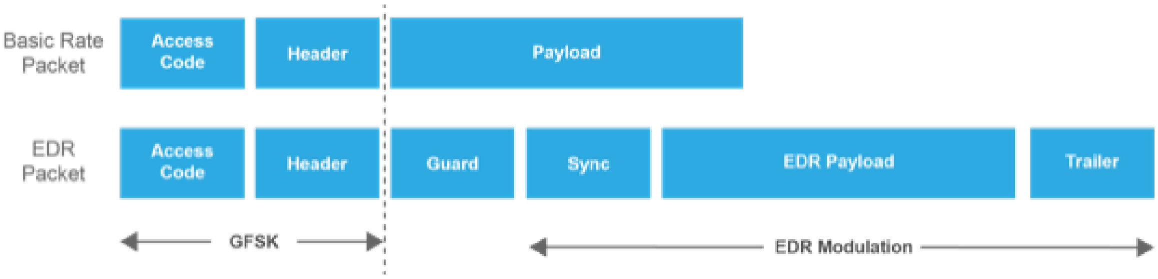


Figure 2.7 Bluetooth Packet Format

- The diagram above shows the packet format for both Basic Rate and Enhanced Data Rate. As we mentioned before, the EDR packet sends the Access Code and Header using the basic rate, then the guard time gives it time to change modulation. The Sync, payload and Trailer are sent using the modulation format.
- One of the most critical aspects of Bluetooth is the Clock. The master device in a Bluetooth connection has a clock that is used to split the time on each physical channel. All slaves in a connection have clocks that are synchronized to the Master clock.
- Synchronizing the clocks on Bluetooth is critical because the radios need to sync up on when they transmit. Because Bluetooth uses precise timeslots for transmissions with the devices alternating, if the clocks are not synchronized there could be issues with devices transmitting at the wrong time.
- Physical Channels
- As we mentioned, there are 79 RF channels. Bluetooth radios use these channels to transmit using a pseudo random frequency hopping algorithm. In addition, this algorithm is adaptive and the channels to be used are dynamically updated at run time depending on interference.
- Because of this, Bluetooth is said to use Adaptive Frequency Hopping, commonly called AFH. This technique allows it to avoid significant interference in the 2.4GHz band. It also

enables multiple Bluetooth systems to coexist in the same space. Bluetooth hops up to 1600 hops per second.

- Access Address
- In order to transmit, Bluetooth devices use at the start of a packet the Access Address. The Access Address is 48-bit and is based on an OUI and address space allocated by the IEEE.
- Transmitting
- While Bluetooth jumps through multiple channels, each channel is divided into 625 µs timeslots. The Master and slave alternate sending data. The master sends data in the even timeslots, while the slave sends data in the odd timeslots.
- Because 625 µs is relatively short, specific packet types can aggregate multiple time slots. The largest packets can transmit in 5 timeslots.
- Sending data in larger packets is more efficient, because there's less overhead, so that helps with higher quality audio applications.

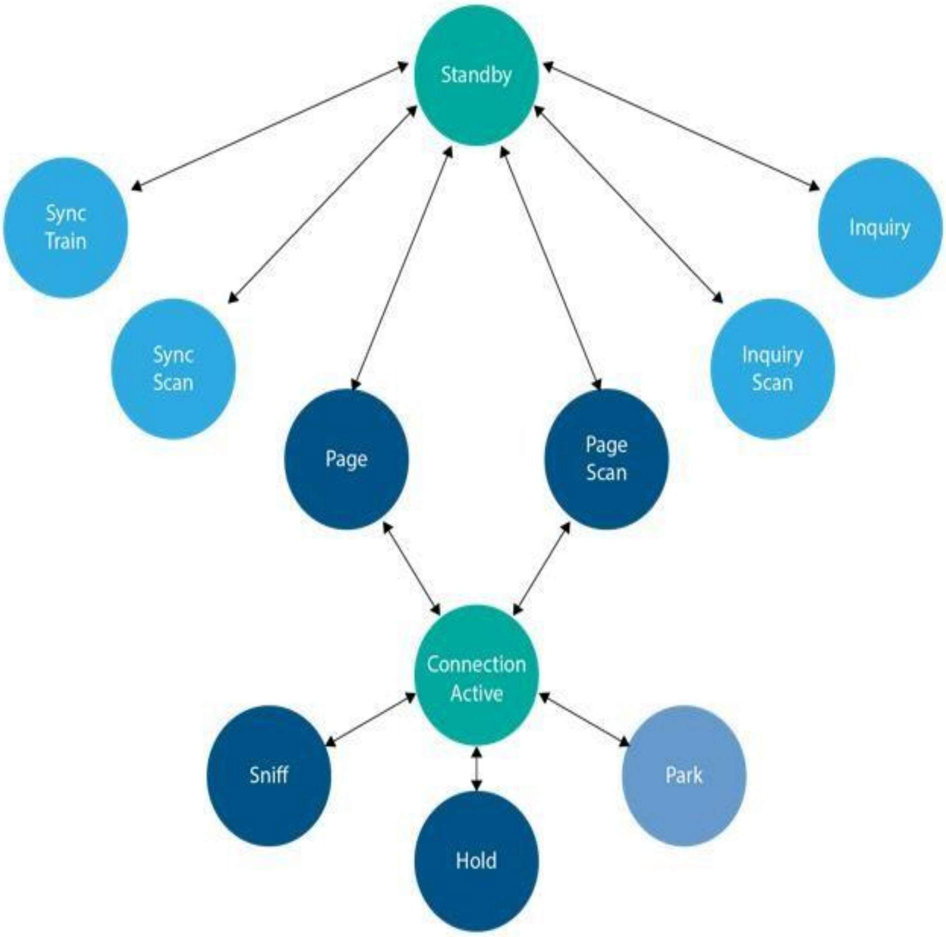


Figure 2.8 Bluetooth Classic Link Controller

The diagram above shows the states of a Bluetooth Classic Link Controller

- Standby
- Inquiry
- Inquiry Scan
- Page
- Page Scan
- Synchronization Train
- Synchronization Scan

When in a connection, some of the states are:

- Active
- Park
- Hold
- Sniff
- Every Bluetooth device starts at **Standby**. If a Bluetooth device wants to connect to another device, the only thing it needs to know is the Bluetooth address. If it has the Bluetooth device address, it can start the Page procedure and "Page" the device so both can connect.
- This process can take some time, but can be sped up if there is information about the clock or page mode of the device we want to connect to.

While the Master initiates the Page, the Slave needs to be in the Page Scan mode waiting for paging events. The device that starts the connection using the Page procedure is automatically the Master of that connection

- In the Page procedure, the master sends a paging message with the slave's Device Access Code (DAC) in different channels it is hopping across, listening in between the transmissions for a response from the slave.
- The issue, and one of the reasons Bluetooth connection establishment takes time is that the clocks of both devices are not synchronized. The slave wakes up to receive packets at different periods, so this can take time.
- **Paging** can be done from **Standby**, meaning there aren't any active connections, or from the connection state.
- Paging is a pretty demanding process, and because of that, it can have an impact on the performance of the active connection. Bluetooth controllers may put the active connection on hold, reduce retransmissions or other things. Because of this, connecting to other devices must be done carefully.
- Bluetooth uses the Inquiry procedure and Inquiry Scan. One device enters the Inquiry state and begins sending inquiries. The device we want to connect to needs to be discoverable, which means it enters the Inquiry Scan.
- Sniff Mode and Sniff Subrating
- Since power consumption is a critical aspect in most Bluetooth devices, it's important to reduce this. Listening and communicating on every time slot will use a lot of power.
- So a specific mode called Sniff allows a slave in the piconet to reduce its activity and avoid listening at every time slot. Sniff Subrating is an additional mode that is interleaved with Sniff mode and reduces even further the sniff anchor points.
- Hold State
- The Bluetooth **Hold** state is a temporary mode that allows a slave to save on power. When a Bluetooth device is placed in Hold mode, the Master and Slave agree on a wakeup time. The slave will then wake up after the specified amount of time.
- Park State
- You may have seen reference to the Bluetooth Park state. This state allowed a slave to reduce its activity if it didn't need to participate in the piconet channel but still wanted to remain synchronized. Aside from very low power consumption, Park was one way to technically have more than 7 slaves. The 7 slave limitation is for active devices in the connection state, but switching devices to parked allowed new devices.
- In the parked state, the slave that's parked wakes up periodically to check for broadcast messages to synchronize with the master. The master uses a beacon train to do the synchronization.
- The parked state is now a deprecated feature as of Bluetooth 5.0.

Discovering Bluetooth Devices

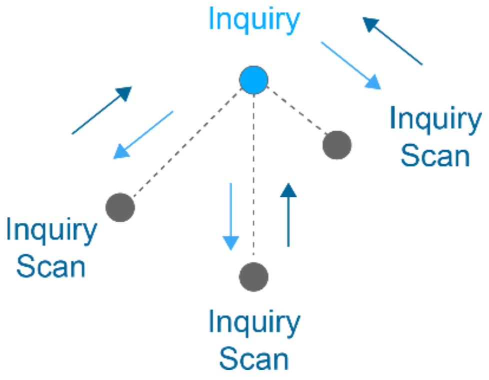


Figure 2.9 Discovering Mode

- When the discovering Bluetooth device enters the inquiry mode, it attempts to discover all devices nearby that are discoverable by collecting the inquiry responses. Devices are not forced to answer the inquiry. The Inquiring device gets the Bluetooth addresses and clocks of all the devices that respond, but the device can also get the Extended Inquiry Response (EIR) that contains local name and services if the discoverable device provides it.
- If you've ever opened the Bluetooth Settings screen in an iOS device or Android and find some devices, they're showing up because when entering that screen the phone starts the inquiry process and is collecting data.
- Like the Paging State, the Inquiry state can be entered from the Standby mode (no current connections) or from the **Connection** state. As with paging, performing an inquiry during a connection puts certain demands on the timing and radios.
- One of the downsides of the Inquiry procedure is that it may take up to 10.24s to fully complete (unless terminated earlier). This is assuming no interference. The inquiry can require longer time to find the actual device. This is one of the reasons Bluetooth Classic takes time to form a connection.

Link Manager Protocol

- The LMP porotcol is the protocol that manages and negotiates the Bluetooth connections between a Master and Slave, including all the logical transports and logical links.
- Each device contains a Link Manager (LM) that sends and receives LMP messages. LMP messages are exchanged over the ACL-C logical link that is carried by the ACL logical transport. These messages also have higher priority than other traffic on this channel.

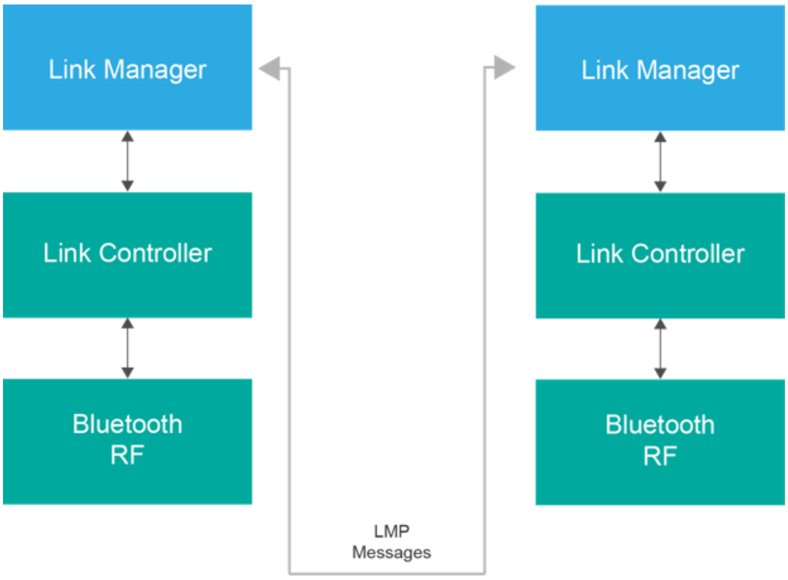


Figure 2.10 LMP Protocol

- The LMP protocol controls everything and is the main control mechanism for everything including pairing, clock adjustment, security, AFH control, etc.
- Pairing and Bonding
- Now that we understand a little more about LMP, we can discussion pairing and bonding, which most will be familiar with. Pairing is simply exchanging data to create a security key for encryption. Bonding means storing that information.

Bluetooth Classic Profiles

- On top of all the Bluetooth layers sit the profiles. These profiles are
- **A2DP** - Advanced Audio Distribution Profile is a profile that allows streaming audio from a source to a sink. For example, when you stream music from your iPhone to your car, this is done using the A2DP profile.
- **HFP** - Hands-Free Profile used in Bluetooth headsets
- **SPP** - Serial Port Profile emulates serial ports over Bluetooth allowing
- **PBAP** - Phone Book Access Profile allows access to a phone's Phone Book, for example to display in a car to allow dialing
- **MAP** - Message Access Profile allows access to a phone's Phone Book, for example to display in a car to allow dialing
- **AVRCP** - A/V Remote Control Profile allows a Bluetooth device to act as a remote control, for example controlling video playback

Bluetooth Chipset Manufactures

- One of the largest chipset providers is Qualcomm which acquired CSR plc a few years ago. CSR chipsets were used in volume in headsets and a multitude of applications. Qualcomm and Realtek tend to dominate audio related applications, which are the highest volumes one.
- Qualcomm (previously CSR)
- Broadcom
- Cypress Semiconductor - acquired IP from Broadcom
- Texas Instruments
- Realtek

Bluetooth Smart/Low Energy

- Bluetooth Low Energy (BLE) is a low power wireless communication technology that can be used over a short distance to enable smart devices to communicate.
- Some of the devices such as smart phone, smart watch, fitness tracker, wireless headphones and computer
- BLE is a relatively new Bluetooth standard defined by the Bluetooth Special Interest Group (SIG) with a focus on low energy. It has enabled device manufacturers to add a low power communications interface on existing solutions.
- It has also been used to create new low power devices such as beacons that can be powered by a small coin cell battery for months or even years.
- BLE has a wide range of possibilities and is implemented in a broad set of fields such as health, fitness, security, home automation, home entertainment, smart industry and IoT (Internet of Things). It's also close at hand in the smartphones and laptops that we use every day.
- Apple was an early adopter of BLE in smartphones with release of the iPhone 4s in 2011. Today, the majority of Android and iOS devices on the market incorporate BLE for communication and interaction with other devices.
- A BLE device is acting in either a central or peripheral role and is sometimes also referred to as a client or server.
- Central (Client)
- A device that initiates commands and requests, and accepts responses.
- Examples: computer, smartphone
- Peripheral (Server)
- A device that receives commands and requests, and returns responses
- Examples: a temperature sensor, heart rate monitor
- The peripheral role is BLE devices - things like headphones, fitness trackers, heart rate monitors, etc.
- A device that advertises its availability for connection and provides an interface for communication is acting as a peripheral.
- BLE uses a hierarchical data structure to define the information exchange structure. A BLE device acting as a peripheral will advertise services and characteristics that can be used for communication with the device.
- These attributes are defined using a GATT (Generic Attributes) profile. Characteristics expose values as small packets of information that can change over time. Characteristics are grouped together with similar types into services.

GATT

- GATT - Generic Attribute Profile, and it defines the way that two Bluetooth Low Energy devices transfer data back and forth using concepts called Services and Characteristics.
- It makes use of a generic data protocol called the Attribute Protocol (ATT), which is used to store Services, Characteristics and related data in a simple lookup table using 16-bit IDs for each entry in the table.
- The peripheral is known as the GATT Server, which holds the ATT lookup data and service and characteristic definitions, and the GATT Client (the phone/tablet), which sends requests to this server.
- All transactions are started by the main device, the GATT Client, which receives response from the secondary device, the GATT Server.

- When establishing a connection, the peripheral will suggest a 'Connection Interval' to the central device, and the central device will try to reconnect every connection interval to see if any new data is available, etc.,
- A pre-defined collection of Services that has been compiled by either the Bluetooth SIG or by the peripheral designers
- Services are used to break data up into logic entities, and contain specific chunks of data called characteristics.
- A service can have one or more characteristics, and each service distinguishes itself from other services by means of a unique numeric ID called a UUID, which can be either 16-bit (for officially adopted BLE Services) or 128-bit (for custom services).
- The lowest level concept in GATT transactions is the Characteristic, which encapsulates a single data point (though it may contain an array of related data, such as X/Y/Z values from a 3-axis accelerometer, etc.)

GAP

- GAP is an acronym for the Generic Access Profile, and it controls connections and advertising in Bluetooth. GAP is what makes your device visible to the outside world, and determines how two devices can (or can't) interact with each other.
- GAP defines various roles for devices, but the two key concepts to keep in mind are Central devices and Peripheral devices.
- Peripheral devices are small, low power, resource constrained devices that can connect to a much more powerful central device. Peripheral devices are things like a heart rate monitor, a BLE enabled proximity tag, etc.
- Central devices are usually the mobile phone or tablet that you connect to with far more processing power and memory.
- There are two ways to send advertising out with GAP. The Advertising Data payload and the Scan Response payload.

  Both payloads are identical and can contain up to 31 bytes of data, but only the advertising data payload is mandatory, since this is the payload that will be constantly transmitted out from the device to let central devices in range know that it exists.
- The scan response payload is an optional secondary payload that central devices can request, and allows device designers to fit a bit more information in the advertising payload such a strings for a device name, etc.

- There are two ways to send advertising out with GAP. The Advertising Data payload and the Scan Response payload.

  Both payloads are identical and can contain up to 31 bytes of data, but only the advertising data payload is mandatory, since this is the payload that will be constantly transmitted out from the device to let central devices in range know that it exists.
- The scan response payload is an optional secondary payload that central devices can request, and allows device designers to fit a bit more information in the advertising payload such a strings for a device name, etc.

- By including a small amount of custom data in the 31 byte advertising or scan response payloads, you can use a low cost Bluetooth Low Energy peripheral to sent data one-way to any devices in listening range.
- This is known as Broadcasting in Bluetooth Low Energy. This is the approach use by Apple's iBeacon, for example, which inserts a custom payload in the main advertising packet, using the Manufacturer Specific Data field.

- Once we establish a connection between peripheral and a central device, the advertising process will generally stop and will typically no longer be able to send advertising packets out anymore, and you will use GATT services and characteristics to communicate in both directions.

BLE Mote:

- BLE mote is a system on chip based device for Bluetooth Low Energy based applications. This mote is compliant to the Bluetooth 4.0 standards with Low Energy Profile support.
- Highly integrated System on Chip with ARM Cortex M0 microcontroller with
- 32 kB RAM, 256 kB flash Memory
- Supports various Serial Communication Interfaces like SPI, UART, I2C, Timers, ADC
- CPU independent Programmable Peripheral Interconnect (PPI)
- Real Timer Counter (RTC)
- Watchdog Timer (WDT)
- External Flash Memory
- 8Mb Flash memory with Write Protection and Deep Power Down Mode
- RF subsystem
- 2.4 GHz ISM Band RF Transceiver compliant to Bluetooth 4.0 LE standards
- 250 kbps, 1 Mbps, 2 Mbps supported data rates
- GFSK Modulation
- Programmable Transmit power of +4 dBm to -20 dBm (in 4 dB steps)
- High Receiver Sensitivity (-93dBm in BLE) Low Power (Peak Rx -93dBm @ 13mA, Peak Tx 0dBm @ 10.5mA)
- Ultra low power multiple down modes
- Security sub system
- AES Hardware Encryption Engine (AES Electronic Codebook Mode Encryption, AES CCM Mode Encryption), Accelerated Address Resolver, Random Number Generator
- Expansion headers for connecting Ubi-Sense, Ubi-DAC and External Sensors
- Intelligent power system with rechargeable lithium polymer battery

Beacon Protocols:

- Beacon protocols are standards of BLE communication. Each protocol describes the structure of a data packet beacons broadcast.
- Bluetooth beacons are small and wireless battery-powered radio transmitters that use BLE as their transmission protocol.
- The transmission distance around 10–30 meters for interior spaces and the hardware is highly cost-effective and low maintenance. This is because each Bluetooth beacon consists of only a small microprocessor, a radio, and a battery.
- Bluetooth beacons enable the connection between the physical and digital world by creating a communication bridge between enabled devices and the person carrying them.

Examples of Bluetooth Beacon System

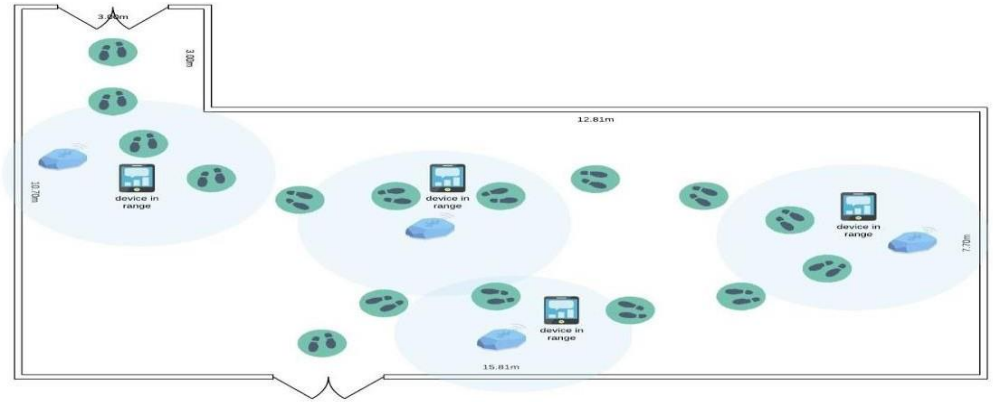


Figure 2.11 Example Bluetooth Beacon

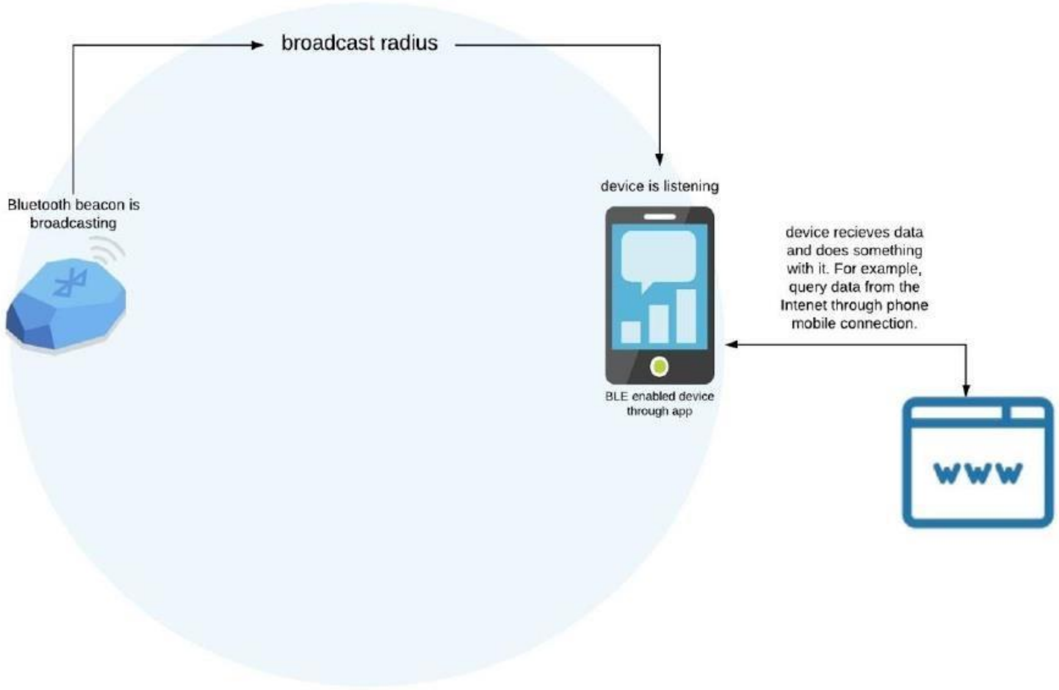

broadcast radius
Bluetooth beacon is broadcasting
device is listening
device recieves data and does something with it. For example, query data from the Intenet through phone mobile connection.
BLE enabled device through app
www

Figure 2.12 Example Beacon system

- Bluetooth beacons work by transmitting packets of data that are picked up by a compatible receiving device via radio waves.
- These packets of data are either self-contained or are triggers to events on the receiving device such as push notifications, app actions, and prompts.
- A Bluetooth beacon has a theoretical maximum radius distance of less than 100m. It can also have up to 6ms latency from a non-connected state.

Advantages and Disadvantages of Bluetooth Beacons:

- One of the major advantages of Bluetooth beacons is that they are cheap and easy to install.
- It is a physical device that can either be fixed or move with objects or people to help track their location. It is essentially a transmitter that you just have to install, and all that's left to do is configure the actions that the beacon is supposed to perform.
- In addition to low cost, the ongoing maintenance required is also minimal due to the long battery life.
- While the beacons don't listen for a response, the receiving device can perform actions based on the beacon's instructions.
- This includes, and is not limited to, things like check-ins on social media, location-based actions, push notifications or sending data via the user's Internet connection.
- A disadvantage of Bluetooth beacons is that they don't work by themselves. A beacon is one part of a system, meaning that the entire setup relies on users carrying a compatible device (in most cases).
- In some systems, the receiver is instead a fixed device installed in a facility, and the beacons are mobile. One example of this is an asset tracking system with a fixed locator device and the beacons are attached to assets for the purpose of tracking their location within a facility.
- Bluetooth beacon triggers can also be limited by the quality of the receiving device's connection to the Internet. Sometimes, a roadblock can be as simple as a user needing to accept consent requirements when automatically logging into Wi-Fi hotspots first.

Estimote supports twelve protocols:

- Estimote Monitoring
- Estimote Connection
- Estimote Location
- Estimote Telemetry
- Nearable
- iBeacon
- Eddystone UID
- Eddystone EID
- Eddystone URL
- Eddystone TLM
- Estimote Monitoring is the default protocol in both Location and Proximity Beacons and it was built as a mix of Estimote Location and iBeacon, taking the best features of both protocols. It offers various improvements in accuracy and beacon detection and is currently the most reliable protocol broadcasted by our beacons.
- Estimote Connection allows to connect to a beacon and change its settings. we cannot turn it off.
- Estimote Location is brand new packet, design specifically to work with our Indoor Location SDK.
- Estimote Telemetry is a packet that broadcasts information from sensors, GPIO, battery state, and firmware version.
- Nearable is to include more sensor data in a single packet.
- Eddystone and iBeacon were developed by Google and Apple respectively. All Estimote Beacons can broadcast these. Estimote Connection, Estimote Location, Estimote Telemetry are protocols that were introduced with Estimote Location Beacons.
- Generic Advertiser is the name we use for packets that we can configure. In practical terms, we can use this protocol to broadcast data with any structure we like. It gives more flexibility than the default packets

Estimate Beacons:
Estimote Beacons are shipped with default settings adjusted for high signal responsiveness and optimal equate power consumption

Bluetooth 5:

- Bluetooth 5.0 is the latest version of the Bluetooth wireless communication standard. It’s commonly used for wireless headphones and other audio hardware, as well as wireless keyboards, mice, and game controllers.
- Bluetooth is also used for communication between various smart home and Internet of Things (IoT) devices.
- With Bluetooth 5.0, devices can use data transfer speeds of up to 2 Mbps, which is double what Bluetooth 4.2 supports.
- Devices can also communicate over distances of up to 800 feet (or 240 meters), which is four times the 200 feet (or 60 meters) allowed by Bluetooth 4.2. However, walls and other obstacles will weaken the signal, as they do with Wi-Fi.

Bluetooth Mesh Protocols

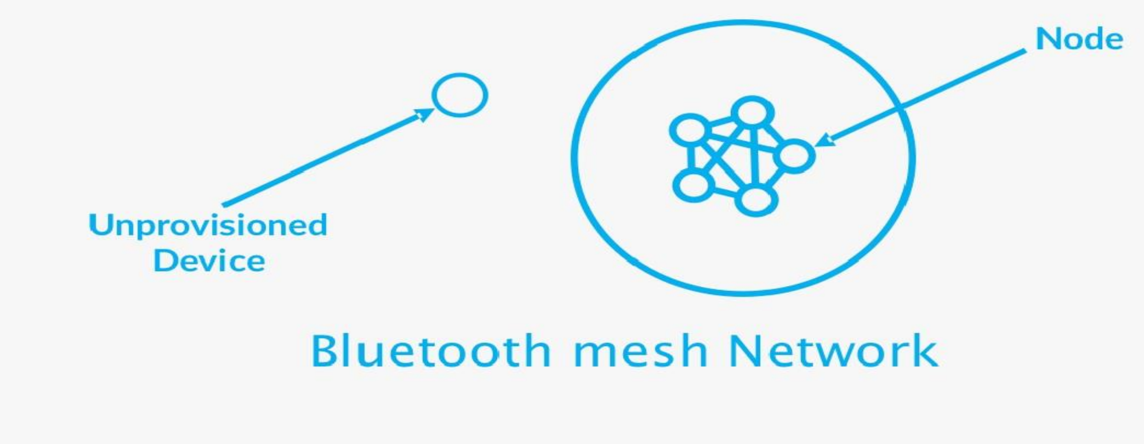


Figure 2.13 Mesh Network

- A node is a device that has joined a Bluetooth mesh network. Devices that are not part of the network are called unprovisioned devices. Once an unprovisioned device gets provisioned, it joins the network and becomes a node.

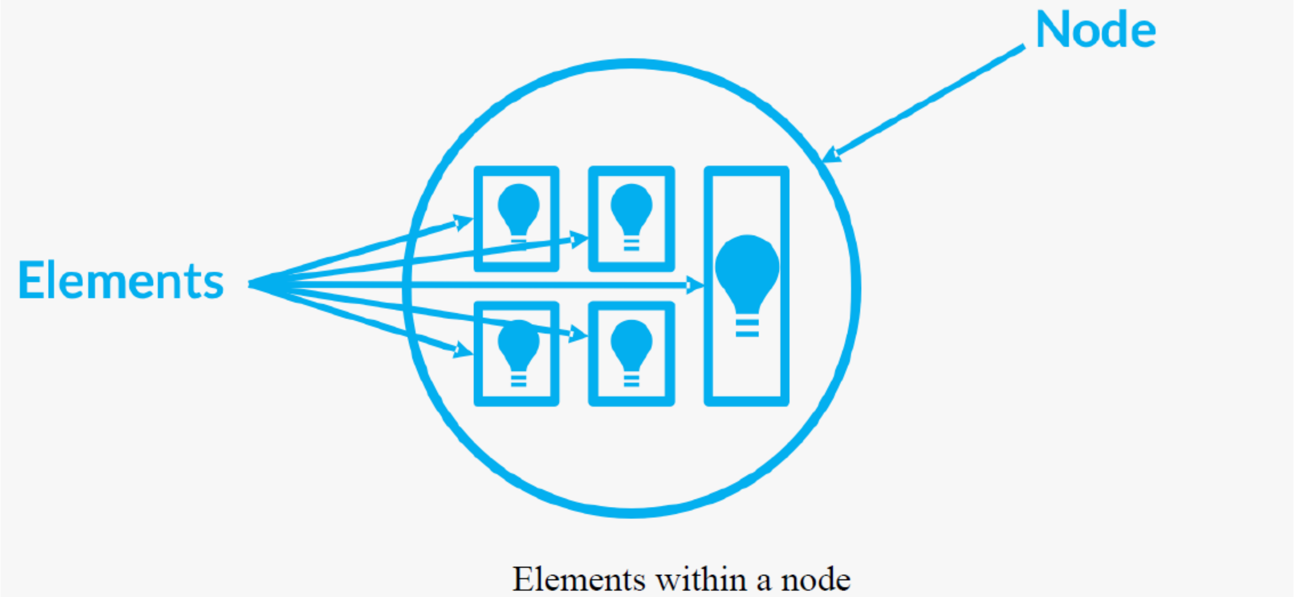


Figure 2.14 Elements

- A node may contain multiple parts which can be controlled independently. For example, a light fixture may contain multiple light bulbs which can be turned on/off independently. These different parts of a single node are referred to as elements.

States

- Elements can be in various conditions, represented by state values. For example, on and off are states of a lightbulb within a light fixture. A change from one state to another is called a state transition. This can be instantaneous, or it can occur over time, after what's called a transition period. When a state change occurs, it is likely to cause a change in the behavior of an element.
- Some states may be bound to each other, meaning that a change in one state triggers a change in the other. There may be two or more states bound to each other. Let's take for example a light dimmer: it will likely have a level state as well as an on/off state. If the level state value changes to zero, it will trigger the on/off state to transition to off. If the level value changes from zero to a non-zero value, then that triggers the on/off state to transition to on.

Properties

- Properties add some context to a state value. For example, defining that a temperature value is an outdoor or indoor temperature.

There are two types of properties:

- Manufacturer property: provides read-only access
- Admin property: provides read-write access

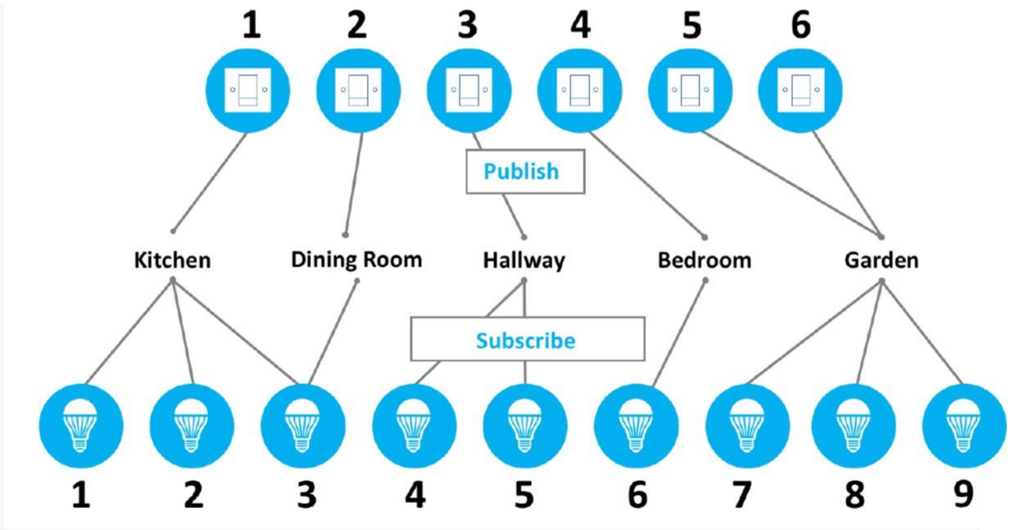
Messages

- In Bluetooth mesh, all communications within the network are message-oriented, and nodes send messages to control or relay information to each other. Messages are the mechanism by which operations on nodes are invoked. If a node needs to report its status, it also sends it via a message. A given message type represents an operation on a state or collection of multiple state values.

- There are three types of messages in Bluetooth mesh, each of which is defined by a unique opcode (operation code):
- A GET message: a message to request the state from one or more nodes.
- A SET message: a message to change the value of a given state.
- A STATUS message: A status message is used in different scenarios: In response to a GET message, containing the state value.
- In response to an acknowledged SET message.
- Sent independently of any message to report the element's status. One example is a message that's triggered by a timer running on the element sending this message.
- Some messages require an acknowledgment message to be sent by the receiver of the original message. An acknowledgment message serves two purposes:
- Confirmation of receipt of the message.
- Return of data related to the message received.
- In the case where a response to the message is not received by the sender, or an unexpected response is received, the sender may resend the message. Multiple acknowledged messages received by a node do not affect the behavior (it's as if the message was received once).
- Addresses
- Messages in a Bluetooth mesh network must be sent to and from an address. There are three types of addresses:
- Unicast Address: an address that uniquely identifies a single node assigned during the provisioning process (which we'll cover in an upcoming post).
- Group Address: an address used to identify a group of nodes. A group address usually reflects a physical grouping of nodes such as all nodes within a specific room.
- A group address could either be: Defined by the Bluetooth SIG, also referred to as a SIG-Fixed Group Address. These include All-proxies, All-friends, All-relays, and All-nodes group addresses.
- Dynamic Group Address, which is defined by the user via a configuration application.
- Virtual Address: an address that may be assigned to one or more elements, spanning one or more nodes. This acts as a label and takes the form of a 128-bit UUID with which any element can be associated. Virtual addresses are likely to be preconfigured at the time of manufacturing.

Publish/Subscribe

- The way messages are exchanged in a Bluetooth mesh network is via the publish-subscribe pattern. From
- In software architecture, publish–subscribe is a messaging pattern where senders of messages, called publishers, do not program the messages to be sent directly to specific receivers, called subscribers, but instead categorize published messages into classes without knowledge of which subscribers, if any, there may be. Similarly, subscriber's express interest in one or more classes and only receive messages that are of interest, without knowledge of which publishers, if any, there are.
- Publishing is the act of sending a message. Subscribing is a configuration used to allow select messages to be sent to specific addresses for processing. Typically, messages are addressed to group or virtual addresses
- Here's an example of a mesh network in a home that's comprised of 6 light switches and 9 light bulbs. The network utilizes the publish-subscribe method to allow nodes to send messages to each other



Publish-subscribe in Bluetooth mesh lighting control system (Source: "Bluetooth Mesh – An Introduction for Developers")

Figure 2.15 Publish - Subscribe

- Nodes may subscribe to multiple addresses. An example of this is light #3 in the above figure, which is subscribed to both the kitchen and the dining room group addresses. Also, multiple nodes may publish to the same address, such as switches #5 and #6 in this example. These two switches control the same group of lights, located in the garden.
  The benefit of using group or virtual addresses is that adding or removing nodes does not require reconfiguration of nodes.

Managed Flooding

- Many mesh networks use routing mechanisms to relay messages across the network. The other extreme is to flood the network with the messages being relayed without consideration of the optimal routes these messages need to take to reach their perspective destinations. Bluetooth mesh uses a technique that's a compromise of both of these techniques. This technique is referred to as **managed flooding**
- Managed flooding relies on broadcasting messages to all nodes within range of the sender node, with a few added optimizations:
- Messages have a TTL assigned TTL stands for time-to-live, which limits the number of hops a message can take across multiple nodes within the mesh network. A value of zero indicates that a message has not been relayed and should not be relayed. This means that a node can send a message to other nodes which are in its direct radio range and indicate that the receiving node(s) should not relay the message. If a message is sent with a TTL ≥ 2, then each time it is relayed, the TTL value gets decremented. A TTL value of **1** means that the message may have been relayed at least once, but that it should not be relayed again.
- Messages are cached Message caching is required by all nodes and requires that messages received that already exist in the cache get immediately discarded.
- Heartbeat messages are sent periodically Heartbeat messages are used to indicate to other nodes that the sender is alive and active within the network.
- Friendship refers to the relationship between two nodes. These two node types are: A low-power node, or LPN, conserves power and is not able to receive mesh messages all the time. This node spends most of its time with the radio turned off.

- A live-powered node called the friend node, which can serve as a proxy for the LPN. The friend node caches messages for the LPN to save power, so that the LPN can stay asleep most of the time and only wake up occasionally. When the LPN wakes up, it polls the friend node to read the cached messages and sends any messages it needs to send to the mesh network.

TEXT / REFERENCES BOOKS

1. Jun Zheng, Abbas Jamalipour,"Wireless Sensor Networks: A Networking Perspective", Wiley India, 1st Edition, 2014.
2. WaltenegusDargie , Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", John Wiley & Sons, 1st Edition, 2010.
3. Edgar H. Callaway, "Wireless Sensor Networks: Architectures and Protocols", CRC Press, 1st Edition, August 2003.
4. Jose A. Gutierrez, Edgar H. Callaway, Raymond Barrett, "IEEE 802.15.4 Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensor Networks", Standards Information Network, 3rd Edition,2011.
5. Kazem Sohraby, Daniel Minoli, TaiebZnati, "Wireless Sensor Networks: Technology, Protocols, and Applications", John Wiley & Sons, 1st Edition, 2007.

PART A

1. Explain how Bluetooth works
2. What are Bluetooth profiles and what are they for?
3. Summarize the functions of GATT
4. Recall the concepts of GAP
5. Classify Bluetooth protocols
6. Report the concept of frame support
7. Generalize the process of bluetooth data transmission

PART B

1. Discuss in details about BLE MOTE
2. Outline the significance of L2CAP and explain its structure
3. Describe the importance of Bluetooth Mesh protocols
4. Illustrate the different states and explian about RFCOMM
5. Summarize the Bluetooth profiles

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – III

WIRELESS SENSOR NETWORKS FOR IOT – SECA5203

UNIT – III STUDY AND DEPLOYMENT OF IEEE 802.15.4 STANDARDS & RPL

Wireless PAN, IEEE 802.15.4 standards, Implementation of ZigBee, Thread etc., Linux support for WPAN, 6, 6LowPAN standard, Ipv6 Routing Protocol for Low-Power (RPL) and Lossy Networks, RPL Border Router, Use cases of MQTT and Rest Services for Cloud Connectivity

PAN network stand for personal area network. In this network all the personal devices are connects to form network. Its range is 10 meters to 33 meters. All devices should be in this range to form network. But devices, node, range make it different form WAN, LAN, MAN network. Some personal devices are laptop computer, mobile phone, cellphone, PDAs, printer etc. It is also called WPAN (wireless personal network). It is always uses to communicate all personal device with each other. But some it is use to connects with higher level network. But they need gateway to connect. A personal area network are wireless or wire interfaces.

Wireless Personal Area Networks (WPANs)

The market for wireless personal area networks is expanding rapidly. As people use more electronic devices at home and in the office, and with the proliferation of peripherals, a clear need for wireless connectivity between these devices has emerged. Examples of the devices that need to be networked are desktop computers, handheld computers, printers, microphones, speakers, pagers, mobile phones, bar code readers, and sensors. Using cables to connect these devices with a PC and with each other can be a difficult task in a stationary location. When you add mobility into the mix, the challenge becomes daunting. If the setup and administration of a WPAN becomes simple and intuitive in the future for the end user, then the most concrete scenario for WPAN technology is cable replacement. This provides a compelling reason to use WPAN technology, and will open the door for more advanced applications in the future.

Here are the main characteristics of a WPAN:

- Short-range communication
- Low power consumption
- Low cost
- Small personal networks
- Communication of devices within a 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. The price point to make a technology attractive is $5 (U.S.) or less. At this level, device manufacturers are willing to incorporate a technology into a broad range of devices for both the consumer and business markets. Interoperability is also imperative. Wireless capabilities are not very useful if they do not allow a device to communicate with other devices and peripherals.

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. Each of these standards is discussed in the following subsections.

WPAN Standards

Many standards are available for personal area networks. Each standard has strengths and weaknesses, making it suitable for specific application scenarios. In some cases, more than one technology will be able to perform a required task, hence nontechnical factors such as cost and availability will factor into the decision as to which technology is more appropriate. Here we take a look at the leading standards in this space. The information provided will give you a solid understanding about where each standard is being used and for what purposes.

IrDA

IrDA, the acronym for Infrared Data Association, is an international organization that creates and promotes interoperable, low-cost infrared data connection standards. IrDA has a set of protocols to support a broad range of appliances, computing, and communication devices. These protocols are typically aimed at providing high-speed, short-range, line-of-sight, and point-to-point wireless data transfer. IrDA protocols use IrDA DATA as the data delivery mechanism, and IrDA CONTROL as the controlling mechanism.

Chances are that you currently own a device that has support for infrared communication. The Infrared Data Association estimates that more than 300 million IrDA enabled devices have been shipped, making it one of the most pervasive wireless technologies in existence. The original goal of IrDA was to provide a cable replacement technology, much like the other PAN standards. The idea was that two computers could communicate simply by pointing them at each other. For example, to print a document, you would simply point the infrared (IR) port at the printer and be able to send the data. No cables would be required. Technically, infrared technology is well suited for such tasks.

The following are some of infrared's features:

- Communication range of up to 1 meter, although a distance of 2 meters can often be reached.
- A low-power option for communication up to 20 centimeters. This requires 10 times less power than the full-power implementation.
- Bidirectional communication.
- Data transmission from 9600 bps to a maximum speed of 4 Mbps.

In theory, using IR for data transfer is a great idea. Unfortunately, even with such ubiquity it is rarely used for its original intent. This may be due to technical challenges in many early implementations, or more plausibly, to the line-of-sight restriction. For IR to work, the communicating devices have to maintain line of sight. This means that they have to situated within the operating range (typically up to 2 meters apart), point at each other, and have no physical impediments. In most office environments, this limitation is not practical for many peripherals such as printers or scanners. Using infrared to transfer data between two devices is more realistic. Two device users can use infrared to transfer information, such as electronic business cards, between one another. Users with Palm devices call this type of transfer *beaming*, as in, "Can you beam me your contact information?" Beyond user-to-user data transfer, infrared is not commonly used for information transfer, since most users do not use two devices with IR ports. While nearly all portable devices have one, the majority of desktops do not. Once again, this limits the effectiveness of IR as a mass-market data transfer protocol. That said, there are some areas where infrared is frequently used. The IrDA CONTROL standard allows wireless peripherals such as keyboards, mice, game pads, joysticks, and pointing units to interact wirelessly with a host device, very often a desktop PC or gaming unit. A host device can communicate with up to eight peripherals simultaneously. The data transmission rate for IrDA CONTROL typically reaches a maximum at 75 Kbps, which is easily fast enough for the type of data being transferred by these types of devices.

One of the major advantages of IrDA from a device manufacturer's perspective is cost. IR ports can be incorporated into a device for as low as $1 (U.S.). This is a very low cost for implementing wireless communication into a device compared to other WPAN standards.

Bluetooth

Bluetooth is a standard for enabling wireless communication between mobile computers, mobile phones, and portable handheld devices. Unlike IR, Bluetooth does not require a line of sight between devices to be effective. It is able to communicate through physical barriers, typically with a range of 10 meters, although with power amplifiers, 100 meters is possible. Bluetooth uses the unlicensed 2.4-GHz spectrum for communication, with a peak throughput of 720 Kbps. It is expected that this throughput will increase to around 10 Mbps with future Bluetooth specifications. The origins of Bluetooth date back to 1994 when Ericsson was researching ways to enable mobile phones to communicate with peripherals. Four years later, in 1998, Ericsson, along with Nokia, Intel, Toshiba, and IBM, formed the Bluetooth Special Interest Group (SIG) to define a specification for small form-factor, low-cost wireless communication. Since then, 3COM, Lucent, Microsoft, and Motorola have joined the Bluetooth SIG as Bluetooth promoters. In addition, well over 2,000 companies have joined the SIG as Bluetooth Adopter/Associate members. This all happened before a single Bluetooth product was commercially available, leading to unprecedented market excitement. People were excited about the futuristic products that would soon be available, expecting that every device, from portable computers to home appliances, would soon incorporate Bluetooth technology. These devices would then interact with one another, transferring data files, contact information, security credentials, and even perform financial transactions. All of this would happen seamlessly without any technical knowledge required from the user. Needless to say, the hype once again surpassed the technology. While Bluetooth will indeed enable those scenarios someday, right now it is most effective as a cable replacement technology. Since a line of sight is not required for communication, getting Bluetooth devices to interact with one another is trivial. Bluetooth provides an auto discovery mode, whereby Bluetooth devices will automatically discover other devices that are within range. Once they are detected, they can start communicating. There is some concern that this will overload the 2.4-GHz spectrum as more Bluetooth devices become available.

To address this issue, the Bluetooth specification defines three device modes:

- **Generally discoverable mode.** This allows a Bluetooth device to be detected by any other Bluetooth device within its proximity.
- **Limited discoverable mode.** Only well-defined devices will be able to detect a device in this mode. This mode will be used when a user has many Bluetooth devices and wants them to discover each other automatically.
- **Nondiscoverable mode.** This makes the device invisible to other devices so it cannot be detected.

When two or more devices connect, they form a piconet, an ad hoc network that can consist of a maximum of eight devices. Every device in a piconet can communicate directly with the other devices. It is also possible to have networks with more than eight devices. In this case, several piconets can be combined together into a scatternet. In a scatternet configuration, not all devices can see each other; only the devices within each piconet are able to communicate. Figure 3.1 helps to illustrate how this works. In this figure there is one scatternet consisting of five piconets; the hands-free mobile phone is a member of three different piconets and is able to communicate directly with the headset, the Bluetooth pen, and the access point, but is not able to communicate directly with the laptops, printer, or fax machine.

The number of Bluetooth devices on the market is growing every day. It is common for mobile phones, PDAs, laptops, and peripherals to come equipped with Bluetooth chips. This has been made possible by the lowered cost of Bluetooth chipsets [currently around $20 (U.S.), with a targeted range of $5 to $10 (U.S.)] in conjunction with increased market demand. Users are now aware of the many compelling features that Bluetooth offers. The leading ones include:

- Cable replacement
- Mobile device networking
- Global ad hoc networking
- Support for both voice and data communication
- Worldwide vendor and product support

Bluetooth Profiles

In order for Bluetooth to realize true ubiquity, interoperability is a key. Bluetooth devices from different vendors have to be able to communicate seamlessly. In order to promote this level of interoperability, the Bluetooth SIG has defined 13 profiles that device manufacturers can use when implementing their products. These profiles help ensure that Bluetooth products are built on a single foundation, allowing for true interoperability.

The entire second volume of the Bluetooth v1.1 specification is dedicated to profile definitions. Each profile is designed for a specific task. Four profiles are foundation profiles, providing the building blocks upon which other profiles are constructed. The other nine profiles are usage profiles. These describe actual usage cases where Bluetooth technology excels. Bluetooth profiles are not meant to be the definitive way to use Bluetooth technology but rather are aimed at providing standards for implementers to build upon. Device manufacturers will base their Bluetooth offerings on these profiles, ensuring that all Bluetooth devices will be able to communicate with one another.

Bluetooth Security

Because cable replacement is one of Bluetooth's primary uses, the overall goal of Bluetooth security is to make the wireless connection at least as secure as cables would be. The Bluetooth specification defines security at the link level. Application-level security is not specified, leaving the developer to choose the security mechanism that is most appropriate for each particular application. The Bluetooth specification defines several security measures that can be employed in various situations. Additionally, each profile definition outlines when security should be implemented for particular usage scenarios. Bluetooth communication can be encrypted for over-the-air communication and has built-in device authentication. The level of encryption is user-defined and can have a key size between 8 and 128 bits. This allows the user to determine what level of security is required. Note that a tradeoff exists between speed and security: Greater key lengths lead to slow communication. For authentication, each Bluetooth device has a unique address so the user can have some faith in the device with which they are communicating.

802.15

802.15 is a specification driven by the Institute of Electrical and Electronics Engineers (IEEE) to develop consensus standards for short-range wireless networks or wireless personal area networks. It has similar goals to Bluetooth in that it looks to address wireless networking of portable and mobile computing devices such as PCs, PDAs, mobile phones, peripherals, and consumer electronics. The 802.15 WPAN Working Group was established in 1999 as part of the Local and Metropolitan Area Networks Standards Committee of the IEEE.

At the time of establishment, the 802.15 WPAN Working Group was aware of the Bluetooth specification and used parts of it as the foundation for the 802.15 standard. The 802.15 WPAN specification is aimed at standardizing the Media Access Control (MAC) and Physical (PHY) layers of Bluetooth, in the attempt to accommodate wider adoption of short-range wireless technology. 802.15 also deals with issues such as coexistence and interoperability within the networks. To accomplish this goal, four task groups have been established, each working on specific components of the 802.15 specification.

They are:

• **802.15 WPAN Task Group 1: WPAN/Bluetooth.** The WPAN Task Group 1 (TG1) has created the WPAN 802.15.1 standard based on the Bluetooth v1.1 specification. To accomplish this, the IEEE licensed technology from the Bluetooth SIG. Specifically, 802.15.1 defines the MAC and PHY specifications for wireless connectivity of devices that are either fixed or portable within the personal computing space. The spec also takes into consideration coexistence requirements with 802.11 wireless local area network (WLAN) devices.

• **802.15 WPAN Task Group 2: Coexistence Mechanisms.** The 802.15 WPAN Task Group 2 (TG2) is developing the recommended practices to facilitate the coexistence of WPAN (802.15) and WLAN (802.11) technologies. Part of this task involves developing a coexistence model to quantify the mutual interference of a WPAN and a WLAN. Once approved, this outcome of TG2's work will become the IEEE 802.15.2 specification.

• **802.15 WPAN Task Group 3: High Rate WPAN.** The 802.15 WPAN Task Group 3 (TG3) is chartered to publish a new standard for high-rate (20 Mbps or higher) WPANs. In addition to high data rates, 802.15.3 also has to provide a means for low-power and low-cost solutions to address the needs of portable consumer electronics, digital imaging, and multimedia applications.

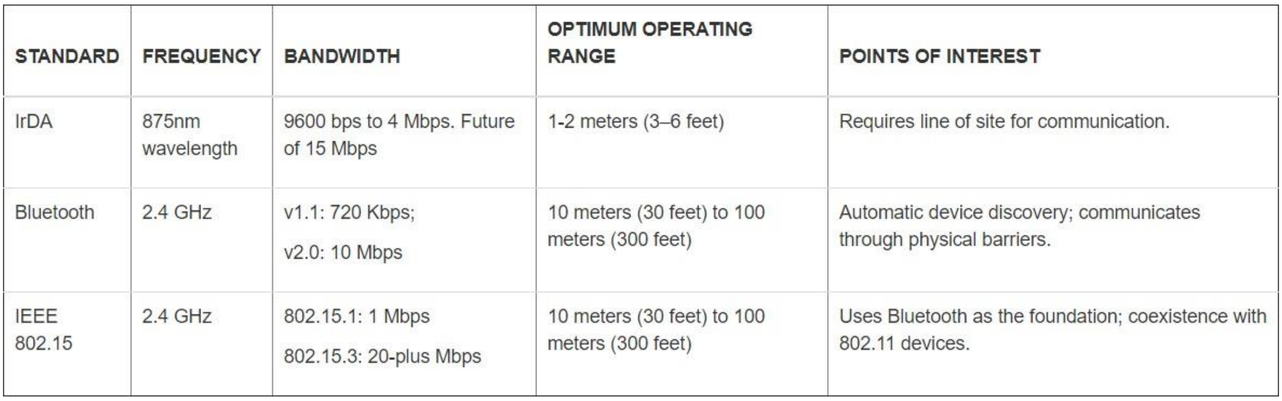
• **802.15 WPAN Task Group 4: Low Rate-Long Battery Life.** The 802.15 WPAN Task Group 4 (TG4) is chartered to establish a low-data-rate (200 Kbps maximum) solution with long battery life (many months to many years) and low complexity. It is intended to operate in an unlicensed international frequency band and is targeted at sensors, interactive toys, smart badges, home automation, and remote controls.

The 802.15 specification is still a work in progress as each of the task groups is at different stages in the specification process. TG1 has completed the 802.15.1 specification and has gotten approval from the IEEE Standards Association (IEEE-SA), while the other groups are still working toward that level. Once completed, the 802.15 WPAN specification will cover all of the current issues surrounding WPAN technology, including Bluetooth compatibility, coexistence with 802.11, high-data transfer rates, and low-power consumption solutions. The combination of all of these will make the IEEE 802.15 specification very attractive for WPAN infrastructure providers.

WPAN Comparison

Of the three WPAN standards, IrDA, Bluetooth, and 802.15, IrDA has been around the longest, and has the highest market penetration, with more than 300 million enabled devices shipped. At the same time, infrared also is the most limiting, as the range is up to 2 meters, and it requires a line of site between communicating devices. The Bluetooth specification addresses these issues by using unlicensed 2.4-GHz spectrum for communication. This allows for communication through physical barriers, as well as larger ranges, typically up to about 10 meters. Bluetooth has also garnered a lot of industry attention, with more than 2,000 companies joining the Bluetooth SIG. In order to provide further standardization for WPAN technology, the IEEE 802.15 specification was developed. The 802.15 specification uses Bluetooth v1.1 as a foundation for providing standardized short-range wireless communication between portable and mobile computing devices. Table 3.2 provides a summary of the leading WPAN technologies.

Table 3.1 Comparison of Wireless PAN Technology



STANDARD	FREQUENCY	BANDWIDTH	OPTIMUM OPERATING RANGE	POINTS OF INTEREST
IrDA	875nm wavelength	9600 bps to 4 Mbps. Future of 15 Mbps	1-2 meters (3–6 feet)	Requires line of site for communication.
Bluetooth	2.4 GHz	v1.1: 720 Kbps; v2.0: 10 Mbps	10 meters (30 feet) to 100 meters (300 feet)	Automatic device discovery; communicates through physical barriers.
IEEE 802.15	2.4 GHz	802.15.1: 1 Mbps 802.15.3: 20-plus Mbps	10 meters (30 feet) to 100 meters (300 feet)	Uses Bluetooth as the foundation; coexistence with 802.11 devices.

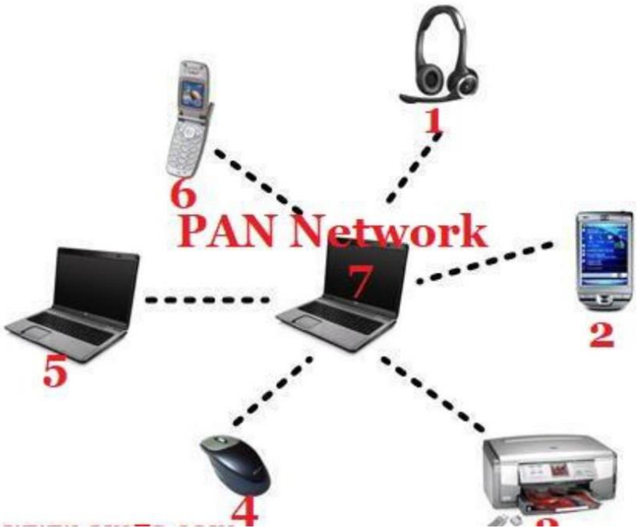


Figure 3.1 Wireless PAN

Bluetooth WPAN:

Bluetooth is uses for short-range radio waves. Uses in a WPAN include, such as pointing devices, keyboards, audio and video head-sets, printers, cell phones and computers. A Bluetooth WPAN is also known as piconet. This is compose of eight (8) active devices and these devices are connects with master slave device. In this network first piconet will be master slave relationship. The range of piconet 33ft or 10 meters, but range can be increase up-to 330 ft or 100ft. Long range Bluetooth routers have large range up-to 1000ft. We can also use this network in mesh network. In this way you can send data from one place to another. There is no need of master slave device in this network.

Infrared Data Association (IrDA):

In Infrared Data Association we use infrared light. Infrared is generally uses in remote controls. Many other devices use IrDA such as printers, keyboards etc. The reach limit of a WPAN varies from centimeters to few meters. IEEE 802.15 has produce standards for PANs operating system.

IEEE 802.15.4 standards

IEEE 802.15.4

IEEE 802.15.4 is a standard that was developed to provide a framework and the lower layers in the OSI model for low cost, low power wireless connectivity networks.

IEEE 802.15.4 provides provides the MAC and PHY layers, leaving the upper layers to be developed for specific higher later standards like Thread, Zigbee, 6LoWPAN and many others. As a result, IEEE 802.15.4 does not take the limelight in the way that other standards might, but nevertheless it forms the basis for a large number of standards and accordingly it its far more widely deployed than may be apparent at first sight. Low power is one of the key elements of 802.15.4 as it is used in many areas where remote sensors need to operate on battery power, possibly for years without attention.

IEEE 802.15.4 basics

The IEEE 802.15.4 standard is aimed at providing the essential lower network layers for a wireless personal area network, WPAN. The chief requirements are low-cost, low-speed ubiquitous communication between devices.

IEEE 802.15.4 does not aim to compete with the more commonly used end user-oriented systems such as IEEE 802.11 where costs are not as critical and higher speeds are demanded and power may not be quite as critical. Instead, IEEE 802.15.4 provides for very low cost communication of nearby devices with little to no underlying infrastructure.

The concept of IEEE 802.15.4 is to provide communications over distances up to about 10 metres and with maximum transfer data rates of 250 kbps. Anticipating that cost reduction will require highly embedded device solutions, the overall concept of IEEE 802.15.4 has been devised to accommodate this.

Table 3.2 IEEE 802.15.4 standard

The IEEE 802.15.4 standard has undergone a number of releases. In addition to this there are a number of variants of the IEEE 802.15.4 standard to cater for different forms of physical layer, etc. These are summarised below in the table.	DETAILS AND COMMENTS
IEEE 802.15.4 VERSION	
IEEE 802.15.4 - 2003	This was the initial release of the IEEE 802.15.4 standard. It provided for two different PHYs - one for the lower frequency bands of 868 and 915 MHz, and the other for 2.4 GHz.
IEEE 802.15.4 - 2006	This 2006 release of the IEEE 802.15.4 standard provided for an increase in the data rate achievable on the lower frequency bands. This release of the standard updated the PHY for 868 and 915 MHz. It also defined four new modulation schemes that could be used - three for the lower frequency bands, and one for 2.4 GHz.

IEEE 802.15.4a	This version of the IEEE 802.15.4 standard defined two new PHYs. One used UWB technology and the other provided for using chirp spread spectrum at 2.4 GHz.
IEEE 802.15.4c	Updates for 2.4 GHz, 868 MHz and 915 MHz, UWB and the China 779-787 MHz band.
IEEE 802.15.4d	2.4 GHz, 868 MHz, 915 MHz and Japanese 950 - 956 MHz band.
IEEE 802.15.4e	This release defines MAC enhancements to IEEE 802.15.4 in support of the ISA SP100.11a application.
IEEE 802.15.4f	This will define new PHYs for UWB, 2.4 GHz band and also 433 MHz
IEEE 802.15.4g	This will define new PHYs for smart neighbourhood networks. These may include applications such as smart grid applications for the energy industry. It may include the 902 - 928 MHz band.

Although new versions of the standard are available for use by any of the higher layer standards, Zigbee still uses the initial 2003 release of the IEEE 802.15.4 standard.

Table 3.3 IEEE 802.15.4 applications

The IEEE 802.15.4 technology is used for a variety of different higher layer standards. In this way the basic physical and MAC layers are already defined, allowing the higher layers to be provided by individual system in use.	DESCRIPTION OF THE IEEE 802.15.4 APPLICATION OR SYSTEM
APPLICATION OR SYSTEM	
Zigbee	Zigbee is supported by the Zigbee Alliance and provides the higher levels required for low powered radio system for control applications including lighting, heating and many other applications.
Wireless HART	Wireless HART is an open-standard wireless networking technology that has been developed by HART Communication Foundation for use in the 2.4 GHz ISM band. The system uses IEEE802.15.4 for the lower layers and provides a time synchronized, self-organizing, and self-healing mesh architecture.
RF4CE	RF4CE, Radio Frequency for Consumer Electronics has amalgamated with the Zigbee alliance and aims to provide low power radio controls for audio visual applications, mainly for domestic applications such as set to boxes,

	televisions and the like. It promises enhanced communication and facilities when compared to existing controls.
MiWi	MiWi and the accompanying MiWi P2P systems are designed by Microchip Technology. They are designed for low data transmission rates and short distance, low cost networks and they are aimed at applications including industrial monitoring and control, home and building automation, remote control and automated meter reading.
ISA100.11a	This standard has been developed by ISA as an open-standard wireless networking technology and is it described as a wireless system for industrial automation including process control and other related applications.
6LoWPAN	This rather unusual name is an acronym for "IPv6 over Low power Wireless Personal Area Networks" It is a system that uses the basic IEEE 802.15.4, but using packet data in the form of Ipv6.

Table 3.4 IEEE 802.15.4 frequencies and frequency bands

The IEEE 802.15.4 frequency bands align with the licence free radio bands that are available around the globe. Of the bands available, the 2.4 GHz (2 400 MHz) band is the most widely used in view of the fact that it is available globally and this brings many economies of scale.

FREQUENCY BAND (MHZ)	**CHANNELS AVAILABLE**	**THROUGHPUT AVAILABLE (KBPS)**	**REGION USE ALLOWABLE**
868 - 868.6	1	20	Europe
902 - 928	10 (2003 rel) 30 (2006 rel)	30	USA
2 400	16	250	Global

IEEE 802.15.4 modulation formats

There were two different modulation schemes defined for IEEE 802.15.4 in the original standard released in 2003. Both these air interface or radio interface configurations are based on direct sequence spread spectrum, DSSS techniques. The one for the lower frequency bands provides a lower data rate in view if the smaller channel width, whereas the format used at 2.4 GHz enables data to be transferred at rates up to 250 kbps.

The 2006 release of the 802.15.4 standard upgraded an number of areas of the air interface and the modulation schemes. There were four different physical layers that were defined. Three used the DSS approach using either binary or offset quadrature phase shift keying, BPSK and OQPSK. An optional physical layer approach was defined using amplitude sift keying, ASK.

IEEE 802.15.4 MAC overview

The purpose of the IEEE 802.15.4 MAC layer is to provide an interface between the PHY or physical layer and the application layer. The as IEEE 802.15.4 does not specify an application layer, this is generally an application system such as Zigbee, RF4CE, MiWi, etc.

The IEEE 802.15.4 MAC provides the interface to the application layer using two elements:

- **MAC Management Service:** This is called the MAC Layer Management Entity, MLME. It provides the service interfaces through which layer management functions may be called or accessed. The IEEE 802.15.4 MAC MLME is also responsible for controlling a database of objects for the MAC layer. This database is referred to as the MAC layer PAN information base or PIB. The MLME also has access to MCPS services for data transport activities.

- **MAC Data Service*:*** This si called the MAC Common Port Layer, MCPS. This entity within the IEEE 802.15.4 MAC provides data transport services between the peer MACs.

IEEE 802.15.4 network topologies

There are two main forms of network topology that can be used within IEEE 802.15.4. These network topologies may be used for different applications and offer different advantages.

The two IEEE 802.15.4 network topologies are:

- **Star topology*:*** As the name implies the start format for an IEEE 802.15.4 network topology has one central node called the PAN coordinator with which all other nodes communicate.
- **Peer to Peer network topology*:*** In this form of network topology, there is still what is termed a PAN coordinator, but communications may also take place between different nodes and not necessarily via the coordinator.

It is worth defining the different types of devices that can exist in a network. There are three types:

- **FFD*:*** Full Function Device - a node that has full levels of functionality. It can be used for sending and receiving data, but it can also route data from other nodes.
- **RFD*:*** Reduced Function Device - a device that has a reduced level of functionality. Typically it is an end node which may be typically a sensor or switch. RFDs can only talk to FFDs as they contain no routing functionality. These devices can be very low power devices because they do not need to route other traffic and they can be put into a sleep mode when they are not in use. These RFDs are often known as child devices as they need other parent devices with which to communicate.
- **Coordinator*:*** This is the node that controls the IEEE 802.15.4 network. This is a special form of FFD. In addition to the normal FFD functions it also sets the IEEE 802.15.4 network up and acts as the coordinator or manager of the network.

These definitions were originally generated for use in Zigbee, but their use has now been introduced with IEEE 802.15.4 network terminology.

IEEE 802.15.4 star topology

In the star topology, all the different nodes are required to talk only to the central PAN coordinator. Even if the nodes are FFDs and are within range of each other, in a star network topology, they are only allowed to communicate with the coordinator node.

Having a star network topology does limit the overall distances that can be covered. It is limited to one hop.

IEEE 802.15.4 peer to peer topology

A peer to peer, or p2p network topology provides a number of advantages over a star network topology. In addition to communication with the network coordinator, devices are also able to communicate with each other. FFDs are able to route data, while the RFDs are only able to provide simple communication. The fact that data can be routed via FFD nodes means that the network coverage can be increased. Not only can overall distances be increased, but nodes masked from the main network coordinator can route their data via another FFD node that it may be able to communicate with.

Implementation of ZigBee T PAGE

ZigBee is the most popular industry wireless mesh networking standard for connecting sensors, instrumentation and control systems. ZigBee, a specification for communication in a wireless personal area network (WPAN), has been called the "Internet of things." Theoretically, your ZigBee-enabled coffee maker can communicate with your ZigBee-enabled toaster. ZigBee is an open, global, packet-based protocol designed to provide an easy-to-use architecture for secure, reliable, low power wireless networks. ZigBee and IEEE 802.15.4 are low data rate wireless networking standards that can eliminate the costly and damage prone wiring in industrial control applications. Flow or process control equipment can be place anywhere and still communicate with the rest of the system. It can also be moved, since the network doesn't care about the physical location of a sensor, pump or valve. The ZigBee RF4CE standard enhances the IEEE 802.15.4 standard by providing a simple networking layer and standard application profiles that can be used to create interoperable multi-vendor consumer electronic solutions. The benefits of this technology go far beyond, ZigBee applications include: Home and office automation Industrial automation Medical monitoring Low-power sensors HVAC control Plus many other control and monitoring uses

Features: – Low power consumption, simply implemented – Users expect batteries to last many months to years – Bluetooth has many different modes and states depending upon your latency and power requirements such as sniff, park, hold, active, etc.; ZigBee/IEEE 802.15.4 has active (transmit/receive) or sleep – Even mains powered equipment needs to be conscious of energy. ZigBee devices will be more ecological than its predecessors saving megawatts at it full deployment. Low cost (device, installation, maintenance) Low cost to the users means low device cost, low installation cost and low maintenance. ZigBee devices allow batteries to last up to years using primary cells (low cost) without any chargers (low cost and easy installation). ZigBee’s simplicity allows for inherent Introduction to Zigbee Technology Page 4 configuration and redundancy of network devices provides low maintenance. High density of nodes per network ZigBee’s use of the IEEE 802.15.4 PHY and MAC allows networks to handle any number of devices. This attribute is critical for massive sensor arrays and control networks. Simple protocol, global implementation ZigBee’s protocol code stack is estimated to be about 1/4th of Bluetooth’s or 802.11’s. Simplicity is essential to cost, interoperability, and maintenance. The IEEE 802.15.4 PHY adopted by ZigBee has been designed for the 868 MHz band in Europe, the 915 MHz band in N America, Australia, etc; and the 2.4 GHz band is now recognized to be a global band accepted in almost all countries.

working of Zigbee

ZigBee basically uses digital radios to allow devices to communicate with one another. A typical ZigBee network consists of several types of devices. A network coordinator is a device that sets up the network, is aware of all the nodes within its network, and manages both the information about each node as well as the information that is being transmitted/received within the network. Every ZigBee network must contain a network coordinator. Other Full Function Devices (FFD's) may be found in the network, and these devices support all of the 802.15.4 functions. They can serve as network coordinators, network routers, or as devices that interact with the physical world. The final device found in these networks is the Reduced Function Device (RFD), which usually only serve as devices that interact with the physical world. As mentioned above several topologies are supported by ZigBee, including star, mesh, and cluster tree. As can be seen in above figure 3, star topology is most useful when several end devices are located close together so that they can communicate with a single router node. That node can then be a part of a larger mesh network that ultimately communicates with the network coordinator. Mesh networking allows for redundancy in node links, so that if one node goes down, devices can find an alternative path to communicate with one another.

Thread

Thread is a secure, wireless mesh networking protocol. The Thread stack is an open standard that is built upon a collection of existing Institute for Electrical and Electronics Engineers (IEEE) and Internet Engineering Task Force (IETF) standards, rather than a whole new standard

Thread General Characteristics

The Thread stack supports IPv6 addresses and provides low-cost bridging to other IP networks and is optimized for low-power / battery-backed operation, and wireless device-to-device communication. The Thread stack is designed specifically for Connected Home and commercial applications where IP-based networking is desired and a variety of application layers can be used on the stack.

These are the general characteristics of the Thread stack:

- Simple network installation, start-up, and operation: The Thread stack supports several network topologies. Installation is simple using a smartphone, tablet, or computer. Product installation codes are used to ensure only authorized devices can join the network. The simple protocols for forming and joining networks allow systems to self-configure and fix routing problems as they occur.
- Secure: Devices do not join the network unless authorized and all communications are encrypted and secure. Security is provided at the network layer and can be at the application layer. All Thread networks are encrypted using a smartphone-era authentication scheme and Advanced Encryption Standard (AES) encryption. The security used in Thread networks is stronger than other wireless standards the Thread Group has evaluated.
- Small and large home networks: Home networks vary from several to hundreds of devices. The networking layer is designed to optimize the network operation based on the expected use.
- Large commercial networks: For larger commercial installations, a single Thread network is not sufficient to cover all the application, system and network requirements. The Thread Domain model allows scalability up to 10,000s of Thread devices in a single deployment, using a combination of different connectivity technologies (Thread, Ethernet, Wi-fi, and so on).
- Range: Typical devices provide sufficient range to cover a normal home. Readily available designs with power amplifiers extend the range substantially. A distributed spread spectrum is used at the Physical Layer (PHY) to be more immune to interference. For commercial installations, the Thread Domain model allows multiple Thread networks to communicate with each other over a backbone, thus extending the range to cover many mesh subnets.
- No single point of failure: The Thread stack is designed to provide secure and reliable operations even with the failure or loss of individual devices.
- Low power: Devices efficiently communicate to deliver an enhanced user experience with years of expected life under normal battery conditions. Devices can typically operate for several years on AA type batteries using suitable duty cycles.
- Cost-effective: Compatible chipsets and software stacks from multiple vendors are priced for mass deployment, and designed from the ground up to have extremely low-power consumption

Linux support for WPAN

Platforms already running Linux would benefit from native 802.15.4 and 6LoWPAN subsystems

● 802.15.4 transceivers can easily be added to existing hardware designs

● Battery powered sensors on the other hand are more likely to run an OS like RIOT or Contiki
● Example 1: Google OnHub AP which already comes with, de-activated, 802.15.4 hardware
● Example 2: Ci40 Creator board as home IoT hub

6LoWPAN

In the Internet a packet passes through many different interconnected networks on its way from source to destination. Thus, considering the link layer technology of each traversed network, there is need of an ``IP-over-X" specification (i.e., of an adaptation layer) to define how to transport IP packets. Following this need, in the process of shaping the IoT world, the IETF IPv6 over Low power WPAN (6LoWPAN) working group [6LoWPAN WG] started in 2007 to work on specifications for transmitting IPv6 over IEEE 802.15.4 networks [IEEE802.15.4]. Typically, Low power WPANs are characterized by: small packet sizes, support for addresses with different lengths, low bandwidth, star and mesh topologies, battery supplied devices, low cost, large number of devices, unknown node positions, high unreliability, and long idle periods during when communications interfaces are turned off to save energy. Given the aforementioned features, it is clear that the adoption of IPv6 on top of a Low power WPAN is not straightforward, but poses strong requirements for the optimization of this adaptation layer. For instance, due to the IPv6 default minimum MTU size (i.e., 1280 bytes), a no-fragmented IPv6 packet would be too large to fit in an IEEE 802.15.4 frame. Moreover, the overhead due to the 40 bytes long IPv6 header would waste the scarce bandwidth available at the PHY layer. For these reasons, the 6LoWPAN working group has devoted huge efforts for defining an effective adaptation layer in [rfc4944,6lowpanhc]. Further issues encompass the auto-configuration of IPv6 addresses [rfc2464], the compliance with the recommendation on supporting link-layer subnet broadcast in shared networks [rfc3819], the reduction of routing and management overhead, the adoption of lightweight application protocols (or novel data encoding techniques), and the support for security mechanisms (i.e., confidentiality and integrity protection, device bootstrapping, key establishment and management).

Protocol data units may be as small as 81 bytes, far below IP and above
• In all cases, reuse existing protocols before creating new ones
• Address mismatch between MTU sizes of LoWPAN's and IPv6
• Support stateless auto configuration of IPv6 addressing
• Specify header compression (use of existing and/or new techniques eg. header reconstruction, header short circuiting, etc)
• Define security mechanisms, security configuration and bootstrapping
• Specify network management
• Specify routing suitable for LoWPAN networks, topology
• Specify methods to enable and disable IPv6 over LoWPAN.
• Specify hooks within routing layer to enable in network processing
• Specify light weight discovery mechanisms
• Specify any changes needed for L3 + layers
• Specify implementation considerations and BKM's of an IPv6 stack

Ipv6 Routing Protocol for Low-Power (RPL) and Lossy Networks
Low-Power and Lossy Networks (LLNs) are a class of network in which both the routers and their interconnect are constrained. LLN routers typically operate with constraints on processing power, memory, and energy (battery power). Their interconnects are characterized by high loss rates, low data rates, and instability. LLNs are comprised of anything from a few dozen to thousands of routers. Supported traffic flows include point-to-point (between devices inside the LLN), point-to-multipoint (from a central control point to a subset of devices inside the LLN), and multipoint-to-point (from

devices inside the LLN towards a central control point). This document specifies the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), which provides a mechanism whereby multipoint-to-point traffic from devices inside the LLN towards a central control point as well as point-to-multipoint traffic from the central control point to the devices inside the LLN are supported. Support for point-to-point traffic is also available. Low-power and Lossy Networks (LLNs) consist largely of constrained nodes (with limited processing power, memory, and sometimes energy when they are battery operated or energy scavenging). These routers are interconnected by lossy links, typically supporting only low data rates, that are usually unstable with relatively low packet delivery rates. Another characteristic of such networks is that the traffic patterns are not simply point-to-point, but in many cases point-to- multipoint or multipoint-to-point. Furthermore, such networks may potentially comprise up to thousands of nodes. These characteristics offer unique challenges to a routing solution: the IETF ROLL working group has defined application-specific routing requirements for a Low-power and Lossy Network (LLN) routing protocol

RPL Border Router:

The RPL border router sample application for Zephyr provides a HTTP(S) server and net shell for management purposes. Typically border router would be used to connect to IEEE 802.15.4 network but Bluetooth IPSP network functionality is also possible.

The source code for this sample application can be found at: samples/net/rpl_border_router

Requirements

- Real device like Freedom Board (FRDM-K64F) with MCR20A IEEE 802.15.4 support.
- Linux machine with web browser and the screen terminal emulator (optional).
- Ethernet access for management purposes (optional).

Note that there is no support for running an RPL border router in QEMU, as the border router requires access to a real radio network technology such as IEEE 802.15.4, which is not available in QEMU. For testing purpose you can compile the RPL border router for QEMU and do some testing with the web UI. But with QEMU, it is not possible to connect to RPL network and get information about the RPL nodes.

Use cases of MQTT and Rest Services for Cloud Connectivity:

MQTT is one of the most commonly used protocols in IoT. It stands for Message Queuing Telemetry Transport. In addition, it is designed as a lightweight messaging protocol that uses publish/subscribe operations to exchange data between clients and the server. Furthermore, its small size, low power usage, minimized data packets and ease of implementation make the protocol ideal of the “machine-to-machine” or “Internet of Things” world.

Need for MQTT

MQTT has unique features you can hardly find in other protocols, like:

- It’s a lightweight protocol. So, it’s easy to implement in software and fast in data transmission.
- It’s based on a messaging technique. Of course, you know how fast your messenger/WhatsApp message delivery is. Likewise, the MQTT protocol.
- Minimized data packets. Hence, low network usage.
- Low power usage. As a result, it saves the connected device’s battery.
- It’s real time! That’s is specifically what makes it perfect for IoT applications.

Like any other internet protocol, MQTT is based on clients and a server. Likewise, the server is the guy who is responsible for handling the client’s requests of receiving or sending data between each other.

Working of MQTT

MQTT server is called a broker and the clients are simply the connected devices. So:

- When a device (a client) wants to send data to the broker, we call this operation a “publish”.
- When a device (a client) wants to receive data from the broker, we call this operation a “subscribe”.

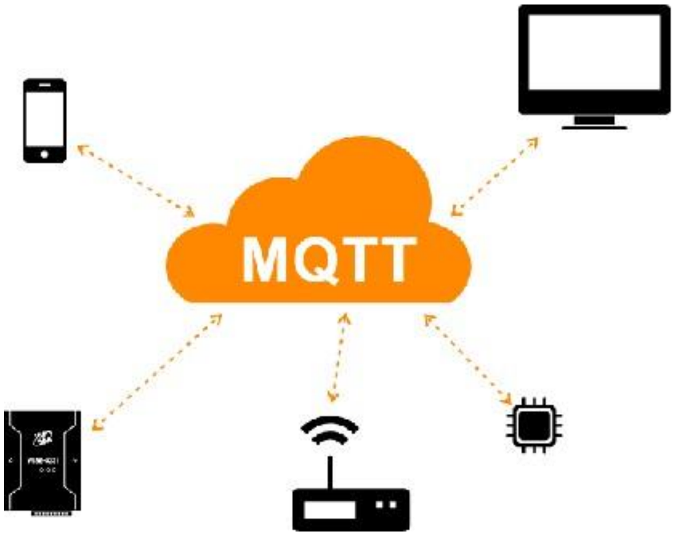


Figure 3.2 MQTT

MQTT Components:

That takes us to the MQTT components, which are 5 as follows:

- Broker, which is the server that handles the data transmission between the clients.
- A topic, which is the place a device want to put or retrieve a message to/from.
- The message, which is the data that a device receives “when subscribing” from a topic or send “when publishing” to a topic.
- Publish, is the process a device does to send its message to the broker.
- Subscribe, where a device does to retrieve a message from the broker.

Cloud MQTT broker
Cloud MQTT is one of the best and easiest cloud-based Mosquitto broker.
Cloud MQTT has a free plan that allows to set up your own CloudMQTT broker instance that will run on their hardware servers. It also has a well designed GUI to monitor the publishing and subscribing processes and topics through an easy to use WebSocket UI.

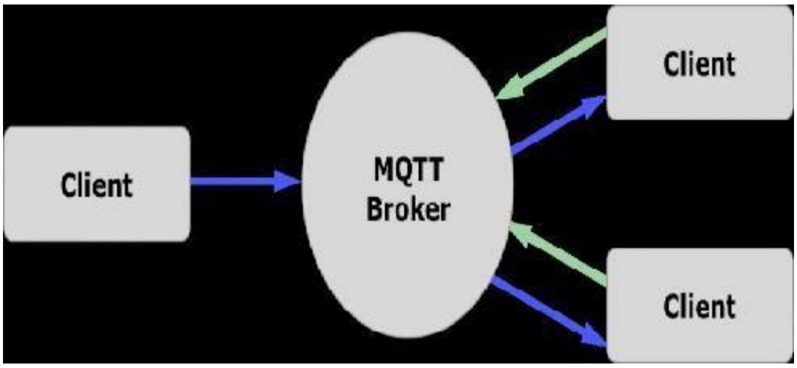


Figure 3.3 MQTT Broker

TEXT / REFERENCES BOOKS

1. Jun Zheng, Abbas Jamalipour,"Wireless Sensor Networks: A Networking Perspective", Wiley India, 1st Edition, 2014.
2. WaltenegusDargie , Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", John Wiley & Sons, 1st Edition, 2010.
3. Edgar H. Callaway, "Wireless Sensor Networks: Architectures and Protocols", CRC Press, 1st Edition, August 2003.
4. Jose A. Gutierrez, Edgar H. Callaway, Raymond Barrett, "IEEE 802.15.4 Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensor Networks", Standards Information Network, 3rd Edition,2011.
5. Kazem Sohraby, Daniel Minoli, TaiebZnati, "Wireless Sensor Networks: Technology, Protocols, and Applications", John Wiley & Sons, 1st Edition, 2007.

PART A

1. Sketch the difference between Zigbee and Thread
2. Elaborate the working of Wireless PAN
3. Summarize and report the various merits of IPv6 over IPV4
4. Interpret the network protocol of MQTT
5. Sketch the concept behind Rest Services for Cloud Connectivity
6. List the importance of RPL Border Router

PART B

1. Illustrate the different transition strategies from IPV4 to IPV6
2. Describe the mapping of multicast address between IPV4 and IPV6 with a neat labelled diagram
3. Illustrate the Linux support for WPAN
4. Implement the sturcure details of IEEE 802.15.4 standards
5. Discuss in detail about Zigbee structure

SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – IV

WIRELESS SENSOR NETWORKS FOR IOT – SECA5203

UNIT – IV CELLULAR TECHNOLOGIES

Introduction to Cellular Technologies, Frequency Reuse Concepts Global System for Mobile Communications (GSM), General Radio Packet Radio Services (GPRS), Code Division Multiple Access (CDMA), 3G/UMTS, 4G/LTE, Introduction to 5G and its challenges

Introduction to Cellular Technologies:

Cellular Network is formed of some cells, cell covers a geographical region, has a base station analogous to 802.11 AP which helps mobile users attach to network and there is an air-interface of physical and link layer protocol between mobile and base station. All these base stations are connected to Mobile Switching Center which connects cells to wide area net, manages call setup and handles mobility.

First Generation Cellular Systems

The United States, Japan, and parts of Europe led the development of the first generation of cellular wireless systems. The first generation systems were characterized by their analog modulation schemes and were designed primarily for delivering voice services. They were different from their predecessor mobile communications systems in that they used the cellular concept and provided automatic switching and handover of on-going calls. Japan’s Nippon Telephone and Telegraph Company (NTT) implemented the world’s first commercial cellular system in 1979. Nordic Mobile Telephone (NMT-400) system, deployed in Europe in 1981, was the first system that supported automatic handover and international roaming. NMT-400 was deployed in Denmark, Finland, Sweden, Norway, Austria, and Spain. Most NMT-400 subscribers used car phones that transmitted up to 15 watts of power. The more successful first generation systems were AMPS in the United States and its variant Total Access Communication Systems (ETACS and NTACS) in Europe and Japan. These systems were almost identical from a radio standpoint, with the major difference being the channel bandwidth. The AMPS system was built on a 30kHz channel size, whereas ETACS and NTACS used 25kHz and 12.5kHz, respectively.

Advanced Mobile Phone Service (AMPS)

AMPS was developed by AT&T Bell Labs in the late 1970s and was first deployed commercially in 1983 in Chicago and its nearby suburbs. The first system used large cell areas and omni-directional base station antennas. The system covered 2,100 square miles with only ten base stations, each with antenna tower height between 150 ft. and 550 ft. Most of the early systems were designed for a carrier-to-interference ratio (CIR) of 18dB for satisfactory voice quality, and were deployed in a 7-cell frequency reuse pattern with 3 sectors per cell. Besides the United States, AMPS was deployed in several countries in South America, Asia, and North America. In the United States, the FCC assigned spectrum to two operators per market—one an incumbent telecommunications carrier and the other a new non-incumbent operator. Each operator was assigned 20MHz of spectrum, supporting a total of 416 AMPS channels in each market. Of the 416 channels, 21 channels were designated for control information and the remaining 395 channels carried voice traffic. AMPS systems used Frequency Modulation (FM) for the transmission of analog voice and Frequency Shift Keying (FSK) for the control channel. Even after the deployment of second generation (2G) systems, AMPS continued to be used by operators in North America as a common fallback service available throughout the geography, as well as in the context of providing roaming between different operator networks that had deployed incompatible 2G systems.

2G Cellular Systems

Improvements in processing abilities of hardware platforms over time enabled the development of 2G wireless systems. 2G systems were also aimed primarily toward the voice market but, unlike the first generation systems, used digital modulation. Shifting from analog to digital enabled several improvements in systems performance. System capacity was improved through (1) the use of spectrally efficient digital speech codecs, (2) multiplexing several users on the same frequency channel via time division or code division multiplexing techniques, and (3) tighter frequency re-use enabled by better error performance of digital modulation, coding, and equalization techniques, which reduced the required carrier-to-interference ratio from 18dB to just a few dB. Voice quality was also improved through the use of good speech codecs and robust link level signal processing. 2G systems also used simple encryption to provide a measure of security against eavesdropping and fraud, which were a source of major concern with first generation analog systems. Examples of 2G digital cellular systems include the Global System for Mobile Communications (GSM), IS-95 CDMA, and IS-136 TDMA systems. GSM is by far the most widely deployed of these systems; IS-95 is deployed in North America and parts of Asia; IS-54 (later enhanced to IS-136) was initially deployed in North America but was later discontinued and replaced mostly by GSM. IS-136 was a TDMA-based system that was designed as a digital evolution of AMPS using 30kHz channels. The Personal Handyphone System (PHS) deployed in China, Japan, Taiwan, and some other Asian countries is also often considered a 2G system. PHS is a cordless telephone system like the Digital Enhanced Cordless Telephone (DECT) system but with capability to handover from one cell to another, and operated in the 1880–1930MHz frequency band. In addition to SMS, 2G systems also supported low data rate wireless data applications. Original 2G systems supported circuit switched data services (similar in concept to dial-up modems), and later evolved to support packet data services as well. Early wireless data services included information services such as the delivery of news, stock quotes, weather, and directions, etc. Limitations in data rate and available space for display in handheld devices meant that specialized technologies, such as the Wireless Access Protocol (WAP), had to be developed to tailor and deliver Internet content to handheld devices.

Frequency Reuse

Frequency Reuse is the scheme in which allocation and reuse of channels throughout a coverage region is done. Each cellular base station is allocated a group of radio channels or Frequencies sub-bands to be used within a small geographic area known as a cell. The shape of the cell is Hexagonal. The process of selecting and allocating the frequency sub-bands for all of the cellular base station within a system is called Frequency reuse or Frequency Planning.

Silent Features of using Frequency Reuse:

- Frequency reuse improve the spectral efficiency and signal Quality (QoS).
- Frequency reuse classical scheme proposed for GSM systems offers a protection against interference.
- The number of times a frequency can be reused is depend on the tolerance capacity of the radio channel from the nearby transmitter that is using the same frequencies.
- In Frequency Reuse scheme, total bandwidth is divided into different sub-bands that are used by cells.
- Frequency reuse scheme allow WiMax system operators to reuse the same frequencies at different cell sites

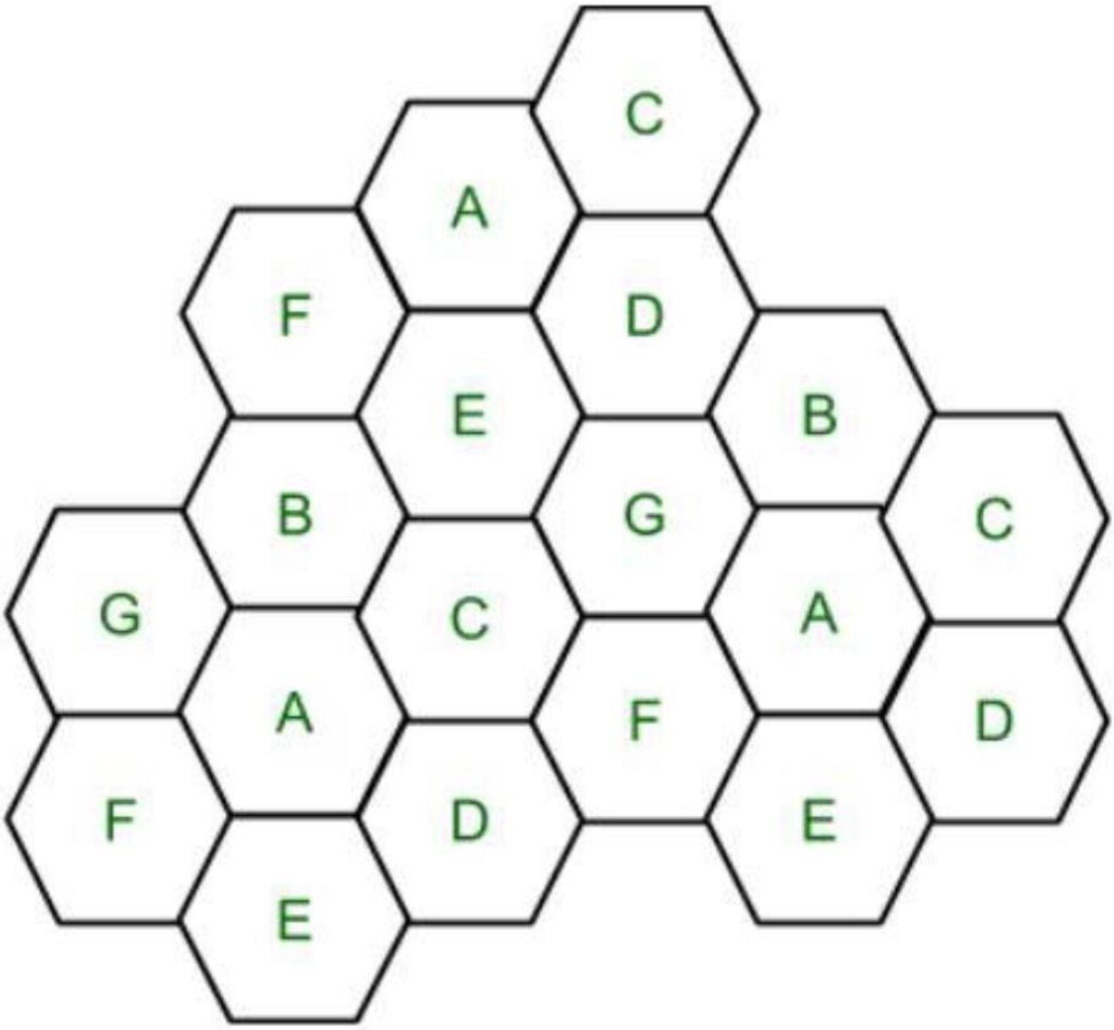


Figure 4.1 Frequency Reuse

Cell with same letter use the same set of channels group or frequencies sub-band.
To find the total number of channel allocated to a cell:
S=Total Number of Duplex Channels available to use
k=Channels allocated to each cell (k<S)
N = Total number of cells or Cluster Size
Then Total number of channels (S) will be,
S = kN
Frequency Reuse Factor = 1/N
In the above diagram cluster size is 7 (A,B,C,D,E,F,G) thus frequency reuse factor is 1/7.
N is the number of cells which collectively use the complete set of available frequencies is called a Cluster. If a Cluster is replicated or repeated 'M' times within the cellular system, then Capacity, C, will be,
C = MkN = MS
In Frequency reuse there are several cells that use the same set of frequencies. These cells are called Co-Channel Cells. These Co-Channel cells results in interference. So to avoid the Interference cells that use the same set of channels or frequencies are separated from one another by a larger distances.

Condition to avoid Co-Channel Interference:
Neighboring cells won't have the same edge or same set of frequency.

GSM: GSM stands for Global System for Mobile communication. Today, GSM is used by more than 800 million end users spread across 190 countries which represents around 70 percent of today's digital wireless market. So, let's see how it works.

In GSM, geographical area is divided into hexagonal cells whose side depends upon power of transmitter and load on transmitter (number of end user). At the center of cell, there is a base station consisting of a transceiver (combination of transmitter and receiver) and an antenna.

GSM Architecture:

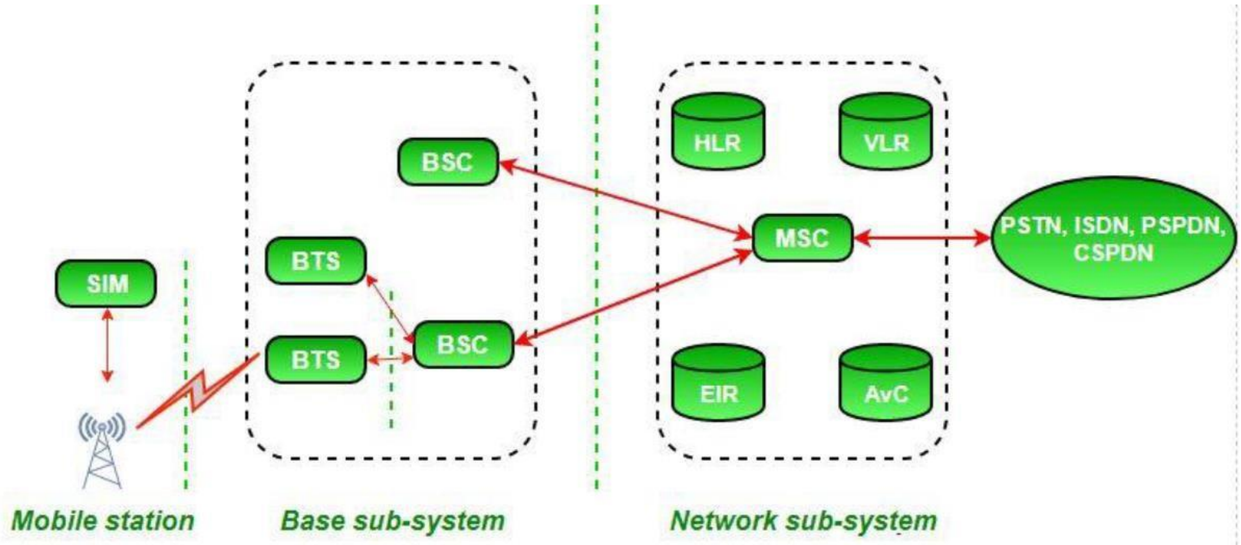


Figure 4.2 GSM Architecture

Function of Components:

1. Mobile station (MS): It refers for mobile station. Simply, it means a mobile phone.
2. Base transreceiver system (BTS): It maintains the radio component with MS.
3. Base station controller (BSC): Its function is to allocate necessary time slots between the BTS and MSC.
4. Home location register (HLR): It is the reference database for subscriber parameter like subscriber's ID, location, authentication key etc.
5. Visitor location register (VLR): It contains copy of most of the data stored in HLR which is temporary and exist only until subscriber is active.
6. Equipment identity register (EIR): It is a database which contains a list of valid mobile equipment on the network.
7. Authentication center (AuC): It perform authentication of subscriber.

Working: GSM is combination of TDMA (Time Division Multiple Access), FDMA (Frequency Division Multiple Access) and Frequency hopping. Initially, GSM use two frequency bands of 25 MHz width : 890 to 915 MHz frequency band for up-link and 935 to 960 MHz frequency for down-link. Later on, two 75 MHz band were added. 1710 to 1785 MHz for up-link and 1805 to 1880 MHz for down-link. up-link is the link from ground station to a satellite and down-link is the link from a satellite down to one or more ground stations or receivers. GSM divides the 25 MHz band into 124 channels each having 200 KHz width and remaining 200 KHz is left unused as a guard band to avoid interference.

Control channels : These are main control channels in GSM :
1. BCH (Broadcast Channel) : It is for down-link only. It has following types – 1. BCCH (Broadcast Control Channel) : It broadcasts information about the serving cell.
2. SCH (Synchronization channel) : Carries information like frame number and BSIC (Base Station Identity Code) for frame synchronization.
3. FCCH (Frequency Correction Channel) : Enable MS to synchronize to frequency.

2. CCCH (Common Control Channel) : It has following types – 1. RACH (Random Access Channel): Used by MS when making its first access to network. It is for up-link only.
2. AGCH (Access Grant Channel) : Used for acknowledgement of the access attempt sent on RACH. It is for down-link only.
3. PCH (Paging Channel) : Network page the MS, if there is an incoming call or a short message. It is for down-link only.

3. DCCH (Dedicated Control Channel) : It is for both up-link and down-link. It has following types – 1. SDCCH (Stand-alone Dedicated Control Channel) : It is used for call setup, authentication, ciphering location update and SMS.
2. SACCH (Slow Associated Control Channel) : Used to transfer signal while MS have ongoing conversation on topic or while SDCCH is being used.
3. FACCH (Fast Associated Control Channel) : It is used to send fast message like hand over message.

GPRS:

GPRS is an expansion Global System for Mobile Communication. It is basically a packet-oriented mobile data standard on the 2G and 3G cellular communication network's global system for mobile communication. GPRS was built up by European Telecommunications Standards Institute (ETSI) because of the prior CDPD, and I-mode packet switched cell advances.

GPRS overrides the wired associations, as this framework has streamlined access to the packet information's network like the web. The packet radio standard is utilized by GPRS to transport client information packets in a structured route between GSM versatile stations and external packet information networks. These packets can be straightforwardly directed to the packet changed systems from the GPRS portable stations.

History of GPRS

GPRS was one of the main advances that empowered a cell system to interface with Internet Protocol systems, accomplishing across the board reception in the mid-2000s. The capacity to peruse the web from a telephone whenever through "dependably on" data networking, while underestimated in a great part of the world today, was as yet an oddity when it was introduced. Indeed, even now, GPRS keeps on being utilized in parts of the world where it has been too expensive even to consider upgrading cell organize framework to move up to newer alternatives.

According to a study on the history of GPRS development Bernhard Walke and his student, Peter Decker, are the inventors of GPRS – the first system providing universal mobile Internet access.

Goals Of GPRS:
1. Consistent IP services
2. Leverage industry investment in IP
3. Open Architecture
4. Service innovation independent of infrastructure

Services Offered:
1. SMS messaging and broadcasting

2. Push-to-talk over cellular
3. Instant messaging and presence
4. Multimedia messaging service
5. Point-to-Point and Point-to-Multipoint services

Protocols supported:
1. Internet Protocol (IP)
2. Point-To-Point Protocol (PPP)

Benefits Of GPRS:

- Mobility: The capacity to keep up consistent voice and information interchanges while moving.
- Cost Efficient: Communication via GPRS is cheaper than through the regular GSM network.
- Immediacy: Allows customers to obtain connectivity when needed, regardless of location and without a lengthy login session.
- Localization: Enables customers to acquire data applicable to their present area.
- EasyBilling: GPRS packet transmission offers an easier to use billing than that offered by circuit switched administrations.

GPRS is an innovation that numerous GPS beacons are using to get up to the minute data with tracking. When the GPS gadget records the information, it would then be able to be transmitted through GPRS to another central location, for example, a PC or through an email. It is the GPRS innovation that takes into consideration ongoing updates to GPS following frameworks. It is this direct GPRS association that gives the client of the GPS system the most reliable information available today.

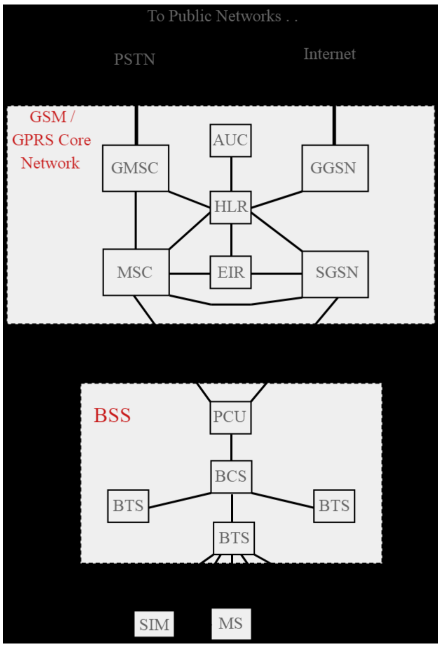


Figure 4.3 GPRS

The main new network architecture entities that were needed are:

- SGSN, Serving GPRS Support Node: The SGSN forms a gateway to the services within the network.
- GGSN Gateway GPRS Support Node: The GGSN, forms the gateway to the outside world.

• PCU, Packet Control Unit: The PCU detects whether data is to be routed to the packet switched or circuit switched networks.

From the diagram given above it can be seen that the GPRS network architecture added some extra elements to the GSM network to enable it to carry the packet data. The PCU added to the base station network routed the data according to whether it was packet or circuit switched.

SGSN

The SGSN or Serving GPRS Support Node element of the GPRS network provides a number of takes focussed on the IP elements of the overall system. It provides a variety of services to the mobiles:

- Packet routing and transfer
- Mobility management
- Attach/detach
- Logical link management
- Authentication
- Charging data

There is a location register within the SGSN and this stores location information (e.g., current cell, current VLR). It also stores the user profiles (e.g., IMSI, packet addresses used) for all the GPRS users registered with the particular SGSN.

GGSN

The GGSN, Gateway GPRS Support Node is one of the most important entities within the GPRS network architecture.

The GGSN organises the interworking between the GPRS network and external packet switched networks to which the mobiles may be connected. These may include both Internet and X.25 networks.

The GGSN can be considered to be a combination of a gateway, router and firewall as it hides the internal network to the outside. In operation, when the GGSN receives data addressed to a specific user, it checks if the user is active, then forwarding the data. In the opposite direction, packet data from the mobile is routed to the right destination network by the GGSN.

PCU

The PCU or Packet Control Unit is a hardware router that is added to the BSC. It differentiates data destined for the standard GSM network (circuit switched data) and data destined for the GPRS network (Packet Switched Data). The PCU itself may be a separate physical entity, or more often these days it is incorporated into the base station controller, BSC, thereby saving additional hardware costs.

GPRS network upgrading

One of the key elements for any network operator is the cost of capital expenditure (capex) to buy and establish a network. Capex costs are normally very high for a new network, and operators endeavour to avoid this and use any existing networks they may have to make the optimum use of any capital. In addition to the capex, there are the operational costs, (opex). These costs are for general maintenance and other operational costs that may be incurred. Increasing efficiency and reliability will reduce the opex costs. Any upgrade such as that from GSM to GPRS will require new investment and operators are keen to keep this to the minimum. The upgrades for the GPRS network are not as large as starting from scratch and rolling out a new network. The GPRS network adds to the existing GSM network. The main new entities required within the network are the SGSN and GGSN, and these are required as the starting point. The base station subsystems require some updates. The main one is the addition of the PCU described above. Some modifications may be required to the BTS, but often only a software upgrade is required, and this may often be achieved remotely. In this way costs are kept to a minimum. The GPRS network architecture can be viewed as an evolution of the GSM network carrying both circuit switched and packet data. The GPRS network architecture was also used as the basis for the 3G UMTS network. In this way network operators could evolve their networks through GPRS and possibly EDGE to the full 3G networks without having to replace and install more new equipment than was absolutely necessary.

CDMA

CDMA (Code-Division Multiple Access) refers to any of several protocols used in second-generation (2G) and third-generation (3G) wireless communications. As the term implies, CDMA is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth. The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHz bands.CDMA employs analog-to-digital conversion (ADC) in combination with spread spectrum technology. Audio input is first digitized into binary elements. The frequency of the transmitted signal is then made to vary according to a defined pattern (code), so it can be intercepted only by a receiver whose frequency response is programmed with the same code, so it follows exactly along with the transmitter frequency. There are trillions of possible frequency-sequencing codes, which enhances privacy and makes cloning difficult. The CDMA channel is nominally 1.23 MHz wide. CDMA networks use a scheme called soft handoff, which minimizes signal breakup as a handset passes from one cell to another. The combination of digital and spread-spectrum modes supports several times as many signals per unit bandwidth as analog modes. CDMA is compatible with other cellular technologies; this allows for nationwide roaming. The original CDMA standard, also known as CDMA One, offers a transmission speed of only up to 14.4 Kbps in its single channel form and up to 115 Kbps in an eight-channel form. CDMA2000 and Wideband CDMA deliver data many times faster. The CDMA2000 family of standards includes 1xRTT, EV-DO Rev 0, EV-DO Rev A and EV-DO Rev B (renamed Ultra Mobile Broadband -- UMB). People often confuse CDMA2000 (a family of standards supported by Verizon and Sprint) with CDMA (the physical layer multiplexing scheme).

CDMA

Code Division Multiple Access is entirely a different approach from the Time Division Multiple Access. CDMA, after digitizing the data, spreads out the date over the entire available bandwidth. Multiple calls are overlapped to each other on a channel which is assigned with a unique sequence code. CDMA is a form of spread-spectrum technique, which means data can be sent in small pieces over a number of frequencies available to use at any time in the specified range.

CDMA Working

All the users' data can be transmitted in a similar way to that of wide band chunk of spectrum. Users Signals are spread over the entire bandwidth by a unique spreading code. At the receiver end, the same code is used to recover the signal. CDMA system requires accurate time stamp on each piece of a signal. Eight and ten separate calls are carried out in the same channel space as one analog call.

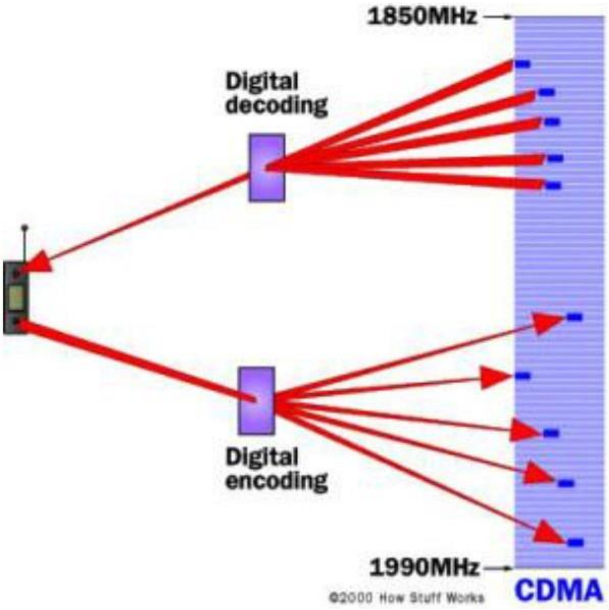


Figure 4.4 CDMA

Code division multiple access technique is an example of multiple access where several transmitters use a single channel to send information simultaneously. Its features are as follows. In CDMA every user uses the full available spectrum instead of getting allotted by separate frequency. CDMA is much recommended for voice and data communications. While multiple codes occupy the same channel in CDMA, the users having same code can communicate with each other. CDMA offers more air-space capacity than TDMA. The hands-off between base stations is very well handled by CDMA.

Features:
Use of wide bandwidth: CDMA, like other spread spectrum technologies uses a wider bandwidth than would otherwise be needed for the transmission of the data. This results in a number of advantages including an increased immunity to interference or jamming, and multiple user access.
Spreading codes used: In order to achieve the increased bandwidth, the data is spread by use of a code which is independent of the data.
Level of security: In order to receive the data, the receiver must have a knowledge of the spreading code, without this it is not possible to decipher the transmitted data, and this gives a measure of security.
Multiple access: The use of the spreading codes which are independent for each user along with synchronous reception allow multiple users to access the same channel simultaneously.

Advantages

Improvement in handover / handoff: Using CDMA it is possible for a terminal to communicate with two base stations at once. As a result, the old link only needs to be broken when the new one is firmly established. This provides significant improvements in terms of the reliability of handover / handoff from one base station to another.

Improvement in capacity: One of the chief claims for CDMA is that it gave significant improvements in network capacity. Original expectations for some of the proponents of CDMA technology were for some very significant improvements, although in reality these were somewhat exaggerated over what real world experience found: 18 fold increase in capacity when compared to AMPS (1G technology used in USA) 6 fold increase in capacity when compared to US TDMA (2G technology used in USA) - similar increases were also claimed over GSM.

3G/UMTS

Edge technique faced an drawback in packet transferring which leads to lower the efficiency in the system. So to overcome it and to standardize a single global network protocol instead of different other techniques 3G was made. International mobile Telecommunications-2000(IMT) known as 3G uses wide band wireless network which made to increase the clarity of signal. A technique called Packet Switching is used to send the Data. Along with Voice Communication services 3G provides data services to Television, video & services like Global roaming works up to range of 2100MHZ with a band width of 15020MHZ. It provides a high speed internet services, video chatting, GPS & Car navigation Digital catalog shopping, Video streaming much faster. Mainly 3G used as a wide band voice channel in which the whole world is taken as village and it creates connections from one person to another no matter where the location of each other is.

Issues of 3G:- Equivalent to 3G the expense of information to utilize 3G is progressively this is because of high band width transmission of 3G advancements; power utilization expanded a considerable measure which prompts decrease the battery life really quick

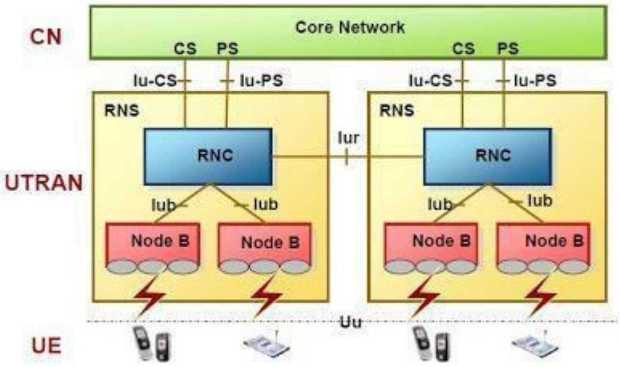


Figure 4.5 Core network

WCDMA or 3G including the RAN (Radio Access Network) and the CN (Core Network). The RAN is used to process all the radio-related functions, while the CN is used to process all voice calls and data connections within the UMTS system, and implements the function of external network switching and routing.

Logically, the CN is divided into the CS (Circuit Switched) Domain and the PS (Packet Switched) Domain. UTRAN, CN and UE (User Equipment) together constitute the whole UMTS system

interface is used between RNC and CN while the Iub interface is adopted between RNC and Node B. Within UTRAN, RNCs connect with one another through the Iur interface.
The Iur interface can connect RNCs via the direct physical connections among them or connect them through the transport network. RNC is used to allocate and control the radio resources of the connected or related Node B. However, Node B serves to convert the data flows between the Iub interface and the Uu interface, and at the same time, it also participates in part of radio resource management.

4G/LTE

- This is the most recent redesign of innovation in versatile correspondence field it is 10times quicker than 3G.
- 4G depends on an innovation called LTE(Long-Term Evolution) a complete IP based innovation for data transmission. Teliasonera which is the first telecom operation in the world to launch 4G which happened in 2009 on December 14, 2009 in the capital of Sweden and Norway.
- LTE which was created later to upgrade 3G network. LTE uses the OFDM modulation technique which provides the spectral efficiency to achieve high data rates but with an addition of multiple share a common channel. The concept of OFDM is to divide the channel in to many narrow subcarriers spacing is an orthogonal which helps to reduce interfere with each other despite the lack of guard bands between them.
- OFDM uses frequency and time to spread the data all across providing high speed & good signal reliability.

Requirement of 4G

- At first after the development of 4G it was only used for military applications and for scientific communication. But later the need of wireless communication for a common person in terms of speed and data rates increased this lead to the implementation of 4g to all other wireless communication devices.
- As the internet revolutionized the world the net of internet on mobile became a main challenge in wireless communication.
- The development of technology from 1G to 2G improved qualities of voice communication and 2g to 3G was upgraded by the need to allow voice and data communication through the wireless device.
- Where 4G implementation had lead to a high quality of voice communication and high data transmission in other needs.

Technology of 4G

- The Technology used in the 4G network is Long Term Evolution (LTE) Standard is mainly based on the GSM/EDGE and UMTS/HSPA, Multiple In Multiple Input Multiple Output (MIMO), Orthogonal Frequency Digital Multiplexing (OFDM).
- This mainly runs on the technique of time division MIMO (Multiple Input Multiple Output) Introduction:- In the year 1988 Bell Laboratories were the first in world to demonstrate the MIMO system under the laboratory conditions.

In the very next year 1999 Gigabit wireless Inc. and Stanford University collaborating and developed a new technique of using MIMO and demonstrated the transmission technique of MIMO they brought up. In MIMO basically at the transmitting and receiving end multiple antennas are used it is an antenna technology application. Diversity:- It is often refer to transmitting and receiving diversity.

- The antennas at the end of each communications circuit are combined together to minimize errors and optimize data speed.
- It is of two types

1) spatial multiplexing
2) spatial diversity

• Spatial Multiplexing:- This form of MIMO help to produce additional Data Capacity by using different paths to carry additional traffic which lead to increase of data throughout the capability

Spatial Diversity:- It is often refer to transmitting and receiving diversity
LTE(Long Term Evolution)
• It is a 4G wireless broadband technology developed by the Third Generation Partnership project (3GPP) .
• LTE provides the highest data rates ever in communication with 100Mbps download stream and 50-30Mbps of upstream.
• LTE is mainly based on the TCP/IP model based. It deals with every type of data voice, video, and messaging traffic.
• LTE uses the MIMO-OFDM technology for the transmission and receiving of data.

Introduction to 5G and its challenges
• It is still quite in its early stages and the the technology likely to appear in the market only by 2020 at the earliest.

• Goals for future 5G include significantly faster speeds (a minimum of 1 Gbps and perhaps up to 10 Gbps) plus lower power requirements to better support huge numbers of new Internet of Things (IoT) devices

• It will have capabilities to provide faster dialing speeds, multiple device connectivity, higher data speeds just to name a few.

• Key technologies to look out for: Millimeter Wave Mobile Communications, Massive MIMO

5G Wireless Technology is the 5th generation of mobile networks and an evolution from the current 4G LTE networks. It is specially designed to fulfill the demands of current technological trends, which includes a large growth in data and almost global connectivity along with the increasing interest in the Internet of Things. In its initial stages, 5G Technology will work in conjugation with the existing 4G Technology and then move on as a fully independent entity in subsequent releases. 5G Wireless Technology is now the latest cellular technology that will greatly increase the speed of wireless networks among other things. So the data speed for wireless broadband connections using 5G would be at a maximum of around 20 Gbps. Contrasting that with the peak speed of 4G which is 60 Mbps, that’s a lot! Moreover, 5G will also provide more bandwidth and advanced antenna technology which will result in much more data transmitted over wireless systems. There are basically 2 main components in the 5G Wireless Technology systems i.e. the Radio Access Network and the Core Network

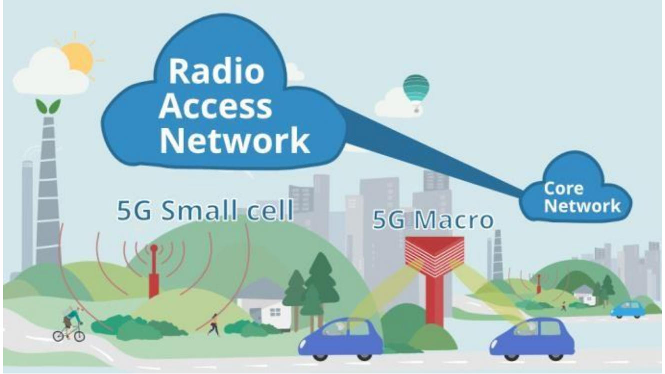


Figure 4.6 5G Network

1. Radio Access Network: The Radio Access Network mainly includes 5G Small Cells and Macro Cells that form the crux of 5G Wireless Technology as well as the systems that connect the mobile devices to the Core Network. The 5G Small Cells are located in big clusters because the millimeter wave spectrum (that 5G uses for insanely high speeds!) can only travel over short distances. These Small Cells complement the Macro Cells that are used to provide more wide-area coverage. Macro Cells use MIMO (Multiple Inputs, Multiple Outputs) antennas which have multiple connections to send and receive large amounts of data simultaneously. This means that more users can connect to the network simultaneously.
2. Core Network: The Core Network manages all the data and internet connections for the 5G Wireless Technology. And a big advantage of the 5G Core Network is that it can integrate with the internet much more efficiently and it also provides additional services like *cloud-based services*, *distributed servers* that improve response times, etc. Another advanced feature of the Core Network is *network slicing*

Benefits of 5G Wireless Technology

5G Wireless Technology will not only enhance current mobile broadband services, but it will also expand the world of mobile networks to include many new devices and services in multiple industries from retail to education to entertainment with much higher performances and lower costs. It could even be said that 5G Technology as much as the emergence of automobiles or electricity ever did!!! Some of the benefits of 5G in various domains are given here:
• 5G will make our smartphones much smarter with faster and more uniform data rates, lower latency and cost-per-bit and this, in turn, will lead to the common acceptance of new immersive technologies like Virtual Reality or Augmented Reality.
• 5G will have the convenience of ultra-reliable, low latency links that will empower industries to invest in more projects which require remote control of critical infrastructure in various fields like medicine, aviation, etc.
• 5G will lead to an Internet of Things revolution as it has the ability to scale up or down in features like data rates, power, and mobility which is perfect for an application like connecting multiple embedded sensors in almost all devices

TEXT / REFERENCES BOOKS

1. Jun Zheng, Abbas Jamalipour,"Wireless Sensor Networks: A Networking Perspective", Wiley India, 1st Edition, 2014.
2. WaltenegusDargie , Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", John Wiley & Sons, 1st Edition, 2010.
3. Edgar H. Callaway, "Wireless Sensor Networks: Architectures and Protocols", CRC Press, 1st Edition, August 2003.
4. Jose A. Gutierrez, Edgar H. Callaway, Raymond Barrett, "IEEE 802.15.4 Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensor Networks", Standards Information Network, 3rd Edition,2011.
5. Kazem Sohraby, Daniel Minoli, TaiebZnati, "Wireless Sensor Networks: Technology, Protocols, and Applications", John Wiley & Sons, 1st Edition, 2007.

PART A

1. Describe Channel Allocation Strategies
2. Write short notes on frequency reuse.
3. Sketch the Base station controller of GSM
4. Illustrate the generation of GSM

5. Interpret the concept behind the services of GSM
6. Recall the term GPRS support nodes

PART B

1. Diffrenciate the structure and working of 3G/UMTS and 4G/LTE
2. Implement the concept behind CDMA with its categories and explain their working with advantage and disadvantage
3. Demonstrate the procedure for 4G/LTE
4. List out the challenges behind 5G and explain
5. Summarize the importance of GPRS and explain its working
6. Explain the architecture of GSM

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF ELECTRICAL AND ELECTRONICS

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

UNIT – V

WIRELESS SENSOR NETWORKS FOR IOT – SECA5203

UNIT V - OVERVIEW OF RECENT IoT WIRELESS TECHNOLOGIES

Introduction to Short range communication, RFID, IrDA, NFC, GPS, Sigfox, NB-IoT, LoRA-WAN Protocol- Terminology, Classes of LoRA Devices, Frequency Bands, Addressing Schemes, Message/Frame Formats, Use Case and Examples, Introduction to Firmware over the Air (FOTA)

Short Range Communication

A number of different wireless technologies have been developed for very short distances. These are referred to as 'short-range wireless communication.' Signals travel from a few centimeters to several meters.

In contrast, signals in medium-range wireless communication travel up to 100 meters or so, while signals in wide-area wireless communication can travel from several kilometers to several thousand kilometers. Examples of short-range wireless communications are Bluetooth, infrared, near field communication, ultraband and Zigbee.

RFID

In recent years, radio frequency identification technology has moved from obscurity into mainstream applications that help speed the handling of manufactured goods and materials. RFID enables identification from a distance, and unlike earlier bar-code technology (see the sidebar), it does so without requiring a line of sight. 1 RFID tags (see figure 1) support a larger set of unique IDs than bar codes and can incorporate additional data such as manufacturer, product type, and even measure environmental factors such as temperature. Furthermore, RFID systems can discern many different tags located in the same general area without human assistance. In contrast, consider a supermarket checkout counter, where you must orient each bar-coded item toward a reader before scanning it.

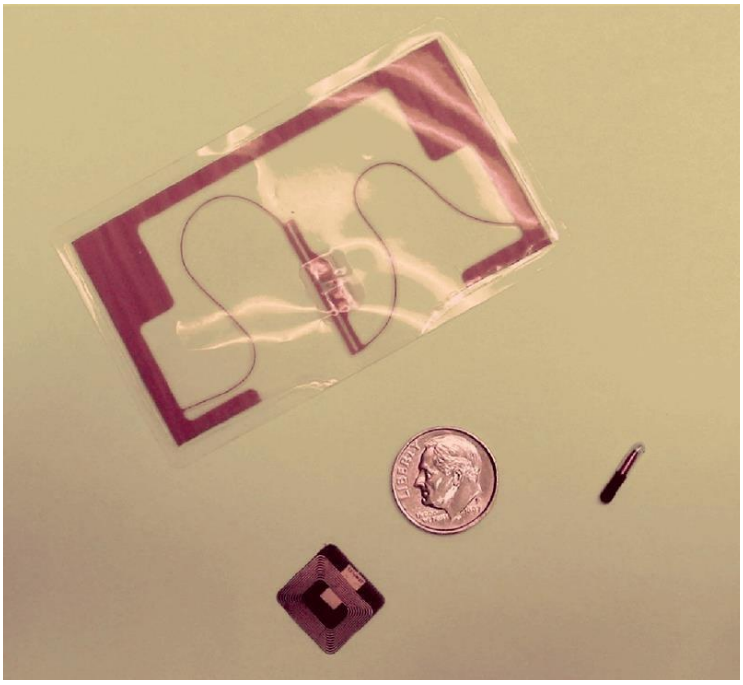


Figure 5.1Three different RFID tags—they come in all shapes and sizes

RFID principles

Many types of RFID exist, but at the highest level, we can divide RFID devices into two classes: *active* and *passive*. Active tags require a power source—they're either connected to a powered infrastructure or use energy stored in an integrated battery. In the latter case, a tag's lifetime is limited by the stored energy, balanced against the number of read operations the device must undergo. One example of an active tag is the transponder attached to an aircraft that identifies its national origin. Another example is a LoJack device attached to a car, which incorporates cellular technology and a GPS to locate the car if stolen.

However, batteries make the cost, size, and lifetime of active tags impractical for the retail trade. Passive RFID is of interest because the tags don't require batteries or maintenance. The tags also have an indefinite operational life and are small enough to fit into a practical adhesive label. A passive tag consists of three parts: an antenna, a semiconductor chip attached to the antenna, and some form of encapsulation.

The tag reader is responsible for powering and communicating with a tag. The tag antenna captures energy and transfers the tag's ID (the tag's chip coordinates this process). The encapsulation maintains the tag's integrity and protects the antenna and chip from environmental conditions or reagents. The encapsulation could be a small glass vial or a laminar plastic substrate with adhesive on one side to enable easy attachment to goods

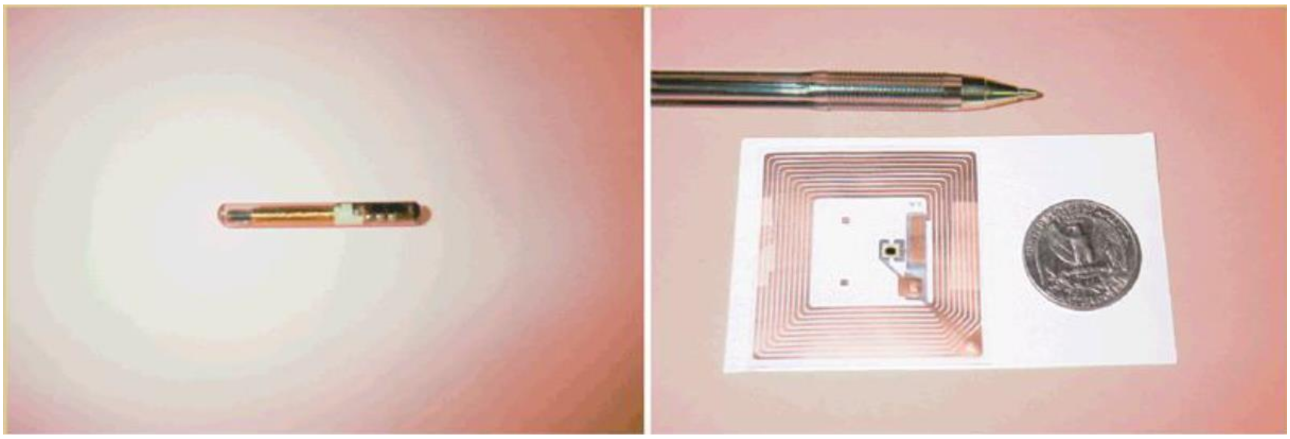


Figure 5.2 RFID Tags

RFID tags based on near-field coupling: (a) a 128 kHz Trovan tag, encapsulated in a small glass vial that's approximately 1 cm long and (b) a 13.56 MHz Tiris tag, which has a laminar plastic substrate (approximately 5 × 5 cm) with adhesive for easy attachment to goods. Two fundamentally different RFID design approaches exist for transferring power from the reader to the tag: magnetic induction and electromagnetic (EM) wave capture. These two designs take advantage of the EM properties associated with an RF antenna—the near field and the far field. Both can transfer enough power to a remote tag to sustain its operation—typically between 10 μW and 1 mW, depending on the tag type. (For comparison, the nominal power an Intel XScale processor consumes is approximately 500 mW, and an Intel Pentium 4 consumes up to 50 W.) Through various modulation techniques, near- and far-field-based signals can also transmit and receive data.

Near-field RFID

Faraday's principle of magnetic induction is the basis of near-field coupling between a reader and tag. A reader passes a large alternating current through a reading coil, resulting in an alternating magnetic field in its locality. If you place a tag that incorporates a smaller coil in this field, an alternating voltage will appear across it. If this voltage is rectified and coupled to a capacitor, a reservoir of charge accumulates, which you can then use to power the tag chip.

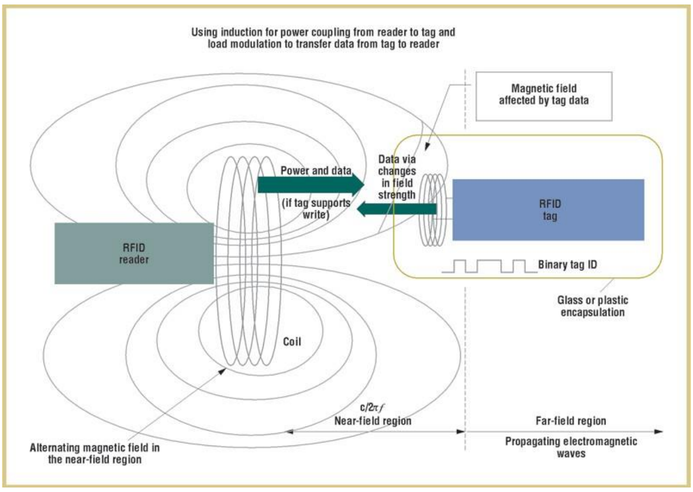

Using induction for power coupling from reader to tag and load modulation to transfer data from tag to reader
Magnetic field affected by tag data
Power and data
(if tag supports write)
Data via changes in field strength
RFID tag
RFID reader
Binary tag ID
Glass or plastic encapsulation
Coil
c/2π f
Near-field region
Far-field region
Propagating electromagnetic waves
Alternating magnetic field in the near-field region

Figure 5.3 Near-field power/communication mechanism for RFID tags operating at less than 100 MHz.

Tags that use near-field coupling send data back to the reader using load modulation. Because any current drawn from the tag coil will give rise to its own small magnetic field—which will oppose the reader's field—the reader coil can detect this as a small increase in current flowing through it. This current is proportional to the load applied to the tag's coil (hence load modulation).

This is the same principle used in power transformers found in most homes today—although usually a transformer's primary and secondary coil are wound closely together to ensure efficient power transfer. However, as the magnetic field extends beyond the primary coil, a secondary coil can still acquire some of the energy at a distance, similar to a reader and a tag. Thus, if the tag's electronics applies a load to its own antenna coil and varies it over time, a signal can be encoded as tiny variations in the magnetic field strength representing the tag's ID. The reader can then recover this signal by monitoring the change in current through the reader coil. A variety of modulation encodings are possible depending on the number of ID bits required, the data transfer rate, and additional redundancy bits placed in the code to remove errors resulting from noise in the communication channel.

Near-field coupling is the most straightforward approach for implementing a passive RFID system. This is why it was the first approach taken and has resulted in many subsequent standards, such as ISO 15693 and 14443, and a variety of proprietary solutions. However, near-field communication has some physical limitations.

The range for which we can use magnetic induction approximates to c/2π *f*, where c is a constant (the speed of light) and *f* is the frequency. Thus, as the frequency of operation increases, the distance over which near-field coupling can operate decreases. A further limitation is the energy available for induction as a function of distance from the reader coil. The magnetic field drops off at a factor of 1/ *r*3, where *r* is the separation of the tag and reader, along a center line perpendicular to the coil's plane. So, as applications require more ID bits as well as discrimination between multiple tags in the same locality for a fixed read time, each tag requires a higher data rate and thus a higher operating frequency. These design pressures have led to new passive RFID designs based on far-field communication.

Far-field RFID

RFID tags based on far-field emissions (see figure 4) capture EM waves propagating from a dipole antenna attached to the reader. A smaller dipole antenna in the tag receives this energy as an alternating potential difference that appears across the arms of the dipole. A diode can rectify this potential and link it to a capacitor, which will result in an accumulation of energy in order to power its electronics. However, unlike the inductive designs, the tags are beyond the range of the reader's near field, and information can't be transmitted back to the reader using load modulation.

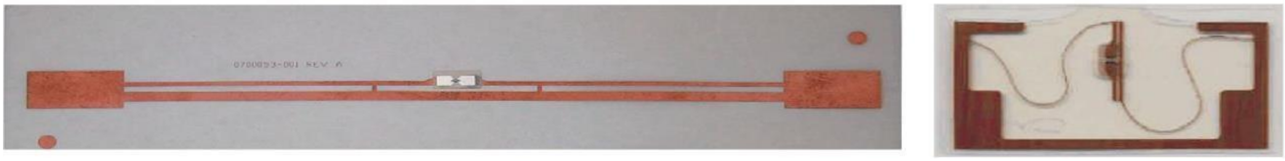


Figure 5.4 RFID tags based on far-field coupling: (a) a 900-MHz Alien tag (16 × 1 cm) and (b) a 2.45-GHz Alien tag (8 × 5 cm).

The technique designers use for commercial far-field RFID tags is back scattering (see figure 5). If they design an antenna with precise dimensions, it can be tuned to a particular frequency and absorb most of the energy that reaches it at that frequency. However, if an impedance mismatch occurs at this frequency, the antenna will reflect back some of the energy (as tiny waves) toward the reader, which can then detect the energy using a sensitive radio receiver. By changing the antenna's impedance over time, the tag can reflect back more or less of the incoming signal in a pattern that encodes the tag's ID.

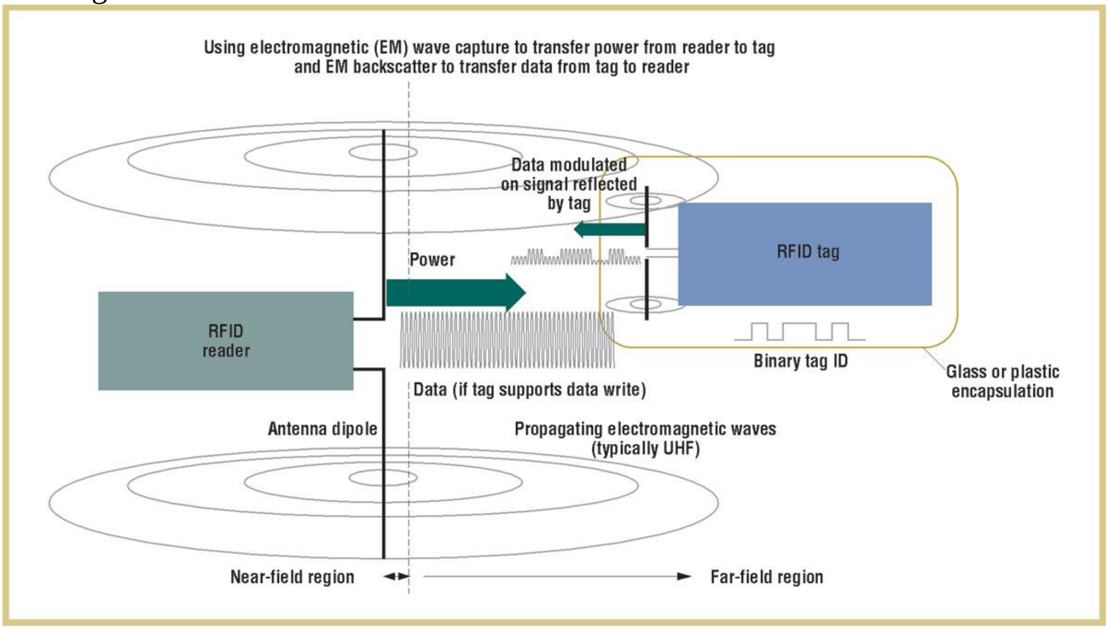

Using electromagnetic (EM) wave capture to transfer power from reader to tag and EM backscatter to transfer data from tag to reader
Data modulated on signal reflected by tag
Power
RFID tag
RFID reader
Binary tag ID
Glass or plastic encapsulation
Data (if tag supports data write)
Antenna dipole
Propagating electromagnetic waves (typically UHF)
Near-field region
Far-field region

Figure 5.5 Far-field power/communication mechanism for RFID tags operating at greater than 100 MHz.

In practice, we can detune a tag's antenna for this purpose by placing a transistor across its dipole and then turning it partially on and off. As a rough design guide, tags that use far-field principles operate at greater than 100 MHz typically in the ultra high-frequency (UHF) band (such as 2.45 GHz); below this frequency is the domain of RFID based on near-field coupling. A far-field system's range is limited by the amount of energy that reaches the tag from the reader and by how sensitive the reader's radio receiver is to the reflected signal. The actual return signal is very small, because it's the result of two attenuations, each based on an inverse square law—the first attenuation occurs as EM waves radiate from the reader to the tag, and the second when reflected waves travel back from the tag to the reader. Thus the returning energy is 1/ *r*4 (again, *r* is the separation of the tag and reader). Fortunately, thanks to Moore's law and the shrinking feature size of semiconductor manufacturing, the energy required to power a tag at a given frequency continues to decrease (currently as low as a few microwatts). So, with modern semiconductors, we can design tags that can be read at increasingly greater distances than were possible a few years ago. Furthermore, inexpensive radio receivers have been developed with improved sensitivity so they can now detect signals, for a reasonable cost, with power levels on the order of –100 dBm in the 2.4-GHz band. A typical far-field reader can successfully interrogate tags 3 m away, and some RFID companies claim their products have read ranges of up to 6 m.

EPC global's work was key to promoting the design of UHF tags (which has been the basis of RFID trials at both Wal-Mart and Tesco (see the sidebar for more information about the trials). EPC global was originally the MIT Auto-ID Center, a nonprofit organization set up by the MIT Media Lab. The center later divided into Auto-ID labs, still part of MIT, and EPC global, a commercial company. This company has defined an extensible range of tag standards, but its Class-1 Generation-1 96-bit tag is the one receiving the most attention of late. This tag can label over 50 quadrillion (50 × 10 15) items, making it possible to uniquely label every manufactured item for the foreseeable future—not just using generic product codes. This isn't necessary for basic inventory control, but it has implications for tracing manufacturing faults and stolen goods and for detecting forgery. It also offers the more controversial post-sale marketing opportunities, enabling direct marketing based on prior purchases.

IrDA

IrDA is an infrared wireless communication technology developed by the Infrared Data Association. Here we compare and contrast specific features of these technologies. IrDA is a specific use of infrared light as a communications medium; Bluetooth technology is a specific use of radio waves as a communications medium. Like the Bluetooth special interest group (SIG), the IrDA specifies hardware and software protocols for wireless communication intended to promote interoperable applications. Although both technologies are wireless, they use different parts of the electromagnetic spectrum with quite different signal propagation characteristics. Because infrared uses the nonvisible infrared light spectrum, IrDA communication is blocked by obstacles that block light (such as walls, doors, briefcases, and people). The signal wavelength used with Bluetooth communication (about 12.5 cm, at its associated frequency of 2.4GHz) is three orders of magnitude greater than that of IrDA. At this wavelength, radio frequency (RF) communications can penetrate many of these sorts of obstacles. Recent advances in infrared technology have enabled more diffuse transmission patterns, although much of the IrDA equipment in use today uses a relatively narrowly focused beam, which usually requires that the two devices engaged in IrDA communication be aligned with (pointed at) each other. RF transmission patterns radiate in some pattern (ideally, spherical) around the radio antenna, so any two devices within range can communicate with each other, whether or not they are "pointed at" each other (in fact, the second device might not be visible at all to the user of the first device, as it could be in another room behind doors and walls or even on another floor of a building, for example). The initial IrDA data rate of 115 kilobits per second (Kbps) has now been enhanced to 1 megabit per second (Mbps), comparable to that of the first Bluetooth radios. Today, IrDA can achieve data rates of up to 4Mbps, with even higher rates already specified and beginning to be implemented. Bluetooth wireless communication occurs at a raw data rate of 1Mbps, with higher speeds being investigated. Infrared Data Association, or IrDA in short, is a group of device manufacturers that developed a standard for transmitting data via infrared (IR) light waves. It provides specifications for the complete set of protocols for wireless IR communication. The main reason for using IrDA had been wireless data transfer over the “last one meter” using point-and-shoot principles. It is famous for secure data transfer, line-of-sight and very low bit error rate that makes it very efficient. IR communication is an inexpensive and widely adopted short-range (1-3m) wireless technology. It is widely used in consumer electronics, automobiles, computers, medical devices, household appliances, commercial services, etc. IrDA-enabled devices can communicate and are bi-directional. IrDA is inexpensive, secure and fast (supporting speeds of up to 100Mbps and even more)

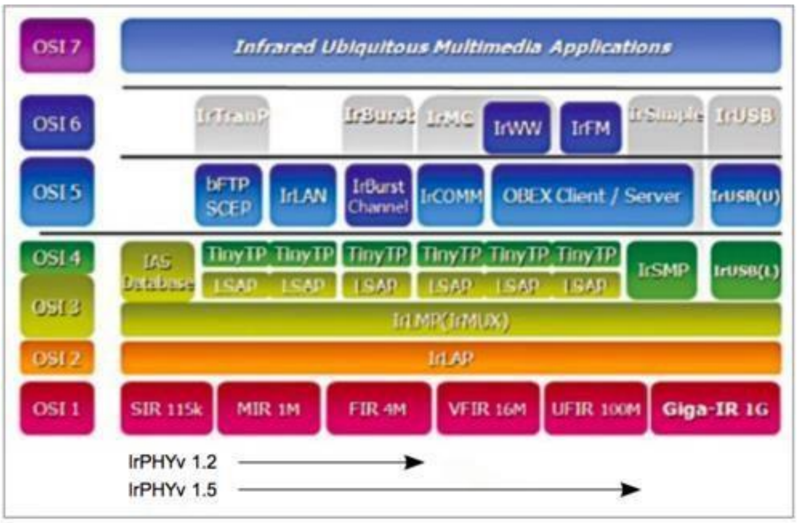


Figure 5.6 Infrared Data Association (IrDA)-protocol-stacks

Infrared physical layer (IrPHY)

This specification is intended to facilitate point-to-point communication between electronic devices. It specifies the optical media interfaces for Serial Infrared (SIR) data transmission and is part of the first layer of the OSI model.

Infrared link access protocol (IrLAP)
This specification is part of the second layer of IrDA specifications. It lies on top of the IrPHY layer and below the IrLMP layer. It represents the data link layer.
Infrared link management protocol (IrLMP)
It is the third layer of IrDA specifications. It defines link management multiplexer and link management information access service.
Transport protocol (TinyTP)
This optional protocol specified in the fourth layer lies on top of the IrLMP layer.
Infrared communication protocol (IrCOMM) The IrCOMM protocol specified in the fifth layer lets the infrared device act like either a serial or parallel port.
Infrared Financial Messaging (IrFM)
This protocol specified in the sixth layer is a wireless payment standard developed by the Infrared Data Association.

NFC:
NFC stands for “Near Field Communication” and, as the name implies, it enables short-range communication between compatible devices. This requires at least one transmitting device, and another to receive the signal. A range of devices can use the NFC standard and will be considered either passive or active.
Passive NFC devices include tags, and other small transmitters, that can send information to other NFC devices without the need for a power source of their own. However, they don’t process any information sent from other sources, and can’t connect to other passive components. These often take the form of interactive signs on walls or advertisements.

Active devices are able to both send and receive data, and can communicate with each other as well as with passive devices. Smartphones are by far the most common form of active NFC device. Public transport card readers and touch payment terminals are also good examples of the technology.

Working of NFC

Just like Bluetooth and Wi-Fi, and all manner of other wireless signals, NFC works on the principle of sending information over radio waves. Near Field Communication is another standard for wireless data transitions. This means that devices must adhere to certain specifications in order to communicate with each other properly. The technology used in NFC is based on older RFID (Radio-frequency identification) ideas, which used electromagnetic induction in order to transmit information. This marks the one major difference between NFC and Bluetooth/WiFi. The former can be used to induce electric currents within passive components as well as just send data. This means that passive devices don’t require their own power supply. They can instead be powered by the electromagnetic field produced by an active NFC component when it comes into range. Unfortunately, NFC technology does not command enough inductance to charge our smartphones, but QI wireless charging is based on the same principle.

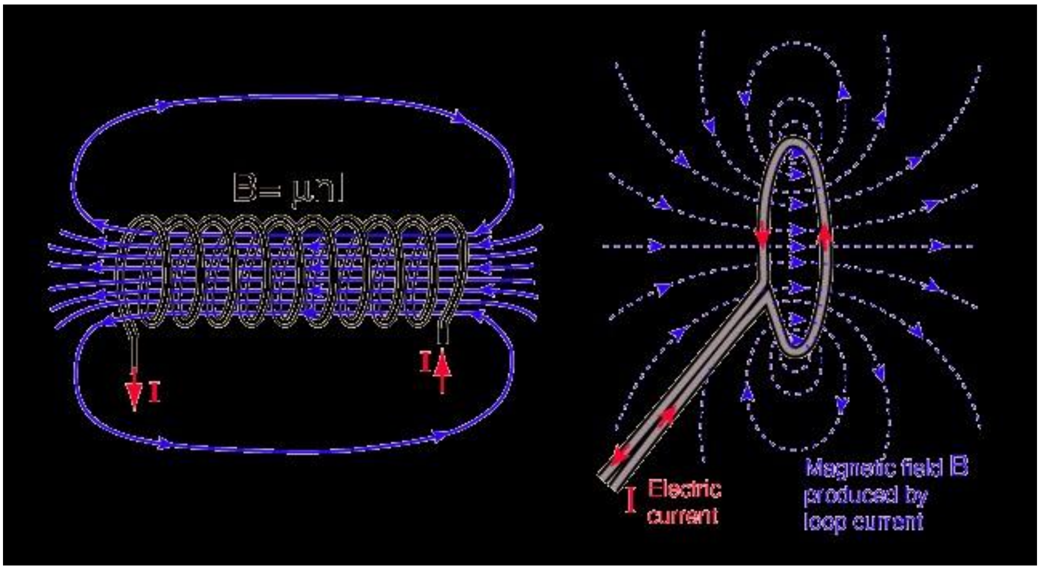


Figure 5.7 NFC

Electromagnetic fields can be used to transmit data or induce electrical currents in a receiving device. Passive NFC devices draw power from the fields produced by active devices, but the range is short The transmission frequency for data across NFC is 13.56 megahertz. You can send data at either 106, 212, or 424 kilobits per second. That’s is quick enough for a range of data transfers — from contact details to swapping pictures and music.

To determine what sort of information will be exchanged between devices, the NFC standard currently has three distinct modes of operation. Perhaps the most common use in smartphones is the peer-to-peer mode. This allows two NFC-enabled devices to exchange various pieces of information between each other. In this mode, both devices switch between active when sending data and passive when receiving.

Read/write mode, on the other hand, is one-way data transmission. The active device, possibly your smartphone, links up with another device in order to read information from it. NFC advert tags use this mode. The final mode of operation is card emulation. The NFC device can function as a smart or contactless credit card and make payments or tap into public transport systems.

Comparisons with Bluetooth

We might think that NFC is a bit unnecessary, considering that Bluetooth has been more widely available for many years. However, there are several important technical differences between the two that gives NFC some significant benefits in certain circumstances. The major argument in favor of NFC is that it requires much less power consumption than Bluetooth. This makes NFC perfect for passive devices, such as the advertising tags mentioned earlier, as they can operate without a major power source.

However, this power-saving does have some major drawbacks. Most notably, the range of transmission is much shorter than Bluetooth. While NFC has a range of around 10 cm, just a few inches, Bluetooth connections can transmit data up to 10 meters or more from the source. Another drawback is that NFC is quite a bit slower than Bluetooth. It transmits data at a maximum speed of just 424 kbit/s, compared to 2.1 Mbit/s with Bluetooth 2.1 or around 1 Mbit/s with Bluetooth Low Energy.

But NFC does have one major advantage: faster connectivity. Due to the use of inductive coupling, and the absence of manual pairing, it takes less than one-tenth of a second to establish a connection between two devices. While modern Bluetooth connects pretty fast, NFC is still super handy for certain scenarios. Namely mobile payments

Sigfox

Sigfox is a network operator dedicated to the Internet of Things (IoT). The Sigfox network is using the UNB (Ultra Narrow Band) and allows devices to communicate with low power on a wide area. The Sigfox network already spans to 45 countries around the world. The Sigfox technology allows the Enless transmitters to send their data (temperature, humidity, metering values…) without distance constraints directly on the Sigfox servers. The data stocked on the Sigfox cloud can then be processed (curves, alarms, thresholds) on platforms through API or Callbacks

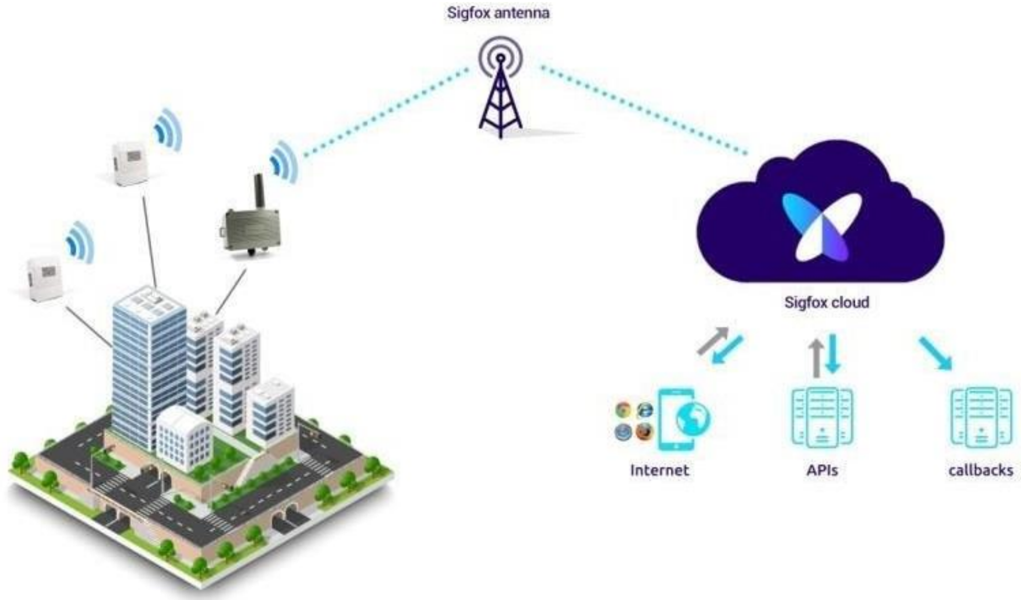


Figure 5.8 Communication via Sigfox protocol

Enless Wireless has developped two distinct Sigfox compatible product ranges.

Supported Sigfox zones:

- Zone 1 (Europe, Oman, Iran, South Africa, Tunisia, UAE)

- Zone 4 (Australia, New Zealand, Singapore, Taiwan, Hong Kong, Colombia, Argentina, Costa Rica, Thailand, Malaysia, Ecuador, Panama, El Salvador)

LoRA

- **LoRaWAN**, which means **Long Range Wide-area network**, is a telecommunication protocol for low-speed communication, by radio, of objects with low power consumption communicating according to **LoRa technology** created in 2009 and connected to the Internet via gateways, thus participating in the Internet of Things.
- This protocol is used for **smart cities and buildings**, industrial monitoring and agricultural applications.
- Lora is part of the **Low Power Wide Area Network (LPWAN) technologies that allow long-range coverage while consuming low power.**

The LoRa/ LoRaWAN protocol allows you to build operated or private networks :

In public mode LoRaWAN:
The data pushed by the transmitters is transmitted to the cloud of the network operator LoRa at a flexible periodicity.

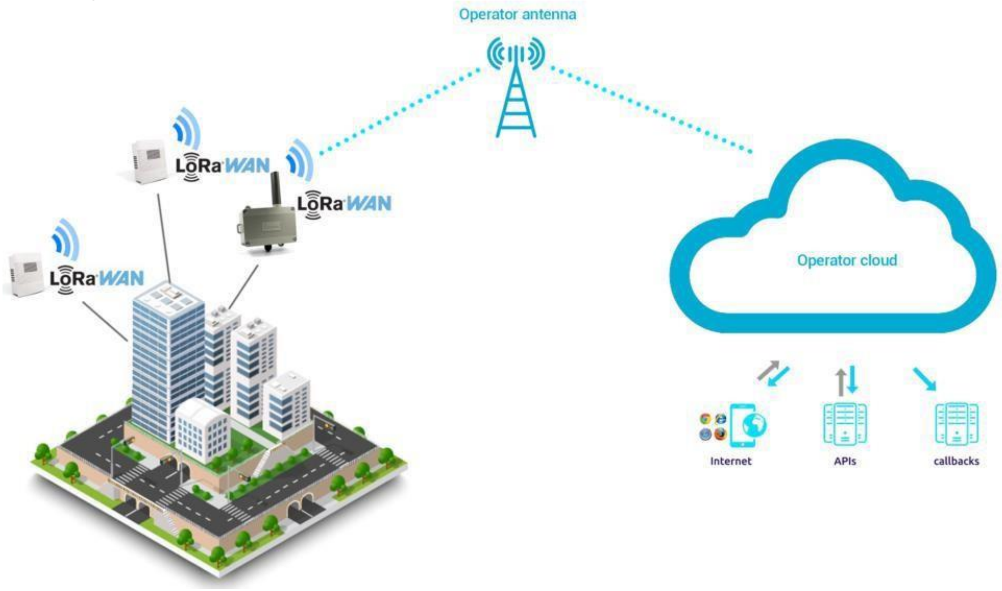


Figure 5.9 Public Mode LoRA WAN

In LoRa Enless Wireless private mode:
The data is transmitted by radio to the Modbus Enless Wireless LoRa receiver, which is usually connected to an PLC.

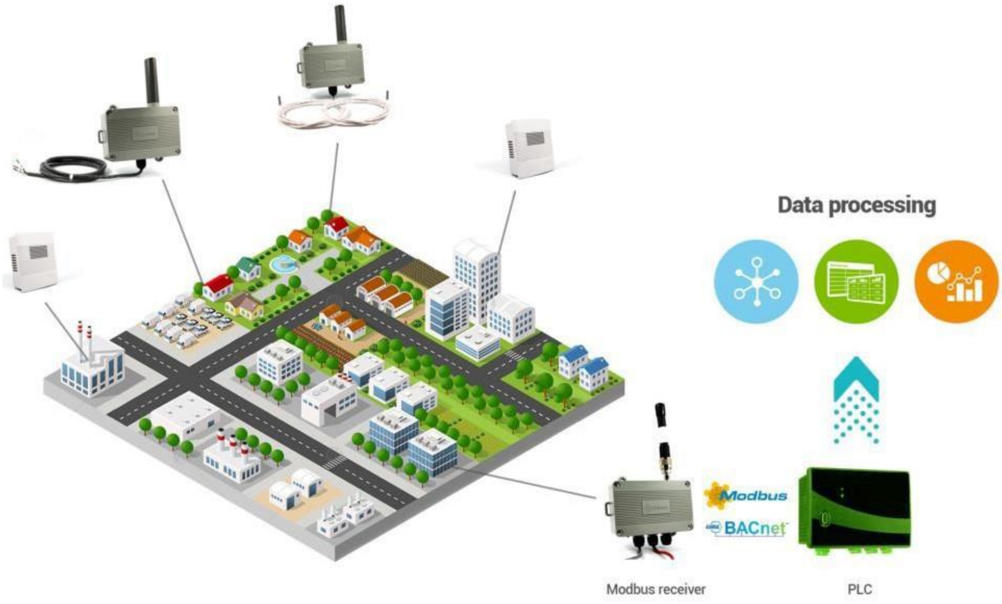


Figure 5.10 Enless Wireless Private Mode

In LoRaWAN private mode:
The data flows directly from our transmitters to the LoRaWAN gateway.

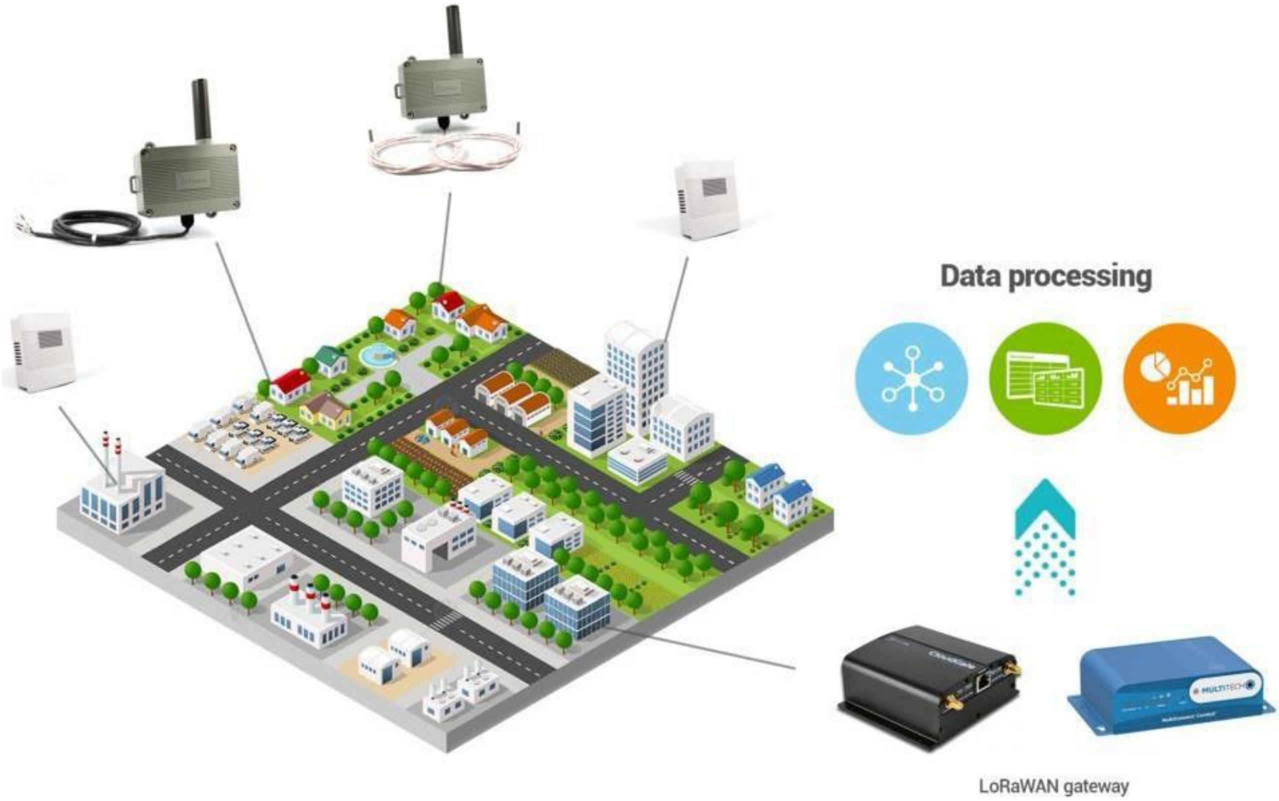


Figure 5.11 Private Mode

In LoRaWAN mode, data formatting (statistics, curves, alarms, etc.) can then be ensured by specific platforms.

The main frequency bands associated with the LoRa protocol are:

Europe: 433 Mhz, 868 Mhz

United States: 915 Mhz

Asia: 430 Mhz

LoRa WAN Protocol

LoRa WAN includes the network layer too so it is possible to send the information to any Base Station already connected to a Cloud platform. LoRaWAN modules may work in different frequencies by just connecting the right antenna to its socket.

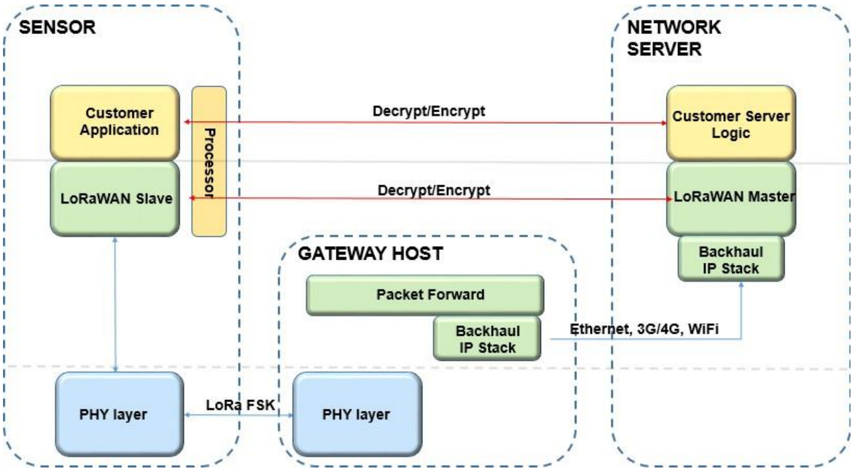


Figure 5.12 LoRa WAN network layers.

NB-IoT

NBIoT is the low energy and low bandwidth version of IoT which is designed for the massive machine-to-machine communications. As the name suggests, it uses narrow bands for its different functions and operations. It needs a bandwidth of just 180 kHz to 200 kHz for its designated processes. In LTE Release 13 and 14, 180 kHz has been proposed as the operating bandwidth for NBIoT. It is a low power wide area (LPWA) technology which can save a lot of power when compared with other forms of IoTs. It is good for large scale economical deployment of IoT for different applications. In true sense, it is leaner, thinner and greener than other IoTs proposed in the recent years. It can be deployed in both the cellular and non-cellular forms. However, cellular forms are popular as they can use the existing cellular architectures for its operations. In LTE Release 13 and 14, it has been standardized according to the compatible LTE provisions and also proposed for connected living environments

A systematic NBIoT architecture is required for its planning, dimensioning, cost estimation, design and final deployment. It does not have a legacy to follow as it is one of the earliest IoTs of its type. However, it is similar to the WSN and the WSNs are there for several years. The existing WSN architecture and topologies can be helpful in its further advancement. It is noteworthy that WSNs did not have a structured and well defined architecture like the cellular systems such as the LTE networks which will form the backbone of NBIoT. Therefore, an LTE cellular framework for NBIoT is the right choice at the moment. The layered structure of NBIoT is helpful in its planning and deployment. In Release 13, several specifications for different layers have been mentioned. NBIoT can be separated into 6 layers as shown in Fig. 1. The physical layer is at the bottom and it is normally the air interface. Physical layer does the similar functions as other WSNs and some added functions as defined in Release 13. Above it is the medium access control (MAC) layer. This has the similar functions like the MAC layer of other networks. It incorporates the protocols for medium access and multiple access techniques. There is a radio link control layer in between the MAC and the upper layers. This layer makes the adaptation of the MAC layer information for radio links. Above it is the packet data convergence protocol layer which provides routing, traffic scheduling, networking and other related tasks. Then above it is the radio resource control layer which takes care of the radio resources of the packets in the channels. NBIoT uses user datagram protocol (UDP) and other cellular mechanism to carry this function. UDP is effective in the wireless networks and thus suitable for NBIoT as well. The topmost layer is the Non- Access Stratum (NAS) which establishes the communication between the user equipment (UE) and the main server of the NBIoT also known as NBIoT central node.

Applications of NBIoT
NBIoT for Agriculture in Developing Countries
NBIoT for Manufacturing in Developing Countries
NBIoT for Healthcare in Developing Countries
NBIoT forResource Management in Developing Countries

Classes of LoRA Devices:
Three different classes (A,B,C) of communication profiles are available in LoRa networks between devices and applications. Each class serves different application needs and has optimised requirements for specific purposes. The key difference between A, B and C profiles is the trade-off made between latency and power consumption.

Class A (« all ») -Battery powered sensors, or actuators with no latency constraint.
Most energy efficient communication class.

• Must be supported by all devices

• End-devices in Class A support bi-directional communication between a device and a gateway. This operation is the lowest power end-device system, for applications which only require downlink communication from the server shortly after the end-device has sent an uplink transmission. Here Uplink messages can be sent at any time, the device then opens two receive windows at specified times after an uplink transmission. If the server does not respond in either of these receive windows, the next opportunity will be after the next uplink transmission from the device. The server can respond in either the first or second https://wiki.thingscalderdale.com/LoRaWAN_Dev_Kit receive windows, the transmission slot scheduled by the end-device is based on its own communication needs with a small variation based on a random time basis (ALOHA-type of protocol). All of the examples from the LoRaWAN workshop come under this class.

Class B (« beacon »)-Battery powered actuators
• Energy efficient communication class for latency controlled downlink.

• Based on slotted communication synchronized with a network beacon.

• The end-devices in class B are bi-directional with scheduled receive slots. This class is similar to Class A, however, Class B devices open extra receive windows at scheduled times in addition to Class A's random receive windows. In order for the end-device to open its receive window at the scheduled time it receives a time synchronized beacon from the gateway, allowing the server to know when the end-device is listening.

class C (« continuous »)-Mains powered actuators

- Devices which can afford to listen continuously.

- No latency for downlink communication.

- Class C end-devices are bi-directional with maximal receive slots. This means that Class C end-devices almost have continuously open receive windows, which are only closed when transmitting. This allows for low-latency communication but is many times more energy consuming than devices in Class A. Due to the amount of energy required to keep a node actively awake running the receiver at all times Class C end-devices are used primarily for AC-powered applications.

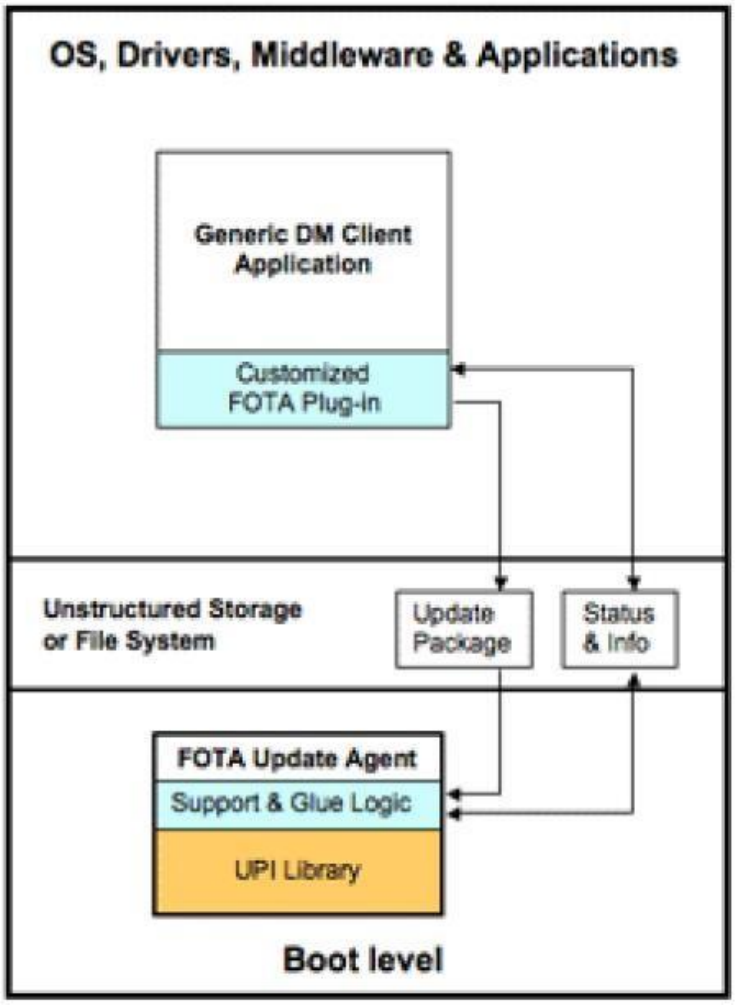
Introduction to Firmware over the Air (FOTA)

Firmware Over-the-Air (FOTA) technology enables device manufacturers and network operators to deliver updated firmware to mobile phones in consumers' hands. Today's mobile devices contain enormous amounts of software, mainly firmware, to support such advanced features as digital cameras, music players and web browsers. There are inevitable issues with such complex software: software defects, missing features and design issues, often created by time-to-market demands in this highly competitive market.

- The need to fix device software over-the-air has made FOTA mainstream, adopted by nearly every major manufacturer and operator. By the end of 2008, 50% of all mobile phones will include FOTA, according to U.K.-based analyst firm, ARCchart. Much can be learned from the successful embedding of FOTA in mobile handsets. However, there are software and a few hardware considerations to effectively implement a FOTA solution. This article focuses on the technology behind FOTA updating in order to assist manufacturers and operators in selecting, integrating and using such a technology. This article is based on real-world, accumulated experience in developing and integrating FOTA software on more than 100 mobile devices.
- FOTA device architecture The mobile industry has adopted a common architecture for Mobile Device Management (DM) systems, enabling mobile operators, handset manufacturers and enterprises to have remote management over the handset, its functions and visibility into its workings. A major reason for operators and OEMs to deploy DM systems is to enable Firmware Over-the-Air (FOTA)–the ability to remotely update devices' firmware.
- The assumption is that the reader is familiar with the overall architecture and basic components of DM systems, which include a horizontal DM server, its vertical plug-in applications and a DM client. These systems utilize the OMA-DM 1.2 standard developed through the Open Mobile Alliance (OMA). This standard ensures that all mobile devices can communicate with and are interoperable with a DM server used by the service provider.
- In contrast, the OMA-DM standards do not include any device-side implementation issues, which are strictly left 'out of scope' of the standards. Therefore, the major complexity of the FOTA update process is often not well understood by those evaluating and integrating FOTA capability into devices.
- FOTA-enabled Device Architecture FOTA implementation on a typical handset includes a standard DM client compliant to the DM protocol, which must include the Firmware Update Management Object (FUMO). FUMO is part of the complete OMA-DM protocol and the actual semantics are expected to be interpreted and carried out by a suitable plug-in added to any provided generic DM

client. This plug-in is responsible for applicative details such as user experience of the update process, properly storing the downloaded Update Package, validating the integrity of and authenticating the package, and signalling the Update Agent to execute ('hand-off') the actual update.

• It is the Update Agent which performs the actual FOTA update on the handset. Later on, upon termination of the update process by the Update Agent, the FOTA plug-in collects status/result information from that process and lets the DM client report it back to the server according to the DM protocol.



The Update Agent is responsible for performing the firmware update, and is separate from the generic DM client-server system.

Figure 5.13 Firmware over the Air

• As shown in Figure, such architecture requires no API between the DM client including its FOTA plug-in and the Update Agent. The Update Agent must work as a stand-alone boot application to enable total updating of the firmware, and any direct API between DM client/plug-in and the Update Agent is almost impossible and not recommended.

• The Update Agent is mainly comprised of the Update Installer (UPI) and its support logic. The UPI is the component that calculates and builds the new firmware version and writes it in-place of the old one. The surrounding support logic provides the hardware-dependent implementation details.

• In order to maintain flexibility and a high degree of updatability of the firmware, it is recommended that the API of the UPI is used only by the support logic and that the whole Update Agent is stored separately in flash from the rest of the firmware to allow easy updating of the Update Agent. In such an implementation, the API of the UPI can also evolve and be later updated over-the-air. Therefore, there should be no dependencies between the rest of the boot loader (which should not be modified) and the Update Agent. This loosely de-coupled architecture of a FOTA-enabled device, whereby specialized adaptors capture device-specific details, simplifies integration into the handset and allows good maintenance of the FOTA mechanisms themselves.

TEXT / REFERENCES BOOKS

1. Jun Zheng, Abbas Jamalipour,"Wireless Sensor Networks: A Networking Perspective", Wiley India, 1st Edition, 2014.
2. Waltenegus Dargie, Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", John Wiley & Sons, 1st Edition, 2010.
3. Edgar H. Callaway, "Wireless Sensor Networks: Architectures and Protocols", CRC Press, 1st Edition, August 2003.
4. Jose A. Gutierrez, Edgar H. Callaway, Raymond Barrett, "IEEE 802.15.4 Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensor Networks", Standards Information Network, 3rd Edition,2011.
5. Kazem Sohraby, Daniel Minoli, TaiebZnati, "Wireless Sensor Networks: Technology, Protocols, and Applications", John Wiley & Sons, 1st Edition, 2007.

PART A

1. Explain how Accuracy is improved in GPS
2. Compare NFC with IrDA and Bluetooth
3. Quote the key components of RFID
4. Sketch in detail the system protocols of IrDA
5. Indicate the use of sigbox zones
6. Quote the use of Narrowband IoT
7. Determine the functions of FOTA.
8. Relate the concept of LoRA and LoRA-WAN

PART B

1. Implement the functions and architecture of RFID and IRDA
2. Demonstrate the structure of FOTA
3. Discuss the types in detail of LoRA
4. summarize the functions of sigbox and explain its architecture
5. Explain the working model of LoRA and also explain the classes of LoRA devices