Bluetooth Basics

<https://learn.sparkfun.com/tutorials/bluetooth-basics> Contributor: JIMB0

What is Bluetooth?

Bluetooth is a standardized protocol for sending and receiving data via a 2.4GHz wireless link. It's a secure protocol, and it's perfect for short-range, low-power, low-cost, wireless transmissions between electronic devices.

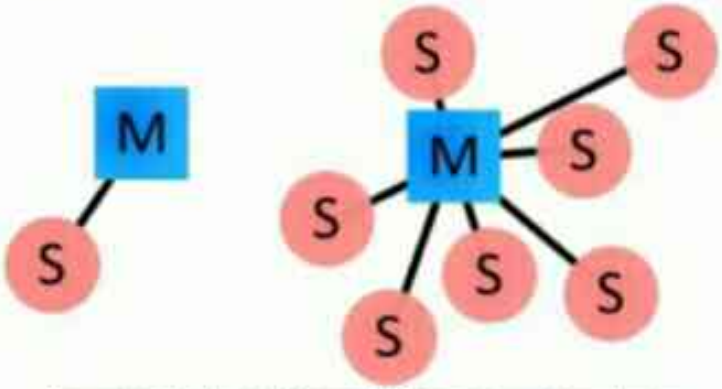
These days it feels like everything is wireless, and Bluetooth is a big part of that wireless revolution. You'll find Bluetooth embedded into a great variety of consumer products, like headsets, video game controllers, or livestock trackers.vIn our world of embedded electronics hackery, Bluetooth serves as an excellent protocol for wirelessly transmitting relatively small amounts of data over a short range (<100 m). It's perfectly suited as a wireless replacement for serial communication interfaces. Or you can use it to create a DIY HID Computer Keyboard. Or, with the right module, it can be used to build a home-brew, wireless MP3-playing speaker. This tutorial aims to provide a quick overview of the Bluetooth protocol. We'll examine the specifications and profiles that form its foundation, and we'll go over how Bluetooth compares to other wireless protocols.

How Bluetooth Works

The Bluetooth protocol operates at 2.4GHz in the same unlicensed ISM frequency band where RF protocols like ZigBee and WiFi also exist. There is a standardized set of rules and specifications that differentiates it from other protocols. If you have a few hours to kill and want to learn every nook and cranny of Bluetooth, check out the published specifications, otherwise here's a quick overview of what makes Bluetooth special.

Masters, Slaves, and Piconets

Bluetooth networks (commonly referred to as piconets) use a master/slave model to control when and where devices can send data. In this model, a single master device can be connected to up to seven different slave devices. Any slave device in the piconet can only be connected to a single master.



Examples of Bluetooth master/slave piconet topologies.

The master coordinates communication throughout the piconet. It can send data to any of its slaves and request data from them as well. Slaves are only allowed to transmit to and receive from their master. They can't talk to other slaves in the piconet.

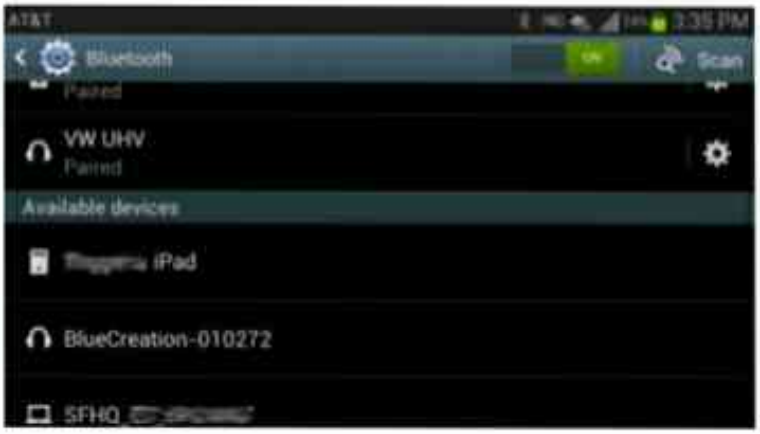
Bluetooth Addresses and Names

Every single Bluetooth device has a unique 48-bit address, commonly abbreviated BD_ADDR. This will usually be presented in the form of a 12-digit hexadecimal value. The most-significant half (24 bits) of the address is an organization unique identifier (OUI), which identifies the manufacturer. The lower 24-bits are the more unique part of the address.

This address should be visible on most Bluetooth devices. For example, on this RN-42 Bluetooth Module, the address printed next to "MAC NO." is 000666422152:The "000666" portion of that address is the OUI of Roving Networks, the manufacturer of the module. Every RN module will share those upper 24-bits. The "422152" portion of the module is the more unique ID of the device.

Bluetooth devices can also have user-friendly names given to them. These are usually presented to the user, in place of the address, to help identify which device it is.

The rules for device names are less stringent. They can be up to 248 bytes long, and two devices can share the same name. Sometimes the unique digits of the address might be included in the name to help differentiate devices.



Connection Process

Creating a Bluetooth connection between two devices is a multi-step process involving three progressive states:

1. Inquiry – If two Bluetooth devices know absolutely nothing about each other, one must run an inquiry to try to discover the other. One device sends out the inquiry request, and any device listening for such a request will respond with its address, and possibly its name and other information.
2. Paging (Connecting) – Paging is the process of forming a connection between two Bluetooth devices. Before this connection can be initiated, each device needs to know the address of the other (found in the inquiry process).
3. Connection – After a device has completed the paging process, it enters the connection state. While connected, a device can either be actively participating or it can be put into a low power sleep mode.
    - Active Mode – This is the regular connected mode, where the device is actively transmitting or receiving data.
    - Sniff Mode – This is a power-saving mode, where the device is less active. It'll sleep and only listen for transmissions at a set interval (e.g. every 100ms).
    - Hold Mode – Hold mode is a temporary, power-saving mode where a device sleeps for a defined period and then returns back to active mode when that interval has passed. The master can command a slave device to hold.
    - Park Mode – Park is the deepest of sleep modes. A master can command a slave to "park", and that slave will become inactive until the master tells it to wake back up.

Bonding and Pairing

When two Bluetooth devices share a special affinity for each other, they can be bonded together. Bonded devices automatically establish a connection whenever they're close enough. When I start up my car, for example, the phone in my pocket immediately connects to the car's Bluetooth system because they share a bond. No UI interactions are required!

Bonds are created through one-time a process called pairing. When devices pair up, they share their addresses, names, and profiles, and usually store them in memory. The also share a common secret key, which allows them to bond whenever they're together in the future.

Pairing usually requires an authentication process where a user must validate the connection between devices. The flow of the authentication process varies and usually depends on the interface capabilities of one device or the other. Sometimes pairing is a simple "Just Works" operation, where the click of a button is all it takes to pair (this is common for devices with no UI, like headsets). Other times pairing involves matching 6-digit numeric codes. Older, legacy (v2.0 and earlier), pairing

processes involve the entering of a common PIN code on each device. The PIN code can range in length and complexity from four numbers (e.g. "0000" or "1234") to a 16-character alphanumeric string.

Power Classes

The transmit power, and therefore range, of a Bluetooth module is defined by its power class. There are three defined classes of power:

Class Number	Max Output Power (dBm)	Max Output Power (mW)	Max Range
Class 1	20 dBm	100 mW	100 m
Class 2	4 dBm	2.5 mW	10 m
Class 3	0 dBm	1 mW	10 cm

Some modules are only able to operate in one power class, while others can vary their transmit power.

Bluetooth Profiles

Bluetooth profiles are additional protocols that build upon the basic Bluetooth standard to more clearly define what kind of data a Bluetooth module is transmitting. While Bluetooth specifications define how the technology works, profiles define how it's used.

The profile(s) a Bluetooth device supports determine(s) what application it's geared towards. A hands-free Bluetooth headset, for example, would use headset profile (HSP), while a Nintendo Wii Controller would implement the human interface device (HID) profile. For two Bluetooth devices to be compatible, they must support the same profiles.

Let's take a look at a few of the more commonly-encountered Bluetooth profiles.

3. WIRELESS LAN BASICS

This chapter discusses various topics of interest to those creating or joining wireless LANs. There are several decisions to make when deploying a Wi-Fi network. Since the original 802.11 specification that came out in 1997, which operated in the 2.4 GHz range at low data rates of 1-2 Mbps, several extensions have expanded the available choices. The marketplace has also responded to customer demand by offering devices that combine 802.11 extensions into one device.

The topics included in this chapter are things to consider in relationship to the requirements of your application.

3.1 Wi-Fi Characteristics

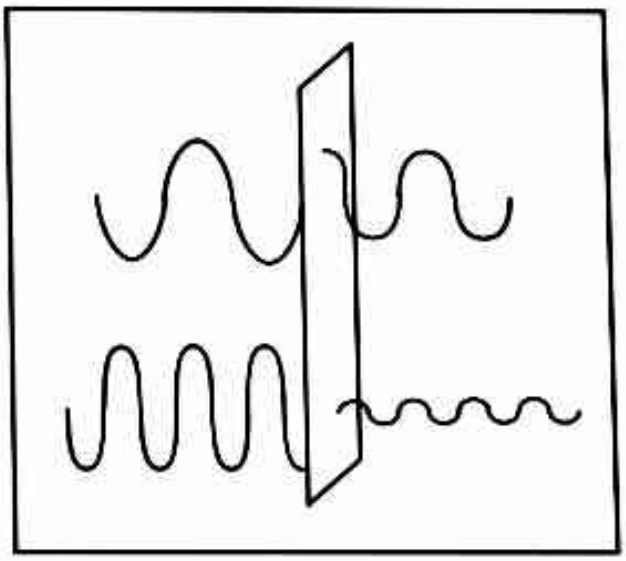
The physical characteristics summarized in Table 2-2 allow you to compare the different 802.11 extensions (802.11a/b/g/n) with one another. This section describes basic characteristics that are common to all Wi-Fi networks.

3.1.1 Operating Frequency

There are two signaling frequencies currently used by Wi-Fi networks:

- 2.4 GHz - Comprises 14 channels, each with a bandwidth of approximately 20 to 22 MHz operating in the ISM band. 802.11b/g networks operate in the 2.4 GHz band. It is a crowded frequency because many devices other than 802.11 devices operate in it. For example, Bluetooth as well as many consumer products such as microwaves, telephones, garage door openers, baby monitors, etc.
- 5 GHz - Comprises 13 channels, each with a bandwidth of approximately 20 MHz operating in the U-NII band. 802.11a networks operate in the 5 GHz band. Currently, this band is less crowded than 2.4 GHz, but this is likely to change as the wireless market continues to grow.

Higher frequency signals have higher attenuation passing through obstacles than do lower frequency signals. This is because some of the energy of the electromagnetic field transfers into the material of the obstacle (cement walls, foliage, etc.) which reduces the strength of the signal.



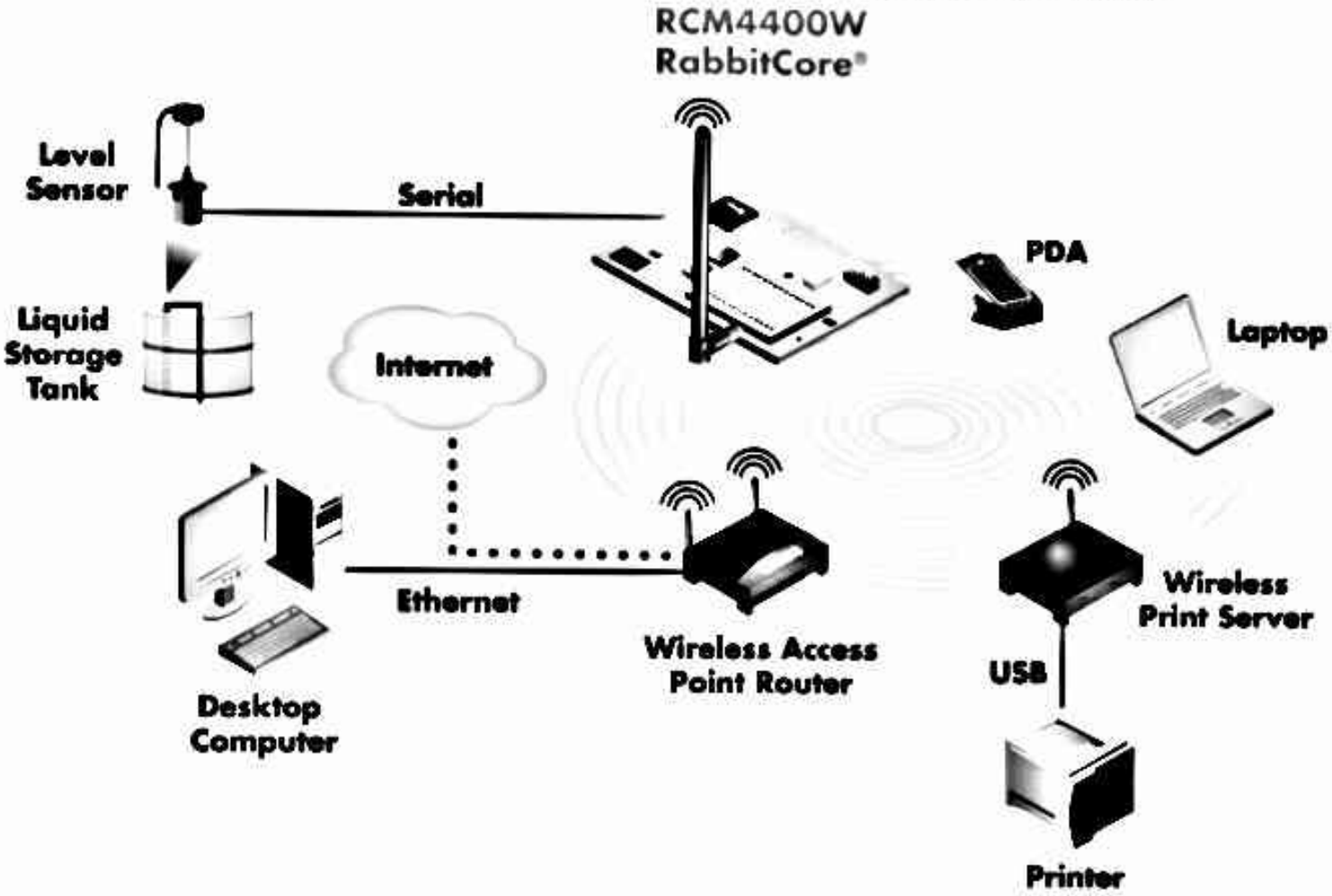
1. OVERVIEW

This manual is intended for embedded systems engineers and support professionals who are not familiar with wireless networking from a theoretical or implementation point of view. The components, organization, and operation of Wi-Fi networks will be presented. There is an emphasis on security issues and the available security protocols.

Wi-Fi is the name given by the Wi-Fi Alliance to the IEEE 802.11 suite of standards. 802.11 defined the initial standard for wireless local area networks (WLANs), but it was considered too slow for some applications and so was superseded by the extensions 802.11a and 802.11b, and later by 802.11g (with the release of 802.11n still pending).

At its most basic, Wi-Fi is the transmission of radio signals[1]. Wireless Rabbits offer the embedded systems engineer many benefits in a wide range of applications. Figure 1 illustrates the Rabbit's role in a sensor monitoring application.

Figure 1. Wireless Local Area Network Connected to the Internet



1. When asked to describe radio, Albert Einstein replied, "You see, wire telegraph is a kind of a very, very long cat. You pull his tail in New York and his head is meowing in Los Angeles. Do you understand this? And radio operates exactly the same way: you send signals here, they receive them there. The only difference is that there is no cat."

1.1 Benefits of Wi-Fi

What are the benefits of Wi-Fi over a more traditional wired network? In particular, what are the benefits for an embedded system application? To begin with, if you study the diagram in Figure 1, you can see the enormous flexibility that a wireless connection brings to an embedded application. The addition of wireless provides more choices for monitoring, control and the dissemination of information. Practically speaking, remote locations become more accessible and costs drop.

The following list summarizes some of the benefits of a Wi-Fi network.

- **Wireless Ethernet**. Wi-Fi is an Ethernet replacement. Wi-Fi and Ethernet, both IEEE 802 networks, share some core elements.
- **Extended Access**. The absence of wires and cables extends access to places where wires and cables cannot go or where it is too expensive for them to go.
- **Cost Reduction**. As mentioned above, the absence of wires and cables brings down cost. This is accomplished by a combination of factors, the relatively low cost of wireless routers, no need for trenching, drilling and other methods that may be necessary to make physical connections.
- **Mobility**. Wires tie you down to one location. Going wireless means you have the freedom to change your location without losing your connection.
- **Flexibility**. Extended access, cost reductions, and mobility create opportunities for new applications as well as the possibility of creative new solutions for legacy applications.

1.2 Wi-Fi Embedded System Applications

The reach of wireless communication in embedded systems continues to grow. Forrester Research, a company that focuses on the business implications of technology change, has reported that in a few short years, up to 95% of devices used to access the Internet will be non-PC devices that use an embedded system.

There are many applications for embedded devices with a Wi-Fi interface:

- Industrial process and control applications where wired connections are too costly or inconvenient, e.g., continuously moving machinery.
- Emergency applications that require immediate and transitory setup, such as battlefield or disaster situations.
- Mobile applications, such as asset tracking.
- Surveillance cameras (maybe you don't want them easily noticed, cables are difficult to hide).
- Vertical markets like medical, education, and manufacturing.
- Communication with other Wi-Fi devices, like a laptop or a PDA.

2. IEEE 802.11 SUITE OF STANDARDS

This chapter discusses the concepts and characteristics specified in the IEEE 802.11 standard. 802.11 is a packet protocol that defines data transmission and manages location-independent network access using radio signals.

Wi-Fi is a physical/link layer interface, as is Ethernet. The layers above the physical and data link layers include TCP/IP. On a practical level, this means that all Rabbit sample programs and customer applications for TCP/IP that are run on an Ethernet interface will also run on a Wi-Fi interface.

2.1 Architecture

This section discusses the architectural components defined by the 802.11 standard. The architecture describes the structure and organization of the network. This knowledge informs various tasks, such things as selecting the right operating mode to suit your application or completing an effective site survey for the physical location of the network.

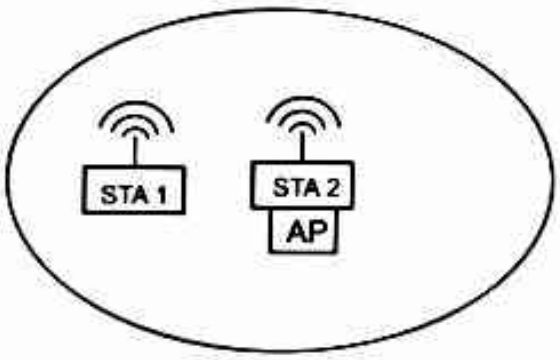
2.1.1 Basic Components

All wireless devices that join a Wi-Fi network, whether mobile, portable or fixed, are called wireless stations (STAs). A wireless station might be a PC, a laptop, a PDA, a phone, or a Rabbit core module. When two or more STAs are wirelessly connected, they form a basic service set (BSS). This is the basic building block of a Wi-Fi network.

A BSS is a set of STAs controlled by a single coordination function (CF). The CF is a logical function that determines when a STA transmits and when it receives.

The BSS shown in Figure 2.1 is an example of the simplest Wi-Fi network possible: two wireless stations. The oval shape around them roughly represents the coverage area.

Figure 2.1

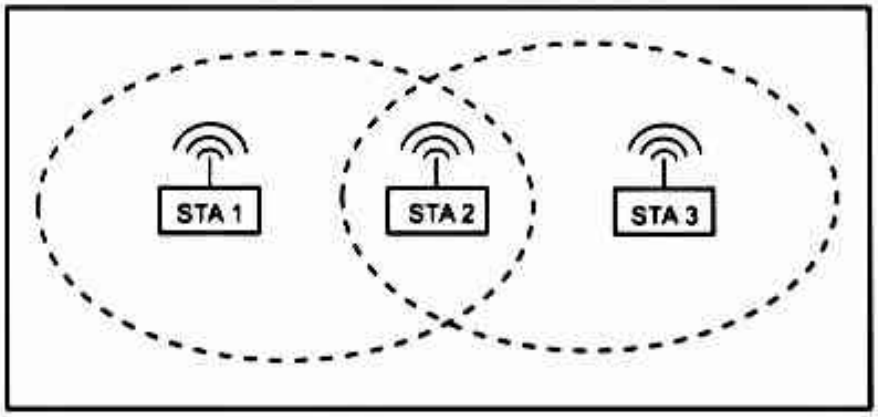


BSS

While a circle may represent the idealized coverage area of a single radio, it is not very accurate in real world situations. Environmental factors cause dramatic variations to the coverage area. For example, a STA with an omnidirectional antenna placed in the corner of a building may have most of its coverage area outside the building and in the adjacent parking lot.

Not all STAs in a BSS can necessarily communicate directly. Consider Figure 2.2. STA 1 and 3 are mutually out of range, thus require use of STA 2 to relay messages.

Figure 2.2



2.1.2 Operating Modes

This section discusses the two operating modes specified in the IEEE 802.11 standard: infrastructure mode and ad-hoc mode. Each one makes use of the BSS, but they yield different network topologies.

The operating mode is selected during the configuration of the wireless station (see Chapter 5 for more details); all wireless stations must select an operating mode before attempting to create or join a Wi-Fi network.

2.1.2.1 Ad-Hoc Mode

The independent BSS (IBSS) is the simplest type of 802.11 network. Wireless stations communicate directly with one another using the ad-hoc operating mode. Such a network follows a peer-to-peer model.

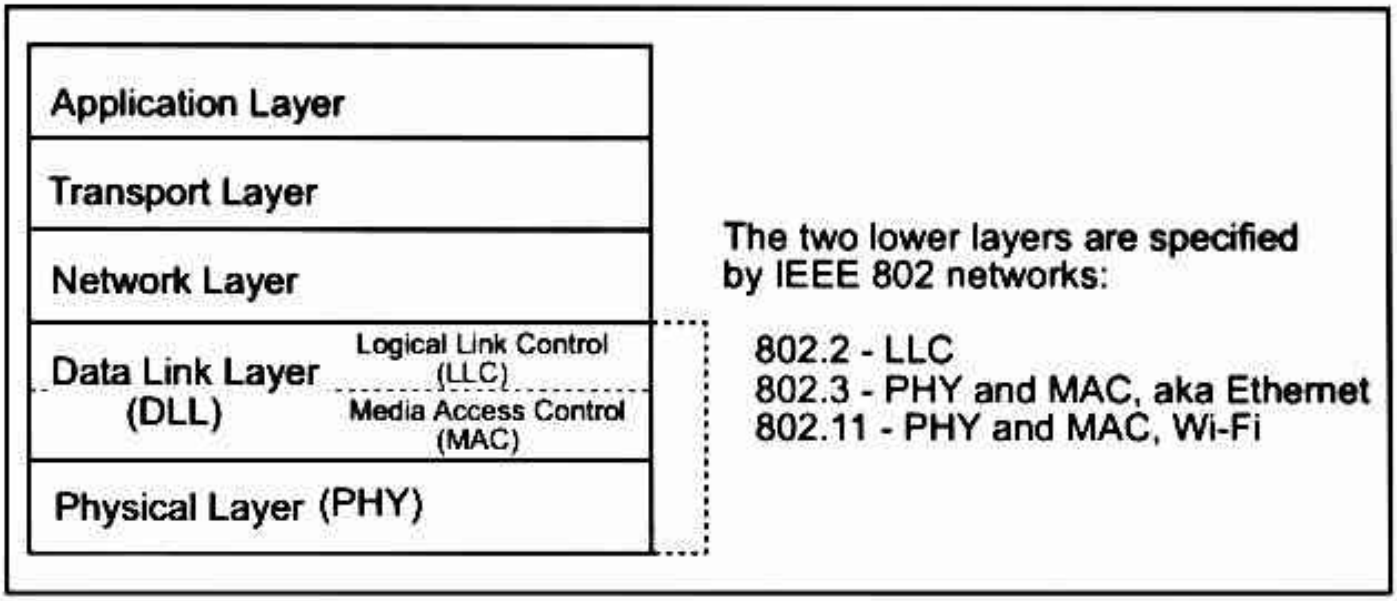
A BSS operating in ad-hoc mode is isolated. There is no connection to other Wi-Fi networks or to any wired LANs. Even so, the ad-hoc mode can be very useful in a number of situations. Because an ad-hoc network can spring up anywhere, it is especially useful in situations that demand a quick setup in areas that do not have any infrastructure, such as emergency sites and combat zones.

As another example of the usefulness of ad-hoc Wi-Fi, consider that it is now common for people to have their laptops with them in business meetings, in airports waiting for flights, or even at their local coffee hang-out. Operating in ad-hoc mode, people can easily and quickly form a network to do things like share large files or anything else they may want to do cooperatively.

2.2 Five-Layer TCP Model

802.11 and its extensions (a, b, g, etc.) define two layers in the five-layer TCP model: the physical layer and the data link layer. These are the same two layers that are defined by 802.3 (Ethernet). The data link layer is actually made up of two layers: media access control (MAC) and logical link control (LLC). The IEEE 802.11 specification defines the MAC sublayer.

Figure 2.6 5-Layer TCP Model



6.1. BLUE TOOTH

- Bluetooth is a wireless technologies and it is used for creating personal networks operating in the 2.4 GHz band. It can work within a range of 10 metres.
- In Bluetooth, networks are usually formed temporarily and the networks are formed with portable devices such as cellular phones, handhelds and laptops.
- Bluetooth technology provides higher level service profiles (i.e., sketch) e.g., FTP (file transfer protocol) like file servers, voice transport, *serial line emulation etc.
- **Bluetooth** is an open wireless technology standard for exchanging data over short distances (using short wavelength transmission). This all is done using fixed and mobile devices and this process ultimately creates personal area networks (PANs) with high level of security.

Name and Logo :

The word Bluetooth is an anglicised version of the Scandinavian Blatand. This technology was named after "King Harald Blatand". This technology aims to provide easy connectivity to complex appliances with the workspace of an individual.

Implementation

- Bluetooth uses a radio technology called ****frequency-hopping spread spectrum**. It basically chops (i.e., runs) up the data and transmits blocks of it on up to 79 bands (1 MHz each) in the range 2402-2480 MHz.
- Bluetooth technology basically operates in type 2.4 GHz Industrial, Scientific and Medical (ISM).
- Each Bluetooth radio channel has a 1 MHz bandwidth and channel hops at a rate approximately 1600 hops per second. In Bluetooth, transmissions are performed in 625 microseconds slots and a single packet is transmitted over a single slot.

For long distance communications, a user may occupy multiple slots using the same transmission frequency. This reduces the hopping rate below 1600 hops/second.

- Bluetooth provides a secure way to connect and exchange information between devices such as smart mobile phones, telephones, laptop, personal computers, printers, Global positioning system (GPS) receivers, digital cameras and video games.
- The bluetooth specifications are developed and licensed by the Bluetooth Special Interest Group (SIG). The Bluetooth SIG consists of more than 13000 companies in the area of telecommunication, computing, networking and consumer electronics.

Communication and Connection

- Bluetooth is a *packet-based protocol* with a master-slave structure. One master may communicate with upto seven slaves. All devices share the master's clock.
- Packet exchange is based on the basic clock, defined by the master and its clock is 312.5 μs.

---

* **Serial Line Emulation** : By providing serial-port emulation, RFCOMM supports legacy (i.e., virtual serial link created by the lower layers of the Bluetooth Protocol.

** **Frequency-hopping** : This is a form of CDMA where a digital code is used to continually change the carrier frequency.

In the simple case of single slot packets the master transmits in even slots and receive in odd slots. The slave receives in the even slots and transmits in the odd slots.

Packets may be 1, 3 or 5 slots long but in all cases the master will transmit in practice and it is based on low-cost transceiver microchips in each device. Table 6.1 shows Bluetooth range.

Table 6.1 : Bluetooth range

Class	Maximum Permitted Power		Range (Approximate)
	mw	dBm	
Class 1	100	20	~ 100 metres
Class 2	2.5	4	~ 10 metres
Class 3	1	0	~ 1 metre

In most cases the effective range of class 2 devices is extended if they connect to a class 1 transceiver. Table 6.2 shows Bluetooth version and data rate in the even slots and the slave transmits in odd slots.

Table 6.2 : Bluetooth version and data rate

Version	Data Rate
Version 1.2	1 Mbit/s
Version 2.0 + EDR	3 Mbit/s
Version 3.0 + HS	24 Mbit/s

The master chooses which slave device to address, typically, it switches rapidly from one device to another device in a round-robin fashion. Simultaneous transmission from the master to multiple other devices is possible via broadcast mode but this practice is not much in use.

Uses

(i) Bluetooth is a standard communication protocol and primarily it is designed for low power consumption.

(ii) Bluetooth is designed for short range (100 m, 10 m and 1 m). Table 6.1 shows Bluetooth range in metres.

List of Applications

(i) Wireless control of and communication between a mobile phone and a handsfree handset. This was one of the earlier because of which Bluetooth technology became very popular. Fig. 6.1 shows a typical Bluetooth mobile phone headset.

(ii) Wireless networking between PCs in a confined space where little bandwidth is required.

(iii) For controls where infrared was traditionally used. For low bandwidth applications where high USB bandwidth is not required and cable-free connection is required.

(iv) Wireless communication with PC input and output devices. The most common being the mouse, keyboard and printer.

Fig. 6.1 shows a typical Bluetooth mobile.

Fig 6.1 : A typical Bluetooth mobile phone headset.

(v) Transfer of files contacts details, calendar appointments and reminders between devices with OBEX.
(vi) Replacement of traditional wired serial communication in test equipment, GPS receivers, medical equipment, bar code scanners and traffic control devices.
(vii) For sending small advertisements from Bluetooth-enabled advertising hoardings to other discoverable and Bluetooth devices.
(viii) Wireless bridge between two industrial Ethernet (e.g., PROFINET) networks.
(ix) Short range transmission of health sensor data from medical devices to mobile phone set-top box or dedicated telehealth devices.
(x) Real-time location systems (RTLS) are used to track and identify the location of objects in real time using 'Nodes or Tags' attached or embedded in the objects.
(xi) Dial-up internet access on personal computers or PDA using a data capable mobile as a wireless modem like Novatelwiffi.

Bluetooth Devices

- Bluetooth exists in many devices, such as :
- i Pod Touch
- Lego Mindstorms NXT
- Play station 3
- PSP GO
- Telephones
- Modems
- Watches
- Bluetooth technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations.
- Blurmoth is commonly used to transfer data with telephones (i.e. ;with a bluetooth headset) or byte data with hand-held computers (transferring files).
- Bluetooth protocols simplify the discovery and setup of services between devices. Bluetooth can advertise all of the services they provide. This ultimately makes services easier, network address and permission configuration can be automated than with many other network types.
- Fig. 6.2 shows a Bluetooth USB dangle with a 100 m range.

Fig 6.2 : A Bluetooth USB dangle with a 100 m range.

Operating System Support

- Apple has supported Bluetooth since Mac OS X 10.2 and this was released in 2002.
- For Microsoft platforms, Windows XP service pack 2 and SP3 releases have native support for Bluetooth 1.1, 2.0 and 2.0 + EDR.
- Linux has two popular Bluetooth stacks, Bluez and Affix. The Affix stack was developed by NOKIA.
- The windows XP and windows Vista/windows 7 Bluetooth support the following Bluetooth for files:
- PAN
- SPP
- DUN
- HID
- HCR

5.15. Wi-Fi

- Wi-Fi is pronounced as *waifi* and it is a trademark of the Wi-Fi alliance (*i.e.*, federation).
- Initially, Wi-Fi was used in place of only the 2·4 GHz 802·11*b* standard. However, the Wi-Fi was expanded to include any type of network or WLAN product based on any of the 802·11 standards.
- The federation has enforced its use to describe only a narrow range of connectivity technologies and that includes wireless local area network (WLAN). It is based on the IEEE 802·11 standards.
- It basically includes device to device connectivity such as Wi-Fi peer to peer AKA Wi-Fi Direct.
- It supports a range of technologies that support PAN, LAN and even WAN connections.
- The technical term "IEEE 802·11" has been used interchangeably with Wi-Fi. Wi-Fi is used by over 700 million people and these are over 750,000 places with Wi-Fi connectivity around the world. These are about 800 million new Wi-Fi devices every year.
- Wi-Fi certified and compliant (obedient) devices are installed in may personal computers, video games, MP3 players, printers and laptop computers.
- The term Wi-Fi means *Wireless fidelity*. The Wi-Fi initially was used advertising slogan but later this phrase was removed from the market.

Uses of Wi-Fi

Wi-Fi system has various uses and let us discuss the same :

(i) **Internet Access** : A Wi-Fi enabled device such as personal computer, video game, smart phone and digital audio player etc. can connect to the internet when they are in the range of a wireless network.

- The coverage area of one or more (interconnected) access points called *hotspots* can comprise (*i.e.*, to reduce) an area as small as a few rooms or as large as many square miles. However coverage in the larger area may depend on a group of access points. Wi-Fi technology has been used in wireless mesh network. For example, it is used in London, U.K etc.
- Wi-Fi can be used at organizations and businesses *e.g.*, airports, hotels and restaurants.
- Routes often set up in homes and other premises provide internet access and internetworking to devices connected by wirelessly to them.

- It is also possible to connect Wi-Fi devices in ad-hoc (i.e., temporary) mode for client-to-client connections without a router.
- Wi-Fi can also connect places that would traditionally not have network access, for example bathroom, kitchens and garden sheds.

(ii) **City-wide Wi-Fi** : In the early 2000s, many city around the world announced plans for city-wide Wi-Fi networks.

- In 2005, Sunnyvale, California became the first cities in the united states to offer city-wide free Wi-Fi.

(iii) **Campus-wide Wi-Fi** : Drexel University in Philadelphia was the first university in the United States to offer completely wireless Internet access across the entire campus in 2000.

(iv) **Direct Computer-to-Computer Communication** : Wi-Fi also allows communications directly from one computer to another computer without the involvement of an access point. This technique is called **ad-hoc mode** of Wi-Fi transmissions.

- Wireless *ad-hoc network* is very popular in multiplayer handheld game, digital cameras and other consumer electronics devices.
- Wi-Fi technology also promotes a pending specification called **Wi-Fi Direct** and this is used for file transfers and media sharing through a new discovery-and security-methodology.

(v) **Future Directions** : Wi-Fi technology in 2010 has spread very widely within business and industrial uses.

- Wi-Fi access points provides fast roming, increased overall network-capacity and network redundancy (i.e., unwanted). This all is obtained by using more channels or by defining smaller cells.
- Wi-Fi also enables wireless voice-applications (VOWLAN or WVOIP).
- Over the years Wi-Fi has been shifted using toward **"Thin access points"**. This process provides more network intelligence and outdoor applications may utilize *mesh topologies*.

Limitations

Spectrum assignments and operational limitations do not operate Wi-Fi system consistently worldwide. Wi-Fi signal actually occupies five channels in the 2·4 GHz band and resulting only three non-overlapped channels in the U.S. (1, 6, 11) and three or four in Europe (1, 5, 9, 13).

Isotropically radiated power (EIRP) is limited to 20dBm (100 mW).

(i) **Reach** : Wi-Fi has limited range. A typical wireless router using 802·11*b* or 802·11*g* with a stock antenna might have a range of 32 m (120 ft) indoors and 95 m (300 ft) outdoors.

- The IEEE 802·11*n* however, can exceed the range by more than two times and range varies with frequency band.
- Wi-Fi in the 2·4 GHz frequency block has slightly better range than Wi-Fi in the 5 GHz frequency block.
- Out door ranges through use of directional antenna can be improved with antennas located several kilometres.
- Technologies such as Bluetooth provide a much shorter propagation of < 10 m.

(ii) **Mobility** : Mobile use of Wi-Fi over wider range is limited *i.e.*, use in an automobile moving from one hotspot to another, known as **Wardriving**.

• Fig. 6.3 shows other wireless technologies are more suitable.

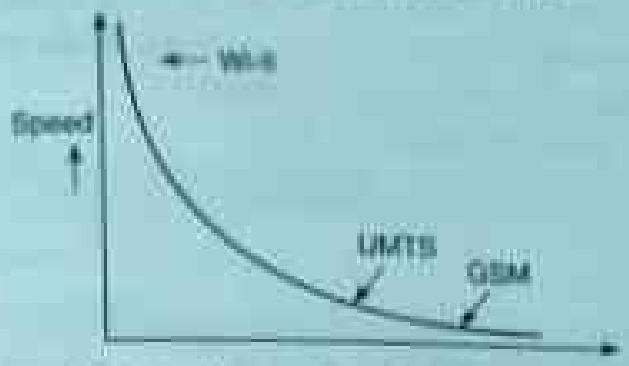


Fig 6.3 : Speed vs mobility of wireless system.

(iv) **Data Security Risks** : Wired Equivalent Privacy (WEP) are easily breakable when correctly configured.

• Wi-Fi Protected Access (WPA 1 and WPA2) solved this problem privacy. But Wi-Fi access typically default to an *encryption-free* (open) mode. This mode does not enable any wireless security *i.e.*, provides open wireless access to a LAN.

• However, such networks may use other means of protection, such as a virtual private network or secure Hypertext Transfer protocol (HTTPS) and Transport Layer Security.

(v) **Population** : On initial startup, many 2·4 GHz 802·11 b and 802·11g access-points default to the same channel. This creates the problem of congestion on certain channels.

• To change the channel of operation for an access point there is requirement to configure device.

(vi) **Channel Population** : Wi-Fi pollution or an excessive number of access points in the area, especially on the same or neighboring channel, can prevent access and also interfere with other devices.

• Channel population problem arises in the 802·11 *g* / *b* spectrum and it is due to reduction in signal to noise ratio. This problem is more in large apartment complexes or office buildings.

• Other devices, such as microwave ovens, security cameras, Blue tooth devices use 2·4 GHz band and these devices can create additional interference.

(iv) **RFID** : The word RFID means Radio-frequency identification. This technology uses communication via electromagnetic waves to exchange data between a terminal and an object. Object may be a product, animal or person.

• RDFI process is used for the purpose of identification and tracking. Some tags can be read from several metres away and beyond the line of sight of the reader.

• Radio-frequency identification process involves *interrogators* (also known as *readers*) and tags (also known as **labels**).

• Most Radio-frequency identification tags contain at least two parts. One of these two parts is an *integrated circuit* and this is used for *processing information, modulating* and *demodulating* a radio-frequency. The other part is an antenna and it is used for receiving and transmitting the signal.

There are three types of RFID tags :

(i) Passive RFID tags

(ii) Active RFID tags

(iii) Battery assisted passive (BAP) RFID tags

(i) **Passive RFID Tags** : These tags do not have power source and require an external electromagnetic field to initiate a signal transmission.

(ii) **Active RFID Tags** : These tags contain a battery and can transmit signals once an external source (interrogator) has been successfully identified.

(iii) **Battery Assisted Passive (BAP) RFID Tags :** These tags require an external source to wake up but these have significant higher forward link capability and helps to cover longer range.

There are a variety of groups which define standards and regulate the use of RFID and these are :

- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)
- ASTM International
- DASH7 Alliance
- EPC Global

RFID has many applications e.g., it is used in enterprise (businees firm) supply chain management to improve the efficiency of inventory tracking and management.

Current Uses

There are three main factors which have increased the usage of RFID and these are :

- Decrease cost of equipment and tags
- Increased performance to a reliable 99%
- Stable international standard around UHF
- In 2010 in Orlando, 16 active projects are being conducted by ODIN technologies, IBM and CSC these two application are passive UHF RFID.

School and Universities

- RFID card system is used to check in and out of the school/building via a specially designed cards.
- Some school use RFID in IDS for borrowing books. Schools have RFID in ID scanner for buying items at a school shop and canteen, Library and also to sign in and sign out for student and teacher's attendance.

Museums

- RFID technologies are now also implemented in end-user application in museums e.g., the custom-designed temporary research application.
- A visitor entering the museum receives an RF tag that is carried as a card. The expert system enables the visitor to receive information about specific exhibits.

Social Retailing

RFID technology is also used in social retailing. For example when customer enters a dressing rooms, the mirror reflects their image and also images of the item being worn by celebrities on an interactive display.

A web cam also projects an image of the customer wearing the item on the website for everyone to see. This creates an interaction between the customers inside the store and their social network outside the store. The technology used in this system is an RFID interrogator mounts in the dressing room and electronic product code RFID tags on the item.

Potential Uses

RFID can be used in a variety of applications such as :

(i) Access management

(ii) Tracking of goods and RFID in retail

(iii) Tracking of persons and animals