ENGINEERING @ SP

SP Singapore Polytechnic

ET1205

WIRELESS TECHNOLOGY APPLICATIONS

(Version 2.0)

School of Electrical & Electronic Engineering

Engineering @ SP

The Singapore Polytechnic's Mission

As a polytechnic for all ages
we prepare our learners to be
life ready, work ready, world ready
for the transformation of Singapore

The Singapore Polytechnic's Vision

Inspired Learner. Serve with Mastery. Caring Community.

A caring community of inspired learners committed to serve with mastery.

The SP CORE Values

- Self-Discipline
- Personal Integrity
- Care & Concern
- Openness
- Responsibility
- Excellence

For any queries on the notes, please contact:

Name: **Melvyn U Myint Oo**
Room: **T16620**
Email: **Melvyn_oo@sp.edu.sg**
Tel: **68790688**

SP Singapore Polytechnic

SP | SCHOOL OF ELECTRICAL & ELECTRONIC ENGINEERING

Industry-Collaborated TECH HUB

Diploma in Aerospace Electronics

Aerospace Engineering Hub

Themed Project : Unmanned Aircraft Applications
Facilities : A320 Flight Simulator
Industries : Aerospace, Air Transport

Industry Partners : AIRBUS, Rolls-Royce

Industry Co-location Lab : ST Engineering Aerospace

Diploma in Computer Engineering

5G & AIoT Technology Hub

Themed Project : Smart Facility Management
Facilities : AIoT Nerve Centre, 5G Garage
SP Connected Solutions Lab
Industries : ICT & Media, Smart City

Industry Partners : ADVANTECH, CONTEC, D'CRYPT, ENVISION, HUAWEI, LINGJACK DIGITAL, unabiz

Industry Co-location Lab : BOSCH Invented for life, ERICSSON, Singtel

Diploma in Engineering with Business

Technology to Business Hub

Themed Project : Technology To Business Venture
Facilities : IdeaBox, T2B Hub
Industries : Entrepreneurship & Start-up

Industry Co-location Lab : SPgroup, GEX VENTURES

APOL, BevEat, BitsGreat, MEMORY ARK, OCTOPUS8, Trackdat, REAL IMPACT, SMARTDB, TOP TASTE, Vaster

Diploma in Electrical & Electronic Engineering

Robotics, Automation & Control Hub

Themed Project : Smart Workflow Solution for I4.0
Autonomous Mobile Robot/Robocup
Facilities : SP-SICK Smart Sensor Lab, SP-Rexroth I4.0 Innovation Lab
Industries : Logistics, Electronics (Manufacturing), Electronics & Chemicals (Manufacturing)

Industry Partners : ABB, BECKHOFF, SEW EURODRIVE, Weidmüller, ZEBRA

Industry Co-location Lab : rexroth A Bosch Company, SICK Sensor Intelligence.

Power & Sustainable Energy Hub

Themed Project : Net-zero Renewable Energy Vertical Farming
Facilities : High Voltage Training, LE & LET Training, Energy Efficiency Lab
Industries : Energy & Power

Industry Partners : CHNT, ebmpapst, sembcorp, SUNLIGHT A CHNT COMPANY

Semicon & Electronics Hub

Themed Project : Artificial Intelligence of Things using FPGA
Facilities : Nanofab & IC Design Labs, Infineon Innovation Lab
Industries : Semiconductor & Electronics

Industry Partners : SSIA

Industry Co-location Lab : ADVANTEST, Infineon

Biomedical Engineering Hub

Themed Project : Engaging Rehabilitation with Data Visualisation & Analytics
Facilities : Biomedical Engineering Lab
Industries : Healthcare

Industry Partners : GE Healthcare, GOLD LITE, Khoo Teck Puat Hospital, NATIONAL INSTRUMENTS

Autonomous & Transportation Systems Hub

Themed Project : 5G-enabled Autonomous Safety Vehicle
Autonomous Underwater Vehicle
Facilities : RSS Lab for RTT Training, Siemens Digital Experience Centre,
SP-TIBCO Adv Mfg Analytics Lab
Industries : Smart Transport, Land Transport

Industry Partners : ST Engineering Land Systems, SMRT, SIIX, SUTD, GreenPower

Industry Co-location Lab : SIEMENS Ingenuity for life, TIBCO

CONTENTS		
		Page
	Module Overview	ModuleOverview – Page 1
Chapter	**Chapter Title**	
1	Understand the development of wireless technologies	Chapter1 Page 1 to Chapter1 Page 20
2	Understand RFID (Radio Frequency Identification) Technology	Chapter2 Page 1 to Chapter2 Page 20
3	Understand Wireless Local Area Network technology	Chapter3 Page 1 to Chapter3 Page 19
4	Understand Wireless Personal Area Network	Chapter4 Page 1 to Chapter4 Page 21
5	Understands Wireless Wide Area Network	Chapter5 Page 1 to Chapter5 Page 24
6	5G Radio Access Technologies	Chapter6 Page 1 to Chapter6 Page 11
7	Building a Wireless Infrastructure for Business	Chapter7 Page 1 to Chapter7 Page 9
	Laboratory Experiments	Lab1 to Lab7

MODULE OVERVIEW

1. Introduction

Wireless Technology Applications is a third year module for DEB/DES.

2. Module Aims

The aim of this module is to introduce the students to the basic knowledge of Wireless Technologies. It will focus on the system aspect of the local area network, wide area network, personal area network and their applications.

LECTURE NOTES

Chapter 1: Understand the development of wireless technologies

Learning Objectives

- Explain "What is wireless technology?"
- Understand the electromagnetic waves and spectrum
- Explain the radio frequency fundamentals
- List the components of wireless communication system
- Understand the basics of radio frequency transmission, modulation and multiple access techniques
- Describe examples of wireless technologies and discuss applications associated with them
- Explain the advantages and disadvantages of wireless technologies

Section 1.1: What is wireless technology?

In 1895, Guglielmo Marconi succeeded in sending wireless signals over a distance of one and a half miles at his father's estate in Pontechio, Italy. The following year, he demonstrated his system in London, England and was granted the world's first patent for a system of wireless telegraphy. With his discovery, it opened up a new technology that has become a very important industry today. (Marconi was awarded the Nobel Prize for Physics in 1909 for his discovery of radio waves.)

According to Whatis website, *wireless technology* is a term used to describe telecommunications in which electromagnetic waves carry signal over part or all of the communication path. Due to different requirements for different types of information like voice, data and video, many wireless technologies have emerged over the past years to provide efficient, convenience and low cost solution for the mass market. Also, these wireless technologies have also been designed for different coverage areas and usage models.

In this module, we will concentrate on the applications of wireless technologies that are used for Personal Area Network (PAN), Local Area Network (LAN), Metropolitan Area Network (MAN) and Wide Area Network (WAN) for Mobile Communication System.

SAQ 1-1: Who has discovered the radio waves in 1895?
SAQ 1-2: Which physical phenomenon has been discovered by Guglielmo Marconi in 1895?

Section 1.2: The electromagnetic waves and spectrum

The fundamental of wireless technologies is the use of electromagnetic waves as data carrier to transmit information. In this section, we will study Radio Frequency (RF) which is the portion of electromagnetic spectrum that can be generated by feeding alternating current to an antenna. This electromagnetic spectrum has been divided into 12 bands based on carrier frequencies and they are used for different applications, as shown in Table 1.1 below.

Band name	ITU band	Frequency and Wavelength	Application
ELF	1	3-30 Hz 100,000 km - 10,000 km	
SLF	2	30-300 Hz 10,000 km - 1000 km	Communication with submarines
ULF	3	300-3000 Hz 1000 km - 100 km	
VLF	4	3-30 kHz 100 km - 10 km	Submarine communication, avalanche beacons wireless heart rate monitors
LF	5	30-300 kHz 10 km - 1 km	Navigation, time signals, AM longwave broadcasting
MF	6	300-3000 kHz 1 km - 100 m	AM broadcasting (540 - 1600 kHz), civil defence, amateur radio
HF	7	3-30 MHz 100 m - 10 m	Shortwave broadcasts, amateur radio, mobile radio, military communication
VHF	8	30-300 MHz 10 m - 1 m	VHF television, FM radio, air traffic control, taxicab, police, navigational aids, pagers
UHF	9	300-3000 MHz 1 m - 100 mm	UHF-TV, space telemetry, radar, military, CB radio, cellular phone, Bluetooth, Wireless LAN
SHF	10	3-30 GHz 100 mm - 10	Mobile phones (W-CDMA), WLAN, WiMAX, most modern Radars (airborne, approach, surveillance and weather), satellite and space communication, common carrier microwave relay
EHF	11	30-300 GHz 10 mm - 1 mm	WiMAX, Radio astronomy, high-speed microwave radio relay, radio service, radar landing system, experimental systems
Ultraviolet visible infrared		Above 300 GHz < 1 mm	Optical communication links (mainly used for telephony and data transmission)

Table 1.1: Radio frequency spectrum

As you can observed in Table 1.1, Radio Frequency Identification (RFID) uses LF (Low Frequency), HF (High Frequency), UHF (Ultra High Frequency) and SHF (Super High Frequency) spectrum; Bluetooth uses UHF (Ultra High Frequency) spectrum and Wireless LAN uses UHF and SHF (Super High Frequency). There are some unique characteristics associated with each RF spectrum.

For ELF (Extremely Low Frequency), SLF (Super Low Frequency, ULF (Ultra Low Frequency) and VLF (Very Low Frequency), the signal attenuation is minimal since in general, signal attenuation increases when the frequency increases. As such, these frequencies can be used to reach areas within a radius of over 1000 km continuously at a low technical cost. These frequencies usually travel along the surface of the Earth and is known as ground waves.

For frequencies in the range below HF, it can be refracted and reflected by the atmosphere. The maximum frequency at which refraction and reflection can occur is known as Maximum Usable Frequency (MUF) and is generally in the range of 10 to 15 MHz. These frequencies are usually known as sky waves since they are returned to Earth from the upper atmosphere.

For VHF, UHF and SHF, they are usually not reflected by the ionosphere, which is the part of the atmosphere that is ionized by solar radiation. Thus, in normal practice, such very short waves are received only within line-of-sight distances. They are known as space waves since they travel only in straight paths. As the frequency increases beyond 30 GHz (EHF and beyond), it may be absorbed selectively by the water vapours present in a clear atmosphere.

SAQ 1.3: What is the name given to frequency band that occupies the 300-3000 Hz?
SAQ 1.4: Which frequency band is used in WLAN?

Section 1.3: The radio frequency fundamentals

1.3.1 Frequency, period and phase

1.3.1.1 Frequency

Frequency is the number of occurrences of a repeating event per unit time. The frequency is usually denoted as *f*. In SI units, the unit of frequency is hertz (Hz), named after the German physicist Heinrich Hertz.
For example, 1 Hz means that an event repeats once per second.

1.3.1.2 Period

The **period** is the duration of one cycle in a repeating event, so the period is the reciprocal of the frequency.

The period is usually denoted as *T*, and is the reciprocal of the frequency *f*: The SI unit for period is the second.

$$T = \frac{1}{f}$$

where T = period in second
f = frequency in Hz

1.3.1.3 Phase

The phase describes the point in time which the signal has advance in its cycle. The phase is identified at the beginning of the cycle.

For an example, a sine wave can be represented as:

$v(t) = V_p \sin(2\pi ft+\theta)$

where v(t) = instantaneous voltage amplitude
V_p = peak voltage amplitude
f = frequency
θ = phase

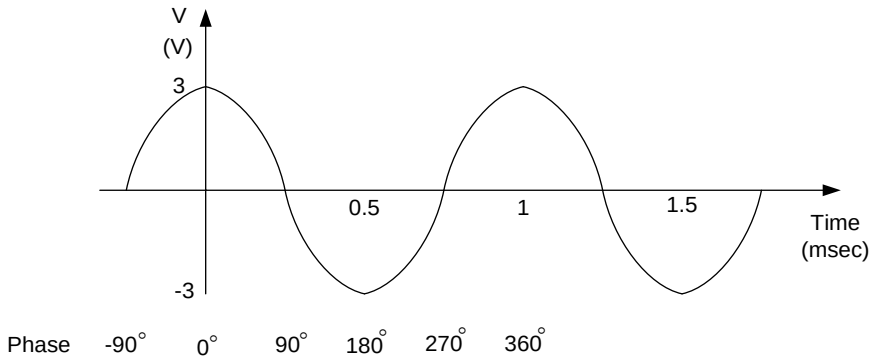


Figure 1-1: A sine wave signal

SAQ 1.5 What are the values of amplitude, frequency and phase of the voltage signal given in Figure 1-1

V_p = _____ V, f = _____ Hz and θ = _____ °

SAQ 1.6 Write the equation of the above voltage signal.

v(t) = _____

SAQ 1.7 What is the period of the above voltage signal?

T = _____ msec

1.3.2 Bandwidth

Bandwidth is typically measured in hertz, and may sometimes refer to *passband bandwidth*, sometimes to *baseband bandwidth*, depending on context. **Passband bandwidth** is the difference between the upper and lower cutoff frequencies of, for example, an electronic filter, a communication channel, or a signal spectrum.

For example, if the lowest frequency a channel can transmit is f_L and the highest is f_H then the bandwidth is the difference between the highest and lowest frequencies:

$BW = f_H - f_L$

where BW is the channel bandwidth in Hz

f_L is the lowest frequency in Hz,

f_H is the highest frequency in Hz.

In case of a lowpass filter or baseband signal, the bandwidth is equal to its upper cutoff frequency. The term **baseband bandwidth** refers to the upper cutoff frequency. In practical, the larger the signal bandwidth will require the larger the channel bandwidth.

SAQ 1. 8 If the lower and upper cutoff frequencies of a telephone line are 300 Hz and 3,400Hz, respectively, what is the bandwidth of this telephone line?

SAQ 1.9 The frequency range of a natural voice for a person is from 100 Hz to 10 kHz. What is the approximate signal bandwidth of this voice signal?

SAQ 1.10 The video signal bandwidth of an image is 5MHz and the hi-fi music signal bandwidth is 20kHz. Which of the above systems is required a larger channel bandwidth to transmit from one point to another?

1.3.3 Decibel (dB)

The **decibel** (**dB**) is a logarithmic unit of measurement that expresses the magnitude of a physical quantity (usually power or intensity) relative to a specified or implied *reference level*. Since it expresses a ratio of two quantities with the same unit, it is a dimensionless unit.

When referring to measurements of *power* or *intensity*, a ratio can be expressed in decibels by evaluating ten times the base-10 logarithm of the ratio of the measured quantity to the reference level. Thus, if L represents the ratio of a power value P_1 to another power value P_2, then L_{dB} represents that ratio expressed in decibels and is calculated using the formula:

$$L_{dB} = 10 \log_{10}\left(\frac{P_1}{P_2}\right)$$

Naturally, P_1 and P_2 must have the same dimension (that is, must measure the same type of quantity), and must as necessary, be converted to the same units before calculating the ratio of their numerical values: however, the choice of scale for this common unit is irrelevant, as it changes both quantities by the same factor, and thus cancels in the ratio (the ratio of two quantities is scale-invariant). Note that if $P_1 = P_2$ in the above equation, then $L_{\text{dB}} = 0$. If P_1 is greater than P_2 then L_{dB} is positive; if P_1 is less than P_2 then L_{dB} is negative.

Rearranging the above equation gives the following formula for P_1 in terms of P_2 and L_{dB}:

$$P_1 = 10^{\frac{L_{dB}}{10}} P_2$$

The unit Decibel is a logarithmic unit. The basic measure of the gain or loss of a communication component is based on the decibel (dB) which is defined as the logarithmic ratio of the two powers:

$$\text{Gain(or loss)dB} = 10\log_{10}\left(\frac{\text{P}_1}{\text{P}_2}\right)$$

For example, it input power is 1 watt and output power is doubled,

$$\text{Power Gain} = \frac{2}{1} = 2$$

$$\text{Or} \quad G_{dB} = 10\log_{10} 2 = 3.01\text{dB}$$

i.e. a gain of 2 times in power is equivalent to 3 dB.

Similarly, a power gain of 100 is equivalent to 20 dB.

One reason for using the decibel is that the overall gain of a system can be easily calculated if the individual component gains or losses are known.

Consider the system shown in Figure 1-2:

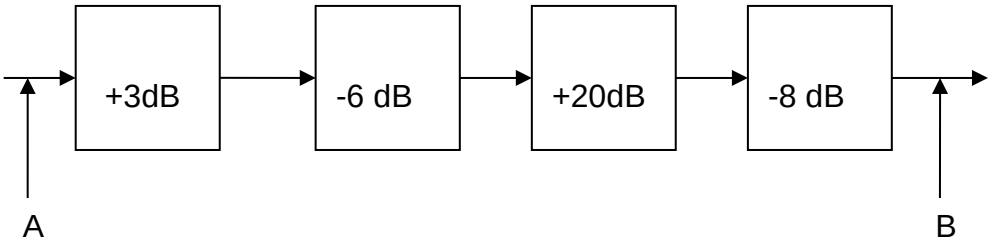


Figure 1-2: Block diagram of a communication system

The overall system gain from A to B is:

G_{Total} = +3dB + (-6dB) + (20dB) + (-8dB) = 9 dB

The decibel symbol is often qualified with a suffix, which indicates which reference quantity or frequency weighting function has been used. For example, "dBm" indicates that the reference quantity is one milliwatt while "dBμV" is referenced to 1μV.

SAQ 1.11 A wireless system was shown in Figure 1-3. Calculate the received signal at the receiver.

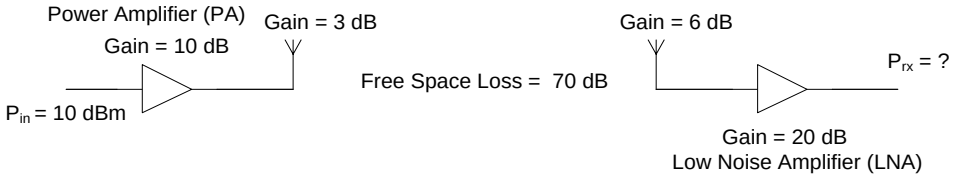


Figure 1-3: Wireless communication system

1.3.4 Effect of radio wave propagation

1.3.4.1 Reflection

Electromagnetic waves are one of the best known and most commonly encountered forms of radiation that undergo reflection. Reflections off near-by objects (e.g. ground, buildings, trees, etc) can lead to multipath signals of similar signal power as the direct signal. This can result in deep nulls in the received signal power due to destructive interference.

1.3.4.2 Attenuation

Attenuation is the drop in the signal power when transmitting from one point to another. Attenuation can be caused by a variety of factors. It can be caused by the transmission path length, obstructions in the signal path, and multipath effects. Objects in the path of the signal generally cause the most attenuation. Man-made objects, such as walls and buildings, can decrease the strength of a signal. Figure 1-4 shows some of the radio propagation effects that cause attenuation. Any objects that obstruct the line of sight signal from the transmitter to the receiver can cause attenuation.

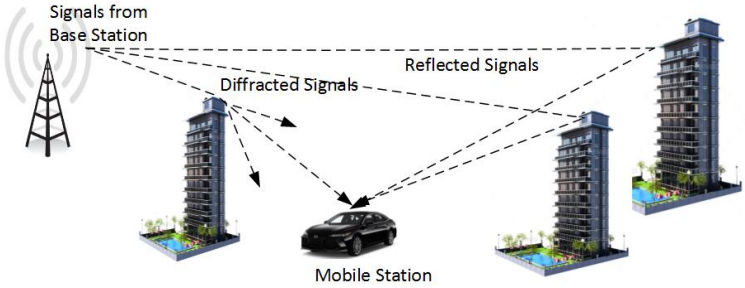


Figure 1-4: Radio propagation effects

Table 1.2 shows examples of different building materials and their effect on radio transmissions.

Type of Material	Use in a Building	Impact on Radio Waves
Wood	Office partition	Low
Plaster	Inner walls	Low
Glass	Windows	Low
Bricks	Outer walls	Medium
Concrete	Floors and outer walls	High
Metal	Elevator shafts and cars	Very High

Table 1.2

1.3.4.3 Multi-path effects

As a radio signal is transmitted, the electromagnetic waves spread out. Some of these waves may reflect off distant surfaces and continues and continue toward the receiver. This results in the same signal being received not only from several different directions but also at different times, since it takes longer for the wave that bounced off a distant surface to reach the receiver. This phenomenon is known as multipath distortion. Multipath distortion can cause reduction in the signal strength of the signal and prevent receiver from picking up a signal strong enough for reliable reception. Multipath distortion gets its name from the fact that as waves arrive at different times and therefore out of phase with one another, the resulting signal at the input of the receiver gets distorted since the amplitudes of both signals get added to each other or subtracted from one another.

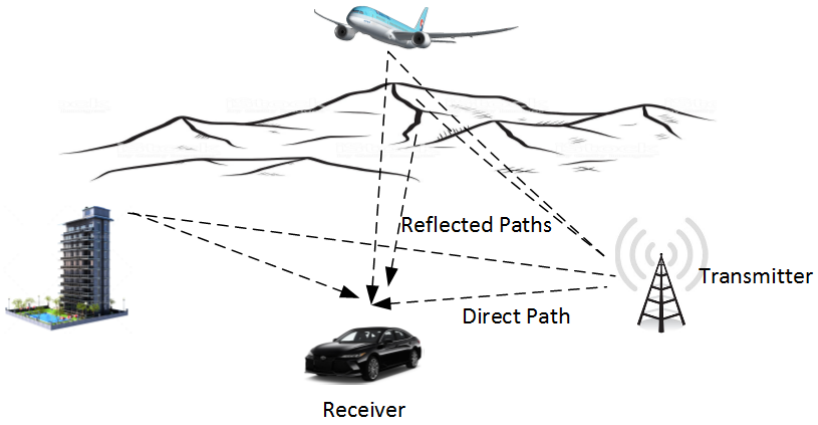


Figure 1-5: Multi-path phenomenon

1.3.4.4 Noise and signal-to-noise ratio (SNR)

The channel or transmission path will always experience some impairments or interference, called noise.

In both analog and digital electronics, noise or signal noise is an unwanted random addition to a wanted signal; it is called noise as a generalisation of the audible noise heard when listening to a weak radio transmission. Signal noise is heard as acoustic noise if played through a loudspeaker; it manifests as 'snow' on a television or video image.

Electronic noise exists in all circuits and devices as a result of thermal noise, also referred to as Johnson Noise. Semiconductor devices can also contribute flicker noise and generation-recombination noise. In any electronic circuit, there exist random variations in current or voltage caused by the random movement of the electrons carrying the current as they are jolted around by thermal energy. Lower temperature results in lower thermal noise. This same phenomenon limits the minimum signal level that any radio receiver can usefully respond to, because there will always be a small but significant amount of thermal noise arising in its input circuits. This is why radio telescopes, which search for very low levels of signal from stars, use front-end low-noise amplifier circuits, usually mounted on the aerial dish, and cooled with liquid nitrogen.

The thermal noise depends on the bandwidth of the system and its temperature. It can be calculated by using the following equation.

$P_n = kT_O B$ Watts

where T_O, temperature of the system at 290°K

B, bandwidth of the system in Hz

k, Boltzmann constant in J/°K (=1.38×10^{-23})

The signal-to-noise ratio (SNR) is an important parameter associated with the channel. SNR defines the ratio of the signal power to the noise power at a specific point in a data communication system.

$$\text{SNR} = \frac{\text{Signal Power, } P_S \text{ at a point in a communication system}}{\text{Noise Power, } P_n \text{ at a point in a communication system}}$$

It may also be defined in decibels, i.e.

$$\text{SNR(dB)} = 10\log_{10}\text{SNR} = 10\log_{10}\left(\frac{P_s \text{ (in Watts)}}{P_n \text{ (in Watts)}}\right)$$

A **high SNR** means that **the signal power relative to the noise interference is high** and will result in a **good quality signal** received.

It can also be used to compare noise performance between different systems.

Section 1.4 Components of wireless communication system

Figure 1.6 below shows the block diagram of a Wireless Communication System.

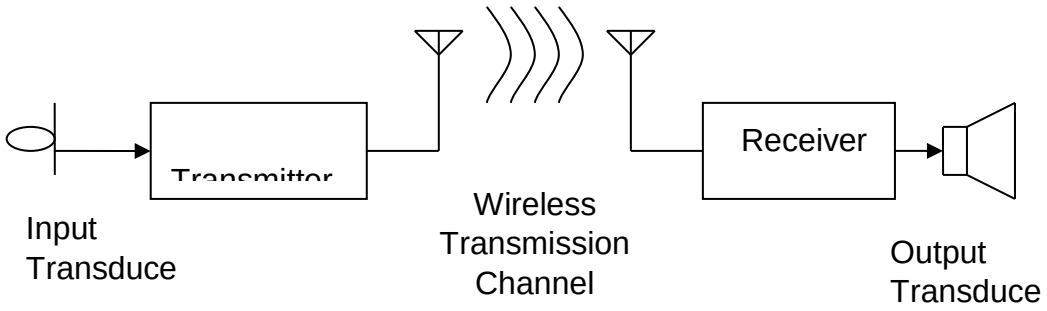


Figure 1-6: Block diagram of a Wireless Communication System

1.4.1 Input Transducer

Since we are dealing with electronic communication systems, the original information must be converted to electrical energy prior to transmission.
This is achieved by a suitable transducer – a device that converts energy from one form to another. The input transducer in an electronic communication system therefore converts other forms of energy into electrical energy.

Two examples of input transducers are:

(a) a microphone which converts sound energy to electrical energy,
(b) a video camera which converts light energy to electrical energy.

1.4.2 Transmitter

It converts the electrical signal into a form suitable for transmission through the channel. It may perform functions like modulation and amplification of the signal from the transducer.

1.4.3 Antenna

For an RF signal to be transmitted or received, the transmitter or receiver must always be connected to an antenna. Figure 1-7 illustrates the symbol for antennas. When a current flows through a conductor, an electromagnetic field is generated around the conductor. If the current is an ac signal, the electromagnetic field can travel away from the conductor and become a radio wave. A transmitting antenna is therefore easily formed by sending an ac signal to a conductor. How far the wave travels depend on many factors, such as the **length of the conductor** and **magnitude of transmit power**.
When the electromagnetic field or radio wave cuts another conductor, a current is induced in that conductor. A receiving antenna is easily formed by sticking into the air and intercepting the radio wave. The shape of the induced waveform is the same as the current sent through the transmitting conductor. The magnitude of the induced current depends on many factors, such as the length of the intercepting conductor and the distance from the transmitting conductor.

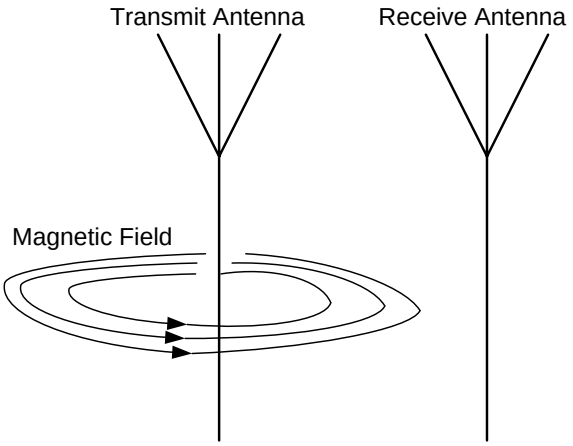


Figure 1-7: Tx and Rx Antennas

1.4.4 Transmission Channel

This is the path or connection between transmitter and receiver. It may be wired for example a pair of wires, coaxial cable, optic fibre or wireless (radio wave, infra-red).
Regardless of type, all transmission media are characterized by attenuation i.e. progressive decrease of signal power with distance.

1.4.5 Receiver

The function of the receiver is to extract the desired signal from the channel and deliver it to the output transducer. It may perform functions like tuning, amplification and demodulation.

1.4.6 Output Transducer

It converts the received electrical signal to another form of energy.
Two examples of output transducers are

(a) a speaker which converts electrical to sound energy
(b) a cathode ray tube (CRT), LCD or Plasma Screen which converts electrical energy to light energy.

Section 1.5: Basics of radio frequency transmission, modulation and multiple access techniques

1.5.1 Mode of transmission

In most wireless communications systems, data must flow in both directions between transmitter and receiver. The flow must be controlled so that the sending and receiving devices know when data will arrive or when it needs to be transmitted. There are three types of data flow: simplex, half-duplex and full-duplex.
Simplex transmission occurs in only one direction, from device 1 to device 2, as seen in Figure 1-8. A broadcast radio or television station is an example of simplex transmission.

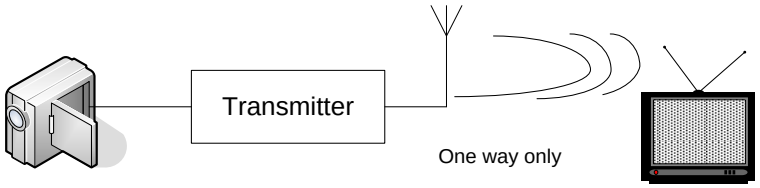


Figure 1-8: Example of Simplex Communication

Half-duplex transmission sends data in both directions, but only on way at a time, as seen in Figure 1-9. Half-duplex transmission is used in consumer devices such as citizens band (CB) radios or walkie-talkies. In order for User A to transmit a message to User B, he must hold down the "talk" button while speaking. While the button is being press, User B can only listen and not talk. User A must release the "talk" button before User B can press his "talk" button. Both parties can send and receive information, but only one at a time.

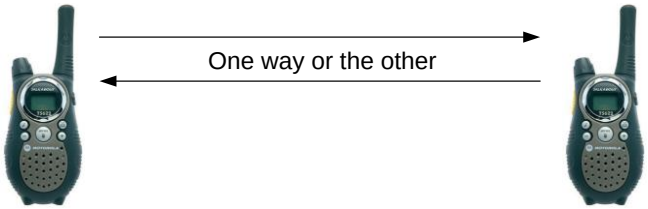


Figure 1-9: Example of Half Duplex Communication
Full-duplex transmissions allow data to flow in both directions simultaneously, as seen in Figure 1-10. A telephone system is an example of a type of full-duplex transmission. Both

parties o a telephone call can speak at the same time and they are able to hear each other. Most modern wireless systems such as cellular telephone use full-duplex transmission.

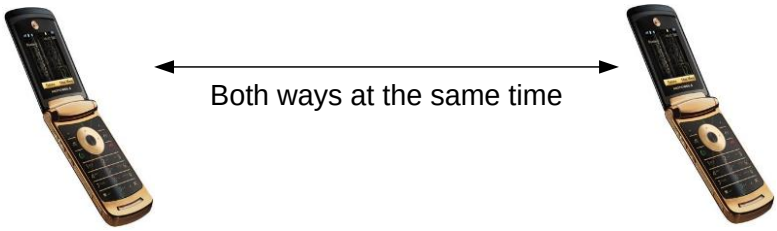


Figure 1-10: Example of Full Duplex Communication

1.5.2 Modulation

Analog modulation

The carrier signal sent in analog radio transmission in simply a continuous electrical signal. Analog modulation is the representation of analog information by an analog signal. There are three types of modulation that can be applied to an analog signal to enable to it to carry information: the high of the signal, the frequency of the signal, and the relative starting point of, or phase of the signal. Examples of analog modulation techniques are:

(i) Amplitude Modulation (AM)
(ii) Frequency Modulation (FM)
(iii) Phase Modulation (PM)

Figure 1-11 shows the amplitude modulated carrier signal in which the amplitude of the carrier was proportionally being changed with respect to the amplitude of an information signal.

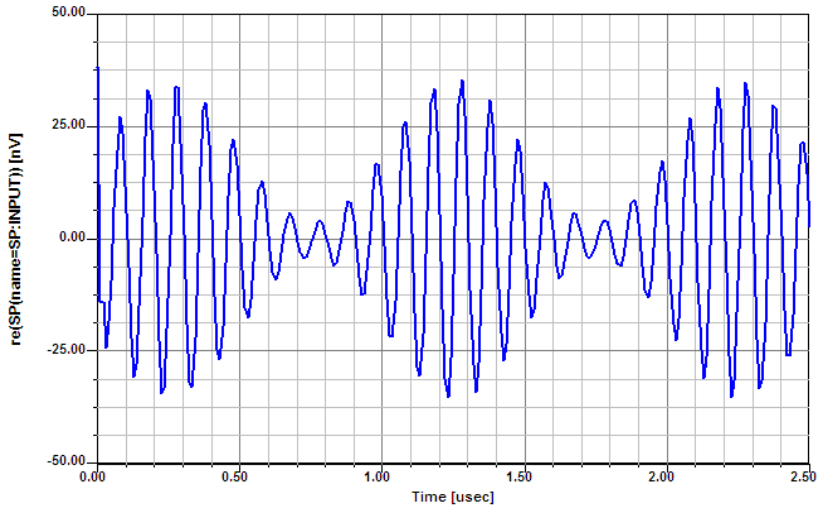


Figure 1-11: AM signal

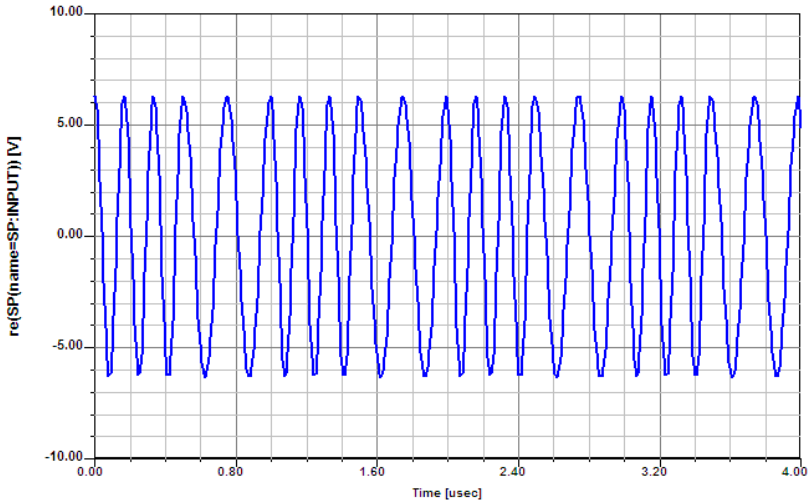


Figure 1-12: FM signal

Digital Modulation

Most modern wireless systems use digital modulation, which is the method of encoding a digital signal onto an analog wave for transmission over a medium that does not support digital signals, such as the atmosphere. In a digital system, the changes are distinct using binary signals, which exist in one of two states, a 1 or a 0, a constant positive or negative (or zero) voltage, on or off. Examples of digital modulation techniques are:

(i) Amplitude Shift Keying (ASK)
(ii) Frequency Shift Keying (FSK)
(iii) Phase Shift Keying (PSK)

Figure 1-13 shows the ASK signal in which the amplitude of the carrier was proportionally being changed with respect to the amplitude of a digital signal.

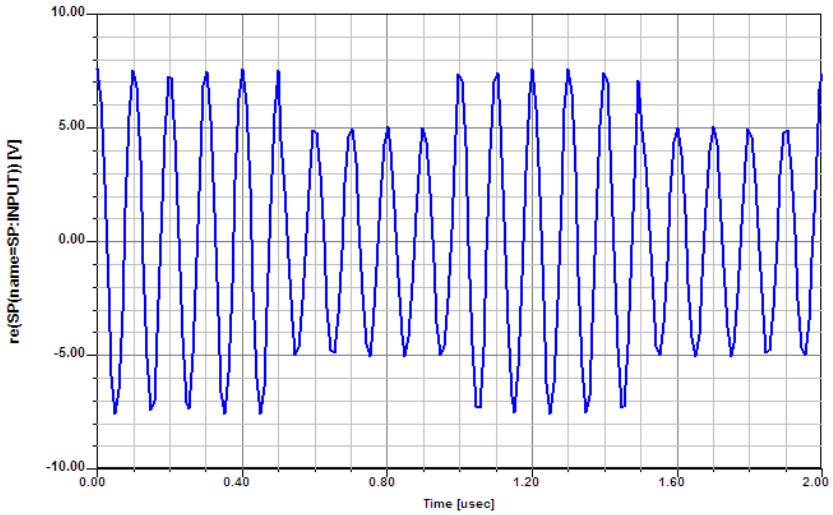


Figure 1-13: ASK signal

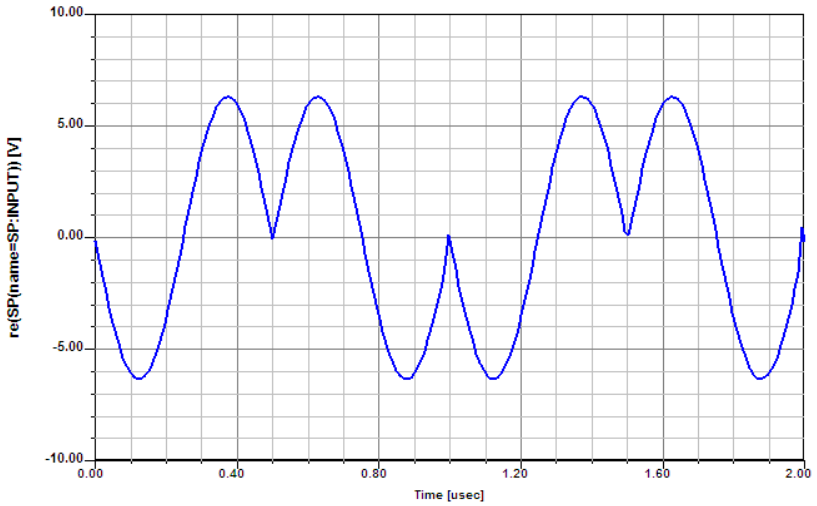


Figure 1-14: PSK signal

1.5.3 Multiple access techniques

Due to a limited number of frequencies are available for radio transmission, conserving the use of frequencies in important.
Several methods allow multiples access; the most significant in terms of wireless communications are Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA).

1.5.3.1 Frequency Division Multiple Access

FDMA divides the bandwidth of a channel (a range of frequencies) into smaller frequencies bands (narrower ranges of frequencies or channels). For example, a transmission band with a 50,000 MHz bandwidth can be divided into 1,000 channels, each with a bandwidth of 50 kHz. Each channel is dedicated to one specific user. This concept is illustrated in Figure1-15 for five users. FDMA is most often used with analog transmissions. FDMA does, however, have some drawbacks. One is that when signals are sent at frequencies that are grouped closely together, an errant signal from one frequency may encroach on its neighbour's frequency. This phenomenon known as **crosstalk**, causes interference on the interference on the other frequency and may disrupt transmission.

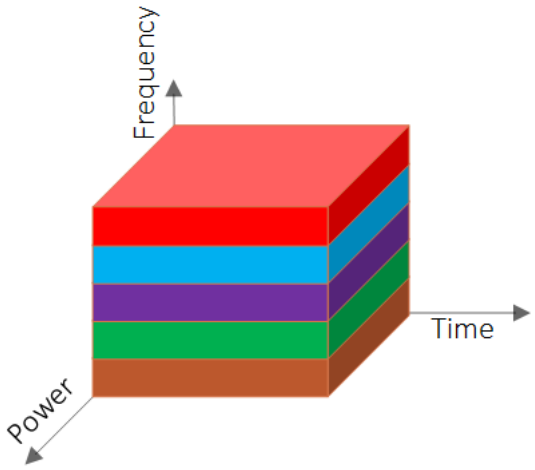


Figure 1-15: FDMA

1.5.3.2 Time Division Multiple Access

TDMA divides the transmission time into several slots. Each user is assigned the entire frequency for the transmission for a fraction of time on a fixed, rotating basis. Because the duration of each time slot is shot, the delays that occur while others use the frequency are not noticeable. Figure 1-16 illustrates TDMA for five users. TDMA has several advantages over FDMA. TDMA uses the bandwidth more efficiently. Also, TDMA allows both data and voice transmissions to be mixed using the same frequency. The combination of FDMA and TDMA as shown in Figure 17, is most often used with digital transmissions.

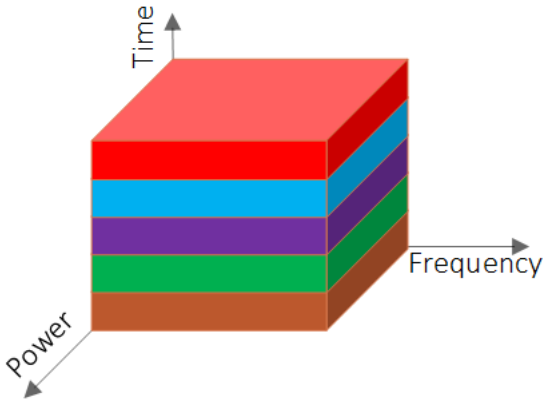


Figure 1-16: TDMA

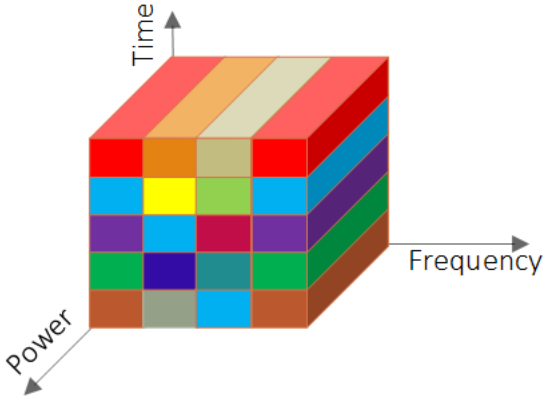


Figure 1-17: FDMA/TDMA

1.5.3.3 Code Division Multiple Access

CDMA is used primarily or cellular telephone communications and is unlike TDMA or FDMA. CDMA uses direct sequence spread spectrum (DSSS) technology with a unique digital spreading code (PN code), rather than separate RF frequency or channels, to differentiate between the multiple transmissions the same frequency range. Before transmission occurs, the high-rate PN code is combined with the data to be sent; this step spreads the signal over a wide frequency band. In DSSS the 1s and 0s of the spreading code are referred to as “chips”, to avoid confusing them with data bits.

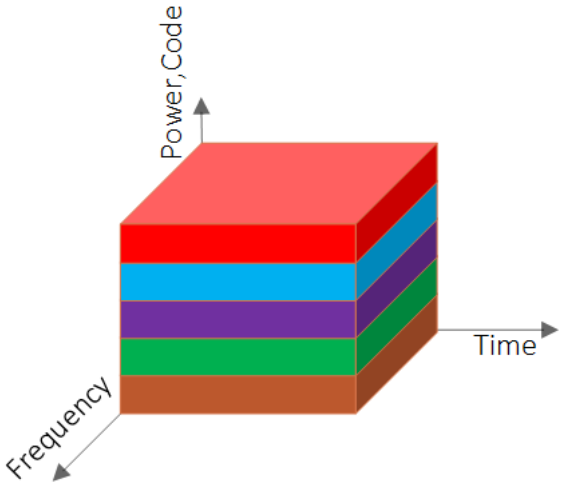


Figure 1-18: CDMA

Section 1.6: Examples of wireless technologies and discuss applications associated with them

WPAN is a small network for interconnecting devices centred around an individual person's workspace. Typically, WPAN uses some short-range wireless technologies that permit communication about 10 meters. Bluetooth, RFID, ZigBee, NFC and UWB are some of the wireless technologies that fall into this category.

Within IEEE, the largest technical institute in the world, a working group known as IEEE 802.15 is formed to investigate wireless technologies for PAN. IEEE 802.15.1 provides resources for those who implement Bluetooth devices. IEEE 802.15.3a provides resources for high data rate WPAN such as UWB. IEEE 802.15.4 provides resources for those who implement ZigBee devices. However, these wireless technologies are heavily promoted by external organizations. Bluetooth technology is promoted by Bluetooth SIG and its current specification is Version 5.0. UWB specification has not been finalized and currently has two proposals from WiMedia Alliance (uses MB-OFDM (MultiBand – Orthogonal Frequency Division Multiplexing)) and UWB Forum (uses DS-UWB (Direct Sequence-UWB)). ZigBee Alliance is promoted by ZigBee Alliance and its current specification is Version 3.0.

RFID standard is maintained by ISO (International Standard Organisation). In general, it can divided into three categories; namely passive, semi-active and active depending on its battery requirements. Battery is not required in passive RFID cards (also known as proximity cards), semi-active RFID cards require battery power up only the RFID tag IC and active RFID cards require battery to power up all the ICs on the cards and to generate the outgoing signals.

SAQ 1.12: Which of the IEEE 802 standards is used in ZigBee technology?
SAQ 1.13: Which of the WPAN technologies provides the high data rate?
SAQ 1.14: Name the promoter of Bluetooth Technology.

Under the PAN and LAN categories, the currently available wireless technologies are:

- Bluetooth
- Wireless LAN

- RFID (Radio Frequency Identification)
- ZigBee
- NFC (Near Field Communication)
- UWB (Ultra-Wide Band)

Besides these existing wireless technologies and due to the new developments in Internet of Things (IoT) which requires to connect among billions of physical devices, equipped with electronics, transducers such as sensors and actuators for various IoT applications and business purposes, there are also a few upcoming wireless technologies that will be introduced to the mass market in the coming years. Among them are a new version of Wireless LAN, LoRa, SigFox, NB-IoT and dedicated Short Range Communication (DSRC) for vehicular communication. There are numerous applications that are currently being used in these wireless technologies. Here, we will list down three of these applications to illustrate the benefits of wireless technologies on improving the quality of life.

The traditional voice application that requires low bandwidth is still very important. In fact, one of the most saleable items for Bluetooth technology is the combination of Bluetooth headsets and Bluetooth-enabled mobile phones that allow users to communicate without having to hold their mobile phones.

The use of Wireless LAN to access the Internet from laptops and Smart phones has been adopted widely. Hotspots with WLAN access have been installed in many places in many countries. For example, our own Singapore Polytechnic campus has been installed with hundreds of access points to allow staff and students to access the Internet easily. With the ever-increasing use of VoIP and free Internet calls like Skype, WLAN has also been used to transfer voice information.

RFID technology is currently used extensively for data acquisition and in supply chain management. For example, in Singapore Polytechnic, RFID technology was used to collect students' attendance when each student taps his/her admission card on the attendance readers. Another example is Wal-Mart, the largest company in the world, has started using RFID to track its stock inventory. As a result, all its suppliers are mandated to tag their pallets and cases, which can amount to 1 billion tags per year. Using RFID technology, the company is able to cut cost significantly, especially on the automatic generation of pick lists of items which were needed to restock the shelves.

The upcoming 5G technology, is predicted to be a disruptive technology that will replace current mainstream technologies that are monopolies by telecommunication industries.

Instead of giving an overview of all these wireless technologies in this module, we will concentrate on a few of them and provide in-depth knowledge on their implementations. In Chapter 2, we will cover RFID, Chapter 3 on Wireless LAN, Chapter 4 on Bluetooth, Chapter 5 on Wide Area Network, Chapter 6 on an introduction to 5G and lastly Chapter 7 Wireless Technologies in Business.

SAQ 1-15: Which of the wireless technologies is used for wireless sensor network?
SAQ 1-16: Which of the wireless technologies is used for voice transfer between a mobile phone and a headset?

WLAN refers to wireless technologies that are used to enable mobile users to be connected to an existing local area network. Unlike the WPAN technologies, IEEE is the main contributor

for WLAN technologies. Currently, the working group IEEE 802.11 has released three specifications, namely IEEE 802.11a, IEEE 802.11b and IEEE 802.11g. The main differences between these three standards are shown in Table 1.3. With the knowledge gained in areas of multiple access, modulation, security and implementations, the working group also published new versions of WLAN standard known as IEEE 802.11n and IEEE 802.11ac.

Standard	Multiple Access Technique	Frequency	Maximum Bit Rate
IEEE 802.11a	OFDM	5.2 GHz UNII	54 Mbps
IEEE 802.11b	DSSS	2.4 GHz ISM	11 Mbps
IEEE 802.11g	OFDM	2.4 GHz ISM	54 Mbps

Table 1.3: The main differences between IEEE 802.11 standards

SAQ 1.17: Which IEEE 802.11 standards provide the maximum bit rate of 54 Mbps?
SAQ 1.18: What is the main difference between IEEE 802.11b and IEEE 802.11a?

Section 1.7: Advantages and disadvantages of wireless technologies

The advantages of wireless technologies can be broadly grouped into the following six categories:

1. Mobility
Wireless technologies provide a seamless communication for users to move around in the network without getting disconnected from the system. This mobility, in turn, increases efficiency and provide service opportunities that are not possible in wired environments.

2. Installation
Installation of wireless systems is simpler and faster compared to wired systems.

3. Flexibility
The configuration of wireless systems can be adapted and changed easily.

4. Cost
The cost of setting up wireless systems are lower compared to wired systems.

5. Scalability
Wireless systems can be scaled from an ad-hoc peer-to-peer network suitable for a small number of users to a large infrastructure network that enable roaming over a large area.

6. Reach
Wireless systems can be extended to places which cannot be reached by wired systems due to cost or legal requirements.

The disadvantages of wireless technologies can be broadly grouped into the following three categories:

1. Security
Due to the unconstrained nature of the communication medium in wireless technologies, hackers may be able to eavesdrop the transmitted information. Therefore, network security has to be addressed. For example, users may have to be authenticated before they are permitted to use the network and information may have to be encrypted prior to transmission.

2. Interference
When the number of user increases, interference from one another may occur and hence disrupt or deteriorate the communication channels.

3. Limited bandwidth
Due to the limited spectrum, the maximum bit rate for wireless systems is always slower than wired systems.

SAQ 1-19: Which of the advantages influence a home user to choose a wireless network compared to a wired network for his/her home network?

SAQ 1-20: Which of the disadvantages is the most important consideration in setting up a wireless network?

Chapter 2: Understand RFID (Radio Frequency Identification) Technology

Learning Objectives

- Explain "What is RFID technology?"
- Understand the fundamentals of RFID system
- Understand the RFID Security
- Explain the advantages and limitations of RFID
- Understand the different types of RFID tags
- List the RFID Standards

Section 2.1: What is RFID technology?

RFID is a technology that can uniquely identify an object, animal or person using radio waves. This is typically achieved with communication between a scanner or RFID reader (interrogator) and a tag (transponder) that contains data on a microchip.

RFID is increasingly used in industry as an alternative to the bar codes. The advantages of RFID compared to bar codes are:

- readers can communicate with tag without direct contact or line-of-sight scanning
- higher data capacity
- read & write capability
- data integrity
- security

Section 2.2: Fundamentals of RFID system

Tags and readers are the main components of an RFID system. Communication of data between tags and readers is by wireless transmission which involves the signal encoding and modulation in the transmitter, demodulation and decoding in the receiver and error detection, error correction and encryption in both transmitter and receiver.

Section 2.2.1: RFID Reader

An RFID reader typically contains an antenna system, a high frequency transceiver, a digital control unit and probably an interface to other systems, as shown in Figure 2-1. The antenna is very important since it is used as a coupling element to the transponder. The high frequency transceiver is used for communication. The digital control unit is used for baseband signal processing. The commonly used interface is RS-232 or RS-485 to enable to the reader to forward received data to another system such as PCs, process control systems and monitoring systems.

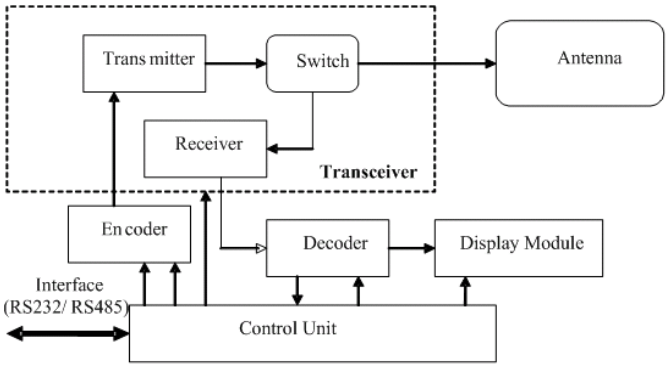


Figure 2-1: RFID reader

There are two ways in which the readers are being used. For stationary readers, they are installed at the points of sale, entrances and exits of supermarket. For mobile readers, they can be used for checking of library books on book shelves.

Section 2.2.2: RFID Tag

Figure 2-2 shows a passive RFID tag which represents the actual data carrying device of an RFID system. The basic components are an antenna or coupling element, an electronic microchip and a power supply circuit. The antenna enables the tag to receive and respond to radio-frequency queries from an RFID reader. The microchip includes a micro controller, memories and a transceiver to provide digital and analogue interfaces. The power required to activate the tag is supplied by electromagnetic induction on the attached coil/antenna. The power supply circuit will rectify the AC voltage to provide a DC internal supply voltage. When sufficient DC voltage is generated, the chip can send data continuously.

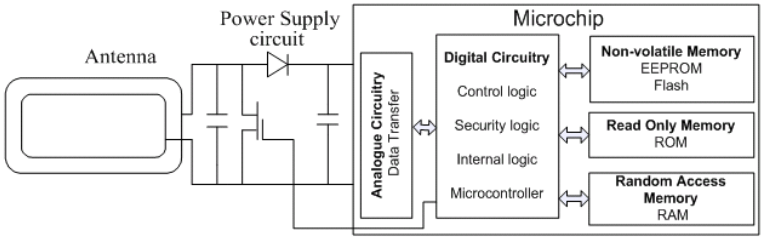


Figure 2-2: RFID tag

SAQ 2.1 Which part of the reader enables the wireless communication between the RFID tags?

SAQ 2.2 Describe the two main functions of antenna at the passive RFID tag.

Section 2.2.3: Signal Coding

Signal coding is a process of representing the transmitted message to its voltage representation so that it matches optimally to the characteristics of the transmission channel. This process involves providing the message with some degree of protection against interference or collision and intentional modification.

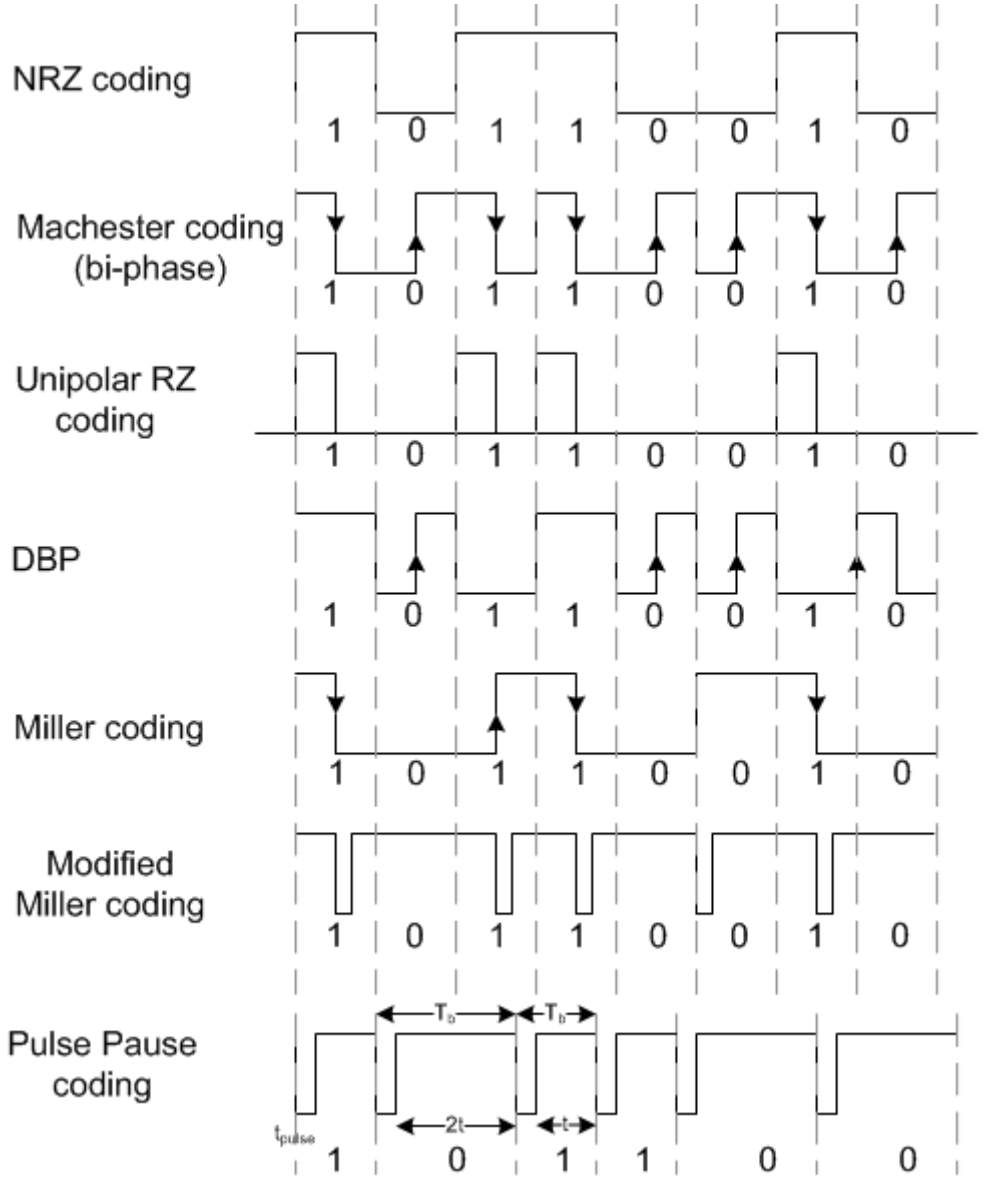


Figure 2-3: Signal coding used in RFID system

Binary ones and zeros can be represented in various line codes. RFID systems normally use one of the following coding procedures, as shown in Figure 2-3.

- NRZ (Non-Return To Zero) code
  A binary 1 is represented by a 'high' signal and a binary 0 is represented by a 'low' signal. The NRZ code is used almost exclusively with FSK or PSK modulation.

- Manchester code
  A binary 1 is represented by a negative transition in the half bit period. A binary 0 is represented by a positive transition in the half bit period. The Manchester code is therefore also known as split-phase coding.
  The Manchester code is often used for data transmission from the transponder to the reader based upon load modulation using a subcarrier.

- Unipolar RZ (Return to Zero) code
  A binary 1 is represented by a 'high' signal in the first half bit period and a 'low' signal in the second half bit period. A binary 0 is represented by a 'low' signal lasting for the entire duration of the bit.

- DBP (Differential Bi-Phase) code
  A binary 0 is coded by a transition of either type in the half bit period, a binary 1 is coded by the lack of a transition. Furthermore, the level is inverted at the start of every bit period, so that the bit pulse can be more easily reconstructed in the receiver (if necessary).

- Miller code
  A binary 1 is represented by a transition of either type in the half bit period, a binary 0 is represented by the continuance of the binary 1 level of the previous bit period over the entire duration of the bit. A sequence of zeros creates a transition at the start of a bit period, so that the bit pulse can be more easily reconstructed in the receiver (if necessary).

- Modified Miller code
  In this variant of the Miller code each transition is replaced by a 'negative' pulse. The modified Miller code is highly suitable for use in inductively coupled RFID systems for data transfer from the reader to the transponder.
  Due to the very short pulse durations ($t_{pulse} << T_{bit}$) it is possible to ensure a continuous power supply to the transponder from the HF field of the reader even during data transfer.

- PPC (Pulse Pause Coding) code
  A binary 1 is represented by a pause of duration *t* before the next pulse. A binary 0 is represented by a pause of duration 2*t* before the next pulse. This coding procedure is popular in inductively coupled RFID systems for data transfer from the reader to the transponder. Due to the very short pulse durations ($t_{pulse} << T_{bit}$) it is possible to ensure a continuous power supply to the transponder from the RF field of the reader even during data transfer.

SAQ 2.3 Which codes are suitable for data transfer from reader to the tag? Why? Provide the answer with a suitable reason.

SAQ 2.4 Draw a pulse sequence of the data byte “10111011b” using Manchester code. LSB (Least Significant Bit) is at the right most and transmitted first.

SAQ 2.5 If 1msec is being required to transmit the above data byte, calculate the data rate in bps (bit per sec).

Section 2.2.4: Digital Modulation

RFID systems use the three basic digital modulations: Amplitude Shift Keying, Frequency Shift Keying and Phase Shift Keying

Section 2.2.4.1: Amplitude Shift Keying (ASK)

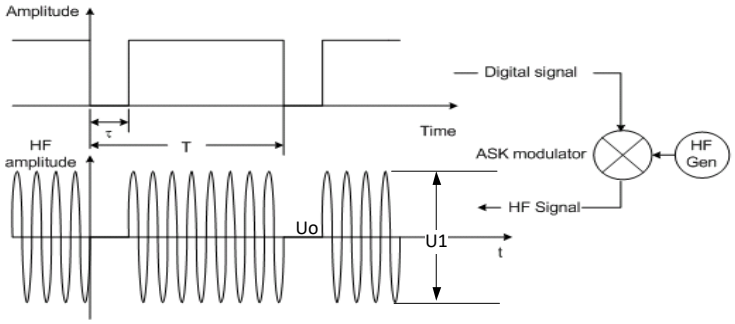


Figure 2-4: Amplitude Shift Keying

In binary amplitude shift keying the amplitude of a carrier oscillation is switched between two states u_0 and u_1 (keying) by a binary code signal, as shown in Figure 2-4. The percent modulation is defined as

$$m = (1 - \frac{u_O}{u_1}) x100$$

Equation 2-1: Percent Modulation for ASK

Section 2.2.4.2: Frequency Shift Keying (FSK)

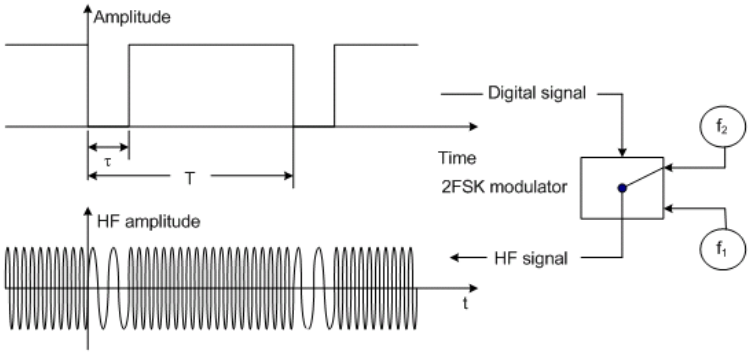


Figure 2-5: Frequency Shift Keying

In binary frequency shift keying the frequency of a carrier oscillation is switched between two frequencies f_1 and f_2 by a binary code signal. The carrier frequency f_C is defined as the arithmetic mean of the two characteristic frequencies. $f_C = \frac{f_1 + f_2}{2}$. The difference between the carrier frequency and the characteristic frequencies is termed the frequency deviation, $\Delta f = \frac{|f_1 - f_2|}{2}$.

Section 2.2.4.3: Phase Shift Keying (PSK)

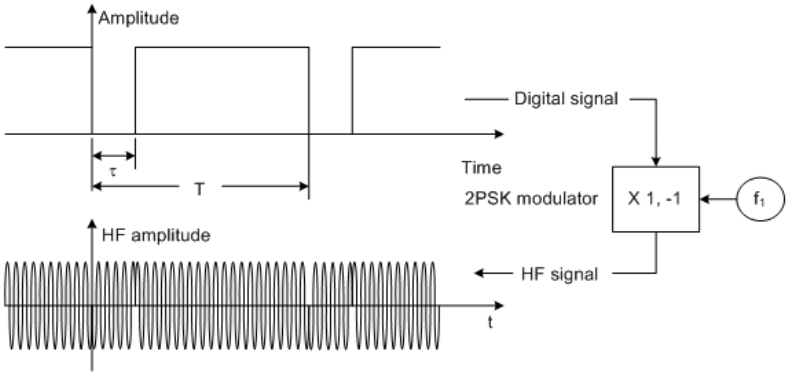


Figure 2-6: Phase Shift Keying

In phase shift keying the binary states '0' and '1' of a code signal are converted into corresponding phase states of the carrier, in relation to a reference phase. In BPSK (Binary Phase Shift Keying), the signal is switched between the phase states 0^o and 180^o. Mathematically speaking, the shift keying of the phase position between 0^o and 180^o corresponds with the multiplication of the carrier by 1 and -1 respectively.

Section 2.2.4.4: Modulation with Subcarrier

In RFID systems, modulation procedures using a subcarrier are primarily used in inductively coupled systems in the frequency ranges 6.78 MHz, 13.56 MHz or 17.125 MHz and in load modulation for data transfer from the tag to the reader. The load modulation of an inductively coupled RFID system has a similar effect to ASK modulation of HF voltage at the antenna of the reader. Instead of switching the load resistance on and off in time with a baseband coded signal, a low frequency subcarrier is first modulated by the baseband coded data signal. ASK, FSK or PSK modulation may be selected as the modulation procedure for the subcarrier. The subcarrier frequency itself is normally obtained by the binary division of the operating frequency. For 13.56 MHz systems, the subcarrier frequencies 847 kHz (13.56 MHz/16), 424 kHz (13.56 MHz/32) or 212 kHz (13.56 MHz/64) are usually used. The modulated subcarrier signal is now used to switch the load resistor on and off.

In Figure 2-7, the baseband signal (data) is modulated with subcarrier by switching on and off the load (the antenna of the tag) and becomes the load modulated signal with subcarrier. Then, the modulated subcarrier signal is modulated with the RF carrier and transmitted back to the reader.

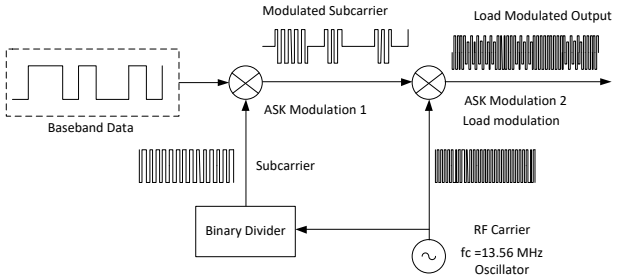


Figure 2-7: Load modulation

The great advantage of using a subcarrier only becomes clear when we consider the frequency spectrum generated. Load modulation with a subcarrier initially generates two spectral lines at a distance ± the subcarrier frequency f_H around the operating frequency, as shown in Figure 2.8. The actual information is now transmitted in the sidebands of the two

subcarrier lines, depending upon the modulation of the subcarrier with the baseband coded data stream. If load modulation in the baseband were used, on the other hand, the sidebands of the data stream would lie directly next to the carrier signal at the operating frequency.

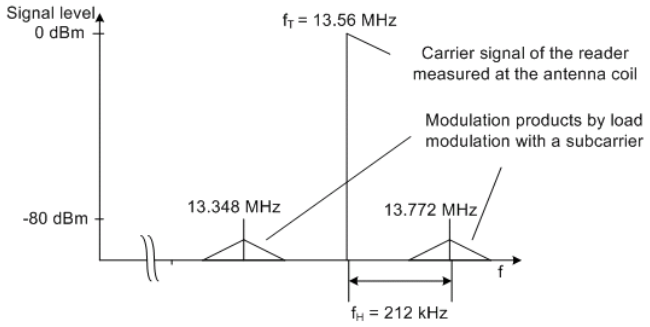


Figure 2-8: Modulation products using load modulation with a subcarrier

In very loosely coupled transponder systems the difference between the carrier signal of the reader f_T and the received modulation sidebands of the load modulation varies within the range 80-90 dB, as shown in Figure 2-8. One of the two subcarrier modulation products can be filtered out and demodulated by shifting the frequency of the modulation sidebands of the data stream. It is irrelevant here whether the frequencies $f_T + f_H$ or $f_T - f_H$ are used, because the information is contained in all sidebands.

SAQ 2.6 Calculate the frequency deviation of the FSK system which transmits with frequency 117 kHz as "0" and frequency 137 kHz as "1".

SAQ 2.7 From the Figure 2-8, answer the following:

(i) The carrier frequency of the system is:_____MHz.

(ii) The subcarrier frequency of the system is: _____kHz.

(iii) What are the frequencies of the two sidebands that carry the data stream or information?

(a) _____MHz

(b) _____ MHz

Section 2.2.5: Data Integrity

When transmitting data using contactless technology, the transmitted data will be corrupted by external noise causing undesired changes to the transmitted data and thus leading to transmission errors. This is shown in Figure 2-9. Currently, there are two types of codes that are used to ensure data integrity. For error-detection codes, it can only detect the presence of erroneous data. For error-correction codes, it not only can detect the presence of erroneous data, but also to correct these erroneous data. In this section, we will study some of the error-detection codes.

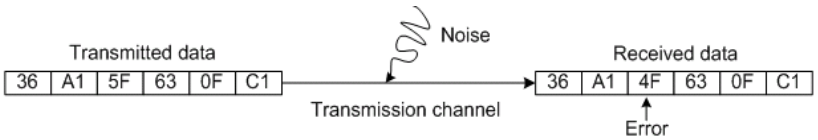


Figure 2-9: Interference during transmission leading to erroneous data

Section 2.2.5.1: Parity check

Parity check is a very simple and therefore a very popular checksum procedure. In this procedure, a parity bit is incorporated into each byte and transmitted with it resulting in 9 bits

being sent for every byte. Before data transfer takes place a decision needs to be made as to whether to check for odd or even parity so that the sender and receiver both check according to the same method.

The value of the parity bit is set such that if odd parity is used an odd number of the nine bits have the value 1. On the other hand, if even parity is used an even number of the nine bits have the value 1. The even parity bit can also be interpreted as the horizontal checksum (modulo 2) of the data bit. This horizontal checksum also permits the calculation of the exclusive OR logic gating (XOR logic gating) of the data bits.

For example, the number E5h has the binary representation 1 1 1 0 0 1 0 1. Using odd parity, $1 \oplus 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus$ parity bit = 1. ($\oplus$ denotes XOR operation.) This gives us the parity bit to be 0.

A parity generator for even parity can be realised by the XOR logic gating of all the data bits in a byte. The order in which the XOR operations take place is irrelevant. In the case of odd parity, the parity generator output is inverted. The implementation of the parity generator is shown in Figure 2-10.

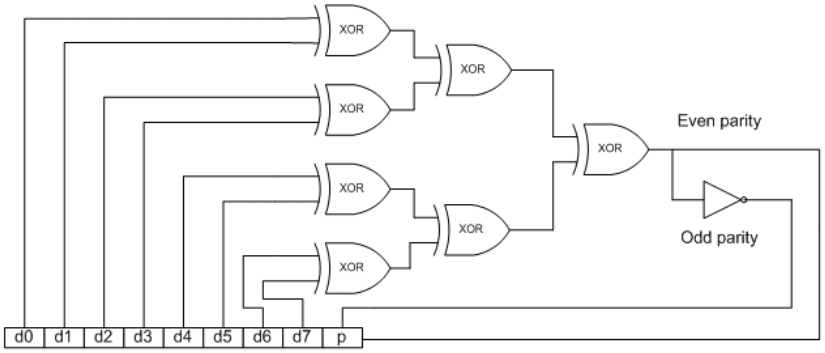


Figure 2-10: Parity generator

Section 2.2.5.2: LRC

Another method is to perform XOR checksum which can be calculated quickly and easily. The XOR checksum is generated by the recursive XOR gating of all the data bytes in a data block. In Figure 2-11, Byte 1 of value 46h is XOR gated with Byte 2 of value 72h. The outcome of this gating with value 34h is XOR gated with Byte 3 of value 61h resulting in 55h. This XOR gating is performed for the remaining bytes in the data block. Then, the final output of the XOR gating known as LRC value is appended to the data block and transmitted with it.

On the receiver, a simple check for transmission errors can be performed by generating an LRC from the received data. The result of this operation must always be zero if there is no transmission error. Any other result indicates that transmission errors have occurred.

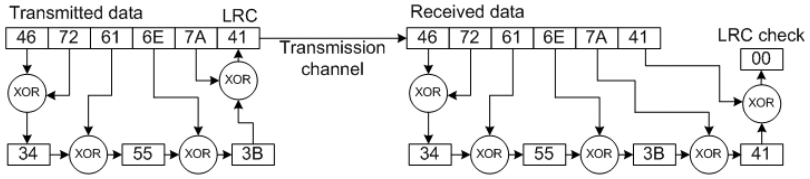


Figure 2-11: LRC generator

The disadvantage of LRC procedure is its unreliability since it is possible for multiple errors to cancel each other and the check cannot detect whether additional bytes have been inserted

into a data block. Therefore, LRCs are primarily used for the rapid checking of very small data blocks (e.g. 32 byte).

Section 2.2.5.3: CRC

The CRC procedure was originally used in disk drives, and can generate a checksum that is reliable enough even for large data quantities. It is also excellently suited for error recognition in data transfer via wire-bound (telephone) or wireless interfaces (radio, RFID). The CRC procedure represents a highly reliable method of recognising transmission errors.

As the name suggests, the calculation of the CRC is a cyclic procedure. Thus the calculation of a CRC value incorporates the CRC value of the data byte to be calculated plus the CRC values of all previous data bytes. Each individual byte in a data block is checked to obtain the CRC value for the data block as a whole.

Mathematically speaking, a CRC checksum is calculated by the division of a polynomial using a so-called generator polynomial. The CRC value is the remainder obtained from this division. To illustrate this operation, we show the computation of a 4-bit CRC sum for a data block of F7h and 38h. The generator polynomial is $x^4+x+1=10011$. In general, a polynomial of order-*k* will generate (*k*-1)-bit CRC sum.

For the first data byte, 11110111b, we append four zero bits to obtain 111101110000b. Then, we divide it with the generator polynomial, 10011b resulting in a remainder of 1111b as shown on the left hand side of Figure 2-12. This remainder is appended to the second data byte to obtain 001110001111b. Again, it is divided with the generator polynomial to obtain a remainder of 0101b as shown on the right hand side of Figure 2-12. Since this is the last data byte, it will be the 4-bit CRC sum.

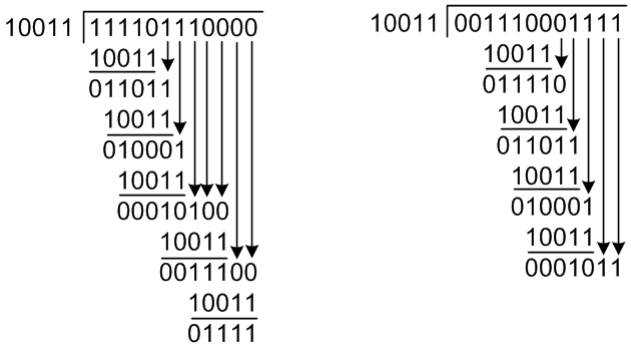


Figure 2-12: An example of CRC computation

SAQ 2.8 In Figure 2-10, if the data byte is "10101110b" and the left most bit is d_0, find the parity bit "p".

SAQ 2.9 In Figure 2-11, if the data byte "7A" received was found to be "75h", find the calculated LRC and output of the LRC check value.

SAQ 2.10 If the generator polynomial is given as x^4+x^2+x+1 in the above CRC example, find the new 4 bit CRC check sum.

SAQ 2.11 Which of the error detection codes requires a generator polynomial to produce checksum?

Section 2.2.6: Read/Write Mechanism

Figure 2-13 shows the simple RFID system consists of a tag and a reader. When an RFID tag passes through the electromagnetic/interrogation zone, it detects the reader's activation signal. When the tag is activated, the tag sends information to the reader. The reader decodes the data encoded in the tag's integrated circuit (silicon microchip) and the data may be passed to the host computer for further processing using suitable application software.

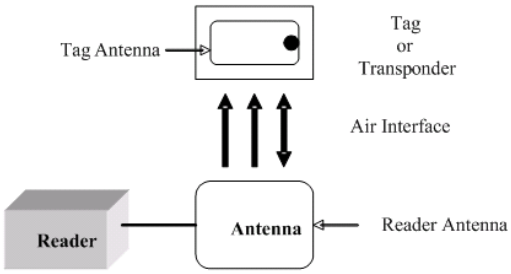


Figure 2-13: RFID system

The two main categories of RFID systems are near-field systems and far-field systems. Figure 2-14 shows the near-field system that employs inductive coupling of the tag to the reactive energy circulating around the reader antenna. The localized oscillatory magnetic field is generated in the reader antenna by connecting the tag as an RF power source to establish a loosely connected "space" transformer. Near field coupling techniques are generally applied to RFID systems operating in the low frequency (LF) and high frequency (HF) bands with relatively short reading distances well within the radian sphere defined by $\frac{\lambda}{2\pi}$.

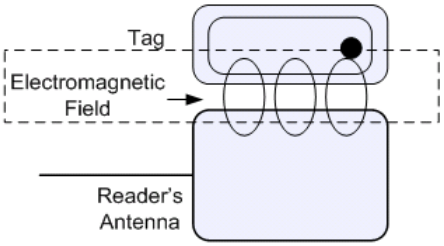


Figure 2-14: Inductive coupling for near field system

Figure 2-15 shows the far-field system that employs radiative coupling of the tag to the real energy contained in propagating electromagnetic plane waves. The far-field coupling is applicable to potentially longer read range ultra high frequency (UHF) and microwave RFID systems.

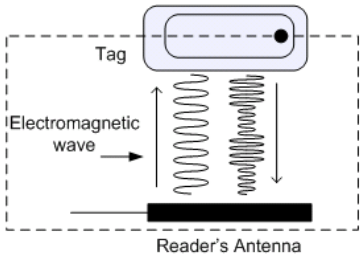


Figure 2-15: Radiative coupling for far field system

Whether it is a near field system or a far field system, it is desirable to communicate with a tag when other similar tags are simultaneously visible to the reader. An anti-collision algorithm allows more tags in the field to be read/write simultaneously. For example, in the case of library books an important design feature is the ability to read and "check-out" multiple books as the same time.

Section 2.2.7: Anti-collision

It is very important that an RFID reader enables to read a correct tag among more than one tag in the reader's field. When multiple tags are energized by the RFID reader in RFID systems, collision among tags will lower the efficiency of the RFID system. Hence, an anti-collision algorithm allows multiple tags to be read/written simultaneously without collision. That will be making sure that only 1 tag talks at any given time. ALOHA and Tree algrithms are generally used as main anti-collision algrithms to solve tag collison.

Section 2.2.8: Practical RFID System

A practical RFID system may consist of several components: tags, tag readers, edge servers, middleware, and application software. Middleware helps to connect RFID equipment to applications. An example of a practical RFID system is the Student Attendance Recording and Tracking (START) RFID System shown in Figure 2-17. The architecture includes the controller/server, databases, tags, tag readers and reader antenna. The function of the controller/server is to manage all communications between the reader/interrogator and the database. The database is to provide an organized repository or collection of data.

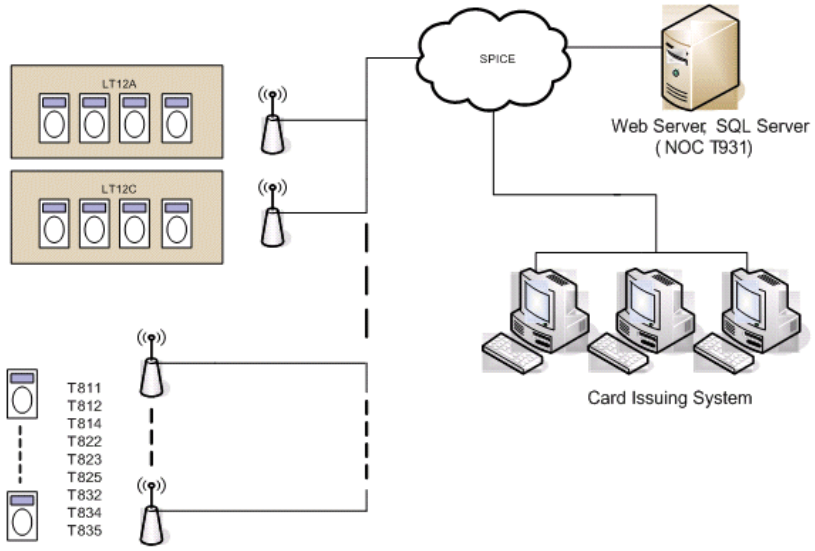


Figure 2-16: START RFID system architecture

The information flow in this system is as follow:

1. The reader is activated by lecturer using the staff RFID tag to start the attendance recording mode for predetermined period.
2. Students tap their student tags at the reader to record their attendance at the corresponding class section.
3. The attendance records with the time stamps are temporarily stored at the reader.

4. The scheduler program at the server sends command to all the readers requesting to retrieve the attendance records at regular interval which is set by the system administrator.
5. Reader sends host an acknowledgement of the request.
6. Server retrieves the attendance records by using ftp commands through Wireless LAN.
7. The server then processes the data such as storing the data to a database or searching the database for a matching identification for the attendance application.
8. Repeat steps 1 through 7.

SAQ 2.12 Is the ez-link card used in SMRT and Transit-link in Singapore the near field RFID application system? If your answer is "Yes", answer "why". If your answer is "No", explain "why".

SAQ 2.13 Is the EPC (Electronic Product Code) UHF class 1 Gen 2 card used in Wal-Mart, USA the near field RFID application system? If your answer is "Yes", answer "why". If your answer is "No", explain "why".

SAQ 2.14 Far-field RFID systems employ:_____ coupling.

SAQ 2.15 If it is required to read/write multiple tags in the activation field, what is to be needed?

Section 2.3: RFID Security

RFID systems are increasingly being used in high security applications, such as access systems and systems for making payments or issuing tickets. However, the use of RFID systems in these applications necessitates the use of security measures to protect against attempted attacks, in which people try to trick the RFID system in order to gain unauthorised access to buildings or avail themselves of services (tickets) without paying.

Modem authentication protocols also work by checking knowledge of a secret (i.e. a cryptographic key). However, suitable algorithms can be employed to prevent the secret key being cracked. High security RFID systems must have a defence against the following individual attacks:

- Unauthorised reading of a data carrier in order to duplicate and/or modify data.
- The placing of a foreign data carrier within the interrogation zone of a reader with the intention of gaining unauthorised access to a building or receiving services without payment.
- Eavesdropping into radio communications and replaying the data, in order to imitate a genuine data carrier ('replay and fraud').

When selecting a suitable RFID system, consideration should be given to cryptological functions. Applications that do not require a security function (e.g. industrial automation, tool recognition) would be made unnecessarily expensive by the incorporation of cryptological procedures. On the other hand, in high security applications (e.g. ticketing, payment systems) the omission of cryptological procedures can be a very expensive oversight if manipulated transponders are used to gain access to services without authorisation.

Section 2.3.1: Mutual Symmetrical Authentication

Mutual authentication between reader and transponder is based upon the principle of three-pass mutual authentication in accordance with ISO 9798-2, in which both participants in the communication check the other party's knowledge of a secret (secret cryptological key).

In this procedure, all the transponders and receivers that form part of an application are in possession of the same secret cryptological key K (→ symmetrical procedure). When a transponder first enters the interrogation zone of a reader, it cannot be assumed that the two participants in the communication belong to the same application. From the point of view of the reader, there is a need to protect the application from manipulation using falsified data. Likewise, on the part of the transponder there is a need to protect the stored data from unauthorised reading or overwriting.

The mutual authentication procedure begins with the reader sending a GET_CHALLENGE command to the transponder. A random number R_A is then generated in the transponder and sent back to the reader (response → challenge-response procedure). The reader now generates a random number R_B. Using the common secret key K and a common key algorithm e_K, the reader calculates an encrypted data block (token 1), which contains both random numbers and additional control data, and sends this data block to the transponder.

$$\text{Token 1} = e_K(R_B//R_A//ID_A//\text{Textl})$$

The received token 1 is decrypted in the transponder and the random number $R\text{-}_A$ contained in the plain text is compared to the previously transmitted R_A. If the two figures correspond, then the transponder has confirmed that the two common keys correspond. Another random number R_{A2} is generated in the transponder and this is used to calculate an encrypted data block (token 2), which also contains R_B and control data. Token 2 is sent from the transponder to the reader.

$$\text{Token 2} = e_K(R_{A2}//R_B//\text{Text2})$$

The reader decrypts token 2 and checks whether R_B, which was sent previously, corresponds with $R\text{-}_B$, which has just been received. If the two figures correspond, then the reader is satisfied that the common key has been proven. Transponder and reader have thus ascertained that they belong to the same system and further communication between the two parties is thus legitimised. This is illustrated in Figure 2-17.

Figure 2-17: Mutual authentication procedure between transponder and reader

To sum up, the mutual authentication procedure has the following advantages:

- The secret keys are never transmitted over the airwaves, only encrypted random numbers are transmitted.

- Two random numbers are always encrypted simultaneously. This rules out the possibility of performing an inverse transformation using R_A to obtain token 1, with the aim of calculating the secret key.
- The token can be encrypted using any algorithm.
- The strict use of random numbers from two independent sources (transponder, reader) means that recording an authentication sequence for playback at a later date (replay attack) would fail.
- A random key (session key) can be calculated from the random numbers generated, in order to cryptologically secure the subsequent data transmission.

Section 2.3.2: Authentication using Derived Keys

One disadvantage of the authentication procedure described in Section 2.3.1 is that all transponders belonging to an application are secured using an identical cryptological key K. For applications that involve vast quantities of transponders (e.g. the ticketing system for the public transport network, which uses several million transponders) this represents a potential source of danger. Because such transponders are accessible to everyone in uncontrolled numbers, the small probability that the key for a transponder will be discovered must be taken into account. If this occurred, the procedure described above would be totally open to manipulation.

A significant improvement on the authentication procedure described can be achieved by securing each transponder with a different cryptological key. To achieve this, the serial number of each transponder is read out during its production. A key K_x is calculated (→ derived) using a cryptological algorithm and a master key K_M, and the transponder is thus initialised. Each transponder thus receives a key linked to its own ID number and the master key K_M.

The mutual authentication begins by the reader requesting the ID number of the transponder, as shown in Figure 2-18. In a special security module in the reader, the SAM, the transponder's specific key is calculated using the master key K_M, so that this can be used to initiate the authentication procedure. The SAM normally takes the form of a smart card with contacts incorporating a cryptoprocessor, which means that the stored master key can never be read.

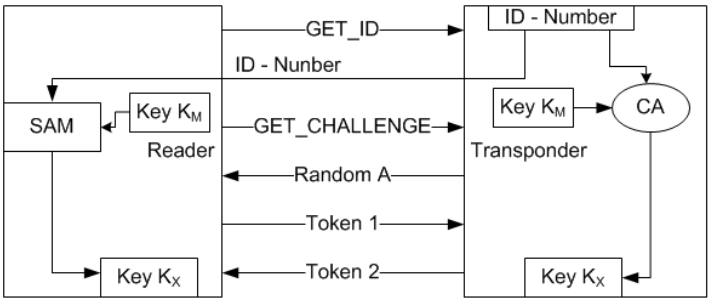


Figure 2-18: Authentication procedure based upon derived keys

Section 2.3.3: Encrypted Data Transfer

Cryptological procedures are used to protect against both passive and active attacks. To achieve this, the transmitted data (plain text) can be altered (encrypted) prior to transmission so that a potential attacker can no longer draw conclusions about the actual content of the message (plain text).

Encrypted data transmission always takes place according to the same pattern. The transmission data (plain text) is transformed into cipher data (cipher text) (→ encryption, ciphering) using a secret key K and a secret algorithm. Without knowing the encryption algorithm and the secret key K a potential attacker is unable to interpret the recorded data. It is not possible to recreate the transmission data from the cipher data.

The cipher data is transformed back to its original form in the receiver using the secret key K' and the secret algorithm (--> decryption, deciphering), as shown in Figure 2-19.

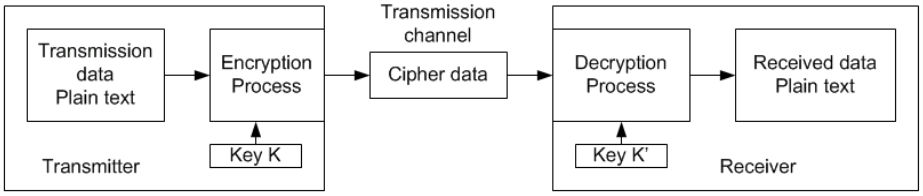


Figure 2-19: Data encryption

SAQ 2.16 Why do we need security RFID for cash payment application?
SAQ 2.17 List the three methods of RFID security.
SAQ 2.18 Write down the algorithm or set of procedures for Mutual Symmetrical Authentication Method in steps.
SAQ 2.19 In mutual authentication method, the token 1 contains:
(i) _____
(ii)_____
(iii)_____ and
(iv)_____.
SAQ 2.20 State the two advantages of using Mutual Symmetrical Authentication?
SAQ 2.21 State the two differences between the Mutual Symmetrical Authentication Method and Authentication Using Derived Keys Method.

Section 2.4: Advantages and limitations of RFID

The advantages of RFID technologies can be listed as follow:

- Contactless
- Writable data
- Absence of line of sight
- Varity of read ranges
- Wide data-capacity range
- Support for multiple tag reads
- Rugged
- Perform smart tasks
- Extreme read accuracy
- The limitations of RFID technologies are as follow:
- Poor performance with RF-opaque and RF-absorbent objects
- Impacted by environmental factors
- Limitation on actual tag reads
- Impacted by hardware interference
- Limited penetration power of the RF energy

- Immature technology

SAQ 2.22 State the two advantages of RFID compared to barcode.

Section 2.5: Types of RFID Tags

There are three types of RFID tags; namely passive, semi-passive or semi-active and active. Passive tags require no internal power source, whereas active tags require a power source.

Section 2.5.1: Passive RFID Tag

Passive RFID tags do not require batteries. The minute electrical current induced in the antenna by the incoming radio frequency signal provides just enough power for the CMOS IC in the tag to power up and transmit a response. Most passive tags signal by backscattering the carrier signal from the reader. This means that the aerial (antenna) has to be designed to both collect power from the incoming signal and also to transmit the outbound backscatter signal. The response of a passive RFID tag is not just a UID but also the tag chip can contain nonvolatile EEPROM for storing data. Lack of an onboard battery, the tag can be much smaller and have an unlimited life span. Passive tags have practical read distances ranging from about 2 mm (ISO 14443) up to about few metres (ISO 18000-6) depending on the chosen radio frequency. Due to their simplicity in design they are also suitable for manufacturing with a printing process for the antennae.

Because passive tags are cheaper to manufacture and have no battery, the majority of RFID tags in existence are of the passive variety. As of 2005, these tags cost an average of $0.24 USD at high volumes. Today, as universal RFID tagging of individual products become commercially viable at very large volumes, the lowest cost tags available on the market are as low as $0.072 USD in volumes of 10 million units or more. Current demand for RFID integrated circuit chips is expected to grow rapidly based on these prices.

In many cases there is a sharp demarcation between the read range of two classes of passive tags; those that have a relatively short read range and those that have a relatively long read range, especially at LF and HF. Like many radio systems, short range RFID systems tend to be less expensive and relatively easy to design and build. Long range RFID systems tend to be more expensive and difficult to build. Typically, the range performance of RFID systems is determined to a major extent by the reader, the frequency band, the power of the signal it radiates and the sensitivity of its receiver.

Section 2.5.2: Semi-Active RFID Tag

Semi-passive RFID tags are very similar to passive tags except for the addition of a small battery. This battery allows the tag IC to be constantly powered. This removes the need for the antenna to be designed to collect power from the incoming signal. Antennas can therefore be optimised for the backscattering signal. Semi-passive RFID tags are faster in response and therefore stronger in reading ratio compared to passive tags.

Section 2.5.3: Active RFID Tag

Active RFID tags or beacons, on the other hand, have their own internal power source which is used to power any ICs and generate the outgoing signal. They may have longer range and larger memories than passive tags, as well as the ability to store additional information sent

by the transceiver. To economize power consumption, many beacon concepts operate at fixed intervals. At present, the smallest active tags are about the size of a coin. Many active tags have practical ranges of tens of metres, and a battery life of up to 10 years.

The major advantages of an active RFID tag are:
It can be read at distances of one hundred feet or more, greatly improving the utility of the device.

- It may have other sensors that can use electricity for power.
- It may have the capability to perform independent monitoring and control.
- It may have the capability of initiating communications.
- It may have the capability of performing diagnostics.
- It may have the highest data bandwidth.

Active RFID tags may even be equipped with autonomous networking; the tags autonomously determine the best communication path.

- The problems and disadvantages of an active RFID tag are:
- The tag cannot function without battery power, which limits the lifetime of the tag.
- The tag is typically more expensive, often costing $20 USD or more each.
- The tag is physically larger, which may limit applications.

SAQ 2.23 State the three advantages of passive RFID tag compared to active RFID tag.

Section 2.6: RFID Standard

How information is communicated to and from the tag has historically been determined by the original designer of the semiconductor device in the tag. These protocols vary widely in the ways the carrier is modulated, how the data is encoded, how the read/write/verify commands are structured, how multiple tags are read without interfering with one another and whether privacy/security services are provided. These varying protocols have relative advantages and disadvantages, depending upon the application being considered. As a result, there are many international RFID standards that are currently being used. These RFID standards exist to help to assure compatibility between systems and vendors.

RFID Standards (Technology/Application/Conformance/Data content)		
Application	Standard	Name
Animal Management	ISO 11784	Code/Data Structure
	ISO 11785	Technical concept
	ISO 14223	Expand Code Structure & Encoding (Data Security)
Freight Containers	ISO 10374	Automatic Identification
	ISO 18185	Electronic Seals for Security
	ISO 23389	Read Write RFID

Identification "Vicinity" Card (cm to 0.7m)	ISO 15693-1	Physical Characteristics
	ISO 15693-2	Air Interface & Initialization
	ISO 15693-3	Anti-Collision & Protocol
Identification "Proximity" Card (mm to cm)	ISO 14443-1	Physical Characteristics
	ISO 14443-2	Radio frequency and power
	ISO 14443-3	Initialization & Anti-collision
	ISO 14443-4	Transmission Protocol
Item Management	ISO 18000-1	Reference Architecture that provides Generic Parameters
	ISO 18000-2	Air Interface below 135 kHz
	ISO 18000-3	Air Interface at 13.56 MHz
	ISO 18000-4	Air Interface at 2.45 GHz
	ISO 18000-5	Air Interface at 5.6 GHz
	ISO 18000-6	Air Interface at UHF; 860 MHz to 960 MHz
	ISO 18000-7	Air Interface at 433 MHz
	ISO 15961	Data Protocol: Application Interface
	ISO 15962	Data Protocol: Data Encoding/Syntax Rules
	ISO 15963	Unique ID
	ISO 18001	Application Requirements Profiles

	ISO 18046	Tag and Reader Performance Test Method
	ISO 18047	Device Conformance Test Method
Near Field Communication	ISO 18092	Near Field Communication Interface & Protocol

Table 2-1: International RFID standards and their applications

In Table 2-1, there are four frequency ranges that are generally used for RFID systems.

- 125/134KHz or low frequency (LF)
- 13.56MHz or high frequency (HF)
- 433/869/915MHz or ultra-high frequency (UHF)
- 2.45/5.8GHz or micro-wave (μW)

In Table 2-2, the typical relative performance of systems employing the various technologies is shown.

Frequency Range	LF 125 KHz	HF 13.56 MHz	UHF 868 - 915 MHz	Microwave 2.45 GHz & 5.8 GHz
Typical Max Read Range (Passive Tags)	< 0.5 m	1 m	3 m	1 m
General Characteristics	Relatively expensive, even at high volumes. Low frequency requires a longer more expensive copper antenna. Additionally, inductive tags are more expensive than a capacitive tag. Least susceptible to performance degradations from metal and liquids, though	Less expensive than inductive LF tags. Relatively short read range and slower data rates when compared to higher frequencies. Best suited for application that does not require long range reading of multiple tags.	In large volumes, UHF tags have the potential for being cheaper than LF and HF tags due to recent advances in IC design. Offers good balance between range and performance - especially for reading multiple tags.	Similar characteristics to the UHF tag but with faster read rates. A drawback to this band is that microwave transmissions are the most susceptible to performance degradations due to metal and liquids, among other materials. Offers the most directional signal, ideal for

	read range is very short.			certain applications.
Tag Power Source	Generally passive tags only, using inductive coupling	Generally passive tags only, using inductive or capacitive coupling	Active tags with integral battery or passive tags using capacitive, E-field coupling	Active tags with integral battery or passive tags using capacitive, E-field coupling
Typical Applications	Access control, animal tracking, vehicle immobilizers, POS application including SpeedPass	"Smart Cards", Item-level tracking including baggage handling (Non-US), libraries	Pallet tracking, electric toll collection, baggage handling (US)	SCM, electronic toll collection
Notes	Largest install base due to the mature nature of low frequency, inductive transponders	Currently the most widely available high frequency worldwide, due mainly to the relatively wide adoption of smart cards	Japan does not allow transmissions in this band. Europe allows 868 MHz whereas the US permits operation at 915MHz, but at higher power levels.	
Data Rate	Slower	<==========>		Faster
Ability to read near metal or wet surfaces	Better	<==========>		Worse
Passive Tag Size	Larger	<==========>		Smaller

Table 2-2: Performance of various RFID Technologies

SAQ 2.24 What is the maximum reading range of LF passive RFID tag?
SAQ 2.25 What is the advantage of LF system compared to microwave system in RFID?
SAQ 2.26 State the three advantages of high frequency microwave system compared to LF system in using RFID?
SAQ 2.27 Provide the three examples of RFID application systems.

Chapter 3: Understand Wireless Local Area Network technology

Learning Objectives

- Explain the architecture of WLAN and distinguish between ad-hoc and infrastructure modes
- Describe the different Implementations of IEEE 802.11 Standard
- Understand the MAC Functional Operation
- Understand the WLAN Frame Format
- Explain the list of Logical Services
- Explain the WLAN Power Management
- Understand the IEEE 802.11 Securities
- Explain the examples of WLAN Applications
- Understand the advantages of WLANs

Section 3.1: IEEE 802.11a/b/g/n/ac Architecture

Wireless Local Area Network (WLAN) or IEEE 802.11 has been a very successful wireless technology for local area network. Today, it is being installed in many companies, homes, educational institutions as well as public places (known as hotspots) to allow users to be connected to the Internet. Not only has it been used to increase user mobility, it is now a cheaper and easier alternative compared to wired networks in setting up a LAN.

The IEEE 802.11 standard specifies only the *first two layers* of the OSI reference model; namely Physical and Data Link layers. (Refer to Figure 3.1 below.) Therefore, it still requires an understanding of the IEEE 802.1 MAC, IEEE 802.2 LLC and higher layer protocols such as IP and TCP. These protocols are covered in Network & Protocol module.

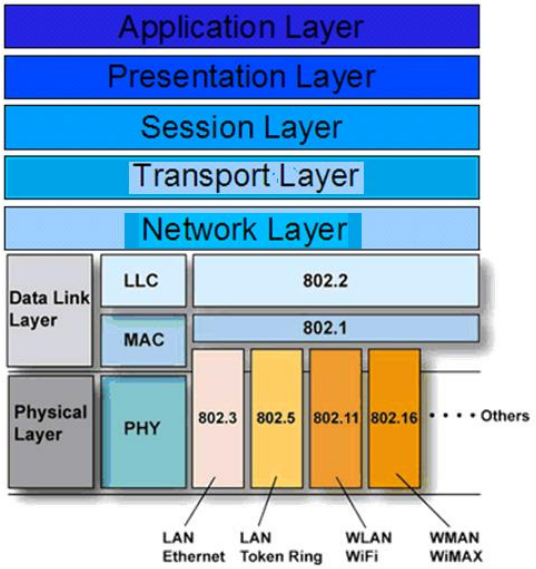


Figure 3.1: OSI layer with emphasis on WLAN

Example 3.1
Why does IEEE802.11 specify only Physical and Data Link layers only?

IEEE802.11 changes the physical connection from wires to wireless. With the change in physical connection, the mechanism to allow multiple devices sharing the same wireless medium is also different from the mechanism used in wired networks. Therefore, the Data Link layer is also different.

The architecture of IEEE 802.11 contains many components. Basic Service Set (**BSS)** is the basic building block, as shown in Figure 3.2, where there are two Stations (**STAs)** as members of each BSS. The two STAs in each BSS can communicate with each other, but not from one STAs in one BSS to another STA in another BSS. This mode of operation is **ad-hoc** and the BSS is known as Independent Basic Service Set (**IBSS)**.

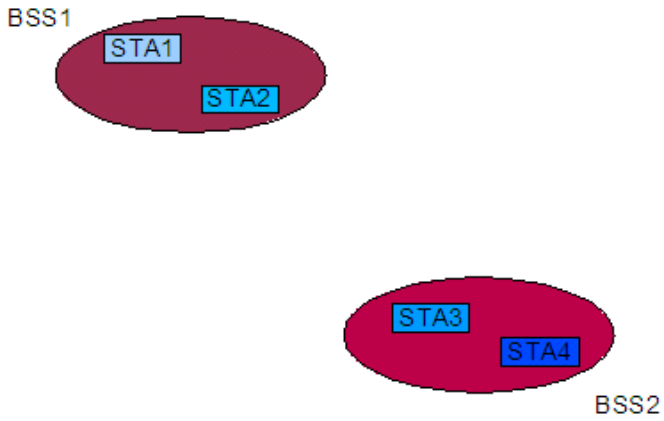


Figure 3.2: Basic service set

Instead of existing independently, multiple BSSs can be interconnected together through a Distribution System (**DS)**, as shown in Figure 3.3. The DS enables mobile device support by providing the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs. To connect a BSS to a DS, an Access Point (AP) is used. It is a STA that provides access to the DS by providing DS services in addition to acting as a STA. This mode of operation is **infrastructure** and the larger network is now known as Extended Service Set (**ESS)**.

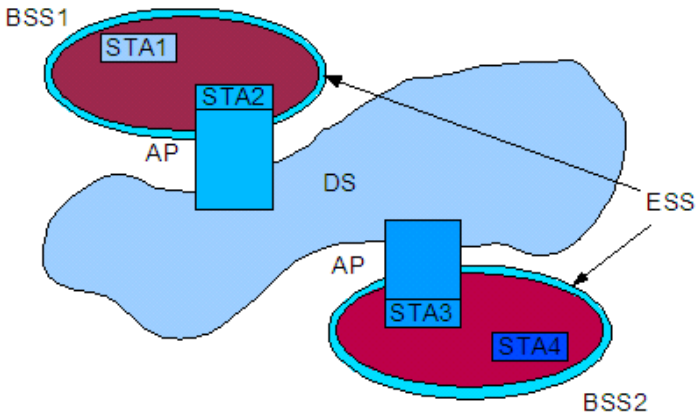


Figure 3.3: Extended service set with distribution system

The key concept of ESS is that it appears the same to a Logical and Link Control (LLC) layer as an IBSS network. The ESS network can have the following configurations:

1. *The BSSs may partially overlap*. This is commonly used to arrange contiguous coverage.
2. *The BSSs could be physically disjointed*. Logically there is no limit to the distance between BSSs.
3. *The BSSs may be physically co-located*.
4. *One or more IBSS or ESS networks may be physically present in the same space as one or more ESS networks*. This may arise when an ad-hoc network is operating in a location that also has an ESS network, or when physically overlapping IEEE 802.11 networks have been setup by different organizations.

Example 3.2
In a hotspot in Starbucks, a user can access Internet through either SingNet or StarHub systems. Which of the four configurations above is used to explain this scenario?

Fourth configuration where one or more IBSS or ESS networks may be physically present in the same space as one or more ESS networks.

To integrate the IEEE 802.11 architecture with a traditional wired LAN, a **portal** is used, as shown in Figure 3.4. It provides logical integration between the IEEE 802.11 architecture and existing wired LAN.

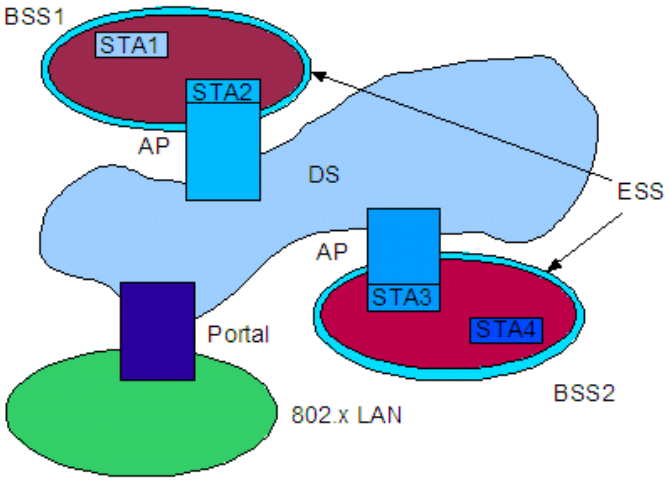


Figure 3.4: Connection to other IEEE 802 LANs

Example 3.3
Wireless networks are inherently less secure than wired networks. Where is the best place to install firewall to filter unauthorized users from accessing sensitive information located in Intranet?

Portal

Section 3.2: Different implementations of IEEE 802.11 standards

The different implementations of IEEE 802.11 standards are shown in Table 3.1 below.

Standard	Multiple Assess Protocol	Frequency	Modulation	Bit rate
IEEE 802.11a	OFDM	5.2 GHz UNII 5.8 GHz ISM	BPSK, QPSK, 16 QAM, 64 QAM	6, 9, 12, 18, 24, 36, 48, 54 Mbps
IEEE 802.11b	DSSS, FHSS	2.4 GHz ISM	DBPSK, DQPSK, CCK	1, 2, 5.5, 11 Mbps
IEEE 802.11g	OFDM	2.4 GHz ISM	BPSK, QPSK, 16QAM, 64QAM	6, 9, 12, 18, 24, 36, 48, 54 Mbps
IEEE 802.11n	OFDM/MIMO	2.4 GHz ISM, 5 GHz (Optional)	BPSK, QPSK, 16QAM, 64QAM	600 Mbps (Max)
IEEE 802.11ac	OFDM/MU-MIMO	5.2 GHz UNII 5.8 GHz ISM	BPSK, QPSK, 16QAM, 64QAM, 256QAM	1.3 Gbps (Max)

Note: ISM ➔ Industrial Science and Medical
UNII ➔ Unlicensed National Information Infrastructure
OFDM ➔ Orthogonal Frequency Division Multiplexing
DSSS ➔ Direct Sequence Spread Spectrum
FHSS ➔ Frequency Hopping Spread Spectrum
MIMO ➔ Multiple Input Multiple Output
MU-MIMO ➔ Multi User MIMO

Table 3.1: Differences between IEEE 802.11a/b/g

New implementations for WLAN, IEEE 802.11n standard and IEEE802.11ac were published in October, 2009 and December, 2013 respectively. IEEE 802.11n can possibly have a maximum bit rate of 600 Mbps and IEEE 802.11ac can possibly have a maximum bit rate of 1,3 Gbps. These standards were incorporated some of the advanced features like OFDM-MIMO and carrier aggregation/channel bonding (CA/CB) techniques that claims to extend the coverage area and increase the bit rate significantly compared to IEEE 802.11a/b/g.

In the next three sections, we will focus to study the additional features added into the IEEE 802.11 standard for IEEE 802.11a/b/g implementations which are mainly on the physical layer.

Example 3.4

Which of the following standards IEEE802.11a/b/g has the best features?

IEEE802.11g has the best features since it has the highest bit rate (similar to IEEE802.11a) and also largest coverage areas (similar to IEEE802.11b).

Section 3.3: IEEE 802.11b

The protocol used for IEEE 802.11b is **Direct Sequence Spread Spectrum**, where the narrow band spectrum is spread to a wider spectrum. This can be achieved by multiplying the data bits with a much longer chip sequence. This concept is illustrated in Figure 3.5 where chip sequence 1001 is used for bit 1 and chip sequence 0110 is used for bit 0.

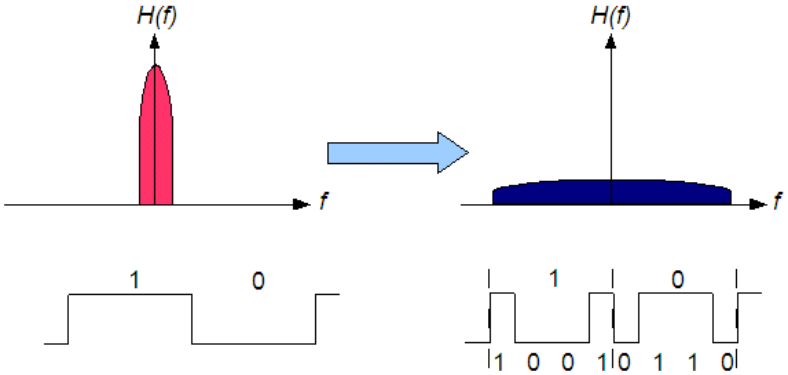


Figure 3.5: Direct sequence spread spectrum

Depending on the signal quality, the modulation technique used will change the bit rate from 1 Mbps (very low signal level) to 2 Mbps to 5.5 Mbps to 11 Mbps (very strong signal level). Though the bit rate changes, the chip rate remains to be 11 Mcps. As a result, the bandwidth is **22 MHz**. This can be achieved using the following modulation technique

- For 1 Mbps, the modulation technique is DBPSK with symbol rate of 1 Mbaud and the number of chips per symbol is 11.

$$\text{Bit rate} = 1 \text{ Mbaud} \times 1 \text{ bits/symbol} = 1 \text{ Mbps}$$

$$\text{Chip rate} = 1 \text{ Mbaud} \times 11 \text{ chips/symbol} = 11 \text{ Mcps}$$

Equation 3.1: Bit rate and chip rate for 1 Mbps

- For 2 Mbps, the modulation technique is DQPSK with symbol rate of 1 Mbaud and the number of chips per symbol is 11.

$$\text{Bit rate} = 1 \text{ Mbaud} \times 2 \text{ bits/symbol} = 2 \text{ Mbps}$$

$$\text{Chip rate} = 1 \text{ Mbaud} \times 11 \text{ chips/symbol} = 11 \text{ Mcps}$$

Equation 3.2: Bit rate and chip rate for 2 Mbps

- For 5.5 Mbps, the modulation technique is DQPSK with symbol rate of 1.375 Mbaud and the number of chips per symbol is 8. Also, CCK is used to encode 2 bits in a 4 complex chip sequence. The overall modulation is known as 2-DQPSK.

Bit rate = 1.375 Mbaud × 2 bits/symbol × 2 bits/chip sequence = 5.5 Mbps

Equation 3.3: Bit rate and chip rate for 5.5 Mbps

- For 1 Mbps, the modulation technique is DQPSK with symbol rate of 1.375 Mbaud and the number of chips per symbol is 8. Also, CCK is used to encode 4 bits in a 16 complex chip sequence. The overall modulation technique is known as 4-DQPSK.

Bit rate = 1.375 Mbaud × 2 bits/symbol × 4 bits/chip sequence = 11 Mbps

Equation 3.4: Bit rate and chip rate for 1 Mbps

Example 3.5
Referring to Equation 3.3 and Equation 3.4, how does CCK is able to increase the bit rate to 5.5 Mbps and 11 Mbps respectively?

CCK refers to a selection method for complex chip sequence based on the transmitted bits. In Equation 3.1 and Equation 3.2, there is only one complex chip sequence used. In Equation 3.3, four complex chips sequences are available which enable two bits ($2^2 = 4$) to be encoded. In Equation 3.4, sixteen complex chip sequences are available which enable four bits ($2^4 = 16$) to be encoded.

As mentioned earlier, IEEE 802.11b operates in the 2.4GHz ISM band and the bandwidth is 22 MHz. Currently, 14 carrier frequencies are defined and they are 5 MHz apart, as shown in Figure 3.6.

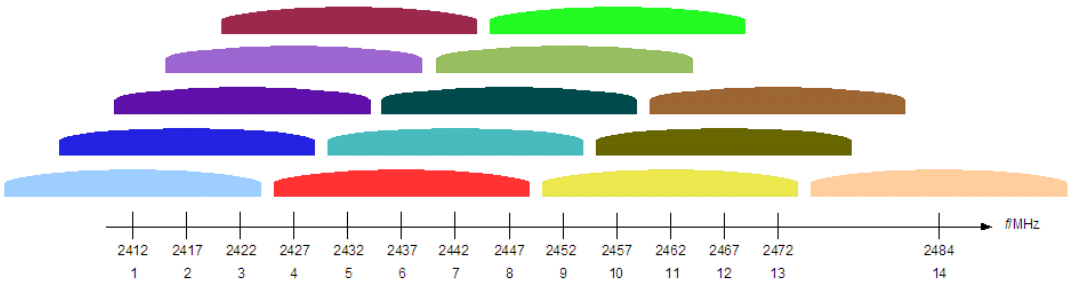


Figure 3.6: Frequency channels available for IEEE 802.11b

In Figure 3.6, it is shown clearly that there are 4 non-overlapping channels available; namely 1, 6, 11 and 14. This means that we can place up to 4 IEEE 802.11b access points on the same location without having much interference from one another. (However, only Japan includes channel 14 into their 2.4GHz ISM band. Therefore, the commonly known 3 non-overlapping channels are 1, 6 and 11.) When more access points are needed on the same location or to provide continuous coverage, some overlapping between these frequency channels may be unavoidable.

Section 3.4: IEEE 802.11a

The protocol used for IEEE 802.11a is **Orthogonal Frequency Division Multiplexing**, where the wide spectrum is divided into many sub-carrier narrowband spectrums, as shown in Figure 3.7. In a very simplistic explanation, OFDM can be viewed as an extension of Frequency Division Multiple Access technique. In FDMA, the spectrum is divided into multiple frequency channels and these frequency channels do not interfere with one another. Then, each user is allocated one of these frequency channels and different users transmit independently of one another over different frequency channels. In OFDM, the frequency channel allocated for one user is further divided into multiple sub-carriers and data from one user is transmitted independently over these sub-carriers. However, in OFDM, the frequency channels are divided such that there is no guard band needed between different sub-carriers and as a result, the maximum number of sub-carriers can be packed together to optimize the frequency channel allocated. In Figure 3.7, you can observe that the peak of any sub-carrier corresponds to the null of all other sub-carriers. As a result, the sub-carriers do not interfere one another.

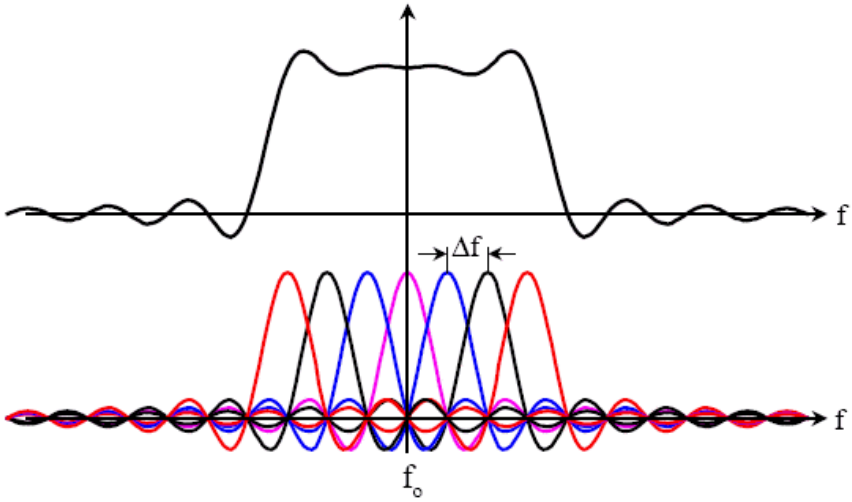


Figure 3.7: Orthogonal Frequency Division Multiplexing

In IEEE 802.11a, the bandwidth for each frequency channel is 20 MHz and there are 52 sub-carriers in each frequency channel. 48 of them are used for data transmission and the remaining four are used for pilot transmission used for synchronization. Depending on the signal quality, the modulation technique and the convolutional coding used will change the bit rate from 6 Mbps (very low signal level) to 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps 36 Mbps, 48 Mbps to 54 Mbps (very strong signal level). Out of these 8 different bit rates, only 6 Mbps, 12 Mbps and 24 Mbps are mandatory. Though the bit rate changes, the symbol rate, $Rate_s$, for each sub-carrier is 0.25 Mbaud.

The calculation for these various bit rates are shown in Table 3.2 below.

Bit Rate (Mbps) $Rate_b$ $=Rate_s \times NDBPS$	Modulation	Coding Rate R	Coded Bits per Sub-Carrier NBPSC	Coded Bits per OFDM Symbol NCBPS =NBPSC × 48	Data Bits per OFDM Symbol NDBPS =NCBPS × R

6	BPSK	$\frac{1}{2}$	1	48	24
9		$\frac{3}{4}$	1	48	36
12	QPSK	$\frac{1}{2}$	2	96	48
18		$\frac{3}{4}$	2	96	72
24	16-QAM	$\frac{1}{2}$	4	192	96
36		$\frac{3}{4}$	4	192	144
48	64-QAM	$\frac{2}{3}$	6	288	192
54		$\frac{3}{4}$	6	288	216

Table 3.2: Different bit rates for IEEE 802.11a

We will illustrate the calculation above using bit rate of 6 Mbps. Since the modulation technique used is BPSK and there are 48 sub-carriers for data transmission, each symbol period will transmit 48 × 1 = 48 bits (NCBPS). However, the 12-rate convolutional coding means that only 24 bits (NDBPS) are actual data and the other 24 bits are parity bits. Since the symbol rate is 0.25 Mbaud, the bit rate is equal to 0.25 Mbaud × 24 bits = 6 Mbps.

Example 3.6
What is the bit rate if the modulation technique is 64-QAM and the convolutional coding is 3/4?

64-QAM means six bits per symbol ($2^6 = 64$). With 48 data channels, the coded bits per OFDM Symbol is 48 × 6 = 288. Then, data bits per OFDM Symbol is 288 × (3/4) = 216. Finally, the bit rate is 0.25 x 216 = 54.

Example 3.7
Simplify the equation for bit rate, $Rate_b$?

Using the notation given in the first row of Table 3.2, $Rate_b = 0.25 \times R \times 48 \times \log_2 M$ where M is the order of modulation.

There are 16 frequency channels allocated in IEEE 802.11a. Out of these 16 frequency channels, there are 12 non-overlapping frequency channels. This is clearly illustrated in Figure 3.8.

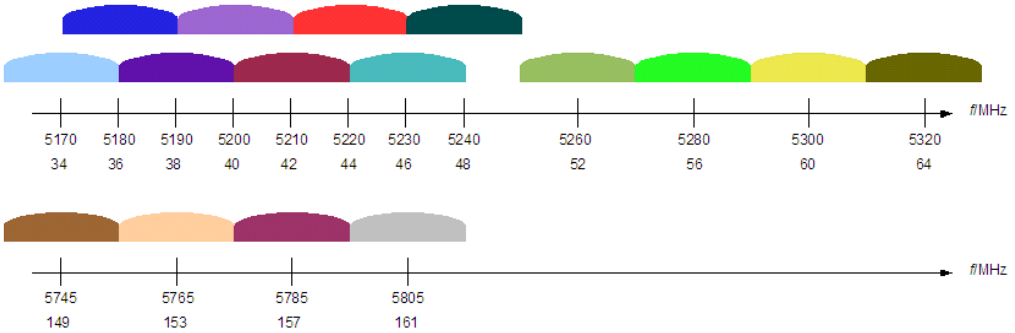


Figure 3.8: Frequency channels available for IEEE 802.11a

Section 3.5: IEEE 802.11g

IEEE 802.11g standard was approved in June 2003, much later than IEEE 802.11a/b which were rectified in 1999. The advantage of IEEE 802.11b compared to IEEE 802.11a is that the coverage or range is much wider than IEEE 802.11a. Its disadvantage is that the bit rate is much lower compared to IEEE 802.11a. Therefore, IEEE 802.11g is approved to marry the better of these two standards. In other words, IEEE 802.11g has the same protocol, modulation technique and error correction capability as IEEE 802.11a, as shown in Table 3.1 and uses the same frequency channels as IEEE 802.11b, as shown in Figure 3.6.

Example 3.8
What is the disadvantage of IEEE802.11g compared to IEEE802.11a?

IEEE802.11g has only 3 (or 4 in Japan) non-overlapping frequency channels whereas IEEE802.11a has 12 non-overlapping frequency channels.

Section 3.6: MAC functional operation

The fundamental access method of the IEEE 802.11 MAC is a Distributed Coordination Function (DCF) known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). (For wired Ethernet, the access method is Carrier Sense Multiple Access with Collision Detection (CSMA/CD) which is being used in Network & Protocol module.) The CSMA/CA is designed to reduce the collision probability between multiple STAs accessing a medium.

Example 3.9
IEEE802.11 specifies the Data Link layer by using CSMA/CD instead of CSMA/CA in wired networks. Why is there a need to change from collision avoidance to collision detection?

Due to the wireless medium, it is not possible to allow multiple STAs to transmit together without interference over the same frequency at the same time and without the use of orthogonal codes. Also, antennas are not able to transmit and receive over the same frequency at the same time. As a result, collision avoidance is not possible because it requires sending packets and listening packets at the same time. Since collision detection is impossible in wireless medium, mechanism has to be in placed to avoid collision.

Section 3.6.1: CSMA/CA without RTS/CTS

For a STA to transmit, it shall sense the medium to determine if another STA is transmitting. If the medium is not determined to be busy, the transmission may proceed. The highest probability of a collision exists at the initial transmission since multiple STAs could have been waiting for the medium to become available again. The CDMA/CA distributed algorithm mandates that a gap of a minimum specified duration known as (IFS exist between contiguous frame sequences. A transmitting STA shall ensure that the medium is idle for this required duration before attempting to transmit. If the medium is determined to be busy, the STA shall defer until the end of the current transmission. After deferral, or prior to attempting to transmit again immediately after a successful transmission, the STA shall select a random backoff interval and shall decrement the backoff interval counter while the medium is idle. The backoff procedure is designed to resolve medium contention conflicts so as to reduce the collision probability at the initial transmission. An example of this **physical carrier-sense mechanism** is shown in Figure 3.9.

Figure 3.9: DCF operation without RTS/CTS

Example 3.10
What is the purpose of the random backoff interval in CSMA?

The random backoff interval attempts to prevent two or more STAs that are waiting for the wireless medium to be available from transmitting together once it is idle.

Section 3.6.2: CSMA/CA with RTS/CTS

A refinement of the method may be used under various circumstances to further minimise collisions - here the transmitting and receiving STAs exchange short control frames (RTS and CTS) after determining that the medium is idle and after any deferrals or backoffs, prior to data transmission. *The exchange of **RTS** and **CTS** frames prior to the actual data frame is one means of distribution of the medium reservation information*. In the Duration/ID field of RTS and CTS frames, it contains the period of time that the medium is to be reserved to transmit the actual data frame and the returning ACK frame. All STAs within the reception range of either the originating STA (which transmits the RTS) or the destination STA (which transmits the CTS) shall learn of this medium reservation. Thus a STA can be unable to receive from the originating STA, yet still know about the impending use of the medium to transmit a data frame. Another means of distributing the medium reservation information is

the Duration/ID field in directed frames. This field gives the time that the medium is reserved, either to the end of the immediately following ACK, or in the case of a fragment sequence, to the end of the ACK following the next fragment.

The RTS/CTS exchange also performs both a type of fast collision inference and a transmission path check. If the return CTS is not detected by the STA originating the RTS, the originating STA may repeat the process (after observing the other medium-use rules) more quickly than if the long data frame has been transmitted and a return ACK frame had not been detected.

The medium reservation information is kept as the **NAV** in each STA. The NAV maintains a prediction of future traffic on the medium and together with the status of the physical carrier sense, they will be used to determine the busy/idle state of the medium. The NAV is updated with the information received in the Duration/ID field but only when the new NAV value is greater than the current NAV value and only when the frame is not addressed to the receiving STA. Figure 3.10 shows an example of the NAV settings based on the reception of the RTS frame and reception of the CTS frame for other STA.

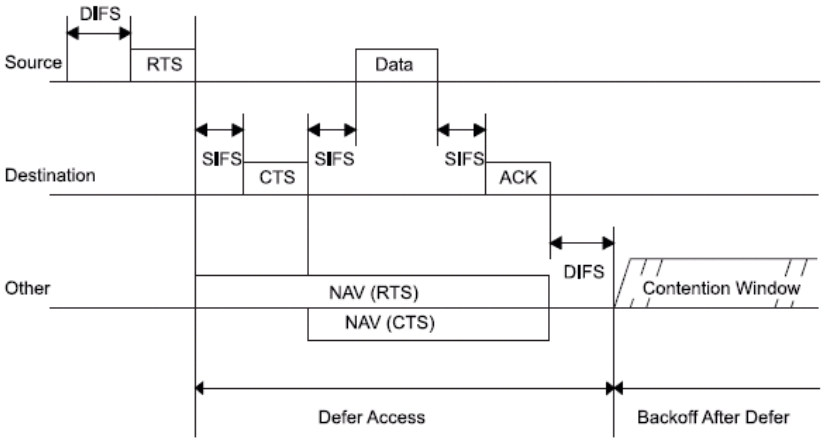


Figure 3.10: RTS/CTS/data/ACK and NAV setting

Another advantage of the RTS/CTS mechanism occurs where multiple BSSs utilizing the same channel overlap. *The medium reservation mechanism works across the different basic service area such that when STA from one BSS transmits, the rest of the STAs in the same BSS or other overlap BSSs will be prevented from transmitting any packets.*

However, it has to be noted that the RTS/CTS mechanism cannot be used for MAC Protocol Data Units (MPDUs) with broadcast and multicast immediate address because there are multiple destinations for the RTS, and thus potentially multiple concurrent senders of the CTS in response. An example of this **virtual carrier-sense mechanism** is shown in Figure 3.11.

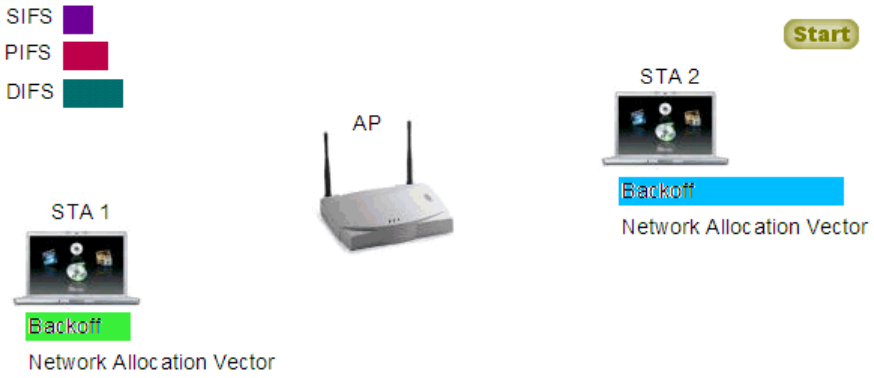


Figure 3.11: DCF operation with RTS/CTS

Example 3.11
In Figure 3.10, explain why the Interframe Space (IFS) between RTS and CTS is SIFS?

This will ensure that the receiver STA is able to transmit CTS before other STAs have the opportunity to transmit other types of packets since SIFS is the shortest.

Section 3.6.3: CSMA/CA with Point Coordination Function (PCF)

The IEEE 802.11 MAC may also incorporate an optional access method call a **PCF**, which is only usable on infrastructure network configurations. *This access method uses a Point Coordinator (**PC**), which shall operate at the access point of the BSS, to determine which STA currently has the right to transmit*. (Note that not all AP can be PC and not STAs are CF-Pollable.) The operation is essentially that of polling with the PC performing the role of the polling master. The PCF uses a virtual carrier-sense mechanism aided by an access priority mechanism. It divides the access time into Contention Free Period (CFP) and the Contention Period (CP), as shown in Figure 3.12.

The PCF controls frame transfers during a CFP while the DCF controls frame transfers during the CP. The PCF shall distribute information within the Beacon management frames to gain control of the medium by setting the Network Allocation Vector (NAV) in STAs. In addition, all frame transmissions under the PCF may use the PIFS that is smaller than the DIFS. The use of smaller IFS implies that point-coordinated traffic shall have priority access to the medium over STAs in overlapping BSSs operating under the DCF access method.

Inside the Beacon frame, it also contains a Delivery Traffic Identification Map (DTIM). The CFPs shall occur at a defined repetition rate, known as CFPRate, which is defined as a number of DTIM intervals. The PC shall use the CFPRate (depicted as a repetition interval in the illustrations in Figure 3.12) which is available in the CF Parameter Set in the Beacon management frame.

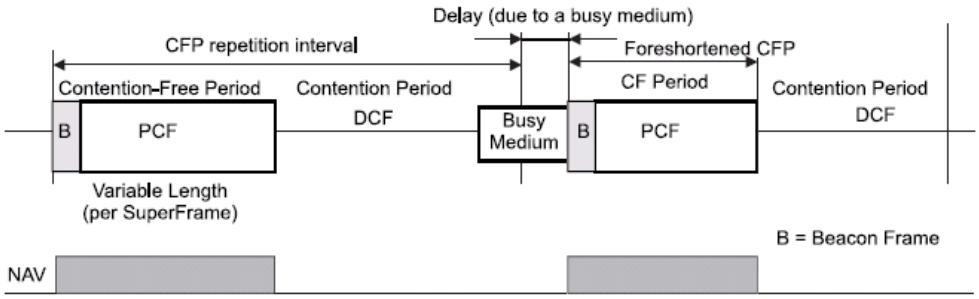


Figure 3.12: DCF and PCF operation

Example 3.12
How STAs operating in PCF does has a higher priority in gaining access to the wireless medium over STAs operating in DCF?

PCF uses PCF IFS (PIFS) which has shorter interval compared to DCF IFS (DIFS) used in DCF.

Section 3.6.4: Interframe space

IFS is the time interval between frames. Four different IFSs are defined to provide priority levels for access to the wireless medium, (WM) listed below from the shortest to the longest time interval.

1. **SIFS** is used for an ACK frame, a CTS frame, the second or subsequent MPDU of a fragment burst, by a STA responding to any polling by the PCF and by a PC for any types of frames during the CFP.
2. **PIFS** is used only by STAs operating under the PCF to gain priority access to the medium at the start of CFP.
3. **DIFS** is used by STAs operating under the DCF to MPDUs and MAC management protocol data units (MMPDUs).
4. **EIFS** is used by DCF whenever the PHY has indicated to the MAC that a frame transmission was begun that did not result in the correct reception of a complete MAC frame with a correct FCS value.

Figure 3.13 shows the some relationships between these IFS.

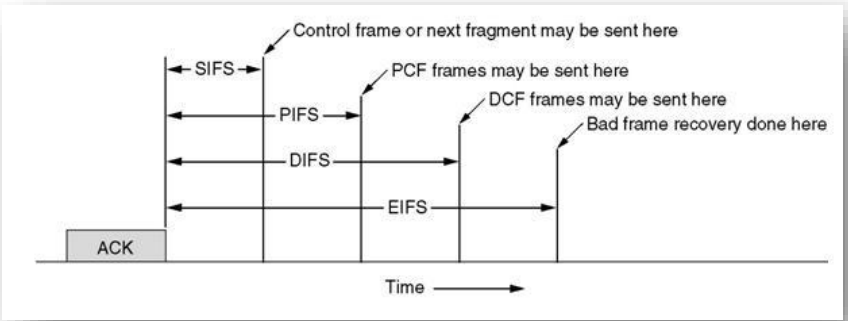


Figure 3.13: Some IFS relationships

Section 3.7: Frame format

It is important to understand the various frames that are available in WLAN so that in the later sections, you will be able to follow the concepts like probing, association, authentication, DCF, PCF and hidden nodes. Therefore, it may not be necessary for you to understand completely this section in your first reading.

Each frame consists of the following basic components:

- A **MAC header**, which comprises frame control, duration, address and sequence control information
- A variable length **frame body**, which contains information specific to the frame type
- A Frame Check Sequence (**FCS)**, which contains an IEEE 32-bit CRC

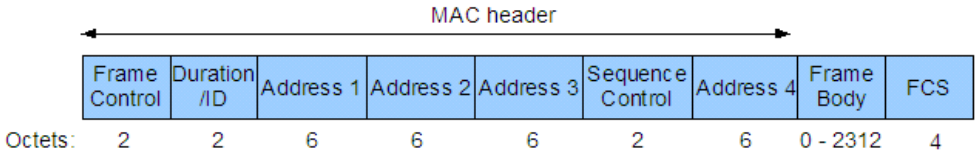


Figure 3.14: MAC frame format

Section 3.8: Logical service

The STA and DS provide nine different logical services for the wireless LAN operation. These services are transmitted using the management, control and data frames. The logical services can be divided into two categories:

- SS is implemented by every STA including AP.
    1. **Authentication**
    2. **Deauthentication**
    3. **Privacy**
    4. **DTIM delivery**

- DSS is provided by DS.
    1. **Association**
    2. **Disassociation**
    3. **Reassociation**
    4. **Distribution**
    5. **Integration**

Section 3.8.1: Relationship between services

To keep track of the authentication and association status, a STA keeps two state variables:

- **Authentication state**: The values are unauthenticated and authenticated.
- **Association state**: The values are unassociated and associated.

These two variables create three local states for each remote STA, as shown in Figure 3.15 below.

- **State 1**: Initial start state, unauthenticated, unassociated.
- **State 2**: Authenticated, unassociated.
- **State 3**: Authenticated, associated.

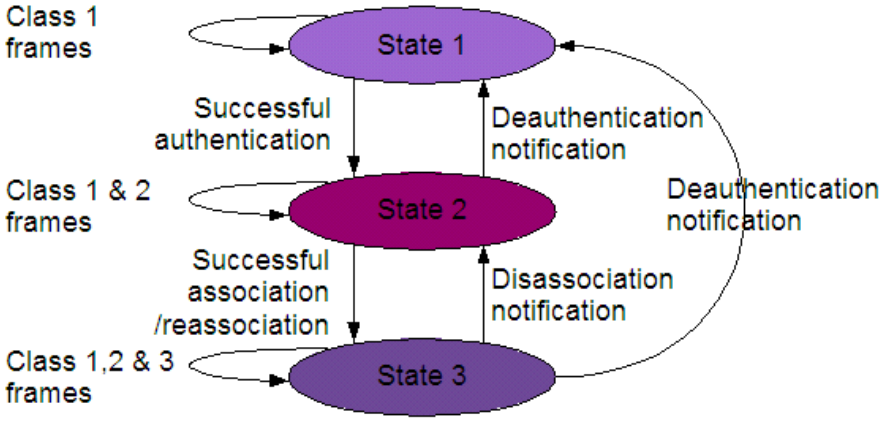


Figure 3.15: Relationship between state variables and services

The current state existing between the source and destination STAs determines the frame types and subtypes that may be exchanged between that pair of STAs. The allowed frame types and subtypes are grouped into classes and the classes correspond to the station state, as shown in Figure 3.15.
In Figure 3.16, the exchange of management packets between STA and two APs for authentication, association and reassociation are shown.

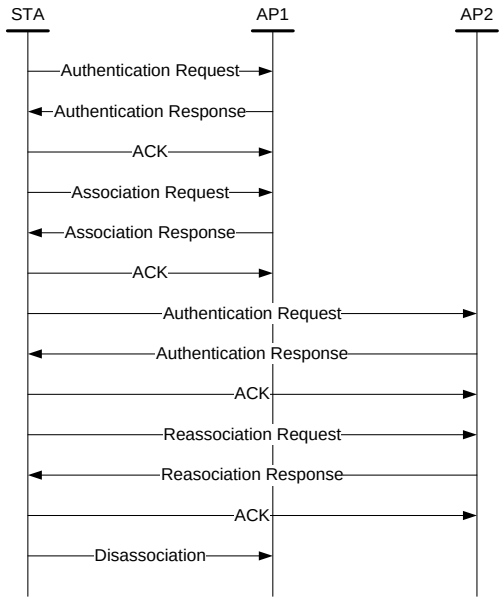


Figure 3.16: Exchange of management packets between STA and Aps

Section 3.9: Power Management

In IEEE 802.11 standards, power management allows the STA to be in sleep mode as much as possible to conserve battery life but still not miss out on data transmission. This can only be used when connecting in infrastructure mode. The key to power management is synchronization. Every STA on a WLAN has its own local timer. At regular intervals, the AP sends out a beacon signal that contains a timestamp to all STAs. When the STAs receive this frame from the AP, they synchronise their local timers with that of the AP.
When an STA goes into sleep mode, the AP is informed of the change. The AP has a record of those STAs that are awake and those that are sleeping. As the AP receives transmissions, it first checks whether the STA is in sleep mode. If it is sleeping, the AP temporarily stores (buffers) the synchronised frames.
At predetermine times, the AP sends out a beacon frame to all STAs. This frame contains a list, known as the Traffic Indication Map (TIM), of the STAs that have buffered frames waiting at the AP. At that same time, all STAs that have been sleeping must awaken and go into an active listening mode. If the STA learns that it has buffered frames waiting, the STA can send a request to the AP for those frames. If it has no buffered frames, it can return to sleep mode.

Section 3.10: IEEE 802.11 Securities

The IEEE 802.11 standard incorporates some basic security measures. Authentication and privacy processes inherent in IEEE 802.11 provide a basic level of user authorisation.

Section 3.10.1: Authentication

Authentication is a process that verifies that the STA has permission to access the network. In IEEE 802.11 WLAN, a Service Set Identifier (SSID) of the network has to be configured at all its APs. For authentication, a STA can be given an SSID in one of two ways. First, the SSID can be manually entered into the STA. Once it is entered, anyone who has access to that STA can see the SSID and freely distribute it. The second way is even less secure. APs can freely advertise the SSID to any mobile device that comes into the range of the AP. The default setting on most of the APs is freely broadcast SSIDs. For security measures to protect your network, APs should be configured not to broadcast the SSID. Hence, turning off SSID broadcast can protect the network against someone finding it unintentionally. When an STA transmits a probe frame, the AP will usually send a response that includes the SSID of the network. An attacker using a sniffing device will also be able to obtain the SSID of the access point as well.

Section 3.10.2: Privacy

Privacy attempts to ensure that the transmitted data are not read by unauthorised users, even if those transmissions fall into the wrong hands. This is accomplished with data encryption, which scrambles the data in a way that it cannot be read and can only be decoded by the intended recipient.

Section 3.10.2.1: Wired Equivalent Privacy (WEP)

The IEEE 802.11 standard provides an optional WEP specification for data encryption between wireless devices to prevent eavesdropping. WEP encryption comes in two versions: 64-bit encryption is actually made up of a 40-bit key (5 bytes or 10 hexadecimal digits) plus a 24 –bit initialisation vector (IV), which is a part of the encryption key that sent in **clear text**, before the encrypted data. Likewise, 128-bit encryption is made up of a 104-bit key plus a 24-bit IV. Some vendors offered 256-bit encryption in their product; however, this equipment also uses the same 24-bit IV. 256-bit encryption may not be compatible between products from different manufacturers.

Section 3.10.2.2: Wi-Fi Protected Access (WPA)

WPA is a standard for network authentication and encryption introduced by the Wi-Fi Alliance, in response to the **weakness in WEP** described in the previous section. WPA uses 128-bit pre-shared keys (PSK), which is also called personal mode. WPA-PSK uses a different encryption key for each client device, for each packet, for each session, unlike WEP, which only varies the 24-bit IV.

WPA employs the temporal key integrity protocol (TKIP), which provide per-packet key-mixing. In addition, TKIP also provides message integrity check (MIC), which uses a combination of variable and static items, such as the current network uptime or the value of a continually incrementing variable and other data items to ensure that the encrypted data has not been tampered with.
TKIP uses a 48-bit hashed initialization vector and also changes the key after a user-specified amount of time.
WPA2 is the version of WPA that has been certified by the IEEE to be compatible with IEEE 802.11i. It adds support for the advanced encryption standard (AES), which meets US government security requirements. However, because AES requires additional processing power, it may not be supported by older hardware.

Section 3.11: Examples of WLAN Applications

Wireless local area networks (WLANs) have become an essential amenity providing broadband coverage of entire campuses, public venues, private enterprises, and government facilities. And with this growth in popularity has come an increasing range of applications, users and bandwidth demands.
Wireless LANs frequently augment rather than replace wired LAN networks-often providing the final few meters of connectivity between a backbone network and the mobile user. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

- WLAN is used primarily for web browsing and e-mail.
- WLAN networks are now being tasked to support more demanding applications such as video surveillance, video conferencing and voice over IP (VoIP) services.
- *Doctors and nurses in hospitals* are more productive because hand-held or notebook computers with wireless LAN capability deliver patient information instantly.
- *Consulting or accounting audit engagement teams* or small workgroups increase productivity with quick network setup.
- *Network managers in dynamic environments* minimize the overhead of moves, adds, and changes with wireless LANs, thereby reducing the cost of LAN ownership.
- *Training sites at corporations and students at universities* use wireless connectivity to facilitate access to information, information exchanges, and learning.
- *Network managers installing networked computers in older buildings* find that wireless LANs are a cost-effective network infrastructure solution.
- *Retail store owners* use wireless networks to simply frequent network reconfiguration.
- *Trade show and branch office workers* minimize setup requirements by installing preconfigured wireless LANs needing no local MIS support.
- *Warehouse workers* use wireless LANs to exchange information with central databases and increase their productivity.
- Network managers implement wireless LANs to provide *backup for mission-critical applications* running on wired networks.
- *Senior executives in conference rooms* make quicker decisions because they have real-time information at their fingertips.

Section 3.12: Advantages of WLANs

The widespread strategic reliance on networking among competitive businesses and the meteoric growth of the Internet and online services are strong testimonies to the benefits of shared data and shared resources. With wireless LANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. Wireless LANs offer the following productivity, service, convenience, and cost advantages over traditional wired networks:

- **Mobility**-Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
- **Installation** Speed and Simplicity-Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- Installation **Flexibility**-Wireless technology allows the network to go where wire cannot go.
- **Reduced Cost**-of-Ownership-While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves, adds, and changes.
- **Scalability**-Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that allows roaming over a broad area.

Chapter 4: Understand Wireless Personal Area Network

Learning Objectives

- Explain "What is a WPAN?"
- Explain introduction to Bluetooth
- List the Bluetooth Protocol Stack
- Explain Bluetooth RF Layer
- Explain Bluetooth Baseband Layer
- Explain Bluetooth Link Manager Layer
- Understand Bluetooth Connection Procedure
- Understand Bluetooth Power Usage
- Describe other Layer and Functions
- List Bluetooth profiles
- Understand Bluetooth Applications
- Lists some examples of WPAN Applications

Section 4.1: What is a WPAN?

A wireless personal are network (WPAN) is a group of technologies that are designed for short-range communications from a few centimetres to about 10 meters, effectively eliminating the need for wires or cables to interconnect multiple devices.
All of these technologies include the ability to network, which means that the devices can communicate with each other. The IEEE is currently developing several different standards for WPANs. Bluetooth, ZigBee, and UWB are intended to enable connectivity for different types of devices and different purposes. Because of their differences, it is very important to understand each standard is implemented. In this chapter, Bluetooth technology will be covered in more details.
In addition to helping eliminate wires and cables, WPANs offer two other key advantages. First, because they are designed to communicate at short ranges, WPAN devices use very little power; therefore, the batteries that power the portable devices tend to last a long time. Second, their short range also helps maintain security and privacy, which has long been a concern with other wireless technologies. The IEEE 802.15 standards for WPANs shown in Figure 4.1 only consist of Physical layer and Data link layer.

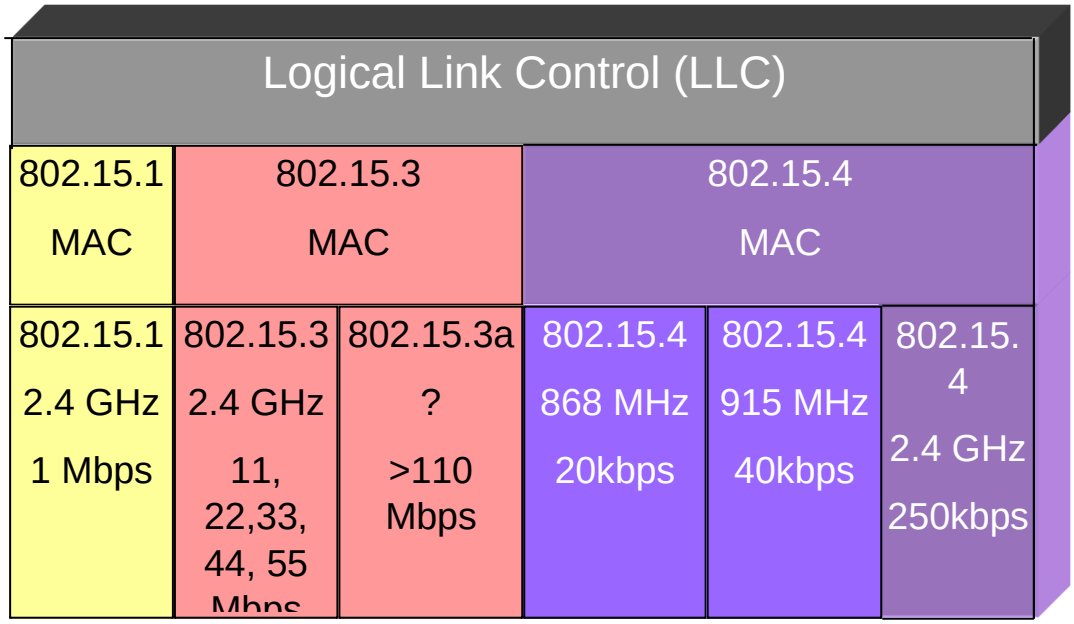


Figure 4.1: IEEE 802.15 Protocol Architecture

Section 4.2: Introduction to Bluetooth

Bluetooth is an industry specification that defines small-form-factor, low-cost wireless radio communications. Bluetooth is supported by over 2,500 hardware and software vendors who make up the Bluetooth Special Interest Group (SIG).
The IEEE licensed this wireless technology from the Bluetooth SIG to adapt and copy a portion of specification as the base material for IEEE 802.15.1; the new standard received final approval on March 2, 2002.

Section 4.2.1: Master and Slave

Bluetooth technology is designed based on a master-slave concept. When a Bluetooth-enabled device **initiates** a connection to another Bluetooth-enabled device, the **initiator** will take the **master** role and the **receptor** will take the **slave** role. The master controls all of the wireless traffic. The slave takes commands from the master.

Section 4.2.2: Piconet and Scatternet

This personal area network comprising of the master and the slave is known as *piconet*. Since there is only one connection from the master to the slave, it is known as *point-to-point* connection. The master can initiate another connection to a Bluetooth-enabled device and accept it into its existing piconet. Now, with one master and two slaves, it is known as *point-to-multipoint* connections. This process can go on until the master has a maximum of seven *active* slaves. Thereafter, if the master requires to accept another Bluetooth-enabled device, it has to either disconnect an existing active slave or to put an active slave into *park* mode

before it can accept it into its piconet. In other words, a master in a piconet can accept maximum of seven active slaves and 255 parked slaves. A master and slave can be switched roles in a piconet.

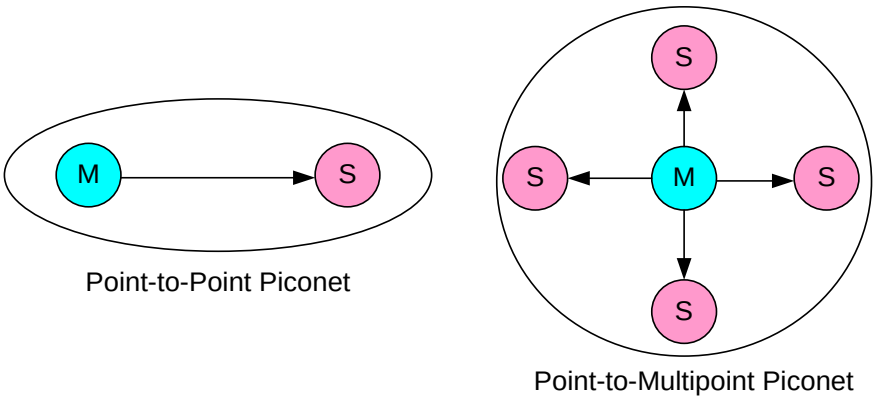


Figure 4.2: Bluetooth piconets

To expand the coverage area of a personal area network, two or more existing piconets can combine together to form a *scatternet*. This can be achieved through

1. a Bluetooth-enabled device that acts as a slave on both piconets, as shown in left-hand-side of Figure 4.3
2. a Bluetooth-enabled device that acts as a master in one piconet and as a slave in the other piconet, as shown in right-hand side of Figure 4.3

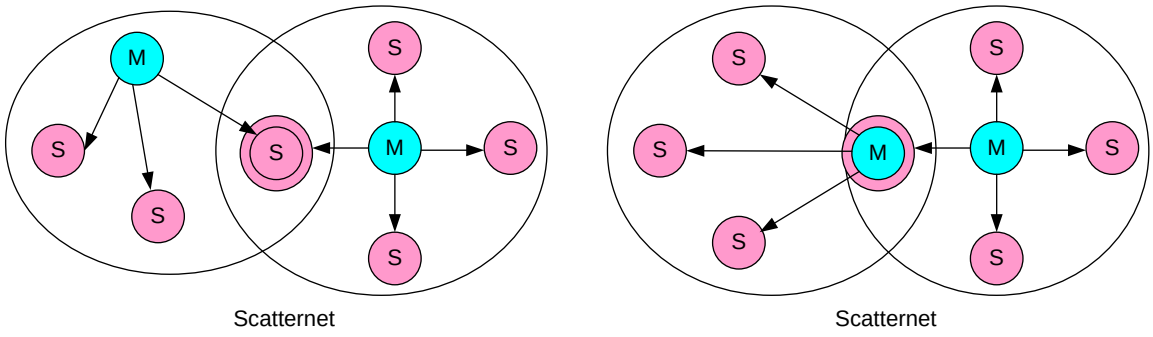


Figure 4.3: Scatternet

Example 4.1

Is it possible to form a scatternet using a Bluetooth-enabled device that acts as a master on both piconets?
No, this is because the two piconets are actually one piconet since there must be one and only one master in each piconet.

Example 4.2

Can an initiator become a slave in a piconet?
Yes, this happens when there is a request for master-slave switch.

Section 4.3: Bluetooth Protocol Stack

Generally speaking, the functions of the stack can be divided into two parts based on how they are implemented. The lower levels of the stack are implemented in the hardware, while the functions of the upper levels of the stack are implemented in software. These functions are discussed in the sections that follow. Figure 4.4 illustrates the Bluetooth protocol stack and compares it to the OSI protocol model.

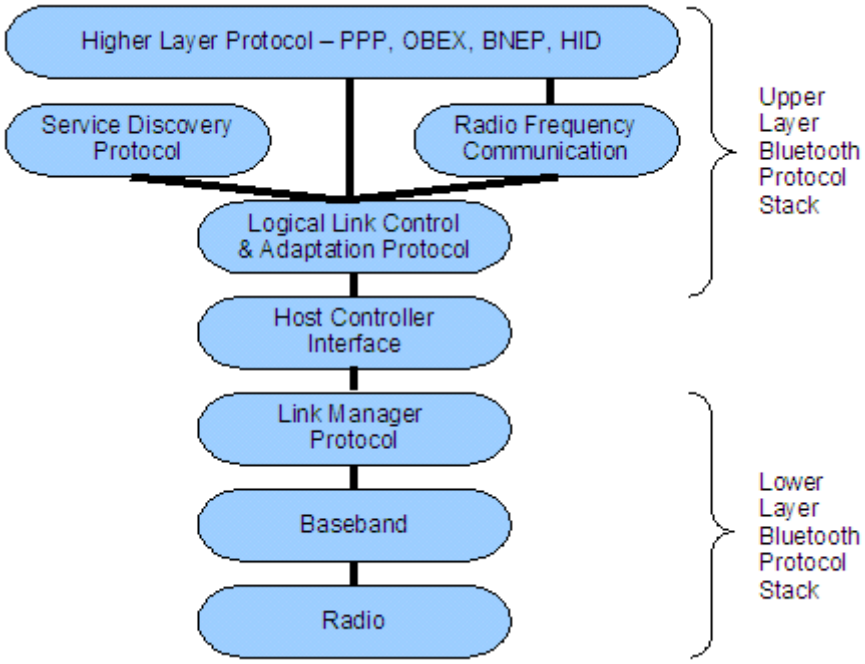


Figure 4.4: Bluetooth Protocol Stack

Section 4.4: Bluetooth RF Layer

At the lowest level of the Bluetooth protocol stack in the RF layer. It defines how the basic hardware that controls the radio transmissions functions. At this level, the data bits (0 and 1) are converted into radio signals and transmitted.

Section 4.4.1: Bluetooth Radio

At the heart of the Bluetooth RF layer is a single radio transmitter/receiver (transceiver). The single tiny chip is called a Bluetooth radio module. Bluetooth has three power classes for transmitting. These determine the communication range between devices and are summarized in the following.
The three different types of radio powers are:

- Class 1 = 100mW (20dBm)
- Class 2 = 2.5mW (4dBm)
- Class 3 = 1mW (0dBm)

This allows Bluetooth devices to connect at different ranges. The typical ranges of the three classes of radios are about 1 meter, 10 meters and 100 meters respectively based on the transmit power and receiver sensitivity. However, keep in mind that because Bluetooth is based on RF transmission, objects such as wells and interference from other sources can affect the range of transmission.

Section 4.4.2: Bit Rate

Bluetooth can transmit at a speed of up to 1 Mbps under the Bluetooth specification (versions 1.1 and 1.2). Most devices list their maximum data rate as 723 kbps, since transmission occurs in both directions with some time slots being used for transmission in one direction and some being used for transmission in the other direction.

Bluetooth version 2.0 adds two new modulations that help it achieve data rates of 2 or 3 Mbps while maintaining full backward compatibility with versions 1.1 and 1.2 at 1 Mbps. This new feature called enhanced data rate (EDR).

Bluetooth 3.0+HS (High Speed) includes a new feature called AMP (Alternative MAC/PHY) that provides theoretical data transfer speeds of up to 24 Mbit/s by the addition of IEEE 802.11 as a high speed transport. The Bluetooth link is used for negotiation and establishment, and the high data rate traffic is carried over a collocated 802.11 link.

The latest version of Bluetooth is Bluetooth version 4.0 called BLE (Bluetooth Low Energy). BLE is a subset of Bluetooth v4.0 with an entirely new protocol stack for rapid build-up of simple links. BLE does, however, use a simpler modulation system and is aimed at very low power applications running off a coin cell. It is very important to know that Bluetooth low energy is not backward-compatible with the previous, often called Classic, Bluetooth protocol. But the Bluetooth 4.0 specification permits devices to implement either or both of the LE and Classic systems. Those that implement both are known as Bluetooth 4.0 dual-mode devices.
Bluetooth LE uses the same 2.4 GHz radio frequencies as Classic Bluetooth, which allows dual-mode devices to share a single radio antenna.

Section 4.4.3.: Modulation Technique

Bluetooth version 1.1 and 1.2 use the frequency shift keying (FSK), which is a binary modulation technique that changes the frequency of the carrier signal. The frequency is higher to send a 1 data bit and lower to send a 0 data bit. The variation of FSK used by Bluetooth is known as two-level Gaussian frequency shift keying (2-GFSK). 2-GFSK uses two different frequencies to indicate whether a 1 or a 0 is being transmitted. The amount that frequency varies, called the modulation index, is between 0.28 and 0.35.

The most important parameters of the modulation are:

modulation type:	2FSK
symbol rate:	1 MHz
modulation index:	0.28 – 0.35
max. frequency deviation:	140 – 175 kHz

baseband filter: Gauss, B*T = 0.5

Section 4.4.4: Radio Frequency

The part of the spectrum in which Bluetooth operates is the 2.4 GHz Industrial, Scientific and Medical (ISM) band. Bluetooth divides this 2.4 GHz frequency into 79 different frequencies, called channels, spaced 1 MHz apart. Bluetooth uses the frequency hopping spread spectrum (FHSS) technique to send a transmission; the specific sequence of frequencies used, or hopping sequence, is called a channel. This means that the radio frequency hops, or changes rapidly, through the 79 different frequencies during transmission. This is illustrated in Figure 4.5. In just one second of Bluetooth transmission, the frequency changes 1,600 times, or once every 625 microseconds.

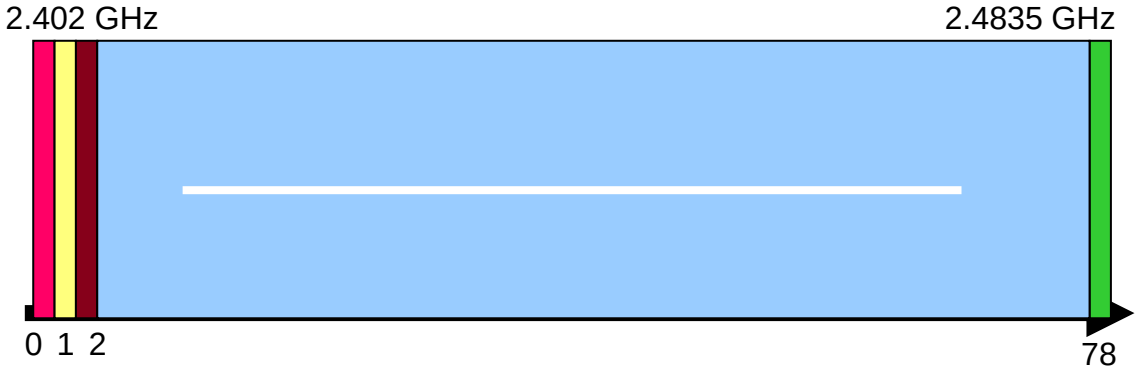


Figure 4.5: Bluetooth frequency channels

Bluetooth uses the same frequency as IEEE 802.11b WLANs. Devices that use Bluetooth can interfere with 802.11b WLANs and vice versa. Several solutions are available to avoid this conflict. Special software can be added to the 802.11b WLAN that manages the traffic flow by telling the 802.11b network to be quite when Bluetooth communications are detected. With the ratification of IEEE 802.15.1, manufacturers following the guidelines of this standard can ensure that 802.11b and Bluetooth work together with a minimum of interference and disruption. Bluetooth version 1.2 adds a feature called adaptive frequency hopping (AFH) that further improves compatibility with 802.11b, Bluetooth accomplishes this by allowing the master in a piconet to change the hopping sequence to that it will not use the frequency channel occupied by 802.11b in the piconet area.

Section 4.4.5: Time Division Duplexing

Bluetooth technology uses **TDD (Time Division Duplexing)**. This means that the master and slave transmit to one another on different time slots. The period for one time slot is **625 µs**. In Bluetooth technology, there are three possible packet size, namely 1-slot, 3-slot and 5-slot packets, as shown in Figure 4.6. As you can see, the master starts its transmission at even slots (channel numbers, n, n+2, n+4, ... in Figure 4.6) and the slave starts its transmission at odd slots (channel numbers n+1, n+3, n+5, ... in Figure 4.2), irrespective of the number of packet size.

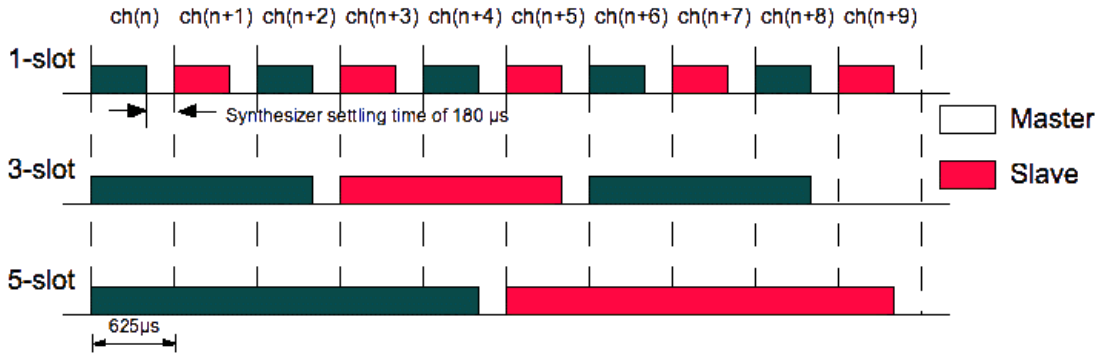


Figure 4.6: Time division duplexing using 1-slot, 3-slot and 5-slot packets

Section 4.5: Bluetooth Baseband Layer

The Baseband layer lies on top of the RF layer in the Bluetooth stack. This layer manages physical channels and links, handles packets, and does paging and inquiry to locate other Bluetooth devices in the area.

Section 4.5.1: Links between Bluetooth Devices

Managing the piconet involves such actions as regulating the steps for attaching and detaching slaves from the master as well as overseeing the master-slave switch. This involves establishing different types of links between Bluetooth devices. There are three types of physical links between devices supported in Bluetooth:

1. **ACL** for data information
2. **SCO** for voice information
3. **e-SCO** for voice information introduced in Bluetooth V1.2

An asynchronous connectionless (ACL) link is a packet-switched link that is used for data transmissions. The ACL link is from one master to all the slaves participating on the piconet. It is sometimes called a point-to-multipoint link. A piconet can support only a single ACL link between one master and up to seven slaves.

A synchronous connection-oriented (SCO) link is a symmetric point-to-point link between a master and s single slave in the piconet. This link functions like a circuit-switched link by using reserved time slots at fixed intervals. A master can support up to three simultaneous SCO links, while slaves can support three SCO links to one master and two SCO links for different master. SCO packets are never retransmitted. An SCO link carries mainly voice transmissions at a speed of 64 kbps.

In the time slots not reserved for the SCO links, the master can establish an ACL and transfer data to any slave. A slave already engaged in a SCO can also have an ACL link.

Extended SCO (eSCO) provides improved voice quality of audio link. It allows retransmission of dropped eSCO packets and the use of CRC error checking.

Section 4.5.2: Bluetooth Device Address:

At the top of the panel Packet Editor the Bluetooth Device Address is located. A 12 digit long address can be entered in the 3 device address fields. The 3 parts, NAP (Non-Significant Address Part), UAP (Upper Address Part) and LAP (Lower Address Part) needs to be entered separately in hexadecimal representation as shown in Figure 4.7.

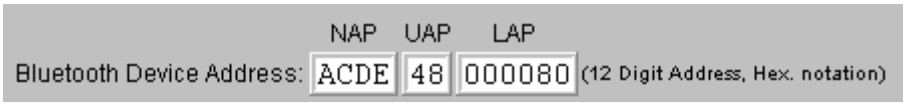


Figure 4.7: Bluetooth address

Section 4.5.3: Bluetooth Frames

The frame of a Bluetooth transmission is illustrated in Figure 4.8. Each frame contains three parts:
Access code (72 bits) – Contains data used for timing synchronization, paging and inquiry
Header (54 bits) – Contains information for packet acknowledgment, packet numbering, the slave address, the type of payload, and error checking
Payload (0-2745 bits) – Can contain data, voice, or both

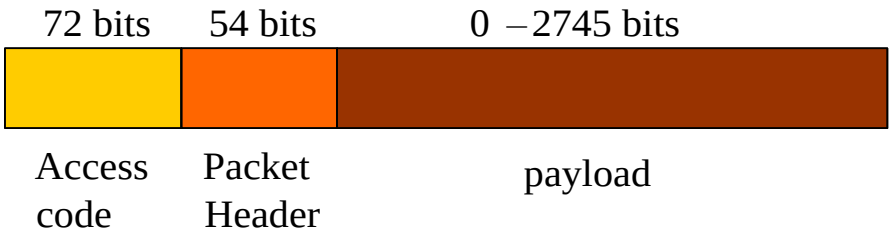
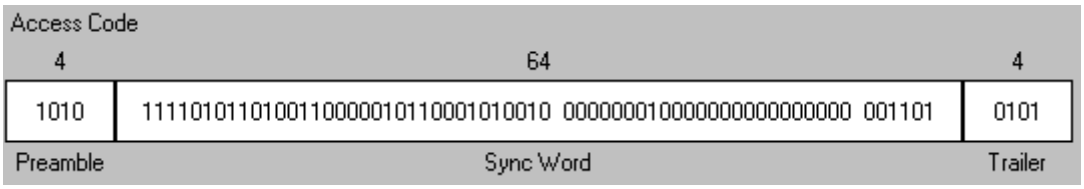


Figure 4.8: Bluetooth Frame

Access code

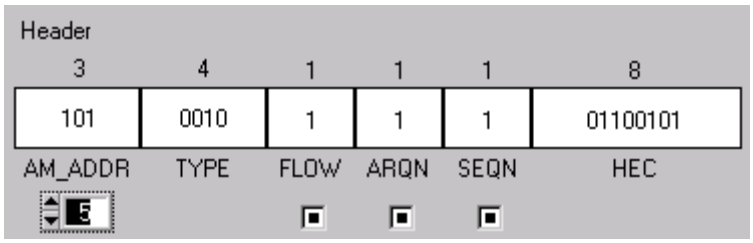
The content of the access code field is entirely calculated from the LAP of the Bluetooth Device Address.
The Preamble and Trailer depend on the leftmost and rightmost bit of the Sync Word, whereas the Sync Word itself is being calculated with an algorithm described in the Bluetooth Core spec. 1.1. The Sync Word is displayed in such a manner that the original LAP can still be seen in the middle of the word.



Bluetooth access code

Packet header

The Header itself consists of 6 parts, the AM address field, the packet type information field, bits for flow control, acknowledge and packet sequence number as well as the HEC (Header Error Check) - a Cyclic Redundancy (CRC) Check for checking the header for errors at the receiver.



Bluetooth Header

AM_ADDR: The Active Member Address specifies the addressed slave in a piconet.

TYPE: The packet's type code.

FLOW: The flow control bit for the master's receiver queue. Shall be set to 1 when the slave is intended to keep on sending packets.

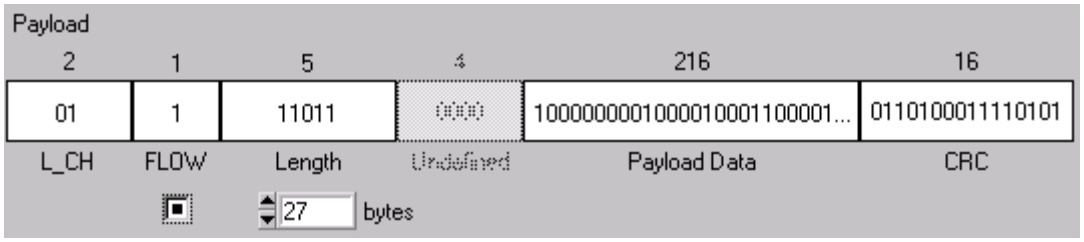
ARQN: Acknowledge bit for received packets. Shall be set to 1 if the last packet has been received without detected errors.

SEQN: Sequence number of the packet. In a real life scenario this bit is being alternated between sent packets, as long as no packet needs to be retransmitted. If it is necessary to retransmit a packet, the new copy gets the same number as the originally sent one.

HEC: The Header Error Check. The HEC code is calculated from the other 5 field settings.

The complete 18 header bits get a simple 1/3 Forward Error Correction (FEC), where every bit is transmitted three times. This makes a total of 54 transmitted header bits. Whitening is applied before the FEC.

Payload:



The payload part consists of a payload header, the payload data and a CRC part. The payload header contains the L_CH information field, an additional flow control bit and a 5

respectively 9 bit long length field. DH3 and DH5 packets also include an undefined field. For DH1 and AUX1 packets instead this field is greyed out.

L_CH: The L_CH code is used for identifying the logical channels. Code 01 (LSB left) identifies a starting L2CAP message, code 10 (LSB left) identifies a continued message part.

FLOW: The flow control bit is used at the L2CAP level to control the information flow independently for every logical channel.

Length: The Length information field describes the number of transmitted information octets (8 bit) in the Payload Data field (payload header and CRC are excluded). The length information can either take up 5 bits of header space for DH1 and AUX1 packets or 9 bits for DH3 and DH5 packets.

Undefined: This field is only present in DH3 or DH5 packets. All 4 bits are set to 0.

Payload Data: The content of the actual data field can be filled either by a PRBS of different type, an entered pattern, all 0 or all 1 or the payload data field can be filled with a user defined file. The file must contain information of ASCII 0 and 1 and is read out cyclically as all the other data sources. That means, the PRBS, a pattern or a file data source is continued in the payload field of the next packet.

CRC: A 16 bit CRC protecting the whole payload field and making error detection possible. This CRC is not used in the AUX1 packets.

Section 4.6: Bluetooth Link Manager Layer

The duties of the Link Manager layer in the Bluetooth stack can be divided into two broad categories: managing the piconet and performing security.

Section 4.6.1: Error Correction

Another management function of the link manager layer is error correction. As explained in the Bluetooth packet header and payload of Bluetooth packet, there are three kinds of error correction schemes used in the Bluetooth protocol: 1/3 rate Forward Error Correction, 2/3 rate Forward Error Correction, and automatic retransmission request.

1/3 rate Forward Error Correction (FEC) – Repeats every bit three times for redundancy. The maximum data rate is effectively divided by 3, hence the term 1/3 rate.
2/3 rate FEC – Adds extra bits to data sent for error correction. These extra bits are examined by the receiving device to determine in an error took place in the transmission. For example, if 8 bits of data were to be sent, they would be expanded into 11 bits, which includes the error correction data. The extra bits reduce the maximum data rate that can be achieved for a transmission, but allows the receiver to detect multiple bits errors and correct single bits errors, preventing retransmission of the data.

Automatic retransmission request (ARQ) – Continuously retransmits the data fields of a data-only or a data-voice packet until an acknowledgment is received or a timeout value is exceeded.

Section 4.6.2: Bluetooth Security

In Bluetooth technology, three security modes are defined as follow.

- Mode 1 (nonsecure) does not enforce any security.
- Mode 2 (service level enforced security) enforces security when an L2CAP channel is established for the required service.
- Mode 3 (link level enforced security) enforces security when baseband ACL link is established.

Section 4.6.3: Link controller state and function

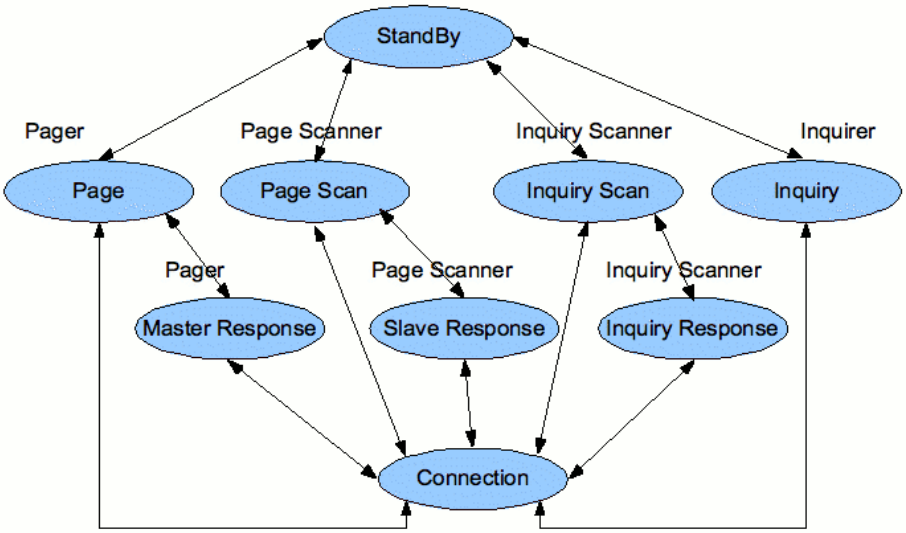


Figure 4.9: Link controller state diagram

Figure 4.9 shows all the possible states in the link controller. There are two major states:

1. Standby
   - Default state. When a Bluetooth-enabled device is not connected, it is in a **StandBy** state. It is a low-power state in which the native clock is running.
2. Connection
   - The device is connected to a piconet as a master or slave.

There are SEVEN interim states, namely Inquiry, Inquiry Scan, Inquire Response, Page Scan, Master Response and Slave Response.

For this section, we will concentrate on the Inquiry, Inquiry Scan, Inquiry Response, Page, Page Scan, Master Response and Slave Response states.

To discover other Bluetooth-enabled devices within its RF range, *the* **inquirer** *has to be in* **Inquiry** *state*. To allow other Bluetooth-enabled devices to discover its existence, *the* **inquiry scanner** *has to be in the* **Inquiry Scan** *state.* To response to an inquiry, *the* **inquiry scanner** *has to be in the* **Inquiry Response** *state to transmit an FHS (Frequency Hopping Synchronisation) packet.*

With the paging procedure, an actual connection can be established. Firstly, the **pager (potential master)** has *to be in* **Page** *state to page* and the **page scanner (potential slave)** *has to be in the* **Page Scan** *state to receive the page*. *Then,* **page scanner** *has to be in* **Slave Response** *state to sends a reply to the* **pager**. *Thereafter, the* **pager** *has to be in* **Master Response** *state to send an FHS packet to the* **page scanner**. Then, **page scanner** *sends its second reply to the* **pager** *at* **Slave Response** *state*. Finally, both the pager and page scanner will transit into Connection state to start exchanging packets in a piconet.

Section 4.7: Bluetooth Connection Procedure

The three procedures involves in establishing a connections are:

1. Inquiry procedure
2. Page procedure
3. Connection procedure

Section 4.7.1: Inquiry Procedure

- It is the first step in establishing a piconet
- Potential Master identifies devices in range that wish to participate in the piconet.

Section 4.7.2: Paging Procedure

- Once the master has founds devices within it's range, it can establish a connection by paging the devices.

Section 4.7.3: Connection procedure

- The connection states starts when the slave is switch to the master timing.

Once the slaves in the Connection states, it can be in one of the four modes operation.

1. Active
2. Sniff
3. Hold
4. Park

Section 4.8: Bluetooth Power Usage

Because most Bluetooth devices are designed to be mobile and require battery power from a laptop computer, PAD or similar device, conserving power is essential. The power consumption of Bluetooth devices varies depending on its connection mode. Transmitting voice through a header uses only 10 milliamps (mA). At this rate, a typical battery would provide 5 hours of use. When data transmissions are occurring, only 6 mA are consumed and a battery can last up to 120 hours before being recharged. When Bluetooth is waiting for a transmission, it only requires 0.3 milliamps, which means the battery, can last up to three months.

Once a Bluetooth device is connected to a piconet, it can be in one of four power-saving modes:

Active – In active mode, the Bluetooth unit actively participates on the channel and consumes an amount of power that corresponds to the type of data that is being transmitted. Over a period of time this amount of power averages out to 2.5 mW in a Power Class 2 device.

Sniff – In sniff mode, a slave device listens to the piconet master at a reduced rate so that it uses less power. The interval is programmable and depends on the application.

Hold - The master unit can put slave units into **HOLD** mode, where only an internal timer is running. Slave units can also demand to be put into **HOLD** mode. Data transfer restarts instantly whenever the slave moves from hold mode back to active mode, but power consumption is kept to a minimum while it is not transmitting. The HOLD is used when connecting several piconets or managing a low power device such as a temperature sensor.

Park – Park mode is the most efficient of power-saving modes. In park mode, a device is still synchronized to the piconet but it does not participate in any traffic. These slaves occasionally listen to the traffic of their master in order to resynchronize and check on broadcast messages, Power consumption in this mode is mere 0.3 mA.

Section 4.9: Other Layers and Functions

Some of the remaining layers and parts of the Bluetooth protocol stack play less significant roles than others. Refer back to Figure 4.4. The Logical Link Control Adaptation Protocol (L2CAP) is the Logical Link Control layer that is responsible for segmenting and reassembling data packets. These data packets are then sent through standard data protocols such as TCP/IP for transmission. The RFCOMM data protocol stands for Radio Frequency Virtual Communications Port Emulation. This data protocol provides serial port emulation for Bluetooth computer's standard serial port, another feature of Bluetooth.
Control information is also transmitted between devices, such as an instruction for device to switch from master to slave. This control information comes through the LMP layer but then bypasses the L2CAP layer, which is only used for transmitted data streams.

The function of Service Discovery Protocol (SDP) is to query device information, services and characteristics and the user may select which services to be connected to.

Section 4.10: Bluetooth profiles

The Bluetooth specification does not cover only the protocol stack but also the services or applications that use Bluetooth technology. This is very different compared to other existing technologies. *The rationale behind the Bluetooth profile specification is to ensure interoperability between Bluetooth-enabled devices from various manufacturers from different industry sectors*. This is not surprising since the vision of Bluetooth is to be the de-facto wireless technology to integrate devices from consumer electronics, telecommunications, computer and networking, automobiles, health care services and many other industry sectors.

In this section, we will briefly describe some of these Bluetooth profiles. More detailed information can be obtained at Bluetooth specification website. Figure 4.10 shows the relationship among the Bluetooth profiles described below.

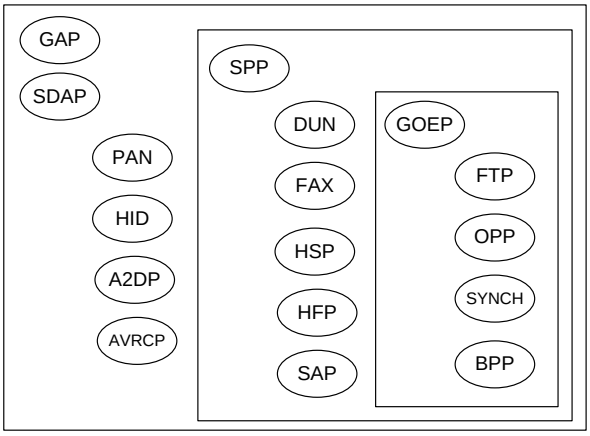


Figure 4.10: Relationship among Bluetooth profiles

Section 4.10.1: Generic Access Profile

GAP is the most basic Bluetooth profile. Its purpose is to make sure that all Bluetooth-enabled devices can successfully establish a baseband link. It defines terminologies like Bluetooth passkey, service discovery, pairing, bonding, trusting etc. Also, it defines the following four modes of operation:

1. Discoverability governs the use of inquiry scan and whether other devices can discover a Bluetooth-enabled device when it comes within their RF range.

- A nondiscoverable device will not perform inquiry scan and cannot be found by an inquiring device.
- A limited discoverability device performs inquiry scan using LIAC.

- A general discoverable device performs inquiry scan using GIAC.

2. Connectability governs the use of page scan and whether other devices can connect to a Bluetooth-enabled device when it comes within their RF range.

3. Pairability governs the use of the link manager's pairing facilities, which are used to create link keys for use on encrypted links

4. Security governs when and how encryption is initiated on a link.

Section 4.10.2: Service Discovery Application Profile

Another basic Bluetooth profile is SDAP. This profile defines the protocols and procedures that shall be used by a service discovery application on a device to locate services in other Bluetooth-enabled devices using the Bluetooth SDP. By providing a standardized method, new profiles can be easily located and identified by a user.

Section 4.10.3: Serial Port Profile

SPP provides RS-232 serial cable emulation for Bluetooth-enabled devices. In this way, legacy applications do not have to be modified to use Bluetooth; they can simply treat a Bluetooth link as a serial cable link. This profile provides the foundation for other profiles: Dial Up Networking, FAX, Headset, Hands-Free, Generic Object Exchange, File Transfer, Object Push, Synchronisation, Basic Printing and SIM Access.

Section 4.10.4: Dial Up Networking profile

DUN profile is used to provide an Internet bridge using a communication device. For example, it allows a laptop to access a telephone network using a cellular phone with a GPRS/3G connection. The AT command is used for the dialling and control layer and PPP is used to carry the IP packets.

Section 4.10.5: Fax profile

Fax profile defines the procedures for sending and receiving faxes without wires. It is very similar to DUN profile in that AT command is used to for the dialling and control layer. However, instead of transferring data, fax information from the following three classes can be transmitted:

- Fax Class 1 TIA-578-A and ITU T.31
- Fax Class 2.0 TIA-592-A and ITU T.32
- Fax Service Class 2

Section 4.10.6: Headset Profile

HSP defines the facilities required to make and receive voice calls from a headset to a cellular phone handset. It defines the following two roles:

- Audio Gateway is the device that is the gateway of the audio, both for input and output
- Headset is the device acting as the remote audio input and output mechanism

Section 4.10.7: Hands-Free profile

HFP defines the minimum set of functions such that a mobile phone can be used in conjunction with a Hands-Free device (e.g. installed in the car or represented by a wearable device such as a headset). It is very similar to Headset profile except that it can be connected to potentially multiple Bluetooth-enabled devices that it is paired with, transfer sound back and forth between these devices and other advanced capabilities.

Section 4.10.8: SIM Access Profile

SAP defines the protocols and procedures that shall be used to access a GSM SIM card, a UICC card or an R-UIM card via a Bluetooth link. For example, with this profile, the user can personalize his/her car-embedded phone with a subscription module in an external device, which is connected via a Bluetooth wireless link.

Section 4.10.9: Generic Object Exchange Profile

GOEP uses IrDA's OBEX layer and defines how it is used within Bluetooth. It also defines two roles: the server device to and from which objects are pushed and pulled and the client device, which can push and/or pull data objects to and from the server. It requires the use of the following OBEX operations: connect, disconnect, put get and setpath. This profile provides the foundation for these four profiles: File Tranfer, Object Push, Synchronization and Basic Printing.

Section 4.10.10: File Transfer Profile

FTP provides wireless data transfer between various Bluetooth-enabled devices. For example, the JPEG photos from a camera mobile phone can be transferred to a laptop using this profile. It also provides the ability to create, browse and delete files and folders.

Section 4.10.11: Object Push Profile

OPP is similar to file transfer profile, except that the type of data transferred is limited to the exchange of business cards in vCard object format. Instead of using OBEX authentication,

the user data can be protected using the authentication and encryption on the Bluetooth baseband links.

Section 4.10.12: Synchronization profile

SYNCH provides a standard way to synchronize personal data between Bluetooth-enabled devices. For example, it could be used to ensure that appointments entered into a calendar application on a laptop are kept up-to-date with a version on a PDA. The synchronization can be triggered automatically without user intervention.

Section 4.10.13: Basic Printing Profile

BPP defines the functionality which allows devices to control a Bluetooth-enabled printer and send print jobs to it without needing a dedicated driver for that printer. The printer can support the following four modes:

- Bluetooth off-line mode - The printer cannot be discovered or connected with
- Bluetooth bonding mode - The printer is waiting to be bonded with a sender
- Bluetooth on-line mode - The printer cannot be discovered but can be connected with
- Public on-line mode - The printer can be discovered and connected with

Section 4.10.14: Personal Area Network profile

PAN profile lays out the rules for carrying IP traffic across Bluetooth connections using BNEP to encapsulate Ethernet packets in L2CAP packet payloads. This method is more efficient and provide higher throughput than using PPP in DUN profile.

This profile provides two connection methods:

1. Devices can connect to a NAP in order to access a remote network where NAP acts as a bridge to the network.
2. Devices can connect directly to one another using GN exchanging data with no outside network involvement.

To enable these two connection methods, three different roles are defined:

1. NAP is a device acting as a bridge to connect to a piconet to an IP network. It forwards packets to and from the network and amongst PAN users.
2. GN is a device which connects to one or more PAN users, forwarding packets between PAN users when more than one is connected.
3. PAN user is a client device which uses the GN or NAP service.

Section 4.10.15: Human Interface Device profile

HID profile allows devices such as a computer mouse, keyboard or tracker ball to communicate with a Bluetooth-enabled laptop using a Bluetooth link. The profile uses the HID protocol which is originated from the USB specification. Since HID devices require a fast response, L2CAP Quality of Service can be used to provide low latency communication. Also, since most PCs already have USB HID drivers, a Bluetooth adapter driver known as a miniport driver can be used to handle Bluetooth specific connection management and passes HID protocol information up to the USB HID driver. This will enable the L2CAP layer to connect to the USB HID driver through the miniport.

Section 4.10.16: Advanced Audio Distribution Profile

A2DP defines the protocols and procedures that realize distribution of audio content of high-quality in mono or stereo on FHS channels. A typical usage case is the streaming of music content from a stereo music player to headphones or speakers. The audio data is compressed in a proper format for efficient use of the limited bandwidth. Surround sound distribution is not included in the scope of this profile.

Section 4.10.17: Audio/Video Remote Control Profile

AVRCP defines the features and procedures required in order to ensure interoperability between Bluetooth devices with audio/video control functions in the Audio/Video distribution scenarios. This profile specifies the scope of the AV/C Digital Interface Command Set, defined by the 1394 Trade Association, to be applied and it realizes simple implementation and easy operability. The AV/C control messages are transported by the AVCTP.

In this profile, the controller translates the detected user action to the A/V control signal, and then transmits it to a remote Bluetooth device. The functions available for a conventional infrared remote controller can be realized in this profile.

Section 4.10.18: Additional Profiles for Bluetooth Low Energy

All current low energy application profiles are based on the generic attribute profile, or GATT, a general specification for sending and receiving short pieces of data known as attributes over a low energy link. Bluetooth 4.0 provides low power consumption with higher baud rates.

Health care profiles

The Continua Health Alliance consortium promotes health care applications in cooperation with the Bluetooth SIG. Profiles for Health care include:
HTP — for medical temperature measurement devices
GLP — for blood glucose monitors
BLP — for blood pressure measurement

Sports and fitness profiles

Profiles for sporting and fitness accessories include:

HRP — for devices which measure heart rate
CSCP — for sensors attached to a bicycle or exercise bike to measure cadence and wheel speed
RSCP — running speed and cadence profile
CPP — cycling power profile
LNP — location and navigation profile

Proximity sensing

"Electronic leash" applications are well suited to the long battery life possible for 'always-on' devices.
Relevant application profiles include:
FMP — the "find me" profile — allows one device to issue an alert on a second misplaced device.
PXP — the proximity profile — allows a proximity monitor to detect whether a proximity reporter is within a close range. Physical proximity can be estimated using the radio receiver's RSSI value, although this does not have absolute calibration of distances. Typically, an alarm may be sounded when the distance between the devices exceeds a set threshold.

Alerts and time profiles

The phone alert status profile and alert notification profile allow a client device to receive notifications such as incoming call alerts from another device.
The time profile allows current time and time zone information on a client device to be set from a server device, such as between a wristwatch and a mobile phone's network time.

Section 4.11: Comparison between Classic Bluetooth and Bluetooth Low Energy

The following table describes the technical details of Classis Bluetooth and BLE.

Technical Specification	Classic Bluetooth technology	Bluetooth low energy technology
Distance/Range (theoretical max.)	100 m (330 ft)	50 m (160 ft)
Over the air data rate	1–3 Mbit/s	1 Mbit/s
Application throughput	0.7–2.1 Mbit/s	0.27 Mbit/s

Active slaves	7	Not defined; implementation dependent
Security	56/128-bit and application layer user defined	128-bit AES with Counter Mode CBC-MAC and application layer user defined
Robustness	Adaptive fast frequency hopping, FEC, fast ACK	Adaptive frequency hopping, Lazy Acknowledgement, 24-bit CRC, 32-bit Message Integrity Check
Latency (from a non-connected state)	Typically 100 ms	6 ms
Total time to send data (det.battery life)	100 ms	3 ms , <3 ms
Voice capable	Yes	No
Network topology	Piconet, Scatternet	Star
Power consumption	1 as the reference	0.01 to 0.5 (depending on use case)
Peak current consumption	<30 mA	<15 mA
Service discovery	Yes	Yes
Profile concept	Yes	Yes
Primary use cases	Mobile phones, gaming, headsets, stereo audio streaming, automotive, PCs, security, proximity, healthcare, sports & fitness, etc.	Mobile phones, gaming, PCs, watches, sports and fitness, healthcare, security & proximity, automotive, home electronics, automation, Industrial, etc.
Frequency channel	79 channels with 1-MHz BW	40 channels with 2-MHz BW
Maximum Transmit Power	100 mW	10 mW
Modulation techniques	GFSK, 4PSK, 8PSK	GFSK

Section 4.12: Bluetooth Applications

Today, Bluetooth chipsets are manufactured at a quantity of five millions every week. It is a low cost, low power, small footprint, open specification, no line-of-sight wireless technology that is embedded in computers, mobile phones, PDAs, MP3 players, headsets, hands-free in car kits and many other devices. Among the most popular Bluetooth applications are

- transfer of voice signal from mobile phone to headset using either HSP or HFP
- transfer of voice signal from mobile phone to hands-free in car kits using HFP and SAP
- transfer of images from camera mobile phone to either another mobile phone or laptop using FTP
- listen to music from MP3 player to stereo headphones using A2DP and AVRCP
- access the Internet from a laptop using a mobile phone as a wireless modem using either DUN or PAN
- connect computer mouse and computer keyboard to a laptop using HID
- exchange business cards from mobile phone to either another mobile phone or laptop using OPP
- synchronizing data between a PDA and a laptop using SYNCH
- printing of images and documents from a mobile phone or laptop to a Bluetooth-enabled printer using BPP
- Blood pressure measurement for Health care using BLP
- temperature measurement devices using HTP
- blood glucose monitoring using GLP
- devices which measure heart rate using HRP
- sensors attached to a bicycle or exercise bike to measure cadence and wheel speed using CSCP
- monitoring running speed and cadence using RSCP
- monitoring cycling power using CPP
- location and navigation using LNP
-

Section 4.13: Examples of WPAN (Bluetooth/ZigBee/UWB/RFID) Applications

Current and future applications for WPAN technology include

- Synchronisation PDAs, cellular and Smartphones, cameras and so on
- Home control systems (smart-home)
- Cordless telephones
- Portable device data exchange
- Industrial control systems
- Location –smart tags used to locate people at home or at the office
- Security systems
- Interactive toys
- Inventory tracking
- Health care and elder care
- Energy monitoring and control (Smart grid) Applications

Chapter 5: Understands Wireless Wide Area Network

Content

- Explain “What is Wireless WAN?”
- Understand the basic of Cellular Network
- Explain the functions of every component in GSM architecture
- Describe the Air interface (TDMA/FDMA) used in GSM
- Understand the evolution path of Wireless WAN
- Describe enhancement from 2.5G GPRS to 2.75G EDGE
- Explain the 3G UMTS system and architecture
- Describe the enhancement from 3G UMTS to 3.5G HSDPA
- Describe the enhancement from 3G UMTS to 3.5G HSDPA
- Describe the enhancements in 4G

Section 5.1: Introduction

A wireless wide area network (WWAN) spans a geographical area as large as an entire country or even the entire world. A WWAN differs from WLAN (wireless local area network) in that it uses mobile telecommunication cellular network technologies such as GSM, GPRS, EDGE, UMTS, CDMA2000, HSDPA, HSUPA or 3G to connect users to a voice or data network through e-mail and Internet connections. WWAN users also can connect to a cooperate network and run business applications from virtually any location around the planet using Smartphones, PDAs and PCMCIA cellular adaptor cards plugged into notebook computers. The BlackBerry® service is just one example of a wireless device in use in business and government today to enhance competitive advantage by responding and making decisions faster.

Enjoy real-time access to emails with no dial-up or login hassle. Email messages sent to your corporate or personal accounts will be automatically delivered to your BlackBerry® smartphone. Therefore, for the user’s perspective, digital cellular technology is ubiquitous.

Section 5.2: Basic of Cellular Network

A radio cell is a smaller area of a cellular mobile network. The size of a cell is determined by a maximum given transmission power and a minimum receiver signal strength for a good voice quality. Hexagonal cell pattern is idealized (Cells overlap irregularly). No uniform cell size, size depends on attenuation as well as expected traffic amount (inner city vs. unpopulated regions). Signal attenuation restricts distance between sender and receiver (~ d^2 in line of sight, $d^{5.5}$ within buildings)

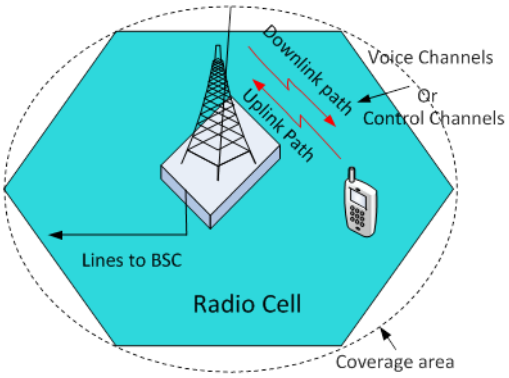


Figure 5.1: A radio cell

A cell contains a base transceiver station having a number of RF channels to provide a smaller coverage area about typical cell radius approximately 30 kilometer.

Cell sizes vary from some 100 m up to 35 km depending on user density, geography, transceiver power etc.

The cellular network consists of cells which are adjacent to each other to extend the coverage area of wireless wide area network. One or more than one BTSs are connected to a Base Station Controller which will provide the link between cellular network and wired telephone world and controls all the base transceiver stations in the cellular networks.

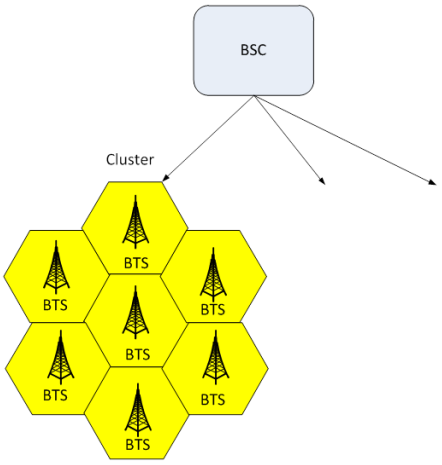


Figure 5.2: A cluster with seven cells

If a mobile user is changed from a cell to other during a phone call, the connection will be passed to the neighbour cell. This is called as handover.

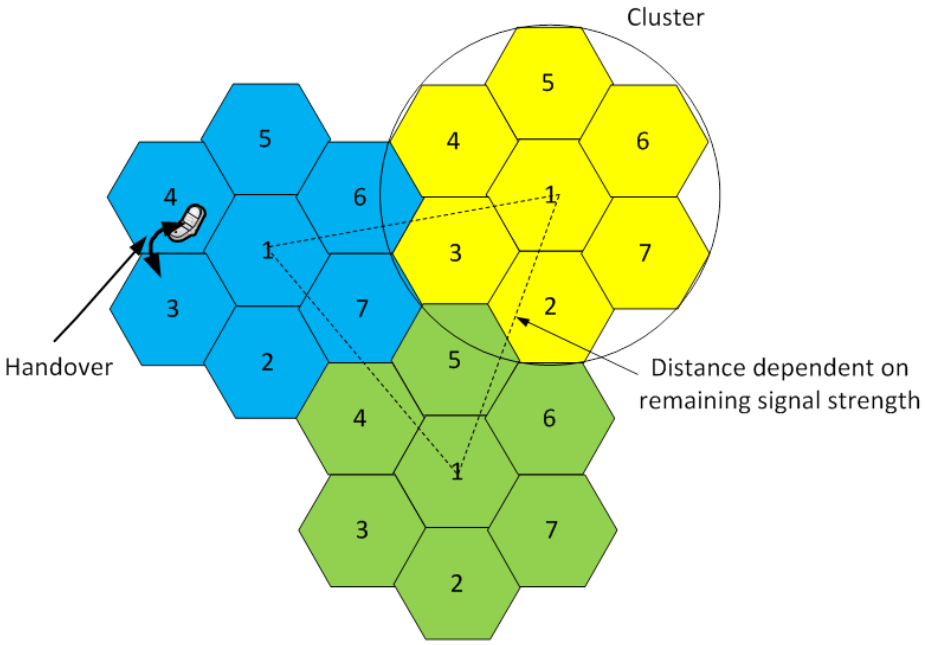


Figure 5.3: A cellular phone handover

Frequency range is very limited and not suited for high number of subscribers. Hence, the re-use of frequency channel at the distant cells was employed by using Space Division Multiple Access (SDMA) to divide the whole area in cells. Therefore, it is intentionally required to lower the transmit power of the BTS at a cell to minimise the interference. Frequency ranges can be re-used in a larger distance without problems of interference. Hence, two subscribers in distant cells can use the same channel simultaneously.

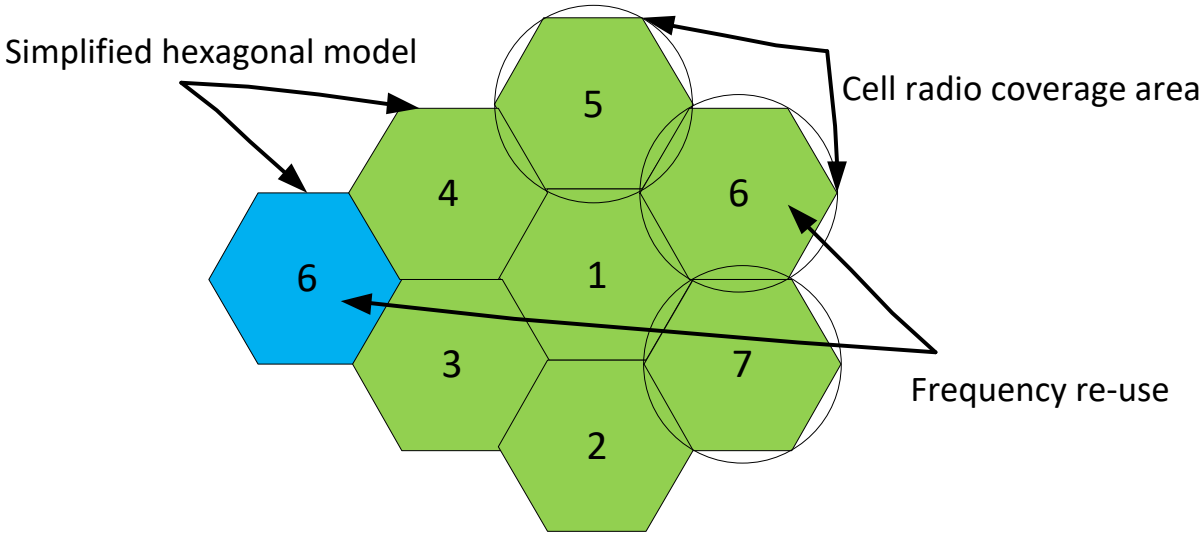


Figure 5.4: Frequency re-use at distinct cells

Cell planning in a cellular is very important that it is required to design the optimum cluster size N in a way to maximize capacity and minimize interferences. If there are m**ore cells per cluster:**

- Less channels per cell
- Lower system capacity
- Less co-channel interference (co-channel cells have larger distance in between)

If there are fewer cells per cluster:

- More channels per cell
- Higher system capacity
- More co-channel interference (co-channel cells are nearby)

Section 5.3: Functions of every component in GSM architecture

Global System for Mobile communication (GSM) is the most successful technology ever implemented by mankind. Interestingly, this is one of the few technologies where there is only one application, that is, for voice communication. The first GSM call was made in Finland on 1st July 1991. After about 20 years, there are now more than 3.4 billion subscribers worldwide and the exciting statistics is that the market penetration is growing exponentially over the past years. New connections are added at the rate of 15 per second, or 1.3 million per day. Therefore, it is important for us to understand this highly successful technology. Please take note that GSM was stopped using in Singapore from 1 April, 2017.

In Figure 5.5, the architecture of a GSM network is shown. There are three main sections:

- Mobile Station (MS), which consists of Mobile Equipment (ME) and Subscriber Identity Module (SIM)
- Base Station Subsystem, which consists of Base Transceiver Station (BTS), Base Station Controller (BSC) and Transcoding Equipment (TCE)
- Network Switching Subsystem (NSS), which consists of Gateway Mobile Switching Centre (GMSC), Mobile Switching Centre (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Authentication Centre (AuC) and Equipment Identity Register (EIR).

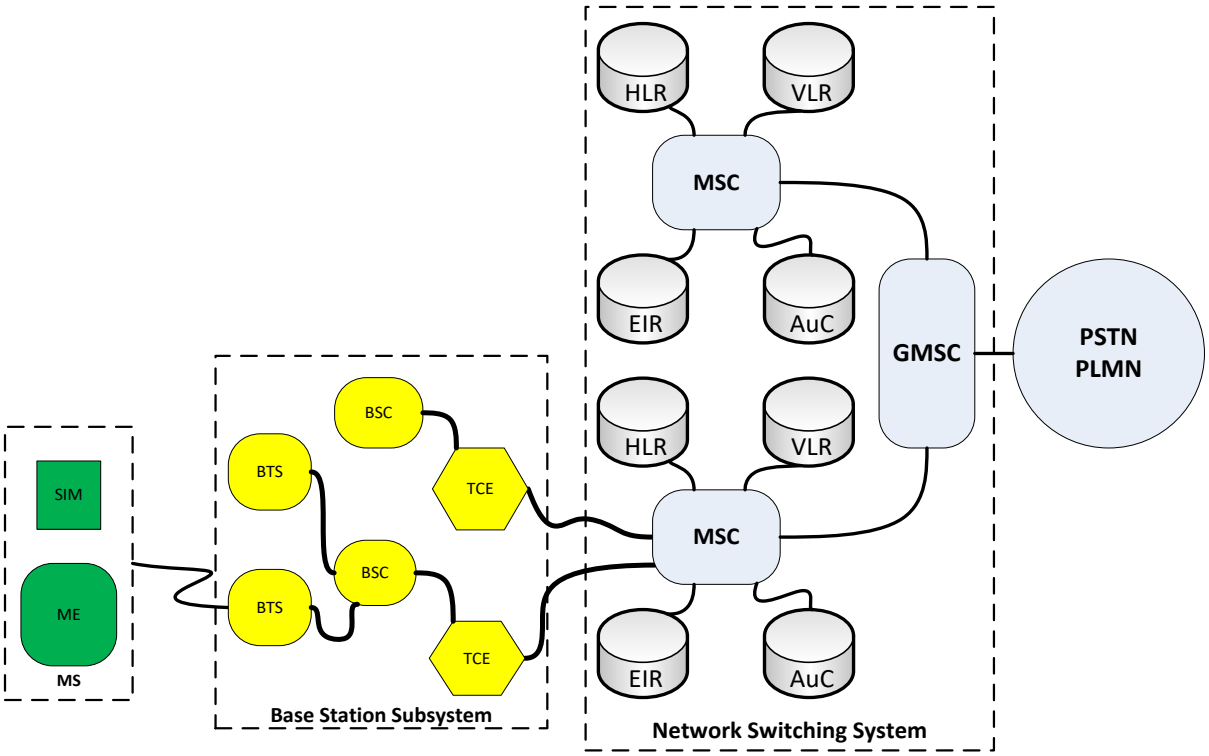


Figure 5.5: GSM architecture

The Mobile Station (MS) is the official name given in GSM standard for what is commonly known as mobile phone or handphone. From the perspective of its operation, it can be divided into two parts:

1. SIM (Subscriber Identification Module), which consists of a microchip and a memory card. Every SIM card contains the IMSI (International Mobile Subscriber Identity) used to identify the subscriber to the system, a secret key for authentication, and other information. It stores data for both the operator and subscriber and as such is unique to each subscriber. Besides it storage functionality, its other main functions include authentication and radio transmission security.
2. ME (Mobile Equipment), which consists of the LCD display, keypad, casing, antenna and all other parts of the Mobile Station. Every Mobile Equipment has its own personal identification known as IMEI (International Mobile Equipment Identity). Its main functions include modulation/demodulation, ciphering/deciphering, channel encoding/decoding and voice encoding/decoding.

The Base Transceiver Station (BTS) is the official name given in GSM standard for what is commonly known as base station. It manages the interface between the GSM network and a few mobile stations through the air interface, which will be described in details in Section 5.4. The major functions include transmission of signals in the desired format, coding and decoding of signals, countering the effects of multi-path transmission by using equalisation algorithms, encryption of data streams, and measurement of quality and received signal power. In other words, Base Transceiver Station performs most of the functions of Mobile Equipment of the Mobile Station and to collect measurements to support the simultaneous operations of a few Mobile Stations inside a particular cell.

The Base Station Controller (BSC) controls the Base Transceiver Stations. Its major functions include management of the radio resources and handover. In other words, it decides when a Mobile Station should switch over from one cell to another cell based on the received signal power measurement obtained from the Base Transceiver Station. Also, it is responsible for control of the power transmitted, its signalling and security configurations.

The next piece of equipment is the Transcoding Equipment (TCE). It is used to convert the bit rate used in GSM vocoder to 64 kbits/s used in I Integrated Services for Digital Network (ISDN). Currently, GSM supports three types of voice coding:

- Full rate at 13 kbits/s
- Enhanced full rate at 12.2 kbits/s
- Half rate at 6.5 kbits/s

The single most important equipment in GSM network is the Mobile Switching Centre (MSC). It is responsible for interconnecting mobile users to other mobile and fixed network users. To support this purpose, it makes use of the three major components of the Network Subsystem.

1. Home Location Register contains the information related to each mobile subscriber, such as the type of subscription, services that the user can use, the subscriber's current location and the mobile equipment status. The database remains intact and unchanged until the termination of the subscription.
2. Visitor Location Register contains the information of subscribers inside a coverage region. Since the subscriber can move from one coverage region to another, the database is dynamic.
3. Authentication Centre is responsible for policing actions in the network. It contains the data required to protect the network against false subscribers and to protect the calls of regular subscribers.
    - For authentication of users, a random number is sent from the GSM network to the Mobile Station. This random number is then encrypted using the authentication key stored both in the SIM and the authentication centre. The encrypted random number is sent back from the Mobile Station to the Authentication Centre and will be compared with its locally encrypted random number.
    - For encryption of communications between mobile users, a new ciphering key is generated for each new connection using the random number used in the authentication process and the authentication key stored in both in the SIM and the Authentication Center.

A Gateway Mobile Switching Centre provides an edge function within a PLMN (Public Land Mobile Network). It terminates the PSTN (Public Switched Telephone Network) signalling and traffic formats and converts this to protocols employed in mobile networks.

Section 5.4: Air interface (TDMA/FDMA)

GSM uses Gaussian Minimum Shift Keying (GMSK) modulation. It is a form of continuous phase FSK. Refer to Figure 5.6 for a waveform comparison between BFSK, BPSK and BMSK modulations. You will notice that the initial phase for BMSK modulation is the same as the BPSK modulation. However, there is no abrupt change in the phase at the boundaries of the symbol period.

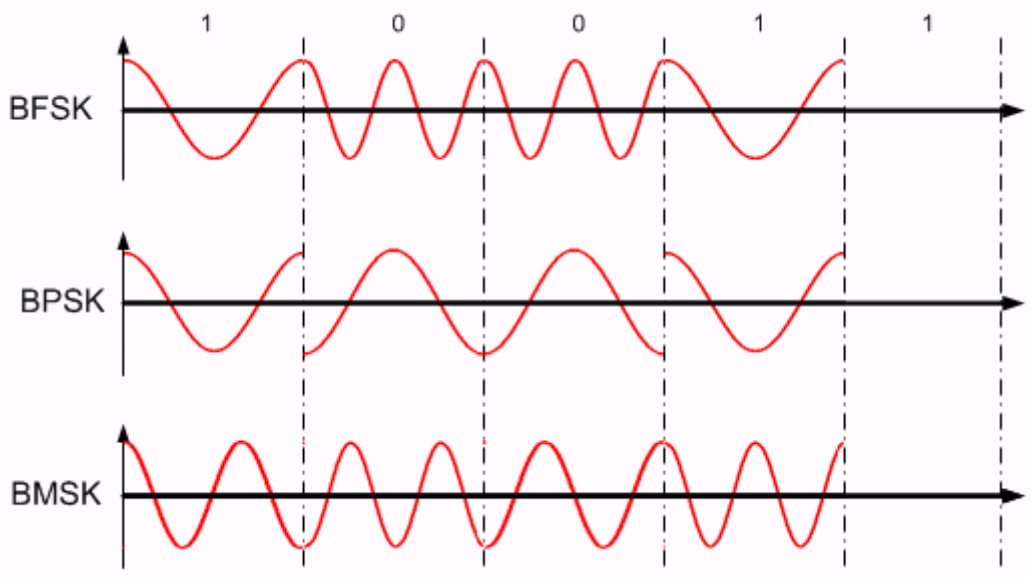


Figure 5.6: Comparison between BFSK, BPSK and MSK modulations

The letter G in GMSK modulation denotes the filtering of the analog signal using a Gaussian filter prior to modulation. The reason GMSK modulation is chosen in GSM is for its high spectral efficiency. **Spectral efficiency** is defined as the number of bits per second that can be transmitted per Hz of bandwidth. For example, an encoding using a single kilohertz of bandwidth to transmit a thousand bits every second has a spectral efficiency of one.

Currently, there are five frequency bands allocated for GSM:

- GSM-400
- GSM-850
- GSM-900
- GSM-1800
- GSM-1900

Since GSM uses FDD (Frequency Division Duplex), the allocated frequency spectrum has to be divided into two groups for uplink and downlink. Table 5.1 shows the frequency allocated for uplink and downlink for the five frequency bands:

Variant	Uplink (MHz)	Downlink (MHz)	Total Bandwidth	Duplex-frequency	Channels
GSM-400	**451-458 and 479-486**	**461-468 and 489-496**	**Twice 14 MHz**	**10 MHz**	**Twice 72**
GSM-850	**824-849**	**869-894**	**Twice 25 MHz**	**45 MHz**	**Twice 124**
GSM-900 (primary band)	**890-915**	**935-960**	**Twice 25 MHz**	**45 MHz**	**Twice 124**
DCS-1800	**1,710-1,785**	**1,805-1,880**	**Twice 75 MHz**	**95 MHz**	**Twice 373**
PCS-1900	**1,850-1,910**	**1,930-1,990**	**Twice 60 MHz**	**80 MHz**	**Twice 300**

Table 5.1: Frequency allocation for uplink and downlink in GSM

GSM uses a combination of FDMA and TDMA. The FDMA part involves the division by frequency into bandwidth of 200 kHz. Each of these frequency channels is then divided in time, using a TDMA scheme. The fundamental unit of time in this TDMA scheme is called a **burst period** and eight burst periods are grouped into a **TDMA frame** which forms the basic unit for the definition of logical channels.

Example 5.1

Find the number of burst period in GSM-900?

The bandwidth allocated for uplink/downlink is equal to (915-890/960-935) 25 MHz. Dividing it by 200 kHz, we obtain 125 frequency channels. Since each frequency channel has 8 burst periods, there are 125×8=1000 burst periods.

The bit rate for GSM is 270.833 kbits/s. In Figure 5.7, it is shown that a **multiframe** consisting of 26 TDMA frames requires 120 ms for transmission of 32500 bits. This means that each TDMA frame has 1250 bits and requires 4.615 ms for transmission and each burst period has 156.25 bits and requires 0.577 ms for transmission.

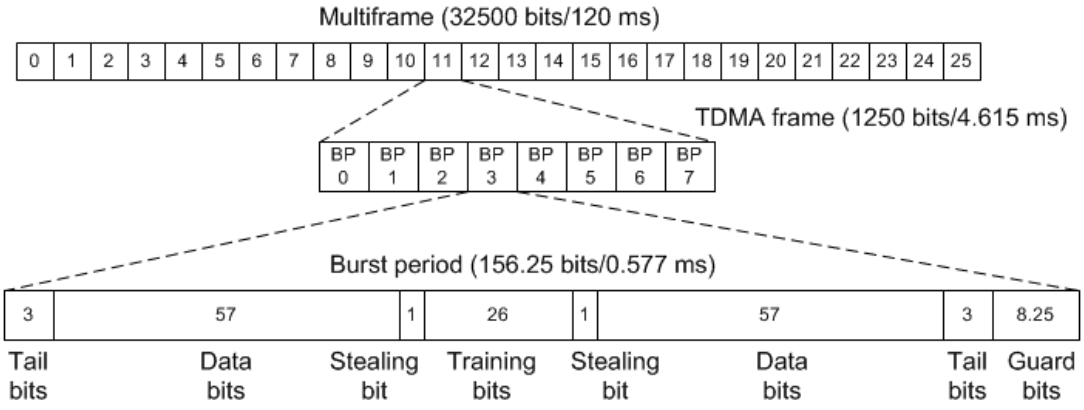


Figure 5.7: GSM frame structure

Channels are defined by the number and position of their corresponding burst periods. They can be divided into dedicated channels and common channels. Dedicated channels are mainly **traffic channels** which are allocated to mobile stations. Each MS is given one burst period in each TDMA frame. Common channels are mainly **control channels** which are used by mobile stations in idle mode. In Figure 5.7, frames 0-11 and 13-24 in multiframe are used as traffic channels, frame 12 is used as SACCH (Stand-alone Dedicated Control Channel) and frame 25 is currently unused. The SACCH is used for most short transactions, including initial call setup step, registration and SMS (Short Message Service) transfer. It has a payload data rate of 0.8 kbit/s. Up to eight SDCCHs can be time-multiplexed onto a single physical channel.

There are four different types of bursts used for transmission in GSM. The burst structure shown in Figure 5.7 is known as normal burst and it is used to carry data and signalling. Out of 156.25 bits, 114 bits are used to data, 26 bits are training sequence used for equalization, 1 stealing bit for each information block (used for FACCH (Fast Associated Control Channel)), 3 tail bits at each end for synchronization and 8.25 guard bits to separate the burst periods. The other three burst structures are F, S and access bursts. The F burst, used on the FCCH (Frequency Correction Channel), and the S burst, used on the SCH (Synchronization Channel), have the same length as a normal burst, but a different internal structure while the access burst is shorter than the normal burst, and is used only on the RACH (Random Access Channel).

For each MS, it will transmit only on one of the eight burst periods and also receive on one of the eight burst periods. Therefore, it is not necessary for MS to transmit and receive at the same time. As shown in Figure 5.8, the uplink and downlink are separated in time by 3 burst periods.

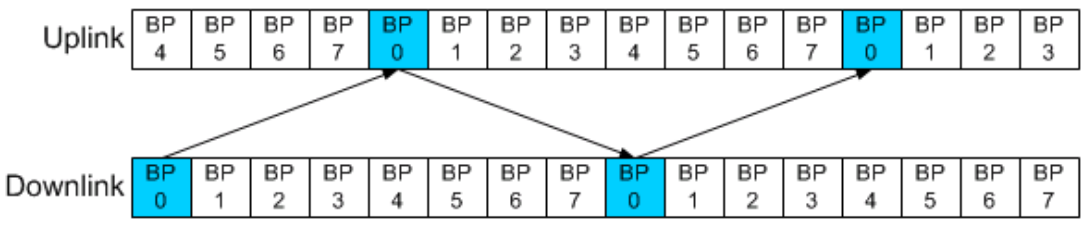


Figure 5.8: Time separation between uplink and downlink

Section 5.5: Evolution path

We have learnt that GSM is the most successful technology ever implemented by mankind. However, GSM is optimized to transfer voice information only. Today, transmission of data information is equally, if not more important, than transmission of voice information. Therefore, GSM network has to evolve from circuit switched network to packet switched network.

In this section, we will study the evolution path from 2G GSM to 2.5G GPRS (General Packet Radio Service) to 3G UMTS (Universal Mobile Telecommunications System) network. One very important consideration in this evolution path is the additional cost that telcos has to invest to upgrade their existing GSM infrastructure. If the additional investment is higher than the potential revenue that telcos will eventually earn from their subscribers, there will be no incentive for them to upgrade their infrastructure.

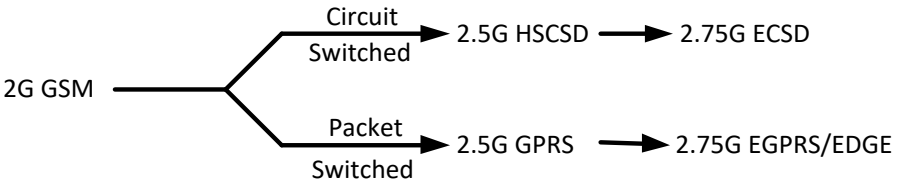


Figure 5.9: Evolution path from 2G to 2.5G network

In Figure 5.9, there are two paths of evolution to enable data transmission. The first path is to continue to use circuit switching network. Using 2.5G HSCSD (High-Speed Circuit Switch Data), the bit rate per burst period/time slot is increased from 9.6 kbps (2G GSM) to 14.4 kbps and with the ability to use up to four burst periods/time slots per TDMA frame, the bit rate can increase to 14.4kbps×4=57.6kbps. To further increase the bit rate, ECSD (Enhanced Circuit Switch Data) allows 48 kbps per time slot and with up to eight time slots per TDMA frame, the maximum bit rate is 48kbps×8=384kbps.

The second path is to use packet switching network. 2.5G GPRS has four different coding schemes. (Refer to Figure 5.10) The difference between different coding schemes lies in the bits allocation between data information and error correction codes. Using CS4 (Coding Scheme) which is least robust but fastest with up to eight time slots, the maximum bit rate is 20kbps×8=160kbps. To further increase the bit rate, EDGE allows nine different coding schemes. (Refer to Figure 5.10) Using MCS9 (Modulation and Coding Scheme) and up to eight time slots, the maximum bit rate is 59.2kbps×8=473.6kbps. The three-fold increase in the bit rate is due to the use of 8PSK modulation with 3 bits/symbol in EDGE compared to the use of BMSK modulation with one bit/symbol in GPRS. The enhancement from GPRS to EDGE is a very good example to illustrate the importance of higher-order modulation to boost up the bit rate in mobile communication system. Other enhancements made in EDGE will be described in Section 5.6.

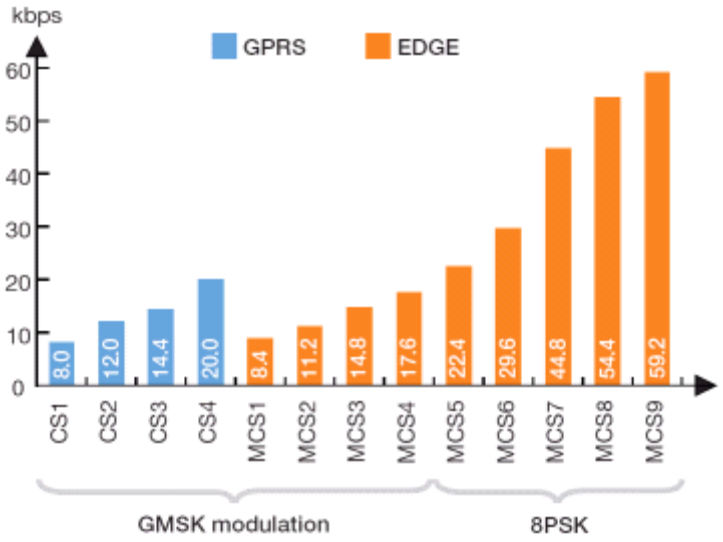


Figure 5.10: Coding used in GPRS and EDGE (Bit rate per time slot is shown in the value on the bar)

To consumers, the main difference between ECSD and EDGE is the mode of payment for the data service. For ECSD, consumers are charged for their connection time since it is circuit-switched while for EDGE, they are charged for the amount of data transferred since it is packet-switched. Therefore, GPRS allows always-on-line connectivity for data transmission. Since packet-switching is the preferred method to transfer data information, our focus in this module will be on packet-switching network.

Next, we will study the changes to the network architecture for evolution from 2G GSM to 2.5G GPRS. In GSM network architecture shown in Figure 5.5, there are three main sections. In terms of cost, the most expensive section is the Base Station Subsystem where hundreds or thousands of BTS have been invested. Therefore, the first section to upgrade from circuit switched network to packet switched network with minimum additional investment is the Network Switching Subsystem. Figure 5.11 shows the additional equipment added to the GSM architecture to support packet switching network (blocks in purple colour).

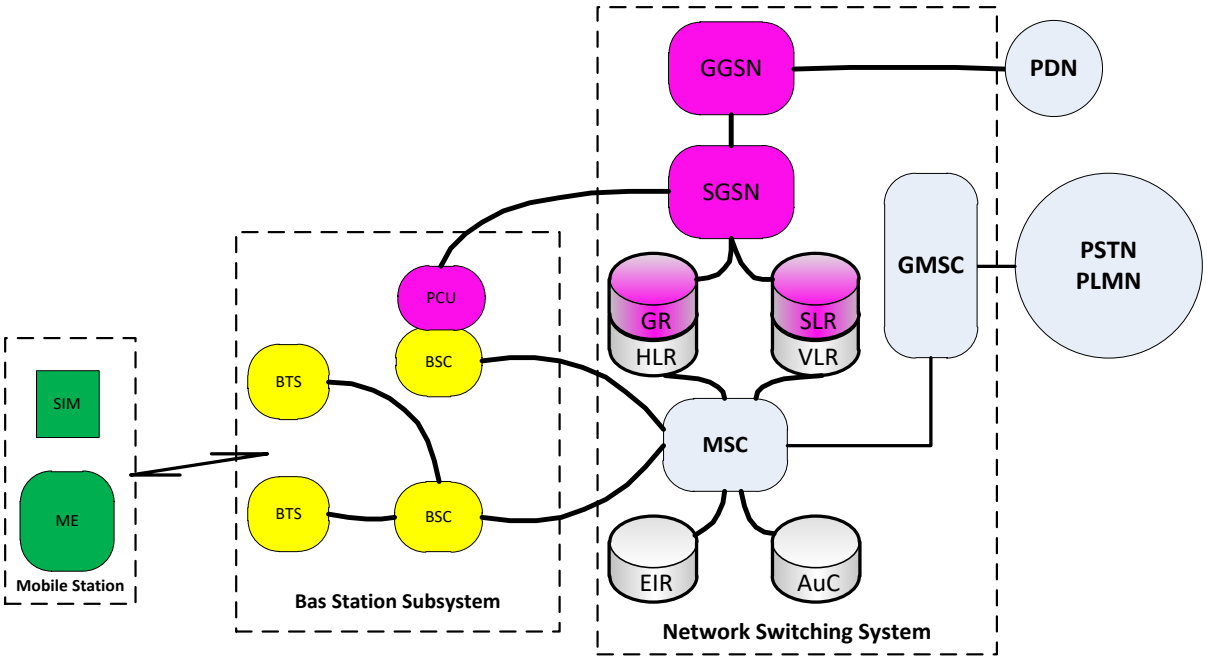


Figure 5.11: GPRS architecture

PCU (Packet Control Unit) is used to separate the voice information and data information received from the Radio Subsystem. For voice information, it is routed, as per normal, to TCE and MSC using circuit-switching. For data information, it is now routed to the new packet-switching network. Other PCU functions include packet segmentation and reassembly both on the downlink and uplink, scheduling for all active transmissions including radio channel management and transmission control like buffering and retransmission.

SGSN (Serving GPRS Support Node) is the equivalent of MSC in the circuit-switching network. It establishes a mobility management context for an attached MS and performs ciphering for packet-oriented traffic.

GR is the equivalent of HLR in the circuit-switching network.

SGSN Location Register (SLR) is the equivalent of VLR in the circuit-switching network.

GGSN (Gateway GPRS Support Node) is the equivalent of GMSC in the circuit-switching network. It is the access point for an external data network and is capable of routing packets to the current location of the mobile.

Though GPRS/EDGE is able to support data transmission, the use of multi-slots in TDMA frame reduces the capacity of the system. To increase the capacity, the Radio Subsystem and Base Station Subsystem have to be upgraded. This involves another round of investment by Telco's to install new Node-Bs in 3G system (equivalent to BTS in 2G GSM). This two-step upgrade of Network Switching Subsystem in 2G to 2.5G evolution and Base Station Subsystem in 2.5G to 3G evolution is the key success in converting from a voice-centric circuit switching to a data-centric packet switching network. Figure 5.12 shows the second phase evolution path.

2.5G GPRS → 2.75G EGPRS/EDGE → 3G W-CDMA → 3.5 HSDPA → 3.75 HSUPA

Figure 5.12: Evolution path from 2.5G to 3G network

In 3G system, the air interface uses WCDMA rather than FDMA/TDMA used in GSM/GPRS/EDGE. The capacity for data transmission is increased because the spectral efficiency for WCDMA at high throughput is greater than the spectral efficiency for FDMA/TDMA. This is shown in Figure 5.13.

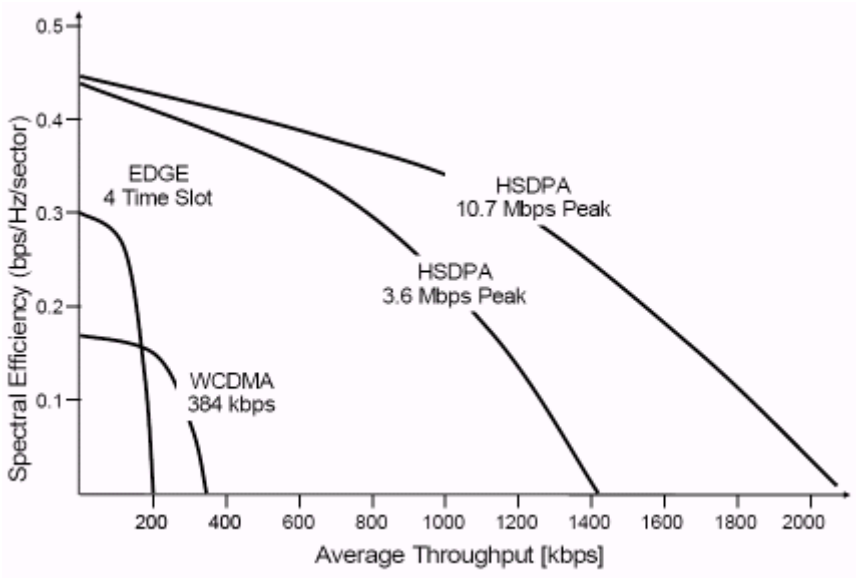


Figure 5.13: Spectral efficiency between EDGE, WCDMA and HSDPA

Section 5.6: 3G UMTS system and architecture

The ITU has defined 384 kbps as the data rate limit required for a service to fulfil the 3rd Generation Mobile Communication System. At the moment, there are three implementations:

1. UMTS-FDD uses two different frequency bands for duplex communication
2. UMTS-TDD uses only one frequency band for duplex communication
3. cdma2000 which is an upgrade from IS-95 system used in USA. (In this module, we will not be discussing on cdma2000.)

3G UMTS uses different frequency spectrum compared to GSM. Table 5.2 shows the existing frequency spectrum allocated for UMTS-FDD and UMTS-TDD and the possibly new frequency spectrum.

UMTS-FDD (uplink)	UMTS-FDD (downlink)	UMTS-TDD
1920-1980 MHz	2110-2170 MHz	1900-1920 MHz or 2010-2025 MHz
New frequency bands		
806-960 MHz, 1710-1885 MHz, 2500-2690 MHz		

Table 5.2: Frequency allocation for 3G UMTS

As explained in Chapter 1, CDMA differentiates the different users using orthogonal codes rather than physical parameters like frequency and time. Unlike GSM, a telco can use up all the allocated spectrum or many telcos have to share among themselves the allocated spectrum. in 3G UMTS, each telco is given 5 MHz spectrum exclusively. For example, in UMTS-FDD shown in Table 5.2, each telco is given exclusively 5 MHz spectrum in the downlink and another 5 MHz spectrum in the uplink. Therefore, the existing frequency band allocated for UMTS-FDD can support up to 12 telcos. Likewise, for UMTS-TDD, each telco is given 5 MHz spectrum and there can be up to 7 telcos.

Besides the mandatory minimum bit rate of 384 kbps, other requirements for 3rd Generation Mobile Communication System are

- Bit rates up to 2 Mbps for pedestrian speed
- Variable bit rate for bandwidth on demand since different services require different amount of bandwidth
- Multiplexing of services with different quality requirements on a single connection
- Delay requirements from delay-sensitive real time traffic (< 200 ms) to flexible best-effort packet data
- Quality requirements from 10% frame error rate to 10^{-6} bit error rate
- Inter-system handovers (from 2G GSM to 3G UMTS and vice-versa) for coverage enhancements and load balancing
- Support of asymmetric upload and download traffic since the download speed for a user is much more important than the upload speed
- High spectrum efficiency
- Co-existence of 2nd and 3rd generation systems
- Co-existence of FDD and TDD modes

The architecture of 3G UMTS system is shown in Figure 5.14. Compared to GPRS architecture in Figure 5.11, the changes are made at the Radio Subsystem and the Base Station Subsystem. To differentiate the network components used in 2.5G and 3G, a new set of equipment names have been given for 3G network components. The MS in 2.5G is known as UE (User Equipment) in 3G, the SIM in 2.5G is known as USIM in 3G, the BTS in 2.5G is known as Node-B in 3G and the BSC in 2.5G is known as RNC (Radio Network Controller) in 3G.

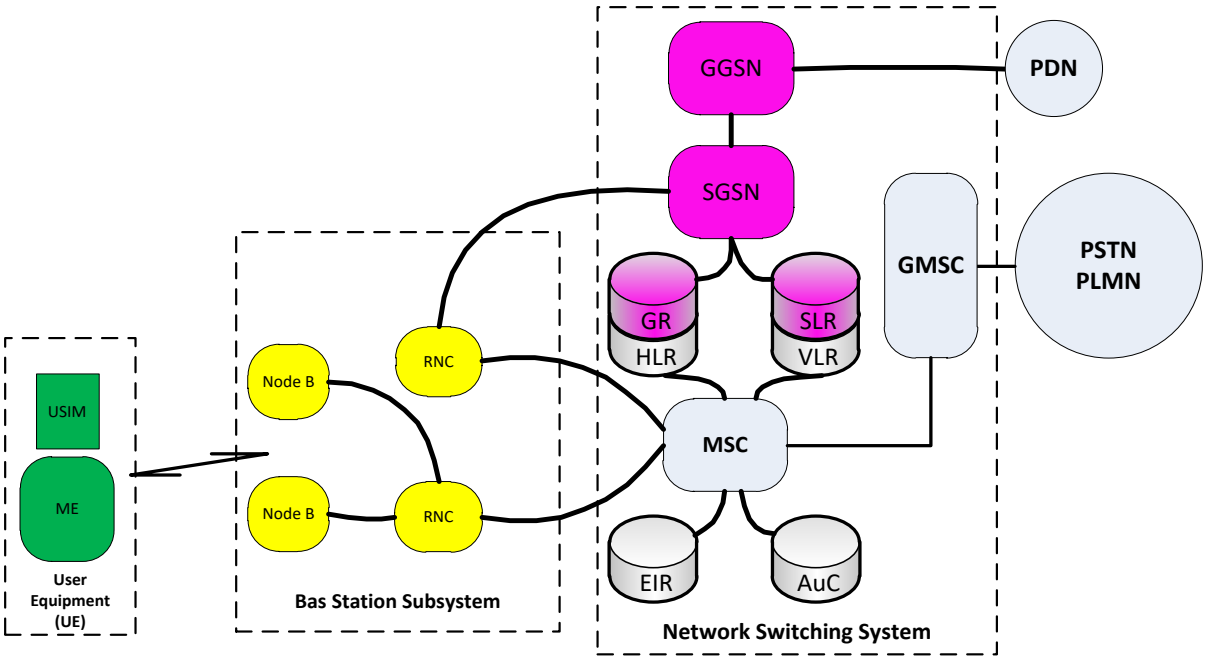


Figure 5.14: UMTS Architecture

In terms of functionalities, there are a few changes:

- The MS is used for voice communication using GSM and data communication using GPRS/EDGE. There is no differentiation in functionalities between different MSs. In 3G, the UE can have different terminal classes for different services based on the maximum bit rate supported. For example, UE can support
  - 32 kbps for basic speech and limited data capabilities
  - 64 kbps for simultaneous speech and data
  - 144 kbps for video telephony
  - 384 kbps, 768 kbps, 2 Mbps for advanced data services
- The MS and BTS in 2.5G use TDMA/FDMA air interface. The UE and Node-B in 3G use WCDMA air interface.
- The BTS in 2.5G only measures the signal quality and does not decide on handover. The Node-B in 3G measures the signal quality, performs inner loop power control and decides on soft handover and softer handover.
  - Hard handover means that all the old radio links in the UE are removed before the new radio links are established. In practice, a handover that requires a change of carrier frequency (inter-frequency handover) is always performed as hard handover.
  - Soft handover means that the radio links are added and removed in a way that the UE always keeps at least one radio link. Soft handover is performed by means of macro diversity, which refers to the condition that several radio links are active at the same time. Normally soft handover can be used when cells operated on the same frequency are changed.
  - Softer handover is a special case of soft handover where the radio links that are added and removed belong to the same Node-B, that is the site of co-located base stations from which several sector-cells are served.

- The BSCs in 2.5G do not communicate with one another. The RNCs in 3G communicates with one another to manage load control, congestion control and outer loop power control.

Section 5.7: Long Term Evolution, LTE

Section 5.7.1 Introduction to LTE

The LTE is the next generation 3GPP radio access network. The LTE network is based on Evolved Packet System (EPS) which is start with the technology direction of third Generation Partnership Project (3GPP) release 8. The EPS is comprised of the radio access network known as Evolved Universal Terrestrial Radio Access Network (E-UTRAN), and an IP core network: the Evolved Packet Core (EPC).

Long Term Evolution (LTE) has been designed to support only packet-switched services. It can be able to provide seamless Internet Protocol (IP) connectivity between user equipment (UE) and the packet data network (PDN), without any disruption to the end users' applications during mobility.

Section 5.10.2 Key Features of LTE

Some key features of release 8 include:

Radio Side (E-UTRAN)

- high spectral efficiency
- very low latency
- support of variable bandwidth
- simplification of radio network and
- Support of packet based services: Multicast, VoIP, etc.

Network Side (Evolved Packet Core – EPC)

- Simple protocol architecture
- Improvement in latency, capacity, throughput, idle to active transitions
- Optimization for IP traffic and services and
- Simplified support and handover to non-3GPP access technologies.

Section 5.10.2.1 E-UTRAN

The E-UTRAN network consists of the physical element, the Evolved NodeB (eNodeB) which is able to function as Node B & RNC in a single entity. Due to the absence of a network controller, it is said to have a flat architecture that will reduce system complexity and cost. It also allows better performance over the radio interface.

Section 5.10.2.2 Evolved Packet Core (EPC)

The EPC handles non-radio related tasks such as all mobility and routing to support heterogeneous access networks such as WiFi, WiMax and even wired technologies and also through to the authentication and billing databases.

Section 5.10.3 LTE Air Interface

In LTE Downlink Transmission Scheme, the Orthogonal Frequency Division Multiple Access (OFDMA) was introduced as a physical modulation protocol to allow the access of multiple users on the available bandwidth. Each user is assigned a specific time-frequency resource.

LTE Uplink Transmission Scheme for FDD and TDD mode is based on SC-FDMA (Single Carrier Frequency Division Multiple Access) with cyclic prefix since SC-FDMA signals have better peak-to-average power ratio (PAPR) properties compared to an OFDMA signal.

LTE supports a subset of bandwidths of 1.4, 3, 5, 10, 15 and 20 MHz. Peak data rates target 100 Mbps (downlink) and 50 Mbps (uplink) for 20 MHz spectrum allocation, assuming 2 receive antennas and 1 transmit antenna at the terminal.

Multiple Input Multiple Output (MIMO) systems form an essential part of LTE in order to achieve the ambitious requirements for throughput and spectral efficiency. MIMO refers to the use of multiple antennas at transmitter and receiver side. For the LTE downlink, a 2x2 configuration for MIMO is assumed as baseline configuration, i.e. two transmit antennas at the base station and two receive antennas at the terminal side. Configurations with four transmit or receive antennas are also foreseen and reflected in specifications. Uplink MIMO schemes for LTE will differ from downlink MIMO schemes to take into account terminal complexity issues. For the uplink, Multi User (MU)-MIMO can be used. The following table summarizes the important characteristics of LTE air interface which includes modulation techniques, sub-carrier spacing, numbers of symbol per frame, symbol duration and type of FEC, etc...

Description	Specifications
Duplex	FDD and TDD
Multiple Access Technique	DL: OFDMA, UL: SCFDMA
Channel Bandwidth	1.4, 3, 5, 10, 15 and 20 MHz
Advanced Antenna Techniques	MIMO 2x2, 4x4
Modulation Type	QPSK, 16-QAM, 64-QAM
Sub-carrier Spacing	15 kHz
Number of symbols per frame	140
Symbol Duration	66.7 us

Forward Error Correction	1/3 Convolutional and Turbo

Section 5.10.4 LTE Frequency Bands

LTE Frequency Bands Covered by different Mobile Operators in Singapore are as following in the Table.

Frequency Band	LTE Uplink, FDD	LTE Downlink, FDD	LTE TDD
1800 MHz	1710 MHz – 1785 MHz	1805 MHz – 1880 MHz	
2600 MHz	2500 MHz – 2560 MHz	2620 MHz – 2680 MHz	2570 MHz – 2615 MHz

Section 5.10.5 LTE System Architecture

Figure 5.15 shows the simplified LTE system architecture which consists of user equipment (UE), E-UTRAN and EPC. As explained early the features of on E-UTRAN and EPC in the previous section, now we will go into the functions of each elements in details.

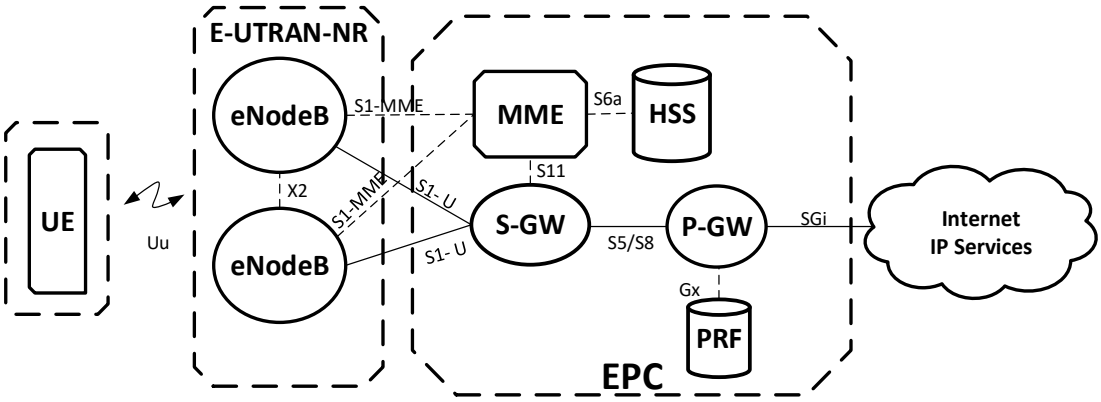


Figure 5.15 Simplified LTE system architecture

User Equipment (UE)

The UE consists of micro-USIM and radio equipment. 3GPP Release 8 defines five LTE user equipment categories depending on maximum peak data rate and MIMO capabilities support. For example, the UE has two transmit antennas but only one transmitter chain and power amplifier. This will keep the UE cost low. A switch will then choose the antenna that provides the best channel to the eNodeB. This decision is made according to feedback provided by the eNodeB.

Enhanced Node-B (eNodeB)

eNodeB is able to handle tasks that related to radio functionality of EPS such as coding, multi-antenna techniques, radio-resource management, fast retransmission, scheduling and adaption control to improve latency and throughput of the network.

All scheduling decisions for downlink and uplink are done in the eNodeB. The scheduling algorithm has to take into account the radio link quality situation of different users, the overall interference situation, Quality of Service requirements, service priorities, etc..

Its functions are summarized as follow.

- Scheduling and dynamic allocation of resources to UEs in both uplink and downlink direction
- Controlling mobility of the UE in connected mode
- State transition from IDLE to connected mode and vice versa
- Admission control and congestion control
- Buffer of the data during handover

Mobility Management Entity (MME)

MME is responsible for Control Plane signalling. Its functions are summarized as follow.

- Interacts with HSS for user authentication, profile download, etc.
- Interacts with eNodeB and S-GW for S-GW selection, tunnel control, paging, handovers, etc.
- Handle mobility management in Idle mode
- Maintain US context during IDLE mode of UE
- Responsible for NSA signalling and NAS signalling security
- Does bearer management for the UE

Serving Gateway (S-GW)

S-GW is responsible for user plane or data plane anchoring for 3GPP access and 2G/3G bearer plane interworking

- Act as mobility anchor for the data bearers
- Buffers the downlink data when UE is in IDLE mode
- Processes all IP packets to/from UE (QoS control, LQI)

Home Subscriber Server (HSS)

HSS carried forward from UMTS and GSM and centralised database holding user profile:

- Interacts with MME for user authentication and profile download
- Stores current location information (e.g. assigned MME, Serving SGW)
- One or more subscription profiles containing IMSI, QoS, Services, etc.

Packet Data Network Gateway (PDN-GW)

Subscriber-aware data plane anchoring for all access networks

- Anchor point in home or visited network for all IP-based access (3GPP or not)
- Session-based user authentication and IP address allocation (IPv4/v6)

- Processes all IP packets to/from UE (QoS control, PCEF, LI)

Policy & Charging Rule Function (PCRF)

User and application-aware policy decision point:

- Interacts with PGW to enforce per session or per flow policies
- Gets event notification from PGW (mobility and/or traffic related)
- Interacts with application for admission control and policy definition
- Supports roaming capabilities

Section 5.7.6 Evolved Packet System Security (EPS Security)

USIM and HSS are required to be used for security in LTE.

There are different set of keys used for ciphering, derived from the same original K stored in the USIM/HSS.

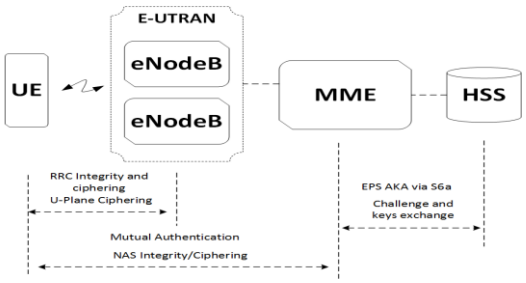


Figure 5.16 LTE security

Section 5.7.7 LTE Advanced, 4G

LTE Advanced is the next milestone in the evolution of LTE, starting from 3GPP Rel. 10. The goals of LTE-A are as follow.

- Increased data throughput
- Improved flexibility of spectrum allocation
- Decrease latency
- Increase reliability data transmission
- Increase in communication efficiency

LTE-A can provide as much as 10x the speed (both uplink and downlink) of LTE. In addition, latency is also lower than 5 msec.

LTE Advanced incorporates multiple dimensions of enhancements which can be grouped into three major categories:

- Carrier aggregation to leverage more spectrum and increase data rates (bps)
- Enhanced MIMO technique to increase spectral efficiency (bps/Hz)
- Relay Node to improve data communication especially cell boundary to increase coverage.

Although, each of these enhancements has its role to play to increase capacity and improve the user experience, the most gain comes from optimizing HetNets.

Section 5.7.7.1 Carrier aggregation

LTE-A utilizes carrier aggregation technique to boost transmission capacity. IMT-A sets the maximum channel bandwidth as 100MHz. In Figure 5.17, the concept of Carrier aggregation is illustrated in contiguous bandwidth.

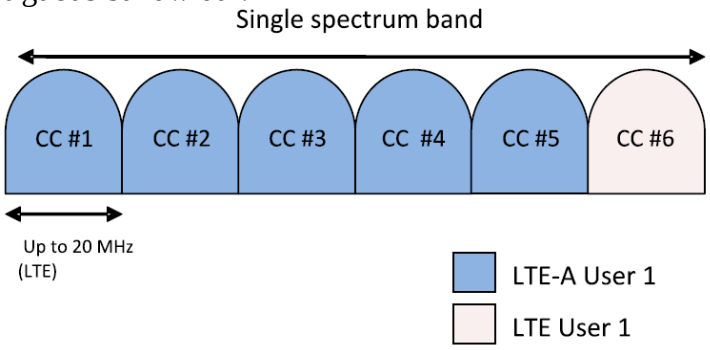


Figure 5.17 Carrier aggregation in contiguous bandwidth

Carrier aggregation not only helps to achieve higher peak data rates, but could also help to achieve better coverage for medium data rates. For medium data rates, it allows the use of lower orders of modulation and lower code rates, which would reduce the required link budget, transmission power, and interference.

Section 5.7.7.2 Enhanced MIMO technique for higher spectral efficiency

The enhanced MIMO technique is based on an adaptive multi-mode framework where the demand of higher data rates and wider coverage is accommodated by selecting the appropriate MIMO scheme according to the current system requirement. The adaptation strategy is chosen based on all the different channel measurements that are gathered at the base station through a low rate feedback mechanism. The following illustrates the main three operating modes.

(i) Single-User MIMO (SU-MIMO): transmit diversity and spatial multiplexing techniques can be selected for transmission in combination with beamforming. This new feature together with a higher-order MIMO (i.e. an increased number of antenna ports) make possible a substantial increase in the peak user data rates.

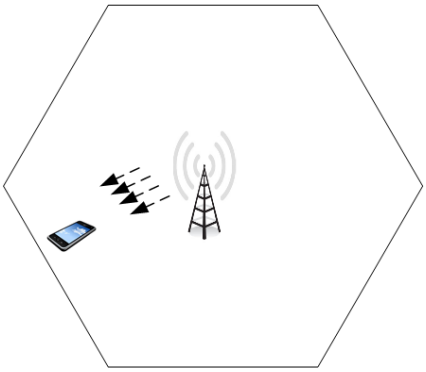


Figure 5.18 Single-User MIMO (SU-MIMO)

(ii) Multi-User MIMO (MU-MIMO): great emphasis is placed in MU-MIMO since it offers the best complexity–performance trade-off. The flexibility of SDMA is increased by allowing a different number of streams to reach each user in order to increase the cell average data rate. SU-MIMO and MU-MIMO constitute what is called single-site MIMO.

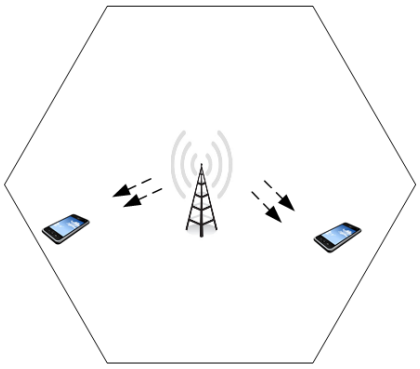


Figure 5.19 Multi-User MIMO (MU-MIMO)

(iii) Cooperative Multipoint (CoMP) MIMO: cell-edge user throughput is boosted by enabling techniques that use coordination in transmission and reception of signals among different base stations, which also helps reducing inter-cell interference. Therefore, CoMP will increase capacity and improve the user experience. Since all the processing and scheduling is centralized, it needs low-latency fibre connections between the processing/scheduling facility and the cells.

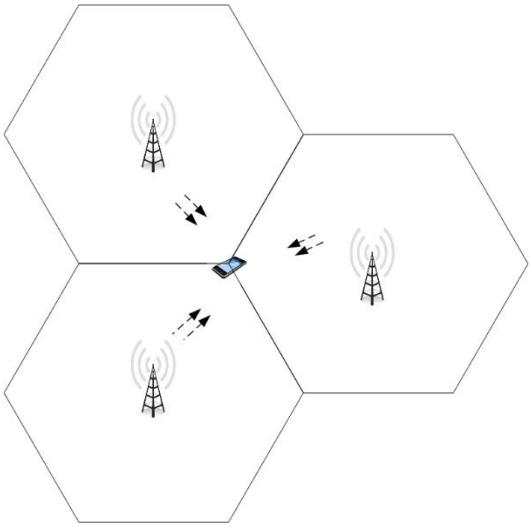


Figure 5.20 Cooperative Multipoint (CoMP) MIMO

Section 5.7.7.3 Relay Node

Relaying is another of the elements that is introduced in LTE-Advanced to improve the performance of LTE, in terms of coverage and throughput. According to 3GPP [13], the use of relays will allow the following improvements.

- Provide coverage in new areas
- Temporary network deployment
- Cell-edge throughput
- Coverage of high data rate
- Group mobility

These improvements can be grouped as ‘‘coverage extension’’ and ‘‘throughput enhancement’’.

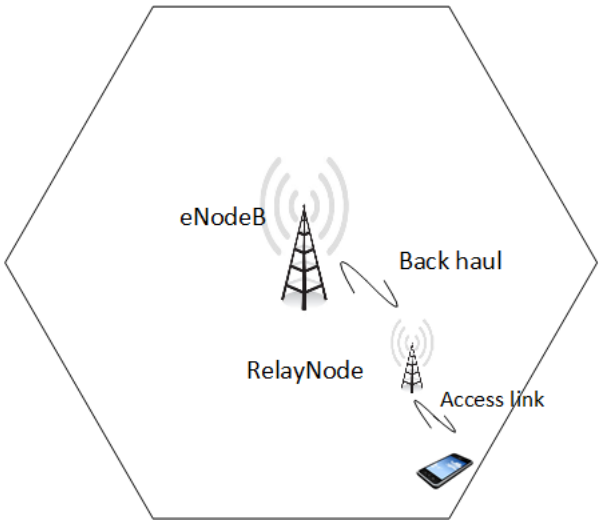


Figure 5.21 Relaying in LTE-A

Section 5.7.8 LTE – Cat M1

LTE-Cat M1 is the simplified industry term for the LTE-MTC low power wide area (LPWA) technology standard published by 3GPP in the Release 13 specification.
It specifically refers to LTE Cat M1, suitable for the IoT. LTE-CatM1 is a low power wide area technology which supports IoT through lower device complexity and provides extended coverage, while allowing the reuse of the LTE installed base. This allows battery lifetime as long as 10 years or more for a wide range of use cases, with the modem costs reduced to 20-25% of the current EGPRS modems.

Section 5.7.9 Narrowband IoT (NB-IoT)

NB-IoT also known as LTE Cat NB1, is a Low Power Wide Area (LPWA) technology that will connect many more devices to the Internet of Things and make many new IoT

applications a reality. It is optimized for applications that need to communicate small amounts of data over long periods of time. Since it operates in licensed spectrum and existing established mobile networks, it is able to provide security, reliability, and guaranteed quality of service. A low device price also cuts the installation cost and reduces the risk of theft. The following is summarized features of NB-IoT. It provides:

- Optimized for very low power consumption +10 year of battery life
- excellent extended long range coverage and deep penetration indoors and underground
- integrated into the cellular system, therefore easy deployment into existing cellular network architecture
- network security & reliability (industry standard based)
- lower component cost

NB-IoT applications focus on low speed, robust data transfer, and an appropriate level of reliability.

Section 5.8: Summary

What do you need to know in this chapter?

- The architecture of GSM with a brief description of the functions performed by each equipment.
- An understanding of GMSK modulation
- The frame structure of GSM
- Two stages of architecture evolution from 2G GSM to 3G UMTS
- Changes made from 2G GSM to 2.5G GPRS
- Changes made in 3G UMTS
- LTE
- LTE-A
- LTE – Cat M1
- Narrowband IoT (NB-IoT)

Chapter 6: 5G Radio Access Technologies

Content

- Explain "What is 5G technology?
- Explain 5G physical layer and features
- Explain 5G Network Architecture
- Understand 5G Security
- Describe the comparison between 5G and LTE
- Describe the applications of 5G

Section 6.1: Introduction

The 5th generation (5G) wireless access technology will address a diverse range of usage scenarios including enhanced mobile broadband (eMBB), massive machine type communication (mMTC) and ultra-reliable and low latency communication (URLLC) – see Figure 6.1.

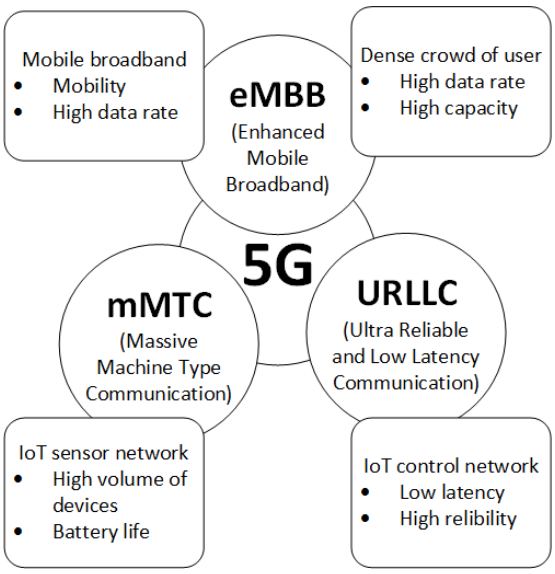


Figure 6.1

The network requirement for 5G can be put into four different scenarios. For the mobile broadband user, it is very important to have the mobility and high data rates. For the dense crowd of user, high data rates, high capacity and partly limited area are required. For IoT control network, low latency, high reliability, resilience and security are very important. For IoT sensor network, the volume of devices and "things" will create new requirements and the battery life time expectation is going to be a few years.

Section 6.2: Physical layer features

5G new radio (NR) offers a flexible interface. The following table describes the summary of key parameters of 5G.

Parameter	FR1,450 MHz – 6000 MHz	FR2, 24.25 GHz – 52.6 GHz
Carrier aggregation	Up to 16 carriers	
Bandwidth per carrier	5, 10, 15, 20, 25, 30, 40, 50, 60, 80, 90, 100MHz	50, 100, 200, 400 MHz
Subcarrier spacing	15, 30, 60 kHz	60, 120, 240 (not for data) kHz
Max. number of subcarriers	3300 (FFT4096 mandatory)	
Modulation scheme	QPSK, 16-QAM, 64-QAM, 256-QAM; uplink also supports π/2-BPSK (only DFT-s-OFDM)	
Radio frame length	10ms	
Subframe duration	1 ms (alignment at symbol boundaries every 1 ms)	
Massive MIMO scheme	Max. 2 codewords mapped to max 8 layers in downlink and to max 4 layers in uplink	
Duplex mode	TDD/FDD	TDD
Access scheme	DL: CP-OFDM; UL: CP-OFDM, DFT-s-OFDM	

Table 6.1: 5G Key parameters

Features	Benefits
mMIMO: massive MIMO	Extends the concept of MIMO to a larger number of transmitters and receivers (> 16 antenna elements) For low band, achieves higher data rates For high bands, allows higher transmission distances.
Adaptive Modulation and variable error correction encoding per RF burst	Ensures a robust RF link while maximizing the number of bits/ symbol for each subscriber unit. Supports BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM.
TDD and FDD duplexing support	Address varying worldwide regulations where one or both may be allowed
Flexible channel widths (e.g. 5MHz, 10MHz, 15MHz, etc)	Provides the flexibility necessary to operate in many different frequency bands with varying channel requirements around the world.
Designed to support smart antenna systems	Smart antennas are fast becoming more affordable and as these costs come down their ability to suppress interference and increase system gain will become important to BWA deployments.

Table 6.2: 5G PHY features

Section 6.3: Architecture of 5G

Section 6.3.1: 5G Network Architecture

gNodeB

One of the biggest change in the 5G Radio Access Network (RAN), known as Next Generation RAN or NG-RAN, architecture is the distributed concept. The gNodeB (5G base-station) is split into gNodeB-Central Unit (CU) and gNodeB- Distributed Unit (DU) where the CU can be placed in the cloud infrastructure.

Access and Mobility Function, AMF

The AMF performs most of the functions that the MME performs in a 4G network. AMF role in 5G standalone registration provides a good overview of the AMF function. AMF is responsible for the following functions.

- Termination of RAN Control Plane interface
- Termination of NAS, NAS ciphering and integrity protection
- Mobility Management
- Lawful intercept (for AMF events and interface to Lawful Intercept System)
- Transparent proxy for routing access authentication and SM messages
- Access Authentication
- Access Authorization
- Security Anchor Function (SEA): It interacts with the UDM and the UE, receives the intermediate key that was established as a result of the UE authentication process; in case of USIM based authentication, the AMF retrieves the security material from the UDM
- Security Context Management (SCM): it receives a key from the SEA that it uses to derive access-network specific keys

User Plane Function (UPF)

The functions of UPF are:

- QoS handling for User plane
- Packet routing & forwarding
- Packet inspection and Policy rule enforcement
- Lawful intercept (User Plane)
- Traffic accounting and reporting
- Anchor point for Intra-/Inter-RAT mobility (when applicable)
- Support for interaction with external DN for transport of signalling for PDU session authorization/authentication by external DN

Session Management Function, SMF

The 5G Session Management Function (SMF) is a fundamental element of the 5G Service-Based Architecture (SBA). The SMF is primarily responsible for interacting with the decoupled data plane, creating updating and removing Protocol Data Unit (PDU) sessions and managing session context with the User Plane Function (UPF).

- UE IP address allocation & management (including optional Authorization)
- Selection and control of User Plane function
- Termination of interfaces towards Policy control and Charging functions
- Control part of policy enforcement and QoS
- Lawful intercept (for Session Management events and interface to Lawful Intercept System)
- Termination of Session Management parts of NAS messages
- Downlink Data Notification
- Initiator of Access Node specific Session Management information, sent via AMF over NG2 to Access Node
- Roaming functionality
- Handle local enforcement to apply QoS SLAs (VPLMN)
- Charging data collection and charging interface (VPLMN)
- Lawful intercept (in VPLMN for Session Management events and interface to Lawful Intercept System)

Authentication Server Function, AUSF

Performs authentication processes with the UE.

Unified Data Management, UDM

UDM supports:

- Authentication Credential Repository and Processing Function (ARPF); this function stores the long-term security credentials used in authentication for AKA
- Storing of Subscription information

Policy Control Function, PCF

PCF provides:

- Support of unified policy framework to govern network behaviour
- Policy rules to control plane function(s) that enforce them

Application Function, AF

AF requests dynamic policies and/or charging control.

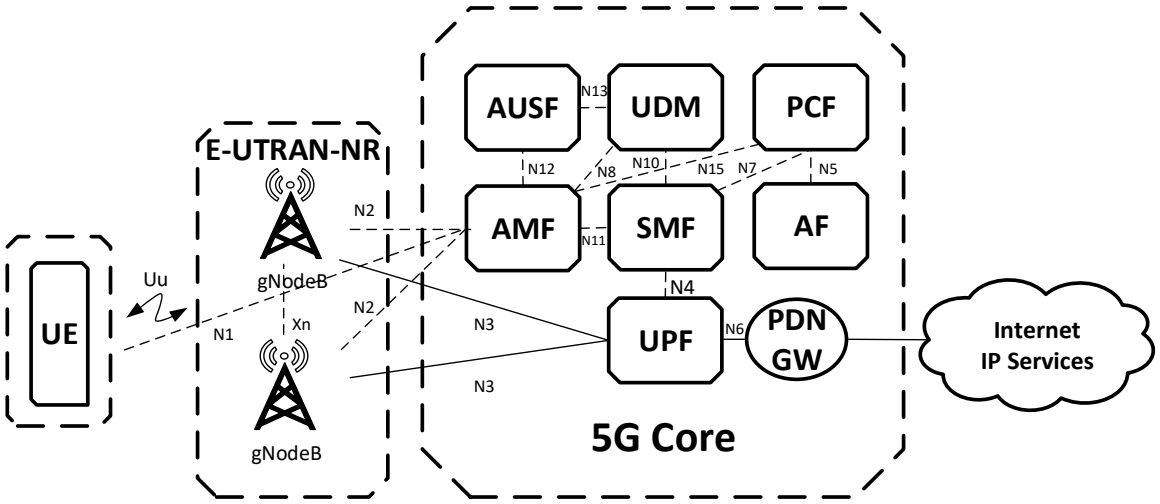


Figure 6.2: 5G network architecture

Section 6.3.2: Service-Driven 5G Architecture

In Figure 6.3, the service-driven 5G network architecture aims to flexibly and efficiently meet diversified mobile service requirements. With software-defined networking (SDN) and Network Functions Virtualization (NFV) supporting the underlying physical infrastructure, 5G comprehensively cloudifies access, transport, and core networks. Cloud adoption allows for better support for diversified 5G services, and enables the key technologies of E2E network slicing, on-demand deployment of service anchors, and component-based network functions. CloudRAN consists of sites and mobile cloud engines. This facility coordinates multiple services, operating on different standards, in various site types for RAN real time resources that require a number of computing resources. Multi-connectivity is introduced to allow on-demand network deployment for RAN non-real time resources. Networks implement policy control using dynamic policy, semi-static user, and static network data stored in the unified database on the core network side. Component-based control planes and programmable user planes allow for network function orchestration to ensure that networks can select corresponding control-plane or user-plane functions according to different service requirements. The transport network consists of SDN controllers and underlying forwarding nodes. SDN controllers generate a series of specific data forwarding paths based on network topology and service requirements. The enabling plane abstracts and analyses network capabilities to implement network optimization or open network capabilities in the form of API. The top layer of the network architecture implements E2E automatic slicing and network resource management.

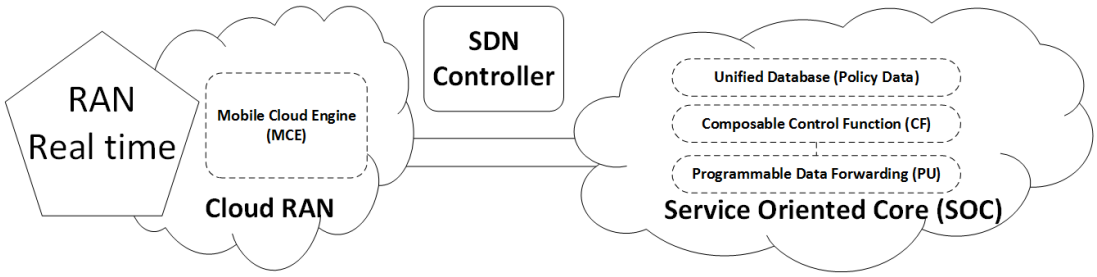


Figure 6.3 Service-driven 5G network architecture

Section 6.4: 5G End to End Network Slicing

In 5G, a single physical network will be sliced into multiple virtual networks that can support different radio access networks (RANs), or different service types running across a single RAN. It is envisaged that network slicing will primarily be used to partition the core network, but it may also be implemented in the RAN. Network slicing is a type of virtual networking architecture in the same family as software-defined networking (SDN) and network functions virtualization (NFV) — two closely related network virtualization technologies that are moving modern networks toward software-based automation. SDN and NFV allow far better network flexibility through the partitioning of network architectures into virtual elements. In 5G, network slicing allows the creation of multiple virtual networks atop a shared physical infrastructure. 5G network slicing enables service providers to build virtual end-to-end networks tailored to application requirements. Network slicing will help to address the cost, efficiency, and flexibility requirements imposed by future.

E2E network slicing is a foundation to support diversified 5G services and is key to 5G network architecture evolution. Based on Network Functions Virtualization, NFV and Software Define Network, SDN, physical infrastructure of the network architecture consists of sites and three-layer DCs. Three-layer cloud DC consists of computing and storage resources shown in Figure 6.4.

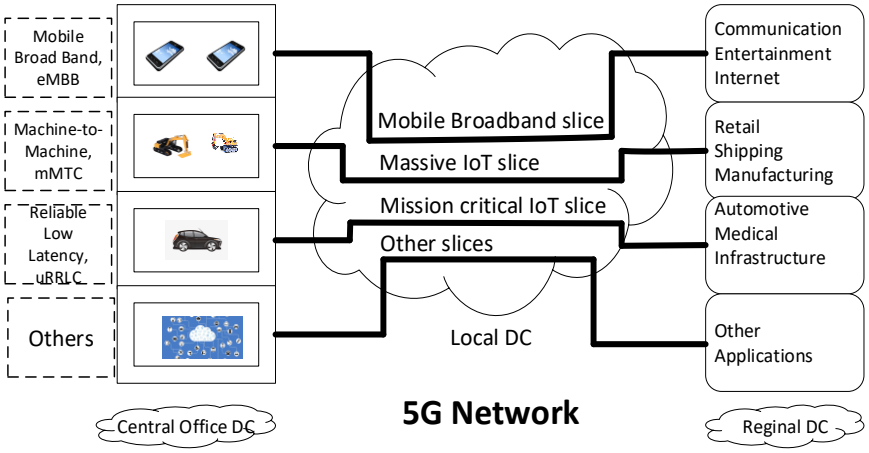


Figure 6.4 End to End network slicing

Section 6.5: 5G Frequency Spectrums and its impact on Data Rate & Cell size

Three key spectrum ranges have emerged. Spectrum below 3GHz-is particularly useful for coverage especially indoor and in rural areas, while spectrum between 3 to 6 GHz is able to offer a mixture of coverage and capacity. This frequency band is unlikely to be able to support the highest potential data rate of 5G without carrier aggregation. Most of the major commercial 5G launches are expected in this spectrum range. For above 24 GHz spectrum, the mmWaves is particularly useful to support very high data rates and short-range connectivity. Some of the importance characteristics are listed in the Table 6.2.

Spectrum range	Bands	Cell Range/Coverage	Date Rate	Bandwidth
< 3 GHz	600 MHz 700 MHz	Deep indoor >1 km	~100 Mbps	FDD 2x10 MHz

	900 MHz 1800 MHz			
3 – 6 GHz	3.4-3.6 GHz 3.6-3.8 GHz 4.5-4.9 GHz	Same grid as LTE1800 ~1 km	~1 Gbps	TDD <100 MHz
mmWaves > 24 GHz	26 GHz 28 GHz 39 GHz	Hot spots Line of sight 100 m	~10 Gbps	TDD <1 GHz

Table 6.2 5G Frequency Spectrum

Section 6.6: UL/DL decoupling

The uplink and downlink decoupling feature intends to separate uplink and downlink of 5G networks onto different frequency bands. It is allowed to configure a low frequency band for the uplink to resolve the issue of limited uplink coverage.
In Figure 6.5, the mobile user prefers to connect to the macro-cell base station, MBS in DL and small-cell base station, SBS in UL. In uplink association, the user uses the fractional path loss compensation power control mechanism for UL power control which depends on the path loss model. Consequently, the user prefers to associate with base station, BS with respect to the path-loss, which will allow the user to reduce their transmission power and the interference on the BS in turn. In other words, the user prefers to associate with the nearest BS in the UL direction in order to reduce its transmission power as well as the interference level at the BS. Thus, this makes the boundaries of BS to be different in UL and DL.

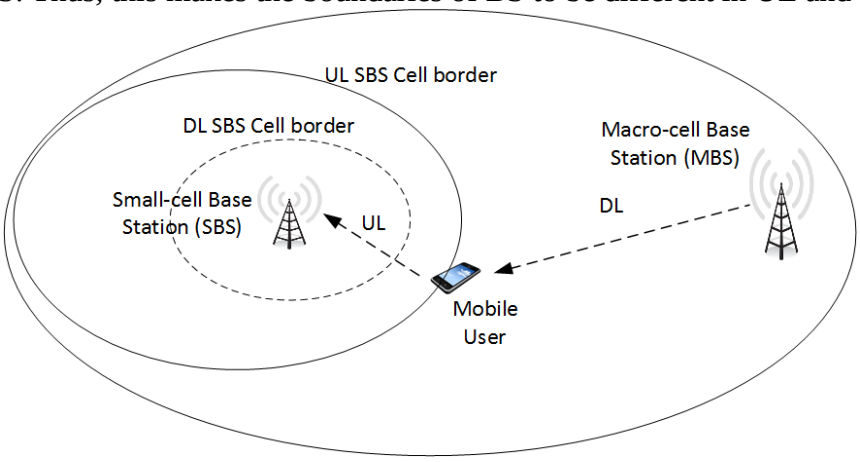


Figure 6.5 Decoupled uplink/downlink user association in a HetNet

Section 6.7: Massive Beamforming in 5G

As the carrier frequency gets higher, the antenna elements get smaller. With this, it becomes possible to pack more elements into a smaller antenna. With more antenna elements, it becomes possible to steer the transmission towards the intended receiver. Since we are concentrating the transmission in a certain direction, coverage is significantly improved. At 15GHz, it is possible to design an antenna with 200 elements that is only 5 cm wide and 20

cm tall. Using massive beamforming with an antenna with 200 elements, it is able deploy a 5G system at 15GHz with 100MHz TDD to improve performance.
With more antenna elements, the beams get narrower, it becomes possible to steer the transmission towards the intended receiver. This will maximize the received signal energy at the mobile in a certain direction, the coverage is significantly improved.

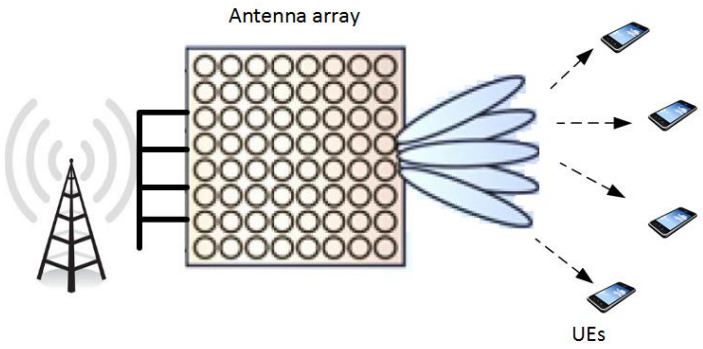


Figure 6.6 Massive Beamforming

Section 6.8: Massive MIMO

Massive MIMO is one of the most important 5G technologies. It will significantly change the traditional network planning, which is based on sector-level wide beams. The antenna pattern of Massive MIMO is no longer a sector-level fixed wide beam, but has been replaced with user-centric dynamic narrow beams instead.
In order to improve spectral efficiency, MU MIMO is introduced to simultaneously enable multiple users with low beam correlation to share the same frequency.
Massive MIMO uses beamforming to form extremely precise user-centric ultra-narrow beams. It aims to project power to user locations, thereby improving coverage and reducing inter-cell interference. Massive MIMO exploits large antenna arrays to spatially multiplex many terminals.
Massive MIMO antenna beams are classified into static and dynamic beams.

- Static beams: Beams can be generated in advance based on the antenna structure and beamforming weight to facilitate planning and simulation.
- Dynamic beams: Multipath identification can be implemented by using the ray-tracing propagation model. User-centric dynamic beams are formed based on multiple paths and measurement results, which is similar to onsite scenarios.
- Multi-path identification: The propagation path between transceivers is calculated using the ray-tracing propagation model to identify multiple paths. Then, the propagation loss is calculated for each individual path.
- Dynamic beamforming: Dynamic weight matrices are calculated based on the measurement results of the multiple paths. Different beams are directed to different UEs based on the calculation results.
- MU space division multiplexing: Spatial multiplexing and related calculations are supported to maximize system capacity.

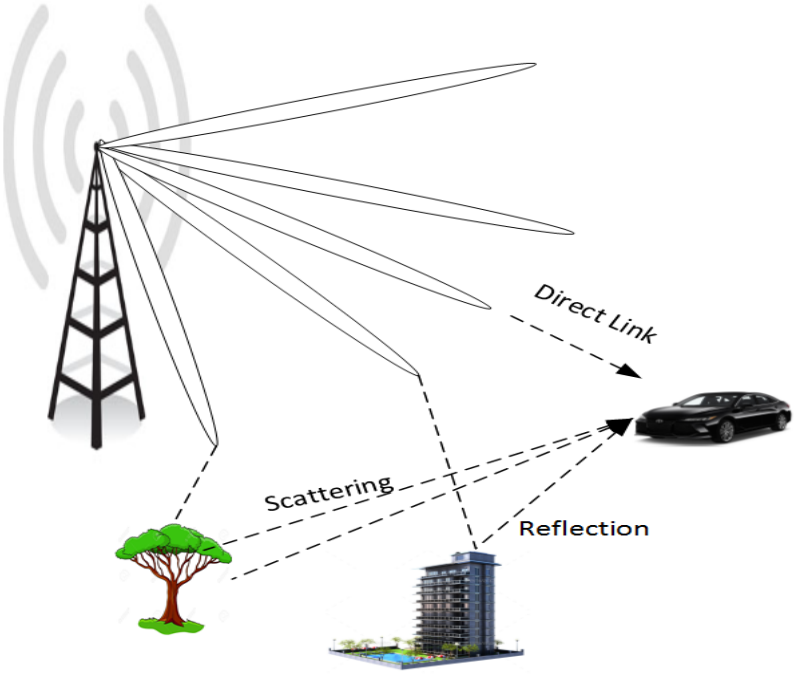


Figure 6.7 Dynamic Beam

Section 6.9: 5G Deployment Option

Standalone (SA) & Non-standalone (NSA)

	Standalone (SA)	Non-standalone (NSA)*
NR radio cells	Directly used by 5G device for control and user planes	Used as a secondary carrier, under the control of LTE base station
Core choice	5G next-gen core (5GCN) which may also anchor IRAT mobility with LTE	4G EPC or 5G next-gen core (5GCN)
Operator perspective	Simple, high performance overlay	Leverages existing 4G deployments
Network vendor perspective	Independent RAN product	Requires tight interworking with LTE
End user experience	Peak bitrate set by NR Dedicated Low Latency transport	Peak bitrate is sum of LTE and NR Latency impacted if routed via LTE

Section 6.10: 5G Security

The 3GPP standardization section (4) focused on security mechanisms in scope for 3GPP, that being the functional elements and interfaces. Additional security considerations related to deployment scenarios of 5G system are covered in this section, including:

System-wide security (horizontal security)

- Network level
- Slicing
- Application level security
- Confidentiality and integrity protection
- Interconnect Service Base Architecture, (SBA)

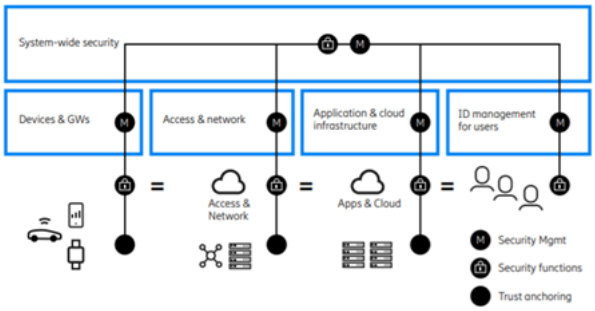


Figure 6.8 5G Security

5G function element deployments (vertical security)

- Network Function Virtualization, (NFV)
- Distributed clouds

Section 6.11: Comparison between LTE and 5G

Features	LTE	5G
Data Rate	1 Gbps	20 Gbps
Latency	10 msec	1 msec
Spectral efficiency	3 bps/cell/Hz	10 bps/cell/Hz
Energy efficiency	200 Wh/TB	1 kWh/TB
Lower IoT power	100 microWh per tx	10 micorWh per tx

Table 6.3 Comparison between LTE and 5G

Section 6.12: 5G Applications

	Category	Applications
Consumers	Mobile Broadband	Smartphones in dense urban area Corporate mobile office
	Fixed Wireless Access	5G for residential homes Wireless SOHO/VPN
	Event experience	Immersive VR360 AR gaming
	In-Vehicle Entertainment	Private cars Public transport
Industries	Critical automation	Collaborative robots/drones Electrical grid tele-protection

	Tele-operation	Video-base remote control Video w/haptic remote control
	Highly interactive AR	Co-present Mixed Reality 360° volumetric video AR/MR
	Mass sensor arrays	Agriculture field sensors Smart city sensors & meters

Table 6.4 5G Applications

Chapter 7: Building a Wireless Infrastructure for Business

Learning Objectives

- Explain "What is Organisational Assessment?"
- Understand the assessment of Existing Network Infrastructure
- Understand the collection of Information for new wireless infrastructure
- Explain the importance of conducting Wireless Site Survey
- Understand the measuring of Return on Investment
- Explain what the developing a Sensible Plan is
- Understand how to get the Right People involved
- Explain "What is Request for Proposal (RFP)?"
- Explain the important to perform a Limited Trial
- Understand the different types of Training
- Understand how to rollout to All Users
- Understand how to provide ultimate support for Business

Section 7.1: Organisational Assessment

When a business decides to invest in wireless technologies, it faces the task of building a new wireless infrastructure. This is much like adding a new network to the organisation. In fact, several of the steps necessary to build this new infrastructure are similar to those needed when adding a new wired network.

An organisational assessment has to be done when adding a wireless infrastructure to a business. This will be the most important part of the process to deploy a wireless infrastructure to an organisation as a whole. Sometimes a change in a procedure or additional personal may meet a perceived need instead of investing in wireless technology that might not be fully justified.

Evaluating the need for wireless technology is a time-consuming process, but it is the essential first step. Evaluating needs involves looking at the organisation and the current network, gathering the basic information and determining costs.

The first step in assessing the need is to step back and examine the organisation or business as a whole. Sometimes users fall into the trap of viewing only their department or unit instead of seeing the big picture of the entire organisation. There are series of basic yet vital questions that need to be asked, including:

- What is the **current size of organisation**?
- How much **growth** is anticipated?
- How do employees in different positions and departments perform their daily activities; meaning do **they need to move around the office and work from different locations**?
- **How frequently does the company move staff to other offices** and need to reconfigure the wiring setup?

Employees that work primarily with one computer at their desks, such as call centre/ customer service operators, may not require wireless access. If the room configuration is static, a wired network will provide performance that is more consistent, in the long run. Although these questions may seem very basic, they can help to refocus the thinking back onto the organisation as a whole and away from one part of it. In addition, questions like that can often reveal a great deal in terms of accessing needs and identifying priorities. The company's employees themselves may not be aware of all the implications of implementing a wireless network, such as the need for new security policies and continuous monitoring as well as potential interference problems that can affect user and application performance an offset the advantages of a WLAN.

Section 7.2: Assessment of Existing Network Infrastructure

The next step is to look at how the organisation or business actually uses its current network. For example:

- How does the **current network** support the organisation's mission?
- What are **the strengths and weakness of the current network**?
- How **many users** does it support?
- **What essential applications** run on the network?

Different industries often have different network requirements. **The banking industry** must have networks offering a **very high degree of security**. The **manufacturing industry** may have networks that must be **completely fault-tolerant and cannot afford any downtime**. **Educational intuitions** may be able to tolerate a small amount of downtime but are faced **with authenticating thousands of new users every few months**. Therefore, each segment is unique and has different network requirements. These factors should be taken into consideration when viewing the current network.

Assessing the current network can help **to identify why a new technology may be needed**. If the current network can be upgraded or adapted to meet the current needs, then wireless technology may not be necessary at this time. However, if **the current network cannot support the anticipated future growth of the business** or there is a clear indication that wireless technology can help the business grow, then the investment may be worthwhile.

The task of assessing the current network can be facilitated by documenting the current network in detail. Networks tend to grow in an unplanned fashion as new users or equipment are suddenly added, so documentation of the network is necessary to gain an overview of the system.

A table like Table 7-1 that summarises the network is useful. If the network is complex, a diagram or layout of the network can also be useful. An example of the diagram is shown in Figure 7-1.

Description	Data
Number of clients	55
Types of clients	35 –Windows 7 20 – Windows XP
Number of servers	1 – Windows 2003
Type of network	Ethernet 100BaseT switched
Type of cable (medium)	Category 5e
Type of devices	5 laser printers, 1 – scanner

Table 7-1: Sample current network table

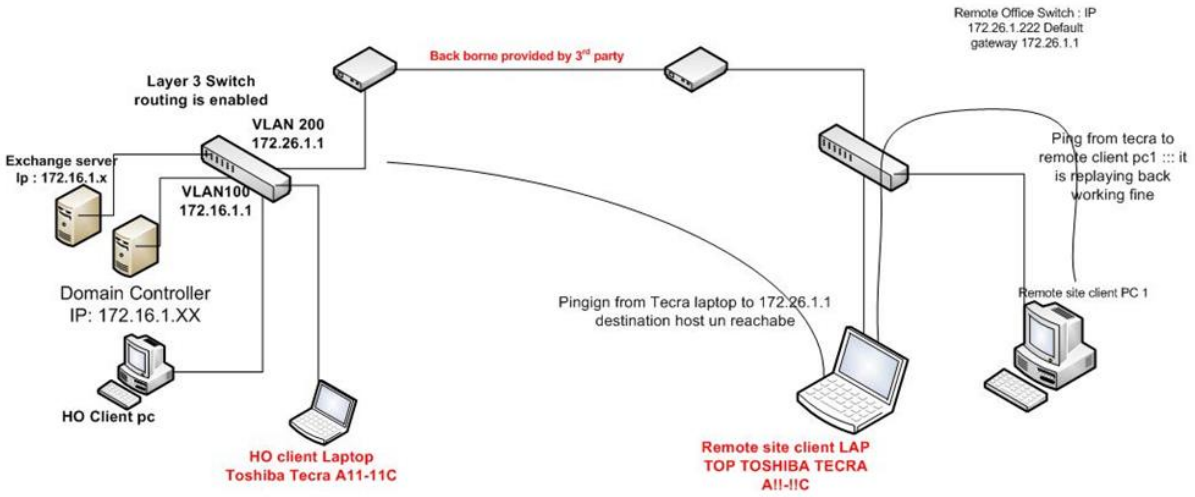


Figure 7-1: Wired LAN Diagram

Section 7.3: Collection of Information for new wireless infrastructure

After the organisation and the current network have been evaluated and it is determined that wireless technology can fit into the current business strategy, the next step is to gather information. With all of the different wireless technologies available and the constant change taking place in the area**, the expertise to gather the information may be beyond that of the current IT staff**. Many organisations turn to **outside consultants and vendors for information at this point**. Some organisation may send out **a request for information (RFI)**.

An RFI is a document that seeks information about what vendors may have to offer. RFIs are general in scope.

For example, a broad statement such as, "The vendor will install a wireless network on the second floor of the building to accommodate 45 users" may be enough to start things rolling. Several different vendors are encouraged to respond with information about the particular products that they sell that will meet those needs.

Once all of the RFIs have been returned, the organisation can examine each of them in detail. Generally, a pattern will emerge from the RFIs that come in from the various vendors. For example, four vendors recommends using Bluetooth, the direction starts to become clear.

Evaluate RFIs with caution. Vendors want to sell a product or service and may **overemphasise the strength of their product while minimising its weakness**. Therefore, **independent research is still needed** after the RFIs have been received.

Section 7.4: Conducting Wireless Site Survey

The information gathered about the current network in preparation for implementing a wireless technology is not complete without a proper wireless site survey. A wireless site survey consists of **measuring the strength and quality of the signal** and the resulting **transmission speeds** and **throughput achievable** in all the different locations around the office where users will need wireless access to the network. In addition, the site survey will **help determine the existence of interference sources**, both internal and external, which will establish the susceptibility of the wireless technology to environmental factors. The survey helps ensure that the actual performance of the network will meet the needs of all the users. For example, a simple wireless site survey to install a WLAN for a small office/home office (SOHO) can be performed using an access point (AP), a wireless adapter card and the client software provided by the adapter card manufacturer. However, a comprehensive site survey, especially for large office buildings, manufacturing plants, multiple floors of a building, or any other complex environments should be performed using more sophisticated software tools and by people who have a level of training and experience that may not be currently available in the organisation. The site survey should ideally be performed using the same type and model of equipment that will be eventually installed. The cost of tools and equipment to perform a site survey is fairly high; purchasing them can only be justified if you will be using these tools on regular basis. There are many prerequisites and steps involved in a site survey. One of the most important and time-saving items to include in the site survey is a building floor plan, preferably one that includes the location of the office furniture items and large machinery. Floor plans will assist in the site survey and yield more detailed and complete reports.

A wireless site survey will identify a number of additional factors regarding the potential implementation of a WLAN, such as:

- Security features and policies required
- Radio signal range (distance requirements)
- Number of channels required (based on user/application load)
- Throughput required
- Location of AP radios and antennas
- Location of client devices, type of client adapters (Wireless Network Interface Cards(WNICs)) and whether external antennas may be required
- Power (electricity) requirements (Power over Ethernet or line?)
- Growth (expansion) requirements and impact on current design
- Potential interference sources and their location, as well as the effect on all of these answers
- Standards and frequencies to be implemented (802.11a or g)
- Requirements for integration with the company's wired network (additional equipment such as switches, firewalls, authentication servers)

The answer to all of these questions will help determine the type and range of equipment that will be required for implementing the wireless technologies and will assist in creating the request for proposal (RFP). **The wireless site survey may be performed** by the company's own technical staff, by a potential vendor, or by a consulting organisation **but should always be done before a vendor provides you with a final proposal**.

Section 7.5: Measuring Return on Investment (ROI)

After the company has collected **potential solutions from vendor RFIs** and **conducted independent research**, it must **determine the costs of the project**. The cost by itself cannot be the sole basis of the decision. Rather, the company must consider the cost in light of the benefit that the project will provide. It may cost $50,000 to implement wireless technology, which might seem like a high **cost**. However, if the new technology will **increase revenue** by $250,000, then that cost may **seem very reasonable**.

Determining the cost in relationship to the benefits is known as calculating return on investment (ROI). In strict accounting terms, **ROI is the profit divided by the investment**. ROI projections are useful when considering the purchase of products or services needed for a business. ROI is best expressed over a specific period of time. For example, you might project that a $50,000 wireless network will save a total of $75,000 in 18 months. The trick with ROIs is to determine all of the costs as well as all of the projected savings.

When determining costs, it is important to consider all costs involved. **Upfront costs** are costs that are necessary to start a project, such as installing the wireless technology in order to start using it. For example, upfront costs for a WLAN include **purchasing APs and wireless NICs** for all devices and computers. The **number of APs depends on the coverage area**, **number of users**, and **types of services needed**. Hardware costs may vary depending on such factors as **performance requirements**, **coverage requirements** and **bandwidth**.

Upfront costs are not the only costs to be considered. **Recurring costs** are often overlooked when determining final costs. A recurring cost is **a cost that a user may continue to pay over an extended period of time**. For example, **if the company leases a free space optics transceiver or a wireless bridge from a local carrier, the annual lease cost is recurring and should be considered as part of the total cost for the technology, over its useful life**. The initial cost of the equipment is usually amortised (reduced) by a certain percentage every year, but lease and maintenance costs either remain the same or may increase over time. The present installation, projected maintenance, hardware or software maintenance contracts, IT staff training and user training should be factored into the total cost of implementation.

A much more difficult task is to determine the savings that can be accumulated. Because the system is not already in place, it may be very difficult to calculate the savings or increased revenue that can accrue. The key here is to be as conservative as possible. Gathering information from other users of the technology can be very helpful.

Section 7.6: Developing a Sensible Plan

Once it is determined that a real need exists that can be solved by implementing wireless technology and the ROI is positive, the next step is to create a plan. The saying that "**those who fail to plan, plan to fail**" is never more true than when considering a new technology. The landscape is littered with projects that were poorly planned at the beginning and abandoned after cost overruns escalate astronomically. **Developing a sensible, workable plan** is perhaps the most critical piece of the entire process. Planning should never be done in a vacuum; instead, the IT staff, users and consultants may all be asked for their input. **Once the plan is completed, a request for proposal (RFP) is sent out to vendors**, who will respond with a formal cost for the project or equipment. A request for proposal is a detailed

planning document that is sent to potential vendors with precise specifications for the products and services that the organisation intends to buy.
Another type of document that is often sent to vendors is **a request for quotation (RFQ)**. **The difference between a RFP and a RFQ is that RFPs ask the vendor to submit a proposal for the entire project, whereas in an RFQ the company has usually preselected the equipment and is simply asking different vendors to provide their most competitive pricing. RFQs are generally used when the project will be entirely designed and implemented by the company's internal staff**.

Section 7.7: Getting the Right People involved

Making an investment in wireless technology involves the efforts of many people. The **most important group is the organization's IT team**. The purpose of using the IT staff is twofold. First, they have a broad background in technology and can contribute much to the dialog regarding their experiences and knowledge base. They are the most trained technologists for the organisation and they need to be treated as such. Nothing alienates an IT staff more quickly than to hire an outside consultant without first tapping the expertise in house.
The most important reason for involving the IT staff at this point is to make them aware of the proposed project, since they will be the ones who will provide technical support and training. This group will be the strongest promoters of the new technology to the users. If the IT staff is **not involved** from the planning process, the project will likely be slow to take off or **even fail**.
Another important group to involve in the planning is **the users themselves**, since they will be the ones who are actually using the new wireless technology. Generally, it is not practical to involve all users at this stage. Instead, a representative group can be selected to participate. However, the group should represent a true cross-section of the user base. Too often the most technological users will enthusiastically support any new technology project, especially if they get to be among the first to test it. The representative group should not just include these types of users. Instead, it should also include the average user, as well as those who have a reputation of opposing to change and new technology. This approach will allow for impartial input to the planning process and it may also serve to get a better cross-section of users on board when the new technology rolls out.
External consultants are generally **the third group that participates** in the planning process. They have the advantage of being outside the organisation and can view the organisation and its needs from **an unbiased perspective**.
A common mistake is to turn an entire project over to consultants and allow them to create the plan. This approach results in a plan that does not benefit from the expertise of the local users and IT staff and may in fact upset them. Instead, **consultants should be included as one source of input, but not the sole source**. It is important **to schedule regular meetings** with consultants and ask them for detailed explanations as the project moves forward. Consultants should provide **in the plan a schedule of activities**, **a list of proposed technology**, and a **phased implementation plan** – **a complete project management plan**. This plan prioritises and allocates time required for the responses from the other participants in the process and also ensures that **the planning phase stays on target**.

Section 7.8: Request for Proposal (RFP)

Once a plan for wireless technology has been designed, the next step is for the organisation to submit a request for proposal (RFP). RFPs are much more detailed than RFIs. An RFP may start with, "The vendor will install an 802.11b WLAN network for 45 users in an area in which users are no more than 275 feet from the access point," and should include more detailed information such as a proposed schedule, known issues (such as a building that contains certain types of hazardous materials like asbestos or chemicals), and any other information that would assist the vendor in creating its response. Some of the key elements to be contained in an RFP include:

Statement of values – A statement of values helps the vendors understand the philosophy of the business and identify its priorities. For example, is network performance more important than the average response time that it takes the vendor to respond to a problem, or the immediate availability of the hardware and software more important than price? A statement of values assists the vendor in developing their response RFP.

Description of operations – A description of the business itself is also helpful for the vendors. This would include any future business plans that might affect the RFP, such as a planned expansion in the branch office building.

Current network and applications – The RFP should describe the current network, such as the number of sites, the current configuration, the applications that are currently being used and the planned additions.

Timetable – The RFP should include a timetable that lists specific dates. An example is shown in Table 7-2.

Proposed Date	Activity
May 1	Date RFP is issued
May 15	Late date that written questions must be submitted by vendors
May 30	Date RFP responses are due
June 15	The week that initial cuts will be mode
July 1	The week that presentations will be made by the finalists
July 15	Date the contract will be awarded
August 15	Date the contract will be finalized
September 10	Date work is to begin
February 12	Date work is to be completed

Table 7-2: Sample RFP timetable

Vendors will respond to the RFP with their proposal for the project. The vendor's response should contain detailed information regarding what will be installed, suggested timelines and how much it will cost. If a site survey has not been performed, it should be included as a mandatory requirement in the RFP. Once all of the RFPs have been received and analysed, the company can make a final decision regarding which vendor to select. **Choosing a vendor should be done carefully by checking the vendor's background and references**. It is very important to take note that **selecting a vendor who submits the lowest-cost RFP can often turn out to be a very costly decision**.

If the technology to be implemented is based on other types of handheld devices, instead of 802.11 WLAN, one of which may appear in the RFPs could be from a wireless application service provider (WASP). A WASP can design and create a wireless application to run on a specific range of devices such as cellular phones, PDAs and other handhelds and can often

deliver the software, hardware, security and networks as one complete package. Because many of the wireless devices, languages and applications are so new and diverse, a WASP may have the expertise needed to get the project up and running quickly. Many WASPs will host the application on their own wireless network, in which case the services are subscribed to rather than purchased. WASPs may become more common and important if a company's planned wireless technology setup includes WiMAX (802.16).

Section 7.9: Perform a Limited Trial

After the RFPs have been received and the vendor has been selected, **it is important to perform a limited trial,** also known in the industry as **a pilot project**. It is usually possible to borrow sample hardware and software from the vendor who won the bid. **The IT staff should be thoroughly involved in the trial, along with a select group of users**. Those **users who were involved in the planning process are good candidates**.
The new wireless technology should be thoroughly tested. **Devices should be connected and then taken offline, the base stations should be disconnected** and other similar activities should be performed to see **how the technology reacts under both normal and unusual circumstances**. **Throughput and applications should be tested**. This is a time in which the IT department can be **introduced to the technology** and **start learning troubleshooting techniques while dealing with the trial group of users**. The **security of the new technology should also be thoroughly tested at this point**. It is **also an opportunity for managers to see the technology in action** so that **they can begin to understand how it will impact the business**.

Section 7.10: Begin Training

After the technology has been tested thoroughly, the next step is to begin training. Do not underestimate this step. **Training provides all users as well as support specialists with the knowledge to effectively operate and support the new wireless technology and can save time and cost during the transition**. Users need to know how to use the new hardware and software and the support staff needs to know how to manage the network and diagnose problems. **Training will increase the effectiveness of the new technology once it is installed because users will have less of a learning curve**. This, in turn, will **minimise the temporary drop in productivity** that is normally associated with the installation of a new system. Also, **well-trained users will have fewer questions and require less IT support**. **The IT staff must be trained first**. This may include on-site training from the vendor if it was included as part of the RFP, or attending workshops or specialised classes that cover the technology. **Once the IT staff has been trained, they in turn can train the users**. Because all users learn differently, a variety of training sessions may be offered to accommodate them. The different types of training include:

- Small group sessions
- Detailed written instructions explaining how to connect to the network and describing potential issues and how to solve them
- Web-based training
- One-on-one sessions

Section 7.11: Rollout to All Users

As the training moves toward completion, the final rollout of the wireless solution to all users can begin. **The most efficient way to do a widespread rollout of a wireless technology is to do it in phases**. **If possible, start with introducing the wireless technology to just one department or unit of the business**. **The IT staff will be able to deal with problems more easily if they only have to deal with one department or unit at a time**. **This also limits the effect of any rollout problems to one department instead of the entire community of users**.

On occasion, a project may need to go live before it is entirely debugged and before every feature is added. If this is the case, it is important that the key users understand this, feel comfortable with the temporary state of the new technology and are aware of the full scale of the project. The key user's leadership among the other users can determine the success of the project.

Once the system is installed and running in a unit, it is a good idea for **the vendor and the IT staff to discuss and identify any problems that may have arisen before additional units are brought on**. IT staff members can also compare notes to determine if the training sessions meet the needs of the users based on the type and number of questions they received. The training can then be tweaked as the remaining users are trained.

Section 7.12: Provide Ultimate Support for Business

Whereas training is primarily done before the new system is turned on, support is the continued follow-up for answering questions and assisting users. User support functions can be organised in a variety of different ways. These include:

- Establish informal peer-to-peer support groups
- Create formal user support groups
- Maintain a help desk centre
- Assign support to the IT department

Each of these has its own set of strengths and weakness. However, establishing and staffing an internal help desk is one of the most effective means of support. A help desk is a central point of contact for users who need assistance using technology. The help desk manages customer problems and requests and also provides support services to solve the problem. The help desk can provide basic information to users, such as why an FSO connection is slower in the rain. The help desk can also be a good source of identifying areas, based on user responses, where improved technology can save the company money. Some suggestions regarding a help desk include:

- Have one telephone number for the help desk.
- Plan for temporarily increased call volume after the new network is installed.
- Create a method to track problems effectively.
- Use surveys to determine user satisfaction and to identify any remaining issues.
- Periodically rotate network personal into the help desk.
- Use information from the help desk to organise follow-up training.

LAB SHEETS

LAB 1: Setting up RFID Basic Commands and PC Interface

Objectives:

Students will learn

- what are the modules inside the RFID contactless smart card reader and its system to provide different types of applications to enable various services.
- the basic command of a reader module, interface to a PC, and read/ write data of Mifare and I-Code RFID cards.

Introduction:

In lectures, students will learn the basic components of an RFID system. In this experiment, students will learn the basic commands of a reader module and how to read/write I-Code, MiFare RFID cards and MiFare Card Personalization function.

Initial Setup

Procedure:

1. Firstly, the reader module of the Training kit should be connected to a laptop via RS232 cable and then the laptop and the training kit are power on.
2. Launch the Demo Software of RFID training kit double clicking on the RFID shortcut icon at the desktop.

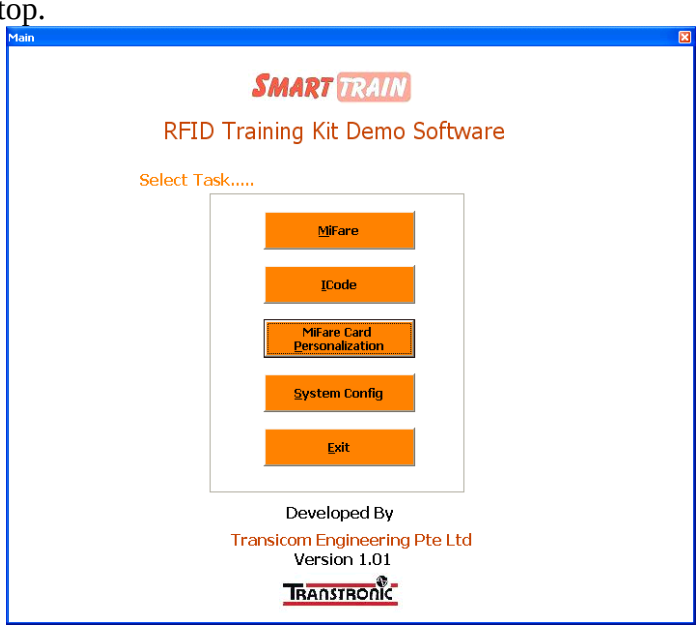


Figure 1: Main system screen

3. Then, click on the **System Config** button to set the communication setting of the com port and the baud rate of the reader. The com port setting can be updated by clicking the update button. It is important to take note that if you want to change the reader baud rate, its initial baud rate and the baud rate of the com port must be same. Click the **Return** button and back to Main menu.

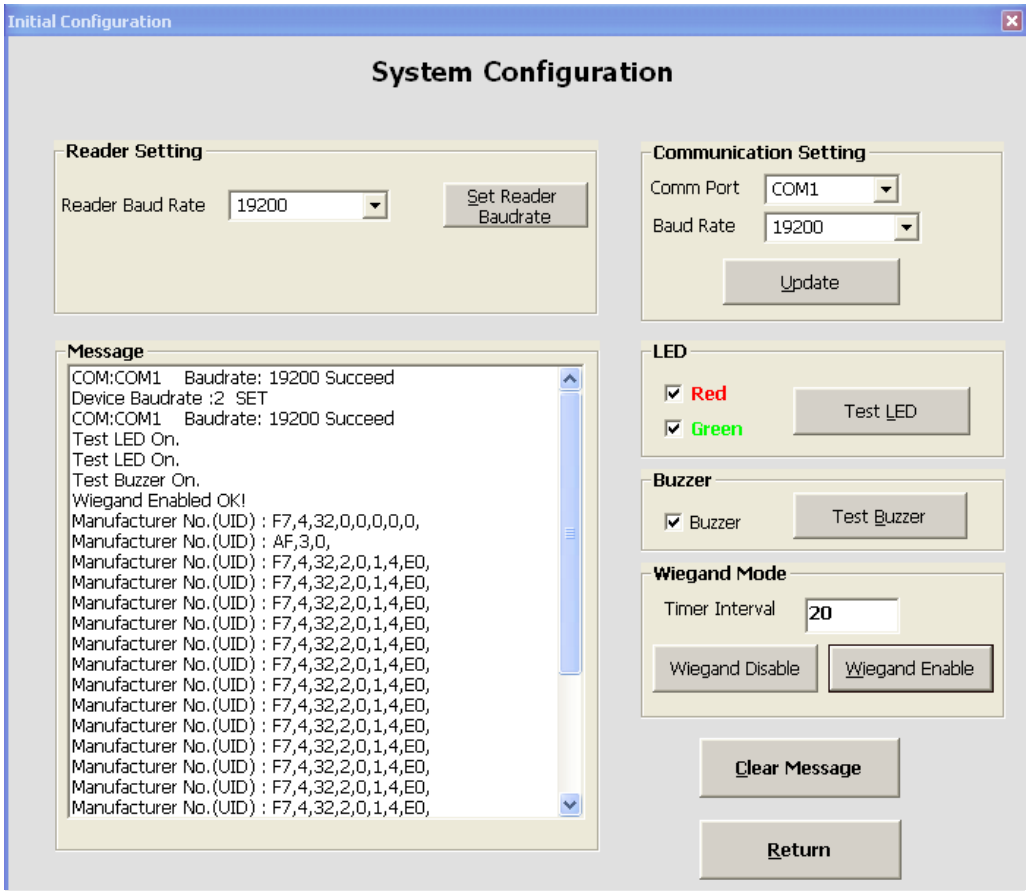


Figure 2: System configuration screen

4. In order to read/write the I-Code RFID tag, click the I-Code button. From the I-Code function window, you are allowed to experiment the I-Code basic commands such as select, reset, read, write and flag setting.

I-Code function

I-Code II Contact less card is complied with ISO15693 standard.

The memory map of the I-Code SL2 chip is as shown in the following Figure. The 1024 bit EEPROM memory is divided into 32 blocks. Each I-Code contains 28 accessible blocks for read/write operations. Each block can hold 4 bytes. The 8 byte-manufacturer number is stored in the block -3 and -4. The EAS, AFI, DSFID are stored in the block-2.

	Byte0	Byte1	Byte2	Byte3	
Block -4	UID0	UID1	UID2	UID3	Unique Identifier Lower bytes
Block -3	UID4	UID5	UID6	UID7	Unique Identifier Higher bytes
Block -2	IntUse	EAS	AFI	DSFID	EAS, AFI, DSFID
Block -1	00	00	00	00	Write Assess Conditions
Block 0	X	X	X	X	
Block 1	X	X	X	X	
Block 2	X	X	X	X	User Data
Block 26	X	X	X	X	
Block 27	X	X	X	X	

Figure 3: EEPROM memory map of I-Code SL2

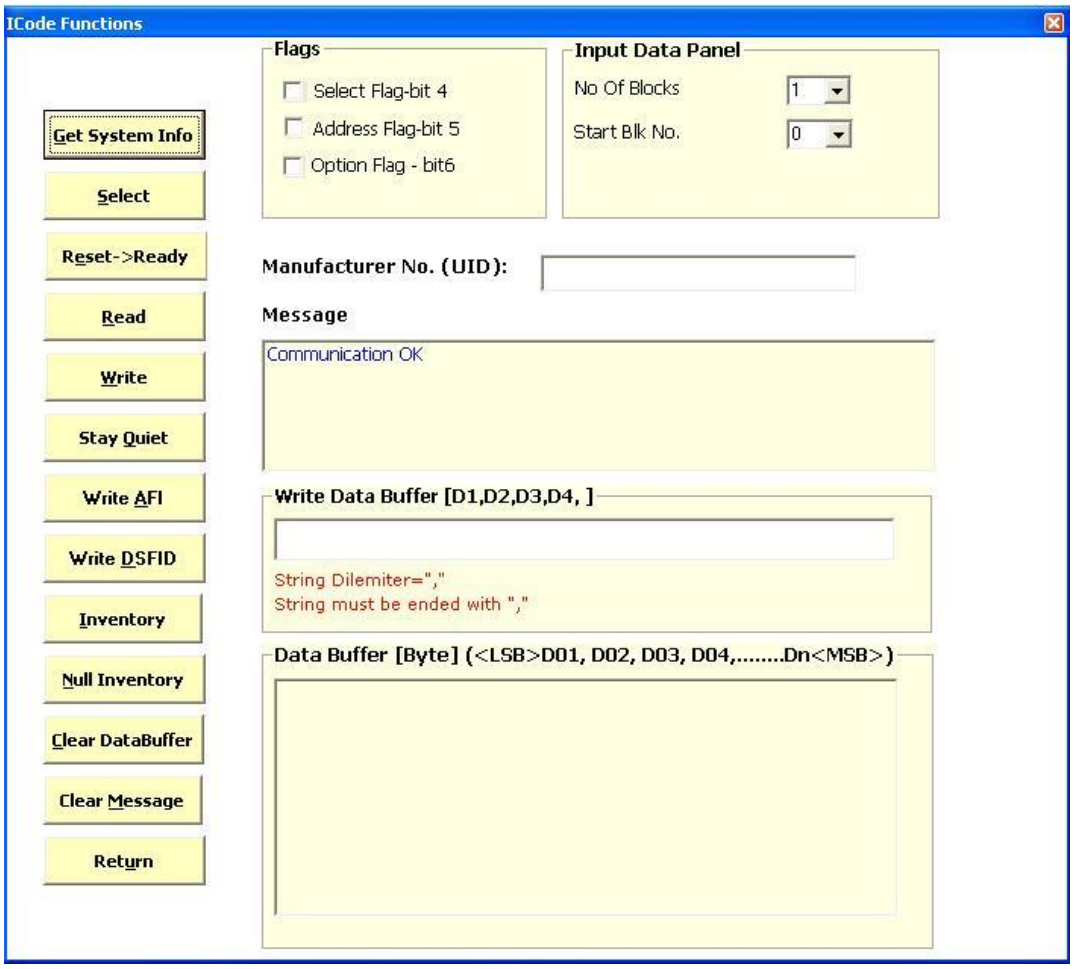


Figure 4: I-Code command screen

I-Code commands:

Procedure

In this section you are required to carry out few I-Code commands to test with the **three** I-Code cards.

1. Launch the I-Code Function window by clicking the ICode button at Main screen.
2. Place one of the I-Code cards on the reader.
3. From the I-Code Function window, click on the **Get System Info** that will Read **8** bytes UID (Unique Identifier), **1** byte DSFID and **1** byte AFI from card. Record the card information in Table 1.
4. Repeat the step 2 and 3 with others two I-Code cards.

Card No.	UID	DSFID	AFI	Remark
1				
2				
3				

Table 1

5. Using **Input Data panel** and **Read** button to retrieve the user data from block 0 to block 3 and record the data.
   Setting: No. of Block: _____, Start Block No.: _____Data.

6. Using **Input Data panel** and **Write** button to write the data "8,9,A,B," at block no. 6 and show it to the lecturer and then rewrite the data "0,0,0,0,".
7. Write **AFI** (Application Family Identifier) as "1" and rewrite "0". AFI value should be keyed in at Write Data Buffer as Hexa Decimal value of **one byte**.
8. Write **DSFID** (Data Storage Format ID) as "1" and rewrite "0". DSFID value should be keyed in at Write Data Buffer as Hexa Decimal value of one byte.
9. To test on the **Select** command, firstly place one of the cards on the reader and click on **Get System Info** to get UID, tick on the **address flag** to be checked and then click on the "Select" button. Then, place all the three cards on the reader and click on Read button. Which card is read?

   Selected One: ☐ One of the other two cards: ☐

10. To test on **Stay Quiet** command, place one of the cards on the reader, click on the **Get System Info** and tick on the **address flag** to be checked. Then, click **Stay Quiet command** button to issue a successful **Stay Quite** Command process. Then, the tick on the address flag to be unchecked. After the **Stay Quite** command has successfully issued, the card will not reply the commands until it is given **Reset -> Ready** command.
    Note: The card at the Stay Quite state shall respond to the commands in address modes.
11. Click **Reset->Ready** that will reset the card from the selected state to ready state.
12. **"Null Inventory"** command: When this command is issued, the UID of one card will return the data if there are more than one card are in the RF field. As an example, if you put card A and card B, and then issue **Null Inventory** command, either A or B with return. After giving Select command to the firstly returned card and issue Stay Quiet command, the card will be in Quiet mode. At this point, again if you give the Null Inventory having both cards A and B in the RF field, the other unchosen card, i.e card B, must reply, since card A is in the **Stay Quite** mode.
13. **Inventory** command: This command will run the anti-collision loop, you may get a card's UID by this command among many cards. The main difference between the NULL INVENTORY and INVENTORY itself is the requirement for UID input when the command is issued. The NULL INVENTORY does not require the UID.

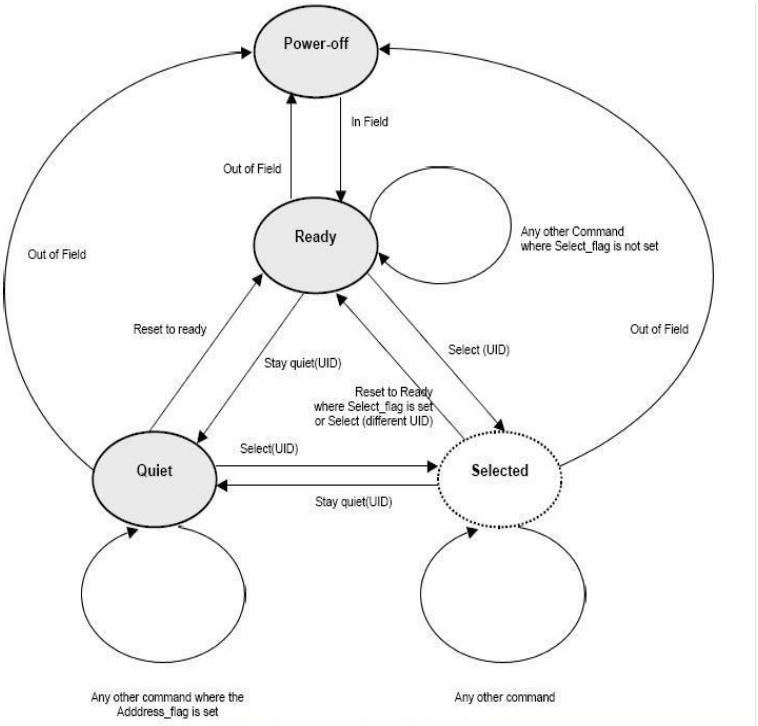


Figure 5: I-Code state diagram

Mifare Function:

In order to read/write the Mifare RFID tag, click the MiFare button. From the MiFare function window, you are allowed to experiment the MiFare basic commands such as:

a. Load Key (to reader)
b. Store Key (in reader)
c. Request/Request All
d. Anti-collision
e. Select
f. Authentication
g. Read
h. Write
i. Increment value
j. Decrement value
k. HighLevel Read
l. HighLevel Write

MiFare contactless smart cards are complied with ISO/IEC 14443A. When the card is positioned in the proximity of the Read Write Device antenna, RF communication interface allows to transmit data to the card.

Each of the MiFare cards contains 16 sectors with 4 blocks each. One block can store 16 bytes of data. At a time, 1 to 4 blocks in one sector of data can be read from the card. Each sector can have individual security key of its own. Before any read or write memory operation, key for each sector has to be authenticated by the loaded key. However, changing security key should be done by experienced person to avoid unnecessary damage to the card.

Card Read/Write Sequence

Mifare Card Function sequence as follow:

a) Select Sector number
b) Select number of blocks to Read (or) Select block number to Write (or) Select block number to Initialize Value Block
c) Request
d) Anti-Collision
e) Select
f) Load Key (not necessary to be in this exact sequence)
g) Authentication
h) Read (or) Write (or) Initialize Value Block

High Level Mifare Card Function sequence as follow:

a) Store Key
b) Select Sector number
c) Select number of blocks to Read (or) Select block number to Write
d) HighLevel Read (or) HighLevel Write

Security key is stored in block 3 of each block. This is also called as Sector trailer. Manufacturer serial number (UID) and data are stored in sector 0 of block 0. This is also called as Manufacturer block.

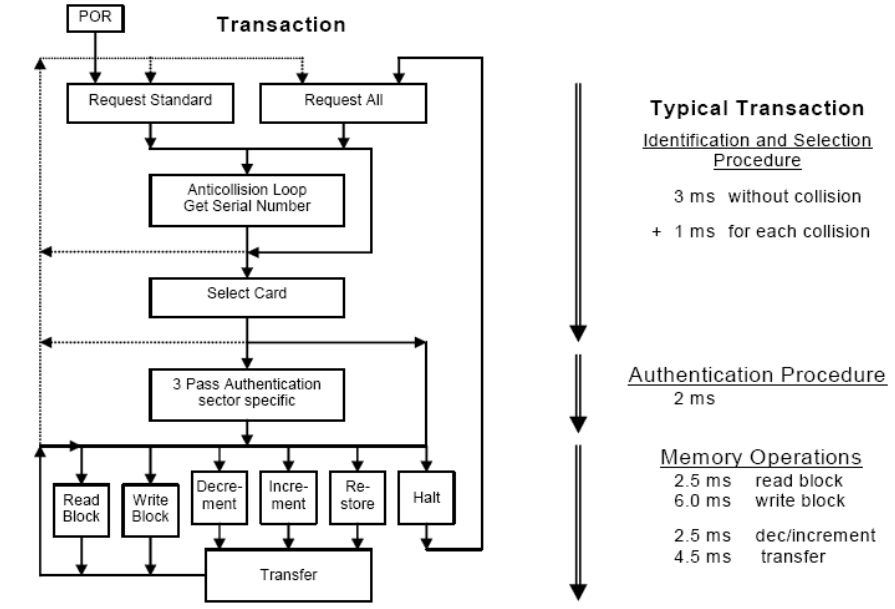


Figure 6: Three pass authentication

Sector	Block	Byte Number within a Block 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Description
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
:	:																	
:	:																	
:	:																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

Figure 7: EEPROM memory map of MiFare MF1ICS50

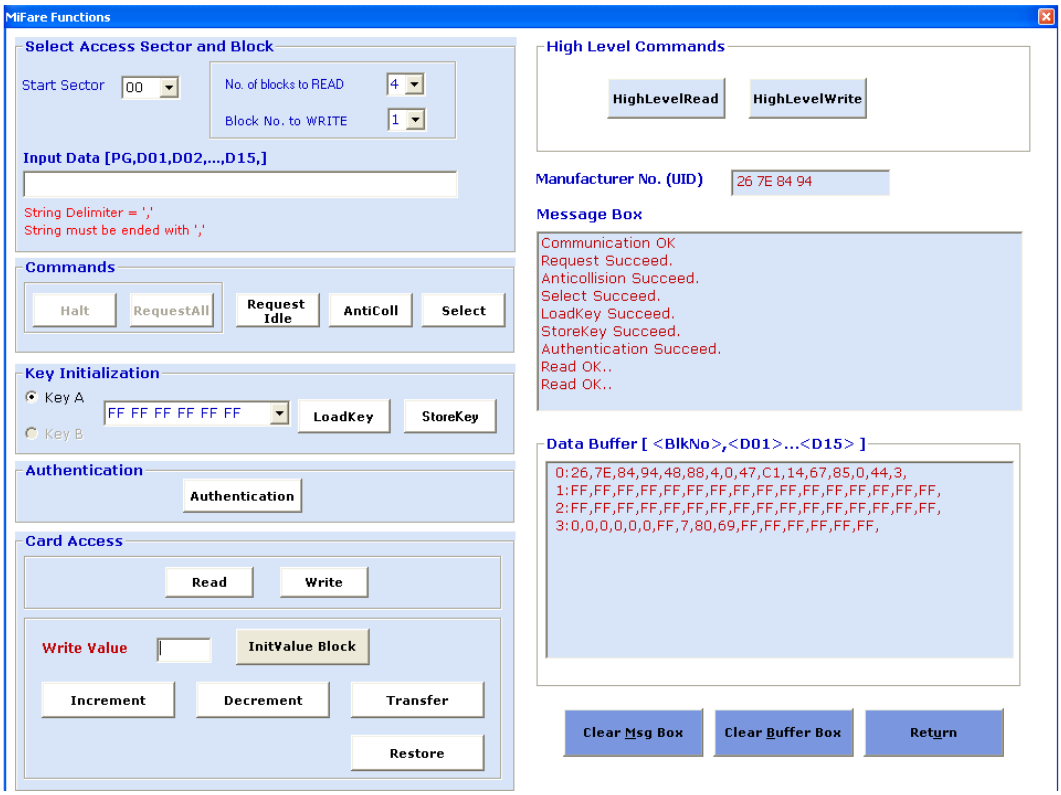


Figure 8: MiFare command screen

Mifare commands:

Procedure

In this section you are required to carry out few MiFare commands to test with the **five** MiFare cards.

1. Launch the MiFare Function window by clicking the MiFare button at Main screen.
2. Place one of the MiFare cards on the reader.
3. From the MiFare Function window, Select Sector number (Default sector "0") > Select number of blocks to Read (Default "1"), Then, click **Request All** > **Anti-Collision** > **Select** > **Load Key** > **Authentication** > **Read**. This sequence will read the **4** bytes UID (Unique Identifier) of the MiFare card that cannot be modified by user. Record the UID of the card in Table 2.
4. Repeat the step 2 and 3 with others four MiFare cards.

Card No.	UID	Remark
1		
2		
3		
4		
5		

Table 2

5. **Read** the data block 0 to 3 of sector 0 of the one of the cards. Record the data in the Table 3.

Setting: Start sector: _____No. of Block to READ: _____,

Data:

Block 0:

Block 1:

Block 2:

Block 3:_____.

6. **Write** the data block of the card no. 1 with the data "A,B,C,D,A,B,C,D,A,B,C,D,A,B,C,D," at the block no. 12 of sector 3 and record the required setting and the whole sequence.

Setting: Start sector: _____Block No. to WRITE: _____.
Sequence: _____
_____.

The following step **7 to 12 are optional**. These are for advanced users.

7. **HighLevelRead** command: High Level Read command combines all the necessary steps needed to carry out reading each block in a single command. Before carrying out using the HighLevelRead command, the Key has to be loaded by Store Key command. The required sector and number of blocks can be chosen in the Select Access Sector and Block Panel.
8. **HighLevelWrite** command: High Level Write Command combines all the necessary steps for writing to a memory block in a single command. As the HighLevelRead command, the key has to be loaded by Store Key command to the requested block.

9. **InitValue Block** command**:** Create and initialize a Value Block in card memory. Select sector number and write Block number from Access Sector and Block Panel to define value block. Since it is a memory operation to the card, the sequential commands of RequestIdle, AntiColl, Select, Authentication and also LoadKey are required to be carried out before this InitValue Command. The Mifare Init Value Block will be created with Mifare Value Block Format.
10. **Increment** command: Add input value to the specified value block. The incremented valued which is stored in MiFare Reader Chip internal value buffer register, will not be written to the Value Block until Transfer command is sent.
11. **Decrement** command: Decrease input value from the specified value block. Decremented value will be updated only after Transfer command is sent. Otherwise value will be still in the internal value buffer register. Before Increment and Decrement commands, the Value Block must be first formatted with the MiFare Value Block Format with InitValue Block Command.
12. **Transfer** command**:** To transfer the data from MiFare Reader's internal Value buffer register to the selected value block.

Questions:

1. What are the basic components of an RFID reader?

2. What are the modules required for an RFID system?

3. What is the maximum size of memory bytes for **user data** of I-Code RFID tag?

4. Understand the select function and describe the command sequence of a select function for the I-Code card.

5. What is the maximum size of memory bytes for the MiFare RFID tag?

6. Describe the command sequence of a MiFare Write operation.

7. Compare the security features of I-Code and MiFare cards.

8. What is the RF frequency used in I-Code system?

9. What is the RF frequency used in MiFare system?

10. Measure the reading range of I-Code and MiFare Card using a ruler and compare their ranges.

11. Draw a table as follow and make comparison between I-Code and MiFare Cards base on their characteristics, features and applications.

Serial No.	Descriptions	I-Code	MiFare	Remarks
1	Frequency			
2	Anti-collision			
3	UID			
4	Memory Size			
5	Security			

LAB 2: Case Study and Experiment for RFID Application using MiFare Smart Card Training Kit

Objectives:

Students will learn

- how to personalize the RFID contactless card to provide different types of applications to enable various services.
- how to setup the RFID contactless smart card reader and its system to provide different types of applications to enable various services.
- how to initialize and activate a suitable application using the user interface.
- how to implement a complete real life application using RFID technology.

Introduction:

In the experiment 1, students have learnt the data structures of the MiFare RFID card it. In this experiment, students will learn how to implement a complete real life application using RFID technology.

Procedure:

Firstly, students are required to personalize the five MiFare cards using **MiFare Card Personalization function**

MiFare card personalisation

1. MiFare Card Personalization function for sample application is needed to be done by clicking the MiFare Card Personalization button.

   Issue four types of cards: **one** Admin card, **one** Lecturer card, **one** Technician card and **one** Student card by using the following commands in sequence, **Erase > Read (to check "successful erase")**, **Select** card type > Enter six digit **Card Serial No**. > Enter ten digit Holder ID > Enter **Credit** Value > **Write**, and then click **Reset** >**Read** to check successful write. If all cards are completely personalized, click **Return** to **main screen**.

Note: Admin card type is for data browsing and for this type of card; it will not be allowed to choose the type of the Applications. For the Vending Machine Application, the credit amount for the card can be set and top up too. Data in sector 0 is reserved by vendor and contains fixed data and not allowed to be changed. Erase will Erase/Clear card user data from Block 4 & 5.

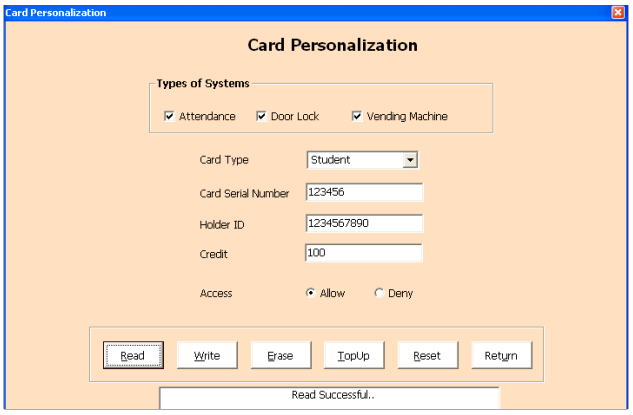


Figure 1: MiFare card personalization

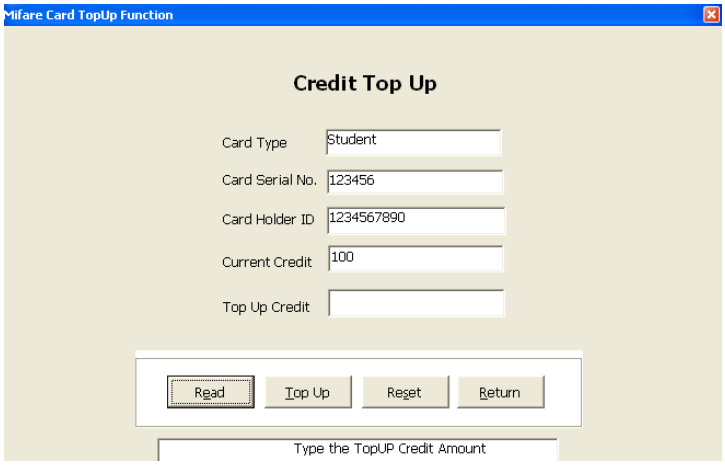


Figure 2: Top up screen

2. Click on the MiFare button at Main screen and read the data block 4 and 5 of sector 1. Record the data in the Table 1.

Card No. 1

No.	Description	Byte	Type	Byte No.	Data	Remark
				Block 4		
1	Card Type	1	ASCII	0		
2	Card Serial No.	4	Long	1 ~ 4		
3	Card Identification Number (Student/Lecturer/Staff ID)	10	ASCII	5~14		
4	BCC for Block 4	1	Char	15		
				Block 5		
5	Current Credit	4	Long	0 ~ 3		
6	Access Valid	1	Char	4		
7	Start Date and Time	5	Char	5 ~ 9		
8	End Date and Time	5	Char	10 ~ 14		
9	BCC for Block 5	1	Char	15		

Card No. 2

No.	Description	Byte	Type	Byte No.	Data	Remark
				Block 4		
1	Card Type	1	ASCII	0		
2	Card Serial No.	4	Long	1 ~ 4		
3	Card Identification Number (Student/Lecturer/Staff ID)	10	ASCII	5~14		
4	BCC for Block 4	1	Char	15		
				Block 5		
5	Current Credit	4	Long	0 ~ 3		
6	Access Valid	1	Char	4		
7	Start Date and Time	5	Char	5 ~ 9		
8	End Date and Time	5	Char	10 ~ 14		
9	BCC for Block 5	1	Char	15		

Card No. 3

No.	Description	Byte	Type	Byte No.	Data	Remark
				Block 4		
1	Card Type	1	ASCII	0		
2	Card Serial No.	4	Long	1 ~ 4		
3	Card Identification Number (Student/Lecturer/Staff ID)	10	ASCII	5~14		
4	BCC for Block 4	1	Char	15		
				Block 5		
5	Current Credit	4	Long	0 ~ 3		
6	Access Valid	1	Char	4		
7	Start Date and Time	5	Char	5 ~ 9		
8	End Date and Time	5	Char	10 ~ 14		
9	BCC for Block 5	1	Char	15		

Card No. 4

No.	Description	Byte	Type	Byte No.	Data	Remark
				Block 4		
1	Card Type	1	ASCII	0		
2	Card Serial No.	4	Long	1 ~ 4		
3	Card Identification Number (Student/Lecturer/Staff ID)	10	ASCII	5~14		
4	BCC for Block 4	1	Char	15		
				Block 5		
5	Current Credit	4	Long	0 ~ 3		
6	Access Valid	1	Char	4		
7	Start Date and Time	5	Char	5 ~ 9		
8	End Date and Time	5	Char	10 ~ 14		
9	BCC for Block 5	1	Char	15		

Card No. 5

No.	Description	Byte	Type	Byte No.	Data	Remark
				Block 4		
1	Card Type	1	ASCII	0		
2	Card Serial No.	4	Long	1 ~ 4		
3	Card Identification Number (Student/Lecturer/Staff ID)	10	ASCII	5~14		
4	BCC for Block 4	1	Char	15		
				Block 5		
5	Current Credit	4	Long	0 ~ 3		
6	Access Valid	1	Char	4		
7	Start Date and Time	5	Char	5 ~ 9		
8	End Date and Time	5	Char	10 ~ 14		
9	BCC for Block 5	1	Char	15		

Note : Card Type: A=Admin, L=Lecturer, S=Student, T=Technician

3. Disconnect the cable at RS-232 port which was connected to the laptop.
4. Then, the reader module of the Training kit should be connected back to its system via RS232 cable and then the training kit is power on as in Figure 3.

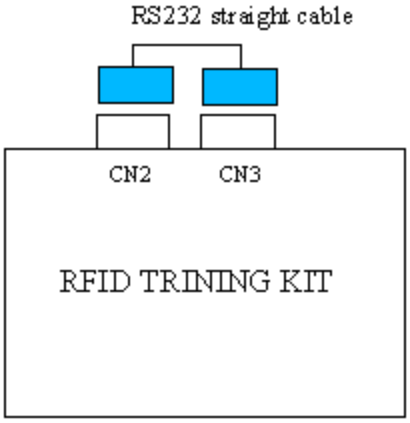


Figure 3 : Setup for Application and Case study

5. By using the five programmed cards you are required to perform the following sample applications are used as Case Study.

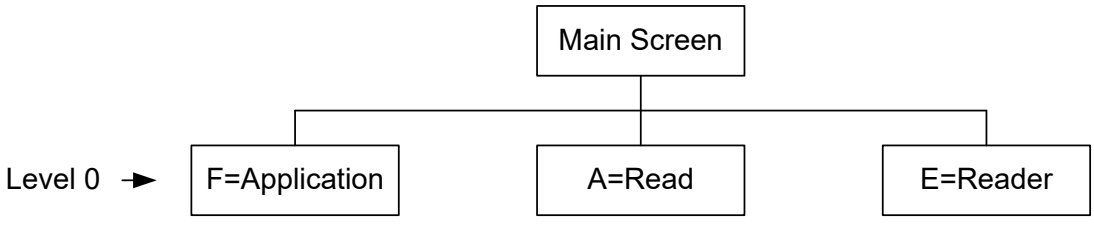
- Hardware Test and Basic Function
- Attendance Recording
- Door Access System
- Vending Machine / Cashless Payment System

Note: MiFare Standard Card with default security key (FF FF FF FF FF FF) is used for all sample applications.

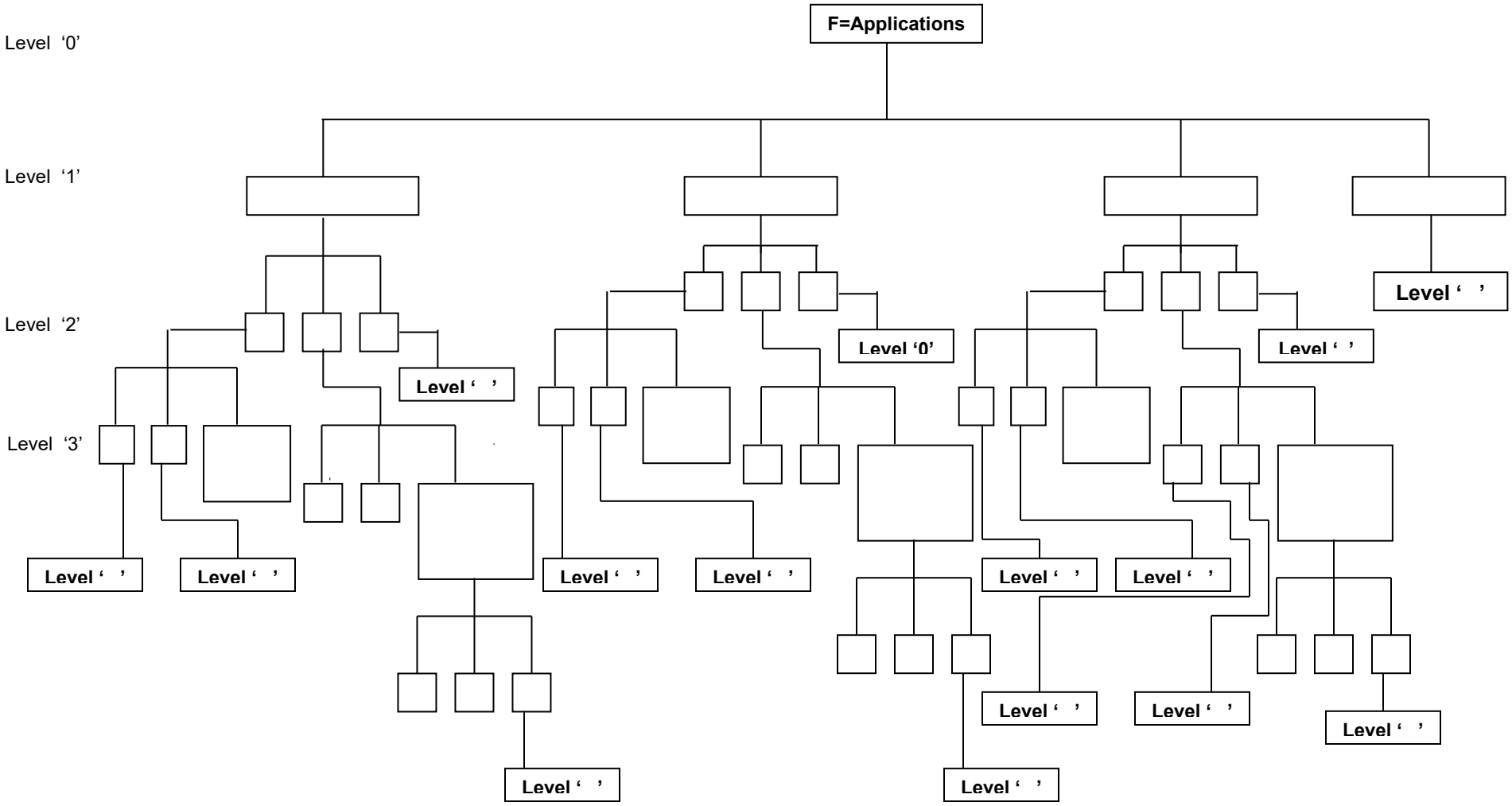
The sample applications are standalone applications which **DO NOT REQUIRE** connecting to a PC.

Commands are entered from the built-in keypad and respond is shown on the LCD display and LED's. External interface can be done from the I/O connector.

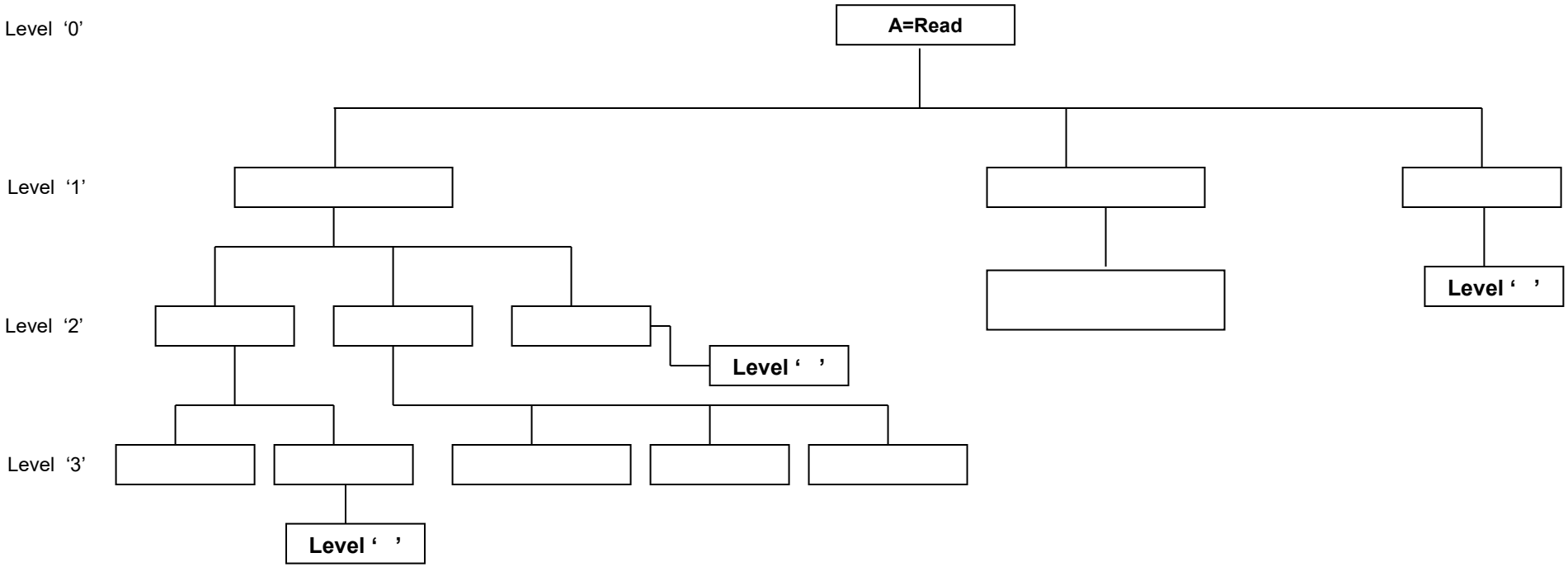
From the above case study, students are required to complete the firmware flow diagrams of the RFID system. The first diagram is given as an example.



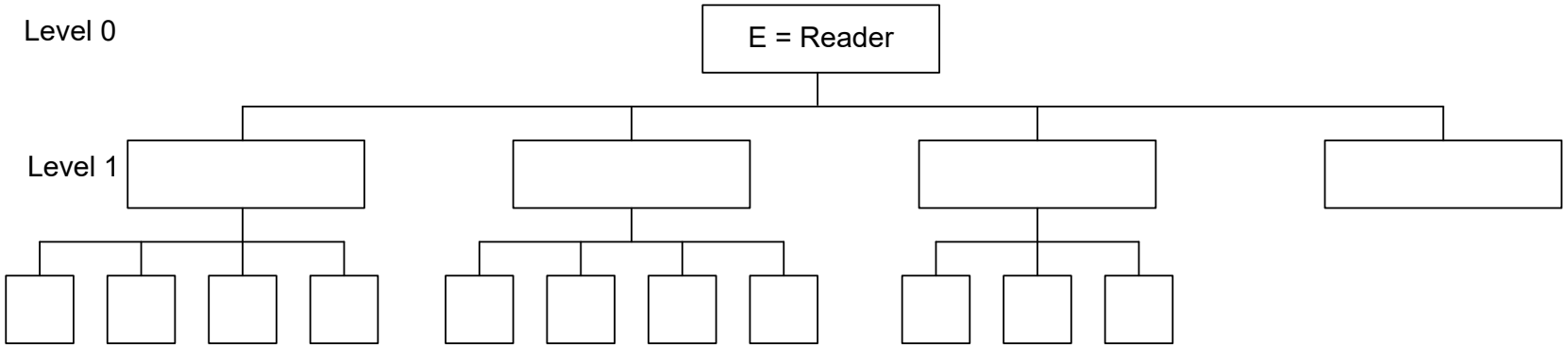
Firmware System Flow Diagram - 1



Firmware System Flow Diagram - 2



Firmware System Flow Diagram - 3



Firmware System Flow Diagram

Appendix
MiFare Card Data Structure used for Applications

No.	Description	Byte		Type	Byte No.	Block	Sector
	Personalization -						
1	Customer's Name	16		ASCII	0 ~ 15	1	0
2	Vendor Company's Name	9		ASCII	0 ~ 8	2	0
3	Card Initialized Date	3		Char	9 ~ 11	2	0
4	Card Initialized Time	3		Char	12 ~ 14	2	0
5	Issue Flag	1		Char	15	2	0
	Read/Write Operation during Issued Card and Personalization						
5	Card Type	1		ASCII	0	4	1
6	Card Serial No.	4		Long	1 ~ 4	4	1
7	Card Identification Number (Student/Lecturer/Staff ID)	10		ASCII	5~14	4	1
8	BCC for Block 4	1		Char	15	4	1
9	Current Credit	4		Long	0 ~ 3	5	1
10	Access Valid	1		Char	4	5	1
11	Start Date and Time	5		Char	5 ~ 9	5	1
12	End Date and Time	5		Char	10 ~ 14	5	1
13	BCC for Block 5	1		Char	15	5	1

Note : Issue Flag ➔ FF = New card, 55 = already issued
Card Type: A=Admin, L=Lecturer, S=Student, T=Technician
Access Valid ➔ door lock authorize flag; 00 = Unauthorize, AA = Authorize

	Byte	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Sec 0	Blk 0	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
	Blk 1	C16	C15	C14	C13	C12	C11	C10	C9	C8	C7	C6	C5	C4	C3	C2	C1
	Blk 2	T	R	A	N	S	I	C	O	M	DD	MM	YY	hh	mm	ss	IsF
	Blk 3																
Sec 1	Blk 4	T	S4	S3	S2	S1	ID	ID	ID	ID	ID	ID	ID	ID	ID	ID	BCC
	Blk 5	CC4	CC3	CC2	CC1	AV	DD	MM	YY	hh	mm	DD	MM	YY	hh	mm	BCC
	Blk 6	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
	Blk 7																

Appendix

MiFare Card Data Structure used for Applications

No.	Description	Byte	Type	Byte No.	Block	Sector
	Personalization -					
1	Customer's Name	16	ASCII	0 ~ 15	1	0
2	Vendor Company's Name	9	ASCII	0 ~ 8	2	0
3	Card Initialized Date	3	Char	9 ~ 11	2	0
4	Card Initialized Time	3	Char	12 ~ 14	2	0
5	Issue Flag	1	Char	15	2	0
	Read/Write Operation during Issued Card and Personalization					
5	Card Type	1	ASCII	0	4	1
6	Card Serial No.	4	Long	1 ~ 4	4	1
7	Card Identification Number (Student/Lecturer/Staff ID)	10	ASCII	5~14	4	1
8	BCC for Block 4	1	Char	15	4	1
9	Current Credit	4	Long	0 ~ 3	5	1
10	Access Valid	1	Char	4	5	1
11	Start Date and Time	5	Char	5 ~ 9	5	1
12	End Date and Time	5	Char	10 ~ 14	5	1
13	BCC for Block 5	1	Char	15	5	1

Note : Issue Flag □ FF = New card, 55 = already issued
Card Type: A=Admin, L=Lecturer, S=Student, T=Technician
Access Valid □ door lock authorize flag; 00 = Unauthorize,
AA = Authorize

LAB 3: Setting Up Wireless LAN IEEE 802.11g Client and Access Point

Objectives:

Students will learn how to

- setup wireless IEEE 802.11g client using external **GW-US54Mini2** USB dongle and the **Planex Wireless Utility** client software to connect SP wireless network
- connect and configure a wireless network with IEEE 802.11g client Adapters and Access Point for Homes/small Offices network
- setup infrastructure and ad-hoc WLAN

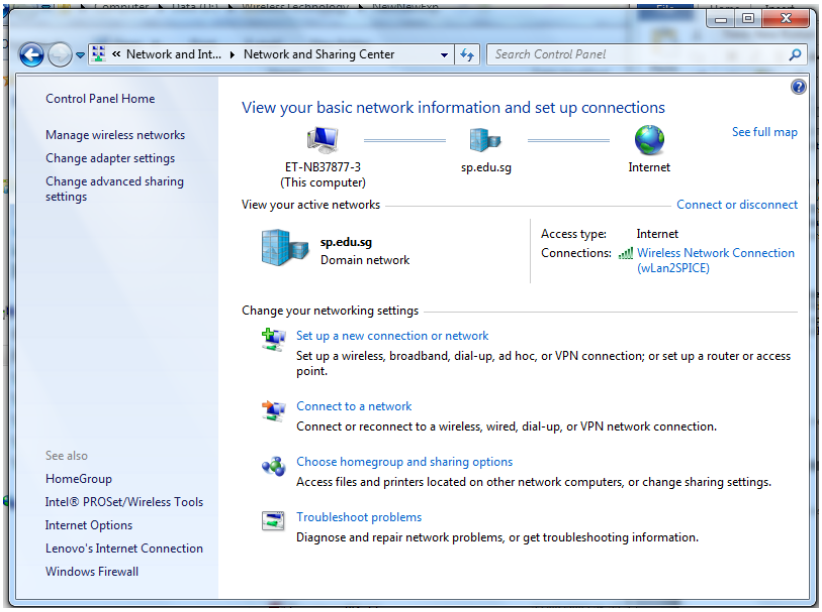
Introduction:

Today, IEEE 802.11 Wireless LAN is used widely to enable mobile users to access the Internet wirelessly. This provides convenience and flexibility to users.
In this experiment, we will learn how to setup the external Wireless LAN client adaptor on the laptop using Planex Wireless Utility client software.

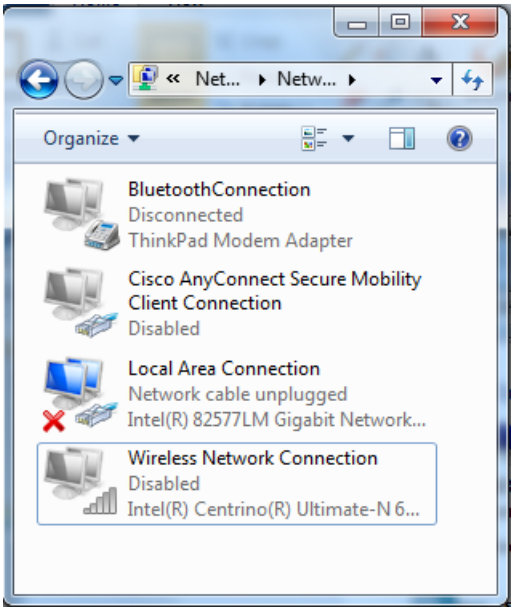
Procedure:

A. Setting up IEEE 802.11g Wireless LAN client using external IEEE 802.11g Wireless Mini-USB Adaptor and its software (Planex Wireless Utility)

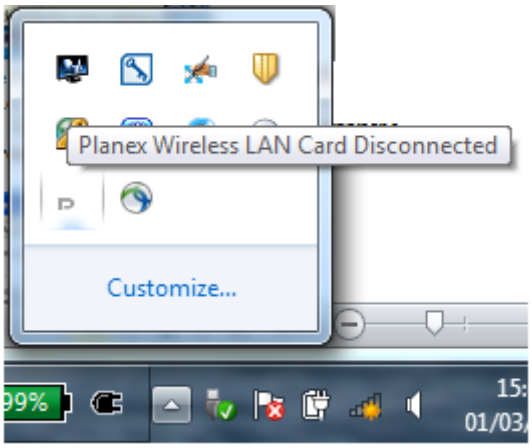
1. Go to Start > Control Panel and click on View network status and tasks at Network and Internet section to open the Network and Sharing Center.



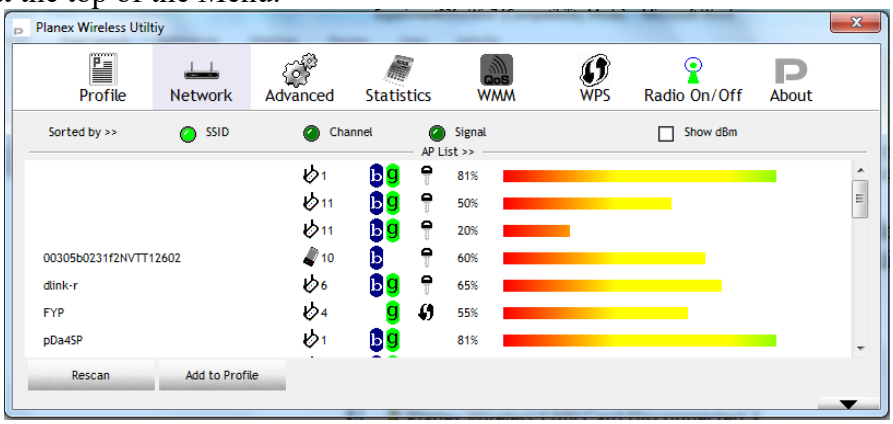
2. Click on the Change adapter settings to show the Network Connection. Right click on the Wireless Network Connection icon and select disable the internal wireless network adaptor as follow.



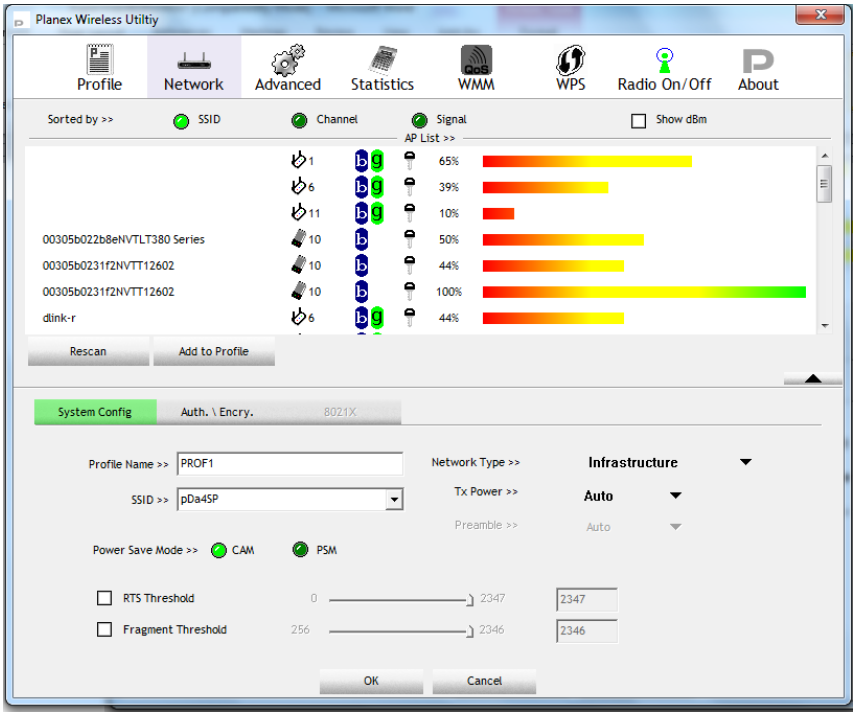
3. Plug in the Wireless LAN IEEE 802.11g Wireless Mini-USB Adaptor to one of the USB ports at the side of the laptop.
4. Since the Driver & Utility of the Wireless LAN IEEE 802.11g Wireless Mini-USB Adaptor **have been installed**, the utility program can be launched by clicking the icon at the bottom right hand corner of the system tray as shown in Figure.



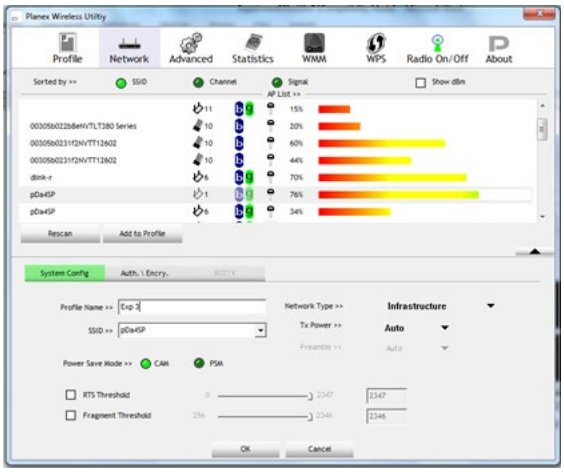
5. Double click in the Planex Wireless LAN icon to launch the utility window and click on Network at the top of the Menu.



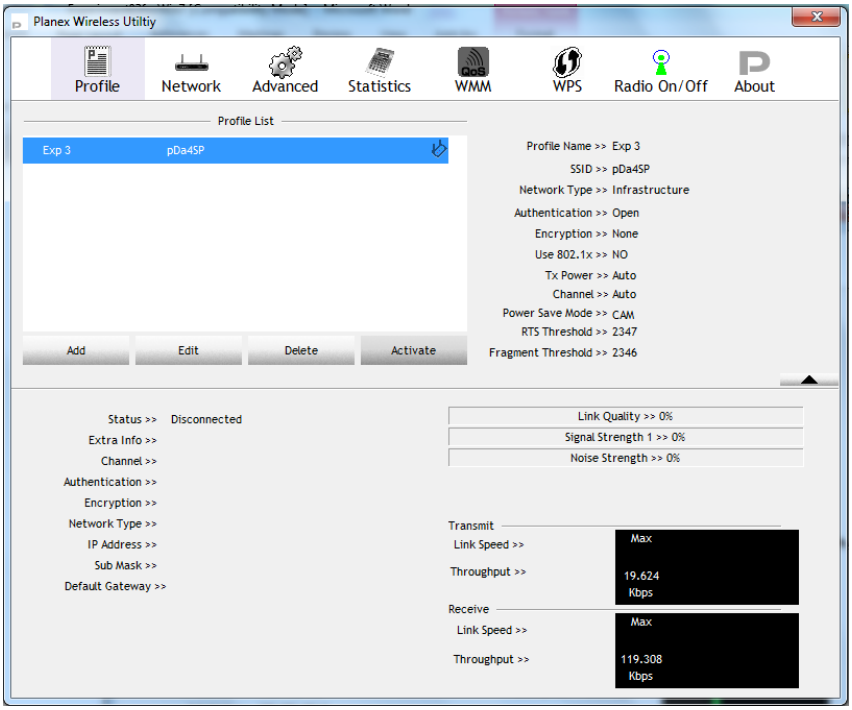
6. Set up a mobile hot spot using your smart phone. For example, SSID “pDa4SP” with your own password as shown in figure.
7. Select your SSID and click on the Add to Profile button to extend the Add Profile window as follow.



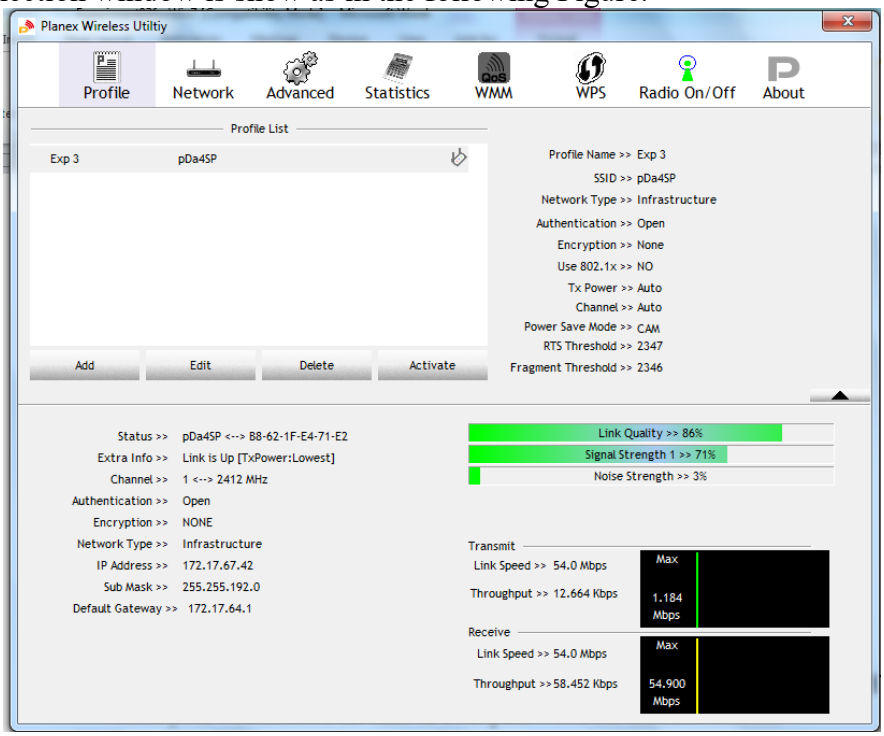
8. Then, define a new profile “Exp 3”, choose Network Type “Infrastructure”, Authentication “TKIP”, Encryption “your own password” and Tx Power “Auto” as shown in Figure below and click OK button.



9. Select the Exp 3 at Profile window and click on the Activate button.



10. The connection window is show as in the following Figure.



11. Once connected, launch Internet Explorer browser to access the Internet.
12. Enter any URL name to access the internet.

B. Setting up IEEE 802.11g Wireless LAN access point without security

1. Power up the Netgear wireless access point and press and hold the reset button at back of the router for 30 seconds to make default setting.
2. Connect the Ethernet straight UTP-5 cable from your laptop RJ-45 port to one of the four ports on your NetGear access point. (You also need to connect another straight UTP-5 cable from the Ethernet RJ-45 port on your access point to either your cable modem or ADSL modem. **This step is skipped in this experiment**.)
3. Go to start and run CMD program. Then, type "ipconfig/all to check the IP address of router to make sure that "192.168.0.1" (sliver color) or " 192.168.1.1" (white color) to check resetting of the router whether it is successful.
4. To configure your Local Area Connection **at the laptop** to a dynamic IP address. Click on Start, type Control Panel to be opened and click on View network status and tasks at Network and Internet section or click on the wireless icon at bottom right hand corner at Window System tray or right click, to open the **Network and Sharing Center**. Click on the Change adaptor settings. Right-click on the Local Area or Ethernet Connection and select Properties. Select Internet Protocol Version 4 (TCP/IPv4) and click on Properties button. Select "Obtain an IP Address automatically".
5. Then, at the CMD program type "ping 192.168.0.1" (sliver color) or "ping 192.168.1.1" (white color) to check the connection to the router whether it is OK.
6. Launch the Internet Browser to the following URL: http://192.168.0.1/start.htm for sliver color and http://192.168.1.1/start.htm for white color router.
7. If prompted for login, use username: **admin** and password: **password.**
8. Click on the *Setup Wizard*. Choose "No. I want to configure the router myself". Click "Next" button as shown in Figure 3 below.

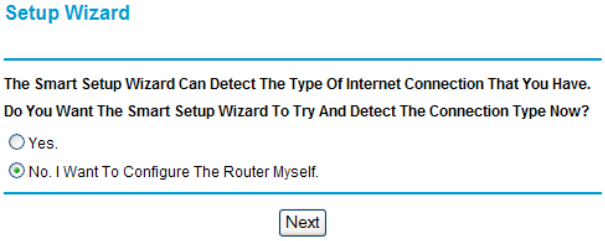
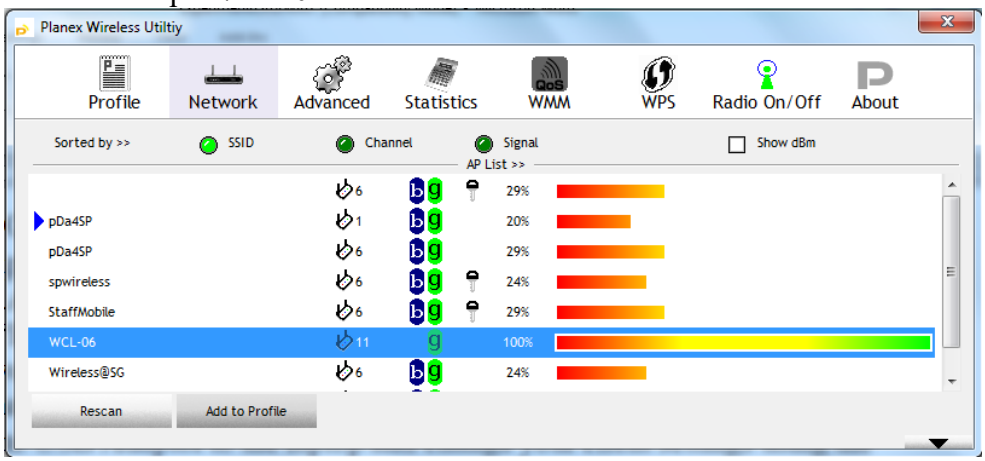


Figure 3

9. Click on the *Wireless Settings* and configure the following parameters:
   - Name (SSID): WCL-XX where XX follows the number on the access point.
   - Country: United States
   - Channel: Select any channel no. from 1 to 13 except channel 1, 6 or 11
   - Mode: g only
   - Security Options: Disable
   - Click "Apply" button.
10. Click on the *Advanced Wireless Settings*. Ensure that both "Enable Wireless Router Radio" and "Enable SSID Broadcast" are checked. Click "Apply" button.
11. Click on the *Advanced LAN IP Setup*. Change the IP Address of the router to 192.168.1XX.1, Starting IP Address to 192.168.1XX.2 and Ending IP Address to 192.168.1XX.100 where XX follows the number on the access point. Click "Apply" button.
12. Disconnect the Ethernet straight UTP-5 cable.

13. Make sure that the built-in wireless LAN adaptor must be remained disable and plug-in Wireless Mini-USB Adaptor to the laptop and change your client settings using the **Planex Wireless Utility** client software.
14. Connect your Wireless Mini-USB Adaptor client to **the new access point (WCL-XX)**. Follow the same steps "7 to 10" as in the section A.



15. Once connected, launch Internet Explorer browser to access http://192.168.1XX.1/start.htm where XX follows the IP of the access point.

D. Setup an ad-hoc WLAN

Ad-hoc WLAN uses only Adaptors to communicate with each other: there is no Access Point. There are four parts to this experiment:

(i) Power off all the Access Points/routers
(ii) Work out with other group to identify a network address
(iii) Change the configuration of the Adapter
(iv) Test out the wireless network.

1. Power off all the Access Points
2. For the ad-hoc network:
   Network IP address: _____
   SSID: _____
   Channel: _____
3. Configure the adaptor
   Change the Adaptor SSID to _____ and Channel to _____.
4. Testing the ad-hoc WLAN
   Test out the connections among the clients in the ad-hoc network.
   Can the client get connected to other ad-hoc network? Why?

   _____

E. Questions

1. Name the devices required to set up a Home/small Office network.

_____

2. Draw a sketch of the NetGear AP and indicating the type of connections available.

3. Draw a diagram to show how these devices are used to setup an infra-structure WLAN.

4. Draw a diagram to show an ad-hoc WLAN.

i. Conclusion

To setup a WLAN, the _____ is usually connected to a wired network.
On the client PC or notebook, a _____ is installed.
In order for a client to join a WLAN, its _____ and _____ must be set accordingly.

LAB 4: Setting Up Wireless LAN IEEE 802.11g Access Point using WEP, WAP key in Network Security and Configuring Filters

Objectives:

Students will learn how to

- setup IEEE 802.11g access point with various security settings such as WEP, WPA-PSK, and MAC filtering
- install firewall filtering for restricted access.

Introduction:

We have learnt how to setup the Wireless LAN client on the laptop using both Windows 7 and Planex Wireless Utility client software in Experiment 3. While, IEEE 802.11 Wireless LAN provides convenience and flexibility to users, on the other hand, it may allow hackers to access the network and eavesdrop on the data transmitted on the network.

In this experiment, we will configure the access point for various security configurations.

Procedure:

A. Setting up IEEE 802.11g Wireless LAN access point with WEP security

1. Power up the Netgear wireless access point and press and hold the reset button at back of the router for 30 seconds to make default setting.
2. Connect the Ethernet **straight** UTP-5 cable from your laptop RJ-45 port to **one of the four ports** on your NetGear access point. (You also need to connect another **straight** UTP-5 cable from the Ethernet RJ-45 port on your access point to either your cable modem or ADSL modem. **This step is skipped in this experiment**.)
3. Configure your Local Area Connection to a dynamic IP address. Click on Start → Control Panel and click on View network status and tasks at Network and Internet section to open the Network and Sharing Center. Click on the Change adaptor settings. Select Local Area Network Connection and right-click on the Local Area Connection and select Properties. Select Internet Protocol Version 4 (TCP/IPv4) and click on Properties button. Select "Obtain an IP Address automatically" .
4. Go to start and run CMD program. Then, type "ping 192.168.0.1" (sliver color) or "ping 192.168.1.1" (white color) to check the connection to the router whether it is OK
5. Launch the Internet Browser to the following URL: http://192.168.0.1/start.htm (for sliver color NetGear access point), http://192.168.1.1/start.htm (for white color NetGear access point).
6. If prompted for login, use username: **admin** and password: **password**.
7. Click on the *Setup Wizard*. Choose "No. I want to configure the router myself". Click "Next" button as shown in Figure 1 below.

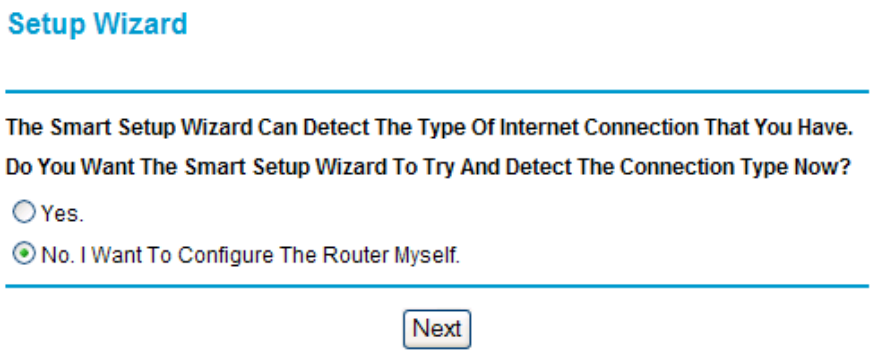


Figure 1

8. Click on the *Basic Settings* and then click "Apply" button to initialize the assess point.
9. Click on the *Wireless Settings* and configure the following parameters:
   - Name (SSID): WCL-XX where XX follows the number on the access point.
   - Country: United States
   - Channel: Select any channel no. from 1 to 13 except channel 1, 6 or 11
   - Mode: g only
   - Security Options: Disable
   - Click "Apply" button.
10. Click on the *Advanced Wireless Settings*. Ensure that both "Enable Wireless Router Radio" and "Enable SSID Broadcast" are checked. Click "Apply" button.
11. Click on the *Advanced LAN IP Setup*. Change the IP Address of the router to 192.168.1XX.1, Starting IP Address to 192.168.1XX.2 and Ending IP Address to 192.168.1XX.100 where XX follows the number on the access point. Click "Apply" button.
12. Change the Security Options to WEP (Wired Equivalent Privacy) in the *Wireless Settings*.
13. There are two ways to enter the WEP key. You can choose to use a 64-bit or 128-bit encryption key or to enter a passphrase.
14. In this lab, we choose "64-bit" encryption key and passphrase "wireless". Click "Generate" button and copy the generated 10 digit Hex key. Then, click "Apply" button.
15. **Disconnect** the Ethernet straight UTP-5 cable
16. **Disable** the built-in wireless LAN adaptor and **plug-in** Wireless Mini-USB Adaptor to the laptop and change your client settings using the **Planex Wireless Utility** client software.
17. **Connect** your Wireless Mini-USB Adaptor client to the new access point (WCL-XX).
18. Once connected, launch Internet Explorer browser to access http://192.168.1XX.1/start.htm where XX follows the IP of the access point.

B. Setting up IEEE 802.11g Wireless LAN access point with WPA-PSK security

1. On the access point, change the Security Options to WPA-PSK (Wi-Fi Protected Access Pre-Shared Key) in the *Wireless Settings*.
2. Enter the passphrase and the key lifetime. (Note: This was applicable only for white color model.)
3. In this lab, we choose "wirelesslan" and the key lifetime to be "60" minutes (Only for White color Router). Click "Apply" button.
4. Change your client settings using the **Planex Wireless Utility** client software.
5. Connect your Wireless Mini-USB Adaptor client to the new access point (WCL-XX).
6. Once connected, launch Internet Explorer browser to access http://192.168.1XX.1/start.htm.

a. Setting up IEEE 802.11g Wireless LAN access point with MAC address filtering

1. MAC address filtering can be applied together with any of the above security settings.
2. On the access point, click on the *Advanced Wireless Settings*. Click on "Setup Access List" button.
3. Click on the "Add" button in Figure 2. Check the MAC address of the Wireless Mini-USB Adaptor and click "OK" button.
4. Check the checkbox "Turn Access Control On" and click "Apply" button, as shown in Figure 2 below.

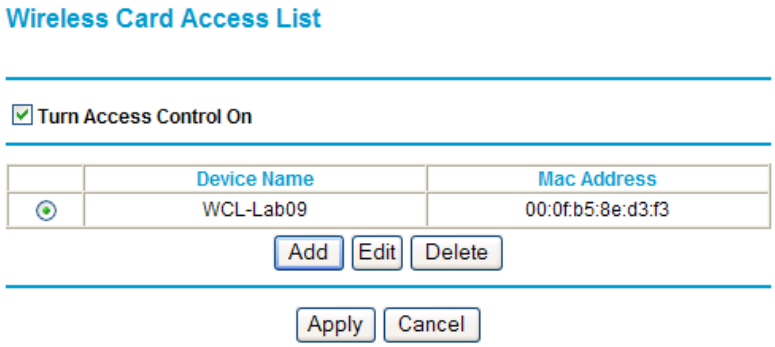


Figure 2

5. This will prevent wireless devices other than the list of MAC addresses shown from accessing the access point.
6. Launch Internet Explorer browser to access http://192.168.1XX.1/start.htm.
7. Change the MAC address to something other than your Wireless PC card.
8. Launch Internet Explorer browser to access http://192.168.1XX.1/start.htm. You should not be able to access this webpage now.

D. Setting up firewall rules

1. WEP, WPA-PSK and MAC filtering security features mentioned above are security features to establish physical connection between access point and clients.
2. Firewall rules for restricted or no access to certain websites for the clients. In NetGear access point, this firewall feature is known as *Block Sites*.
3. In Figure 3, enter the keywords for websites that you would like to block, either permanently (always) or per schedule, as determined in *Schedule*. For example, to block users from accessing http://www.google.com, enter the keyword google.

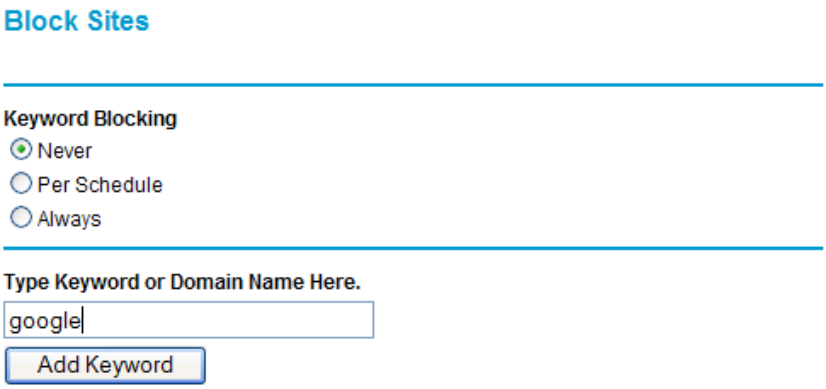


Figure 3

4. Firewall rules can also be applied to restrict certain services or ports on the clients. In NetGear access point, this firewall feature is known as *Block Services*.
5. In Figure 4, click on "Add" button. Enter the starting port number and the ending port number. For example, to prevent users from accessing https service, enter starting port 443 and ending port 443.

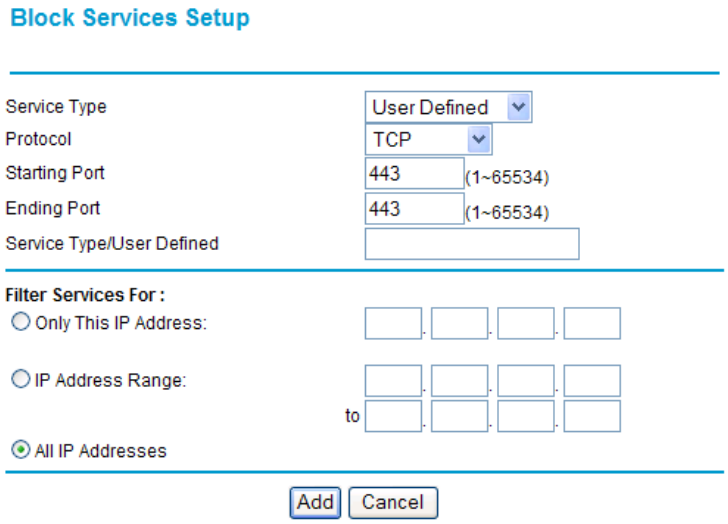


Figure 4

6. You are required to connect the access point to an Internet outlet in order to test out these two firewall rules.

E. Questions

1. What are the non-overlapping frequency channels in Singapore for IEEE 802.11g?

   _____

2. Which security method do you used to enforce the strictest security for the access point?

   _____

3. What is the difference between these two network types: access point (infrastructure) and computer-to-computer (ad-hoc)?

   _____

4. Click on the **Add Profile** button in the **Planex Wireless Utility** client software and select the **System Config** tab.

   a. What is the use of the RTS/CTS Threshold setting?

   _____

   b. What is the use of the Fragmentation Threshold setting?

   _____

i. Conclusion

_____, _____ and _____ filtering are used to enhance the security on the physical connection and _____ rules are used to restrict access based on keywords or port numbers.

LAB 5: Case study on Basics of ZigBee, ZigBee Wireless Personal Network System and Applications

Objectives:

Students will learn how to

- Identify different logical ZigBee devices, frequency channels, PAN ID, MAC addresses, ZigBee short address, etc… by using ZigBee software in Windows 7 laptops.
- setup a point-to-multipoint ZigBee cluster three network using ZigBee training kit on ZigBee software in Windows 7 laptops.
- monitor temperature, humidity and light by using sensor application.
- control LED lights by using switch & light application.
- perform a chat using the Serial Communication application.

Introduction

ZigBee, a specification for communication in a wireless personal area network (WPAN), has been called the Internet of Things (IoT). ZigBee targets the application domain of low power, low duty cycle and low data rate requirement devices.

ZigBee applications include:

- Home and office automation
- Industrial automation
- Medical monitoring
- Low-power sensors
- HVAC control
- Plus many other control and monitoring uses

This experiment provides an introduction to the various components of a ZigBee network. The ZigBee Training Kit consists of hardware and software that allows quick testing of the ZigBee Networking and offers a complete platform for development of ZigBee applications.

The ZigBee Training Kit includes the following components:

- 1 x ZigBee Coordinator Board
- 2 x ZigBee Router Board
- 2 x ZigBee End Device Board
- 2 x External Sensor Board
- 1 x USB Dongle for monitoring the packets transmission over the wireless channel

Figure 6.1 shows a block diagram of a ZigBee network with five nodes.

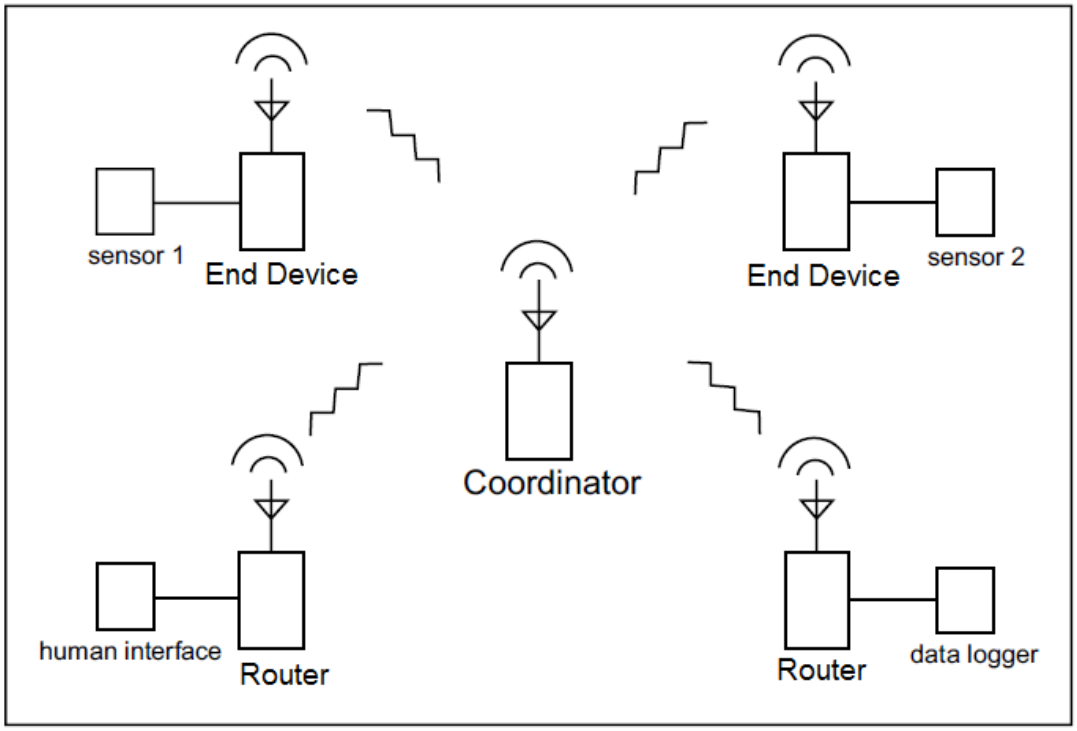


Figure 6.1 ZigBee Network

Components of ZigBee

In ZigBee technology, there are two basic hardware devices called full-function device (FFD) and a reduced-function device (RFD). Three logical devices (coordinator, router and end device) are required to setup a ZigBee network. A network shall include at least one FFD, operating as the PAN coordinator. PAN Coordinator owns the network and starts the network. It allows other devices to join the network and also provides binding and address-table services and saves messages until they can be delivered. It could also have input/output capability but mains powered. Routers are FFDs. They route messages but does not own or start network. It also scans to find a network to join and give a block of addresses to assign and usually mains powered depending on topology. End Device is an RFD. It communicates with a single device and does not own or start network but able to scans to find a network to join. It usually battery powered. An RFD is intended for applications that are extremely simple and do not need to send large amounts of data. An FFD can talk to RFDs or FFDs while an RFD can only talk to an FFD.

Wireless Network Topologies

IEEE 802.15.4 supports star and peer-to-peer topologies. The ZigBee specification supports star and two kinds of peer-to-peer topologies, mesh and cluster tree.
ZigBee-compliant devices are sometimes specified as supporting point-to-point and point-to-multipoint topologies. Figure 6.2 shows the Physical Network Topologies supported by ZigBee.

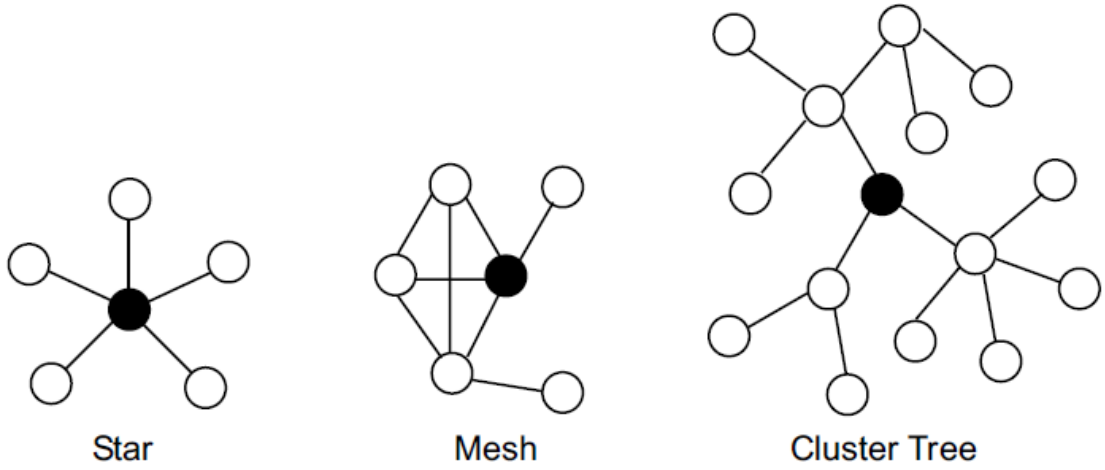


Figure 6.2 Physical Network Topologies supported by ZigBee

IEEE 802.15.4 ZigBee Standard

The following tables describe the summarized specifications of ZigBee standard.

ZigBee info and Parameters			
IEEE802.15.4	Physical/MAC layers		
ZigBee Alliance	upper layer stack and application profiles, compliance and certification testing, branding		
Range	Indoors: up to 30 m Outdoors (line of sight): up to 100 m		
ZigBee Hardware Device	Full Function Device (FFD)	Reduced Function Device (RFD)	
ZigBee Logical Device	Coordinator	Router	End Device
Physical layer protocol	DSSS (direct-sequence spread spectrum)		
Channel access mechanism:	Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)		
Maximum number of nodes per network	64K		

Table 6.1

	ZigBee Wireless Parameter		
Frequency band	868.3 MHz	915 MHz	2.4 GHz
Frequency Range	868 – 868.6 MHz	912 – 928 MHz	2.405 – 2.480 GHz
Raw data rate	20 Kbps	40 Kbps	250 Kbps
Modulation Technique	BPSK	BPSK	O-QPSK
Number of channels	1 (Channel 0)	10 (Channel 1 to 11)	16 (Channel 12 to 27)
Bandwidth required	600 kHz	2 MHz	5 MHz

Table 6.2

Advantages of ZigBee

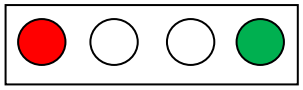
The advantages of using ZigBee are as follow.

- Easy deployment, self-forming
- Reliable and self-healing
- Supports large number of nodes up to 64K
- Easy to deploy
- Very long battery life
- Secure, Network and link keys can restrict access using 128bit Advanced encryption Standard (AES) security
- Low cost
- Can be used globally

Procedure:

Setting up hardware

1. Assume USB driver already installed and all serial switches are closed on the board. Plug USB Type A to B Cable to ZigBee Coordinator Board and laptop. LED4 (Green) is ON which means power is ON the board and then LED1 (Red) is ON that means it can establish ZigBee Network successfully.

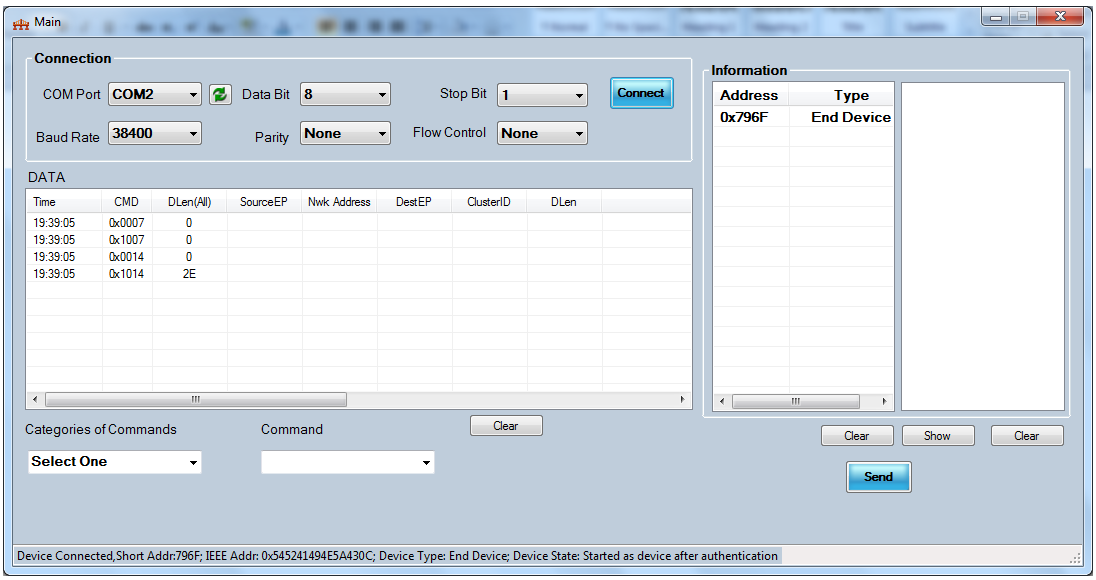


2. Do the same procedure 1 for two ZigBee Router Boards and two ZigBee End Device Boards. Here LED1 (Red) on these boards means they can join ZigBee Network successfully.
3. Plug phoenix connectors between External Sensor Board and ZigBee End Device Board. Make sure that pins ADIN0, ADIN1 and ADIN6 and 3V3 OUT, 5V OUT and GND from ZigBee End Device Board are connected with ADIN0, ADIN1 and ADIN6 and 3V3 IN, 5V IN and GND from External Sensor Board.
4. Do the same procedure 3 for ZigBee Router Board.

Setting up ZigBee training kit software

Since the ZigBee training kit software is designed to fully control from PC, the user is not needed to touch anything on the board.

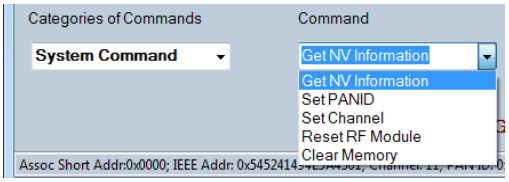
1. Launch the ZigBee training kit Main Interface window by double clicking on the icon at the desktop or to Start ➔ Program ➔ Select ➔ ZigBee Training Kit.



ZigBee Training Kit Main window

2. Select serial com from COM Port Drop down list. If associated COM port can't be seen, green-arrow button can be used for refresh. Use default data. (Data bit = 8, Stop bit = 1, Baud Rate = 38400, Parity = None, Flow = Control None) Click "Connect" 

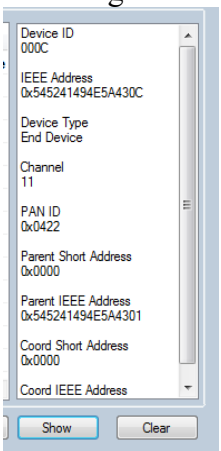
button. The information can be seen at the List view of right side and some information can also be seen at the status bar of window.
3. Get Device Information by selecting the System Command under the categories of Commands as follow.



4. Under the categories of Commands, select "System Command" and then under Command from right drop down list, select "Get NV Information" and then click 

button and then click 

button on the right side of window.

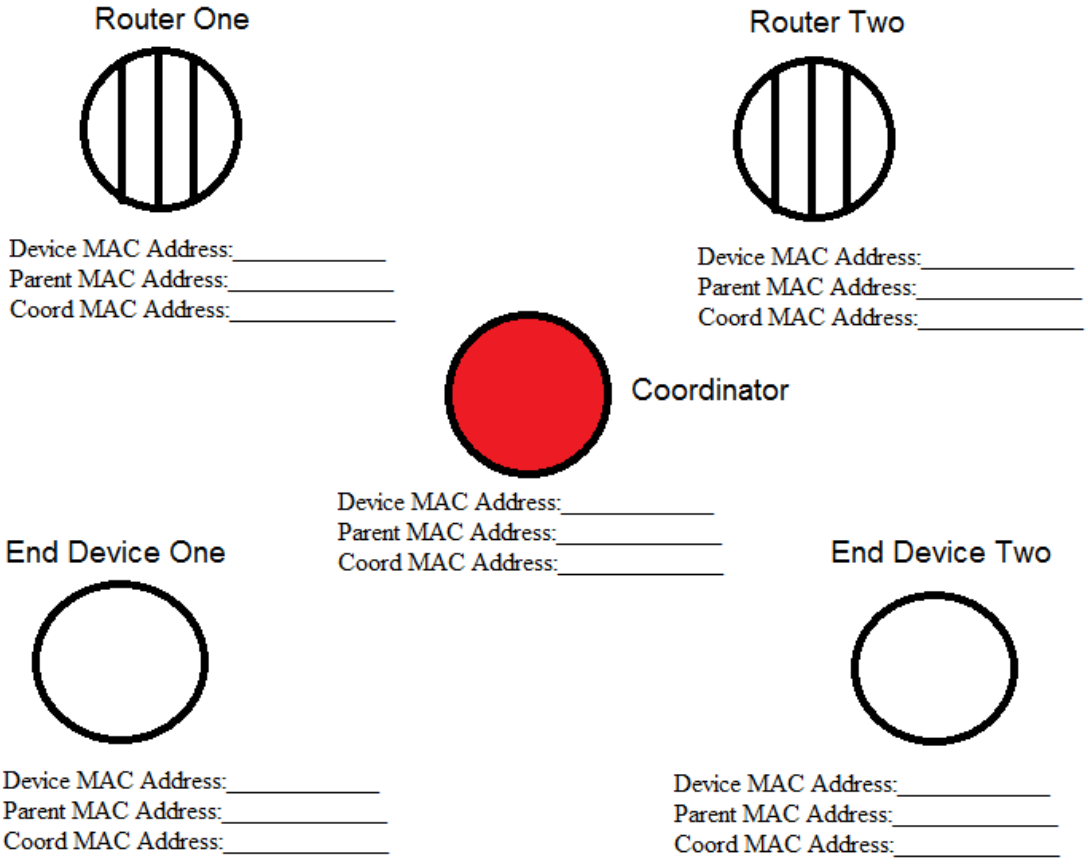


5. Record down the detail information in the following table to identify your device.

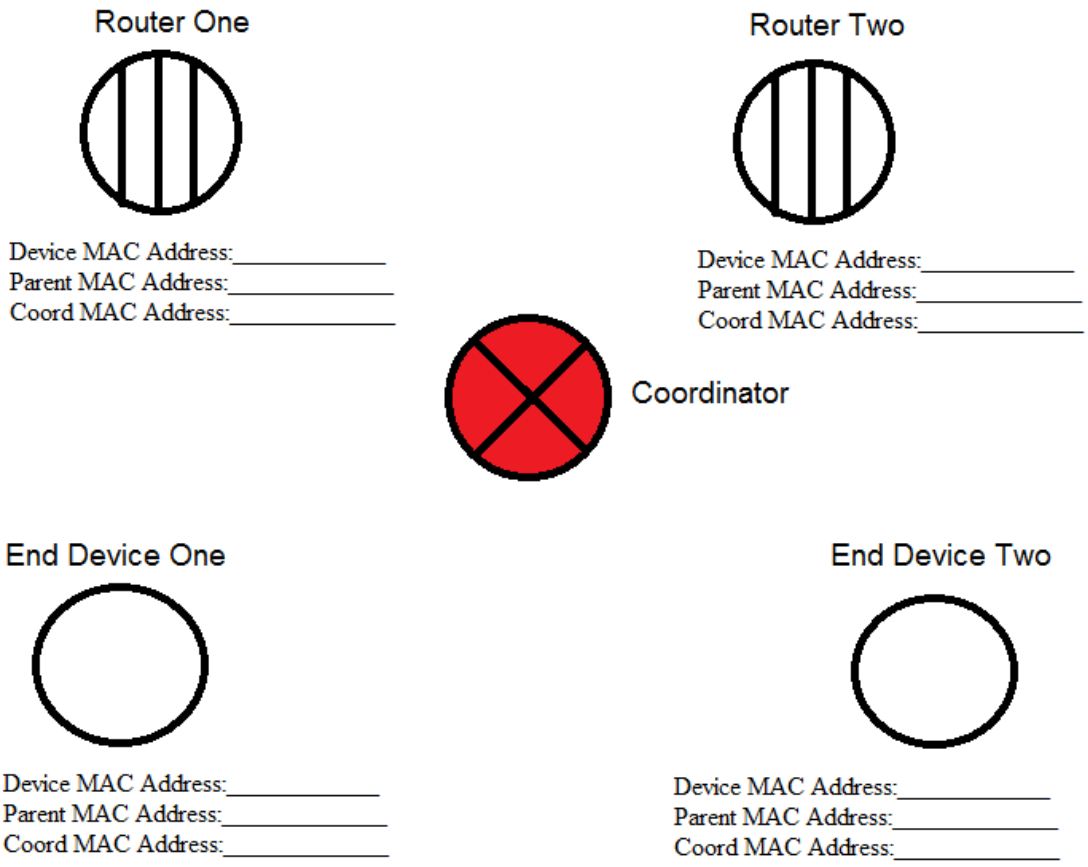
Device ID	

Device IEEE MAC Address	
Device Type	
Channel No.	
PAN ID	
Parent Short Address	
Parent IEEE MAC Address	
Coord Short Address	
Coord IEEE MAC Address	

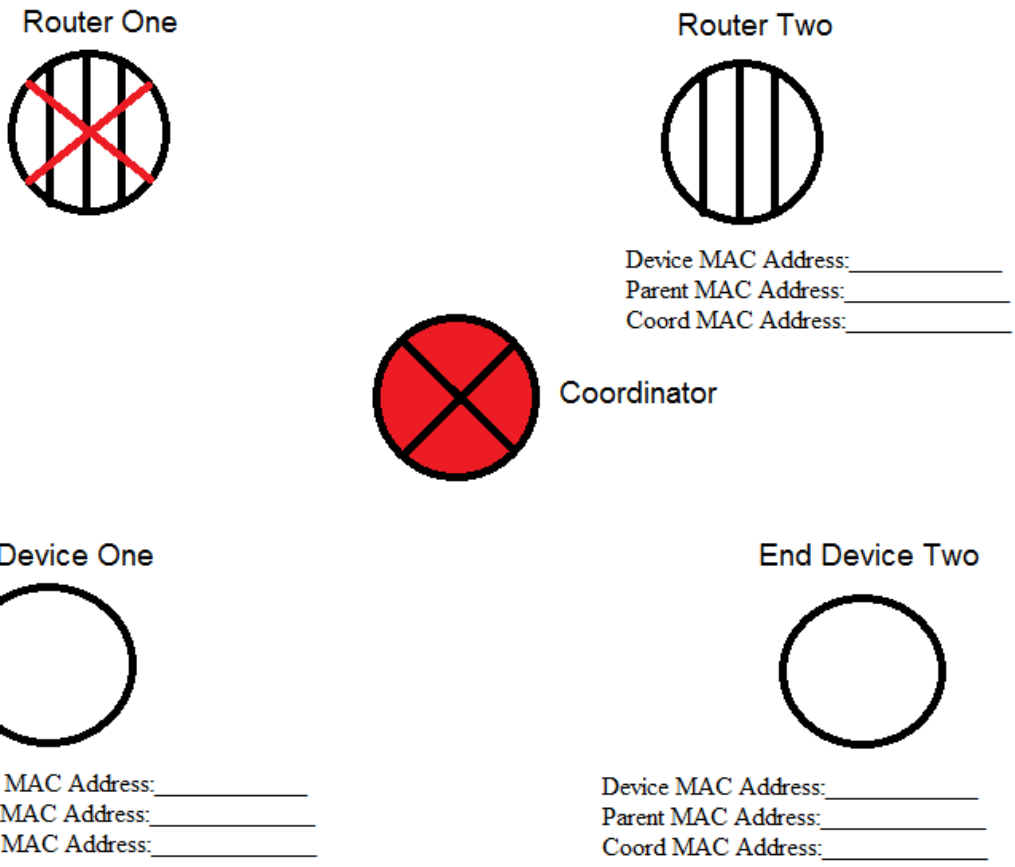
6. Check with your group members for detail of their device information and complete the diagram with their connection.



7. Close the program at Coordinator laptop and unplug the USB cable to turn off the device.
8. Check with your group members for detail of their device information and complete the diagram with their connection.



9. Close the program at Router One and unplug the USB cable to turn off the device.
10. Check with your group members for detail of their device information and complete the diagram with their connection.



11. Close the program at Router Two and unplug the USB cable to turn off the device. Check the status of the two end devices by seeing the LED indicator.
12. Which LED of the end device is blinking? Why?

_____

_____

ZigBee Applications

There are 3 types of application in the ZigBee Training Kit.

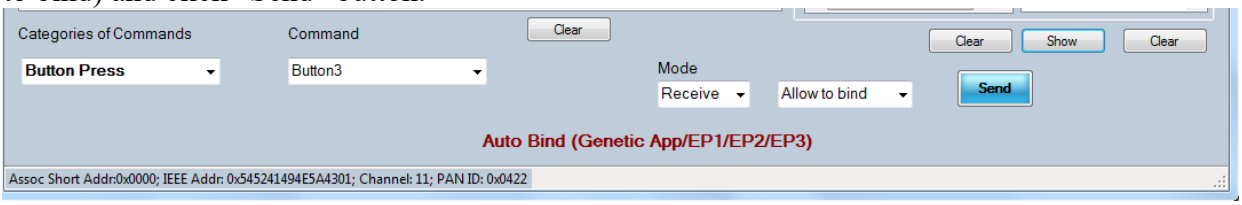
1) Sensor Application
2) Light and Switch Application
3) Serial Application

Sensor Application

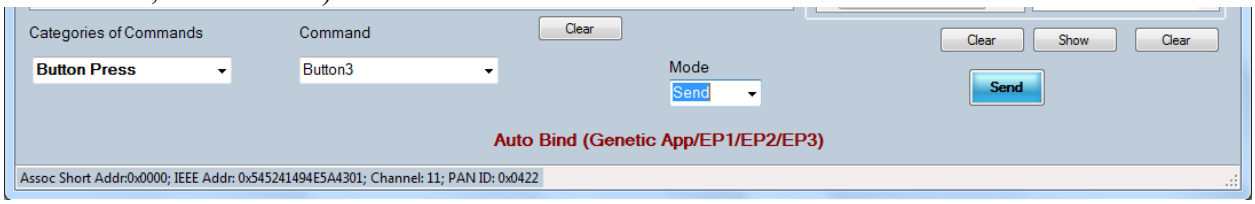
This experiment needs a team work from all the group members. Firstly, the very important step is that identifies and decides who the sender is and who the receiver is. Here, "Sender" becomes sending sensor data and "Receiver" becomes receiving data.

1. Connect back all the devices to laptop through USB cable and launch the ZigBee program. Select the correct serial comm port to be selected and make sure the successful connection by clicking "Connect"  button.

2. Auto binding process is to be used to bind devices to transfer data among each other. The device sends broadcasts the message on the network with: Address, Profile ID, Cluster Lists and compatible device responds and sender application stores binding record in binding table. If you want to be a receiver to collect senor data, select according to the following figure (Command: Button Press ➔ Button3, Mode: Receive ➔ Allow to bind) and click "Send" button.



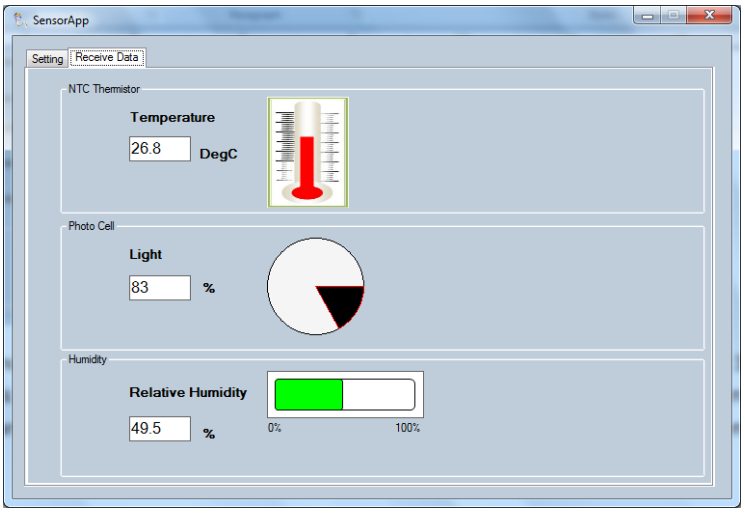
3. From the "sender" side, select according to following figure (Command: Button Press ➔ Button3, Mode: Send) and click "Send" button.



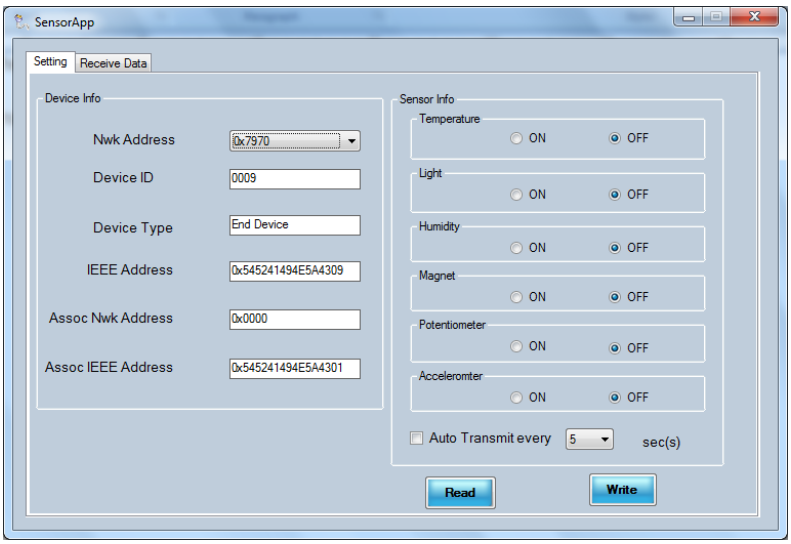
4. The group members must assign two devices: "Sender" and "Receiver" and can choose any two prototype boards: two ZigBee End Device Boards or two ZigBee Router Boards or a ZigBee Router Board and a ZigBee End Device Board.
5. How do you check the successful binding?

_____

6. At the receiver side, click on the Receiver Data tap to display the data of Temperature, Light and Humidity.



7. At the sender side, click on the Setting tap and select on the Device info at Nwk Address from the drop down list to display "Device ID, Device type, IEEE Address, Assoc Network Address, etc..". Then, select Temperature "ON", Light "ON", Humidity "ON" and check the Auto Transmit every "XX" sec. at Sensor info window. Click on the write button to activate the sensors and enable the sending data to the receiver.

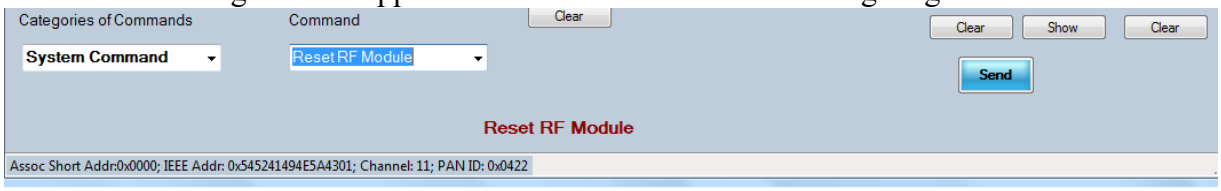


8. How do you know data are sending from the sender?

_____

Light and Switch Application

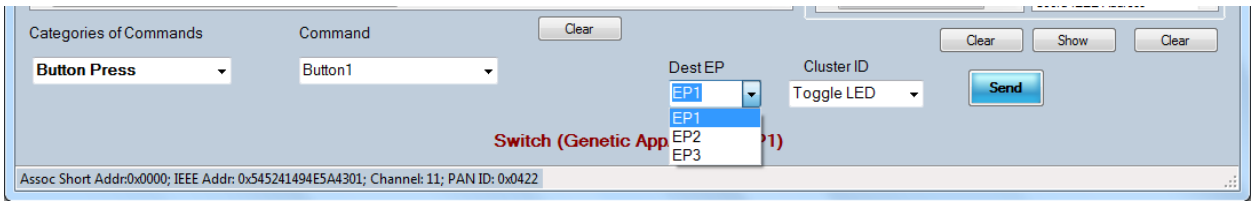
1. Select "Reset RF Module" Command and click "Send" button to reset all the devices before starting the new application as in shown in the following diagram.



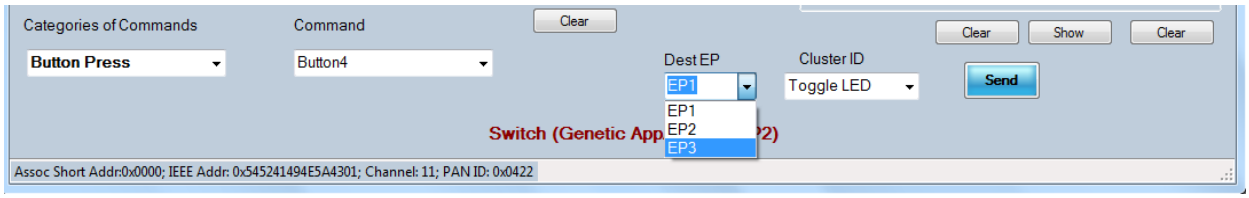
2. Select the correct serial comm port to be selected and make sure the successful connection by clicking "Connect"  button.

3. The experiment again involves a collaboration work among team members. Firstly, sender and receiver are to be decided. Take note that, we already defined "Sender" as Switch and "Receiver" as Light in this application at the prototype boards.
4. If you want to be a receiver to collect senor data, select according to the following figure (Command: Button Press ➔ Button3, Mode: Receive ➔ Allow to bind) and click "Send" button as in Sensor Application.
5. From the "sender" side, select according to following figure (Command: Button Press ➔ Button3, Mode: Send) and click "Send" button to complete the binding process.
6. By using the Button press command and different End point application to turn on and turn off LED at the receiving device as follow.

Button1" means "Switch1 (Endpoint1)" and "Destination EP1" means "LED1". Cluster ID is command for LED status.



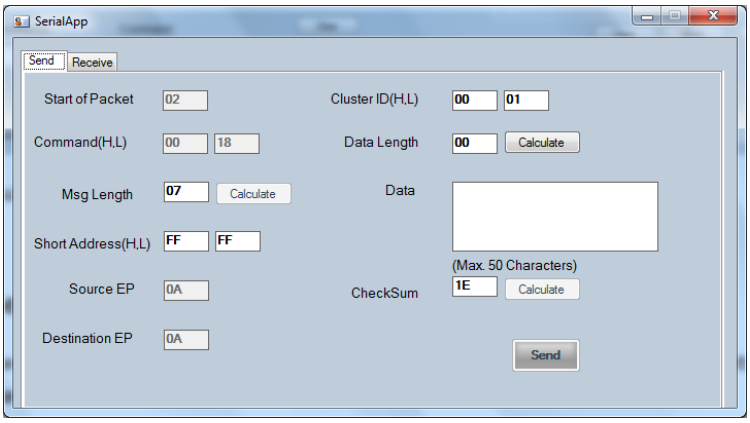
This button4 application is the same as previous one. Only the difference is button4 (Endpoint2) can control all destination Endpoints.



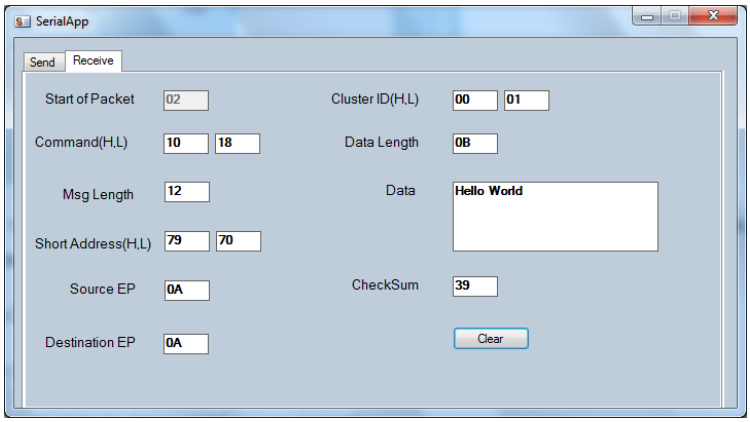
For the button5 application, source EP3 can control all LEDs.

Serial Application

1. Assume we had already done connection and select “Serial Application” from the categories of Commands.
2. There are 2 tabs inside the Serial application: “Send” and “Receive”. For sending data at the “Sender” side.
    - type Data first
    - click calculate button of Data Length
    - click calculate button of Message Length
    - click calculate button of Check Sum
    - click send button



3. For receiving data at the “Receiver” side, the user can see data packet as in the following figure.



4. The above procedure is used the broadcast mode, the user can try by using unicast mode with changing short address. This application can send message vice visa.

Lab 6: Spectrum Analyser and Its Signal Measurements

I Objectives

Students will learn how to:

- Operate the R&S FSV3 Spectrum Analyser to display the frequency spectrum of signals.
- Measure an RF Signal using a spectrum analyser to display at the correct position to provide an accurate reading.
- Describe the RF units as such in dBm, dBμV, dBc, etc.. to measure an RF signal.

II Equipment

R&S FSV3 spectrum analyser

R&S SMB100A RF signal generator

III Introduction

1. The spectrum analyser is used to analyse the characteristics of an RF input signal. It enables direct observation of amplitude, frequency, distortion products, modulation sidebands and frequency conversions. Thus, using a spectrum analyser, frequency and amplitude of an input signal can be viewed in linear and log scales respectively. In comparison to a linear scale, the advantageous increase in the measurement range of a log scale can thus be realised. Additionally, noise being a deterrent to the signal transmission in any communication system, can be measured by a spectrum analyser.

2. However, in this experiment, only the frequency and amplitude of an input signal will be measured.

IV Frequency and amplitude measurement

1. Initial setup

Connect the R&S SMB100A RF signal generator and R&S FSV3 spectrum analyser as shown in Figure 1.

Figure 1: Test setup

Setting up an RF carrier signal from the RF Generator

(i) Set the RF signal generator to generate the following sinusoidal carrier signal:
Frequency: 128 MHz
Output: -30 dBm
Modulation: off
RF output: on

(ii) Set the frequency to 128 MHz by selecting the FREQ hard key and input using the number keys. Select the unit via 

hard key. If you make a mistake while entering a value, select 

to correct it. You may also change the frequency by turning the knob.

(iii) Select LEVEL hard key to set the amplitude to -30 dBm. Select 

to apply the value. You may also change the amplitude by turning knob.

(iv) Select 

to turn **off** the modulation source since **a pure sine wave** is to be generated.

(v) Select 

to turn **on** the RF output.

2. Procedure

(i) To capture and display the spectrum of the RF carrier signal at the spectrum analyzer, set the center frequency of the analyzer by pressing the following keys: **<FREQ>**, 128 **<MHz>**.

(ii) Set the span by pressing the following keys: <**SPAN**>, 2 **<MHz>**.

(iii) Since the default reference level of the display is -10dBm, the signal is 20 dB (two graticule divisions) below the top of the screen using these spectrum analyzer

settings. If desired, adjust the reference level: press **<AMPT>** to activate the reference level, and use the knob or step keys to change the reference level.

(iv) Determine the amplitude and frequency of the signal. You can either press **<PEAK SEARCH>** or press **<MKR>** and move the marker to the signal peak. Read the amplitude and frequency. Record the results in Table 1. See the waveform in Figure 2. Frequency is displayed horizontally, and amplitude is displayed vertically.

(v) Change the units of the spectrum analyzer by pressing **<AMPT>, <Unit>, <dBm>/<dBµV>, etc…**

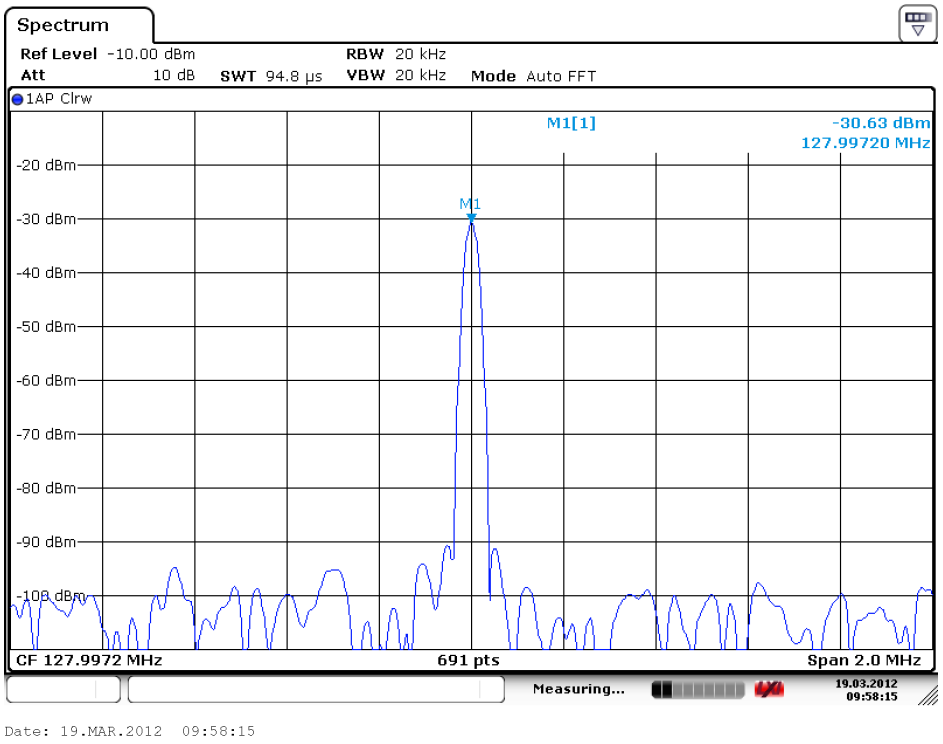


Figure 2: Reading the amplitude and frequency

Frequency, MHz	Amplitude, dBm	Amplitude,dBµV

Table 1: Frequency and Amplitude

(vi) Change the span by pressing the following keys: **<SPAN>, 100 <kHz)** to zoom in the signal as shown in Figure 3.

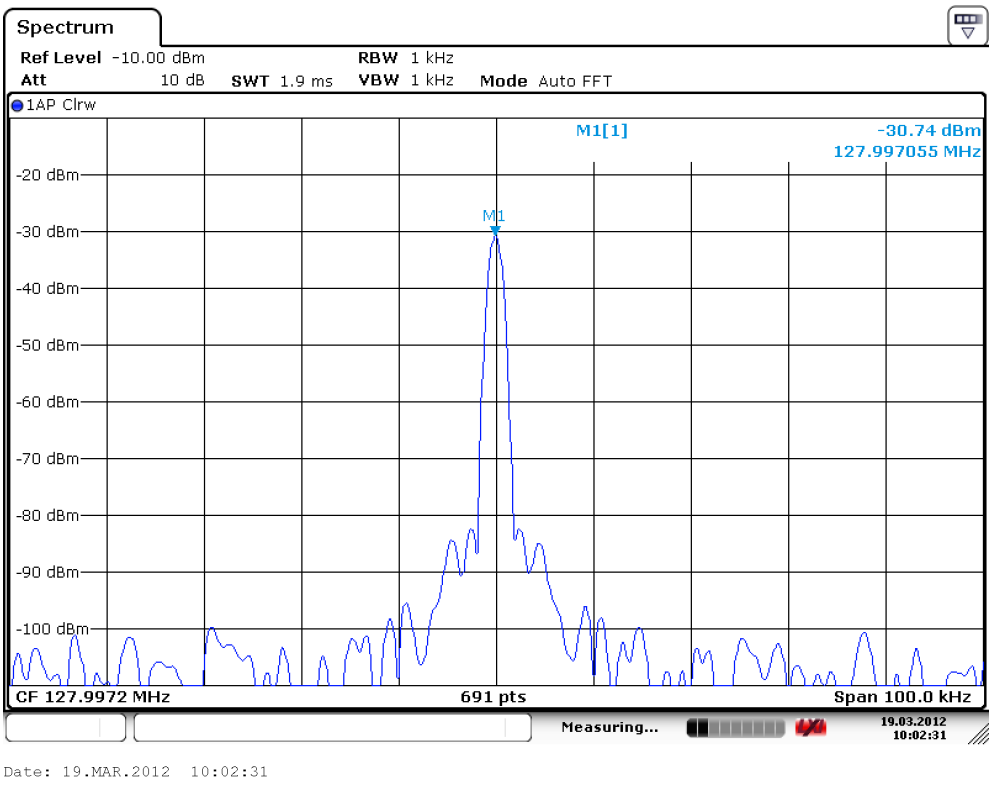


Figure 3: After zooming in on the signal with Span 100kHz

V Comparing different frequency components of an AM modulated RF signal from RF Generator using delta markers

Using the spectrum analyzer, you can easily compare frequency and amplitude differences between signals, such as radio or television signal spectra. The spectrum analyzer delta marker function lets you compare two or more signals when both appear on the screen simultaneously or when only one appears on the screen.

Required setup

(i) Press <**PRESET**> button at the Spectrum analyser.

(ii) Set the RF signal generator to generate the following sinusoidal carrier signal:
Frequency: 128 MHz
Output: -30 dBm
Modulation: on
RF output: on
Modulating signal (f_S): sine wave of 10 kHz
Modulation index (m): 30%

Procedure

(i) Select the carrier frequency and output amplitude (power) of RF signal generator :

Select FREQUENCY hard key➔ 128 ➔ 

Select LEVEL hard key ➔ -30 ➔ 

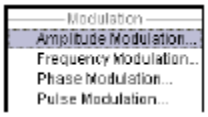
Select 

to turn **on** the RF output.

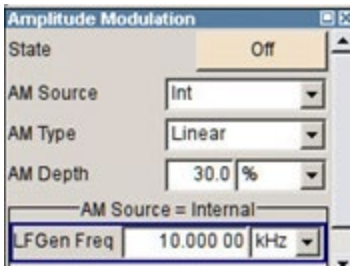
(ii) Set the AM modulation with modulation index of 30%.

Select 

and turn the knob to select the Modulation block. Press the knob and a drop down dialog appeared. Select Amplitude Modulation … to choose AM modulation type



The Amplitude Modulation dialog appeared.



Turn the knob to select the AM DEPTH and press the knob to key the modulation index value ➔ 30 ➔ 

(iii) Set the modulating signal frequency via turning the knob to select the LFGEN FREQ and press the knob to enter the value ➔ 10 ➔ 

(iv) Set the State ON

(v) To display the AM signal at the spectrum analyser, set the centre frequency by pressing the following keys: <**FREQ**>, 128 <**MHz**> and set the span by pressing the following keys: <**SPAN**>, 40 <**kHz**>.
Note: If the signal is not right at the centre of the display screen, then it can be brought to the centre by using the <**FREQ**> button and the knob.

(vi) Press **<PEAK SEARCH>** to place a marker at the highest peak on the display. Read the amplitude and record it in Table 2.

(vii) See the frequency spectrum shown in Figure 4.

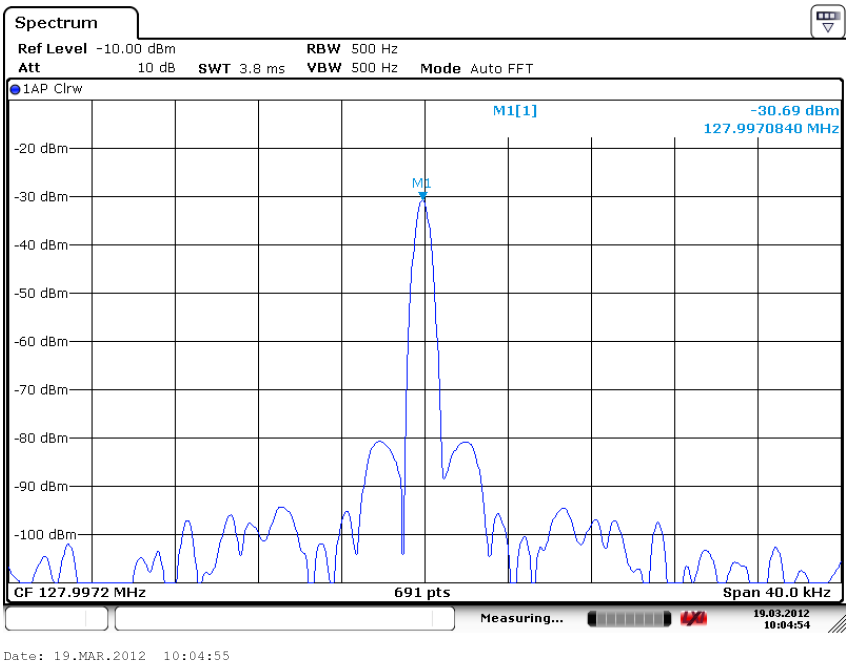


Figure 4: Placing a marker on the AM RF signal

(viii) Press **<MKR>** and activate a Delta marker press <**Marker Norm/Delta**> soft key until the **"Delta" highlight**. Delta maker, D1, will be placed at the one of the sideband components.

(ix) Press <**MKR➔**> and move the marker to another signal peak using the **<Next Peak>** soft keys or the knob.

(x) The amplitude and frequency difference between the markers are displayed in the upper-right corner of the screen. Record the amplitude and frequency of ΔMarker value of the upper and lower sidebands of the AM signal in Table 2.

(xi) See the waveform in Figure 5 & 6.

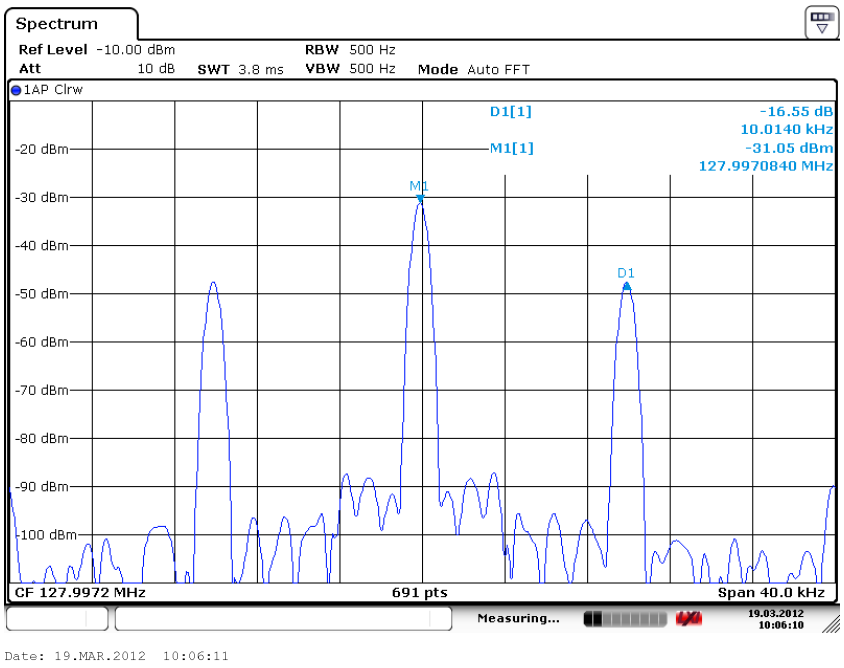


Figure 5: Delta maker at the upper sideband component using the marker delta function

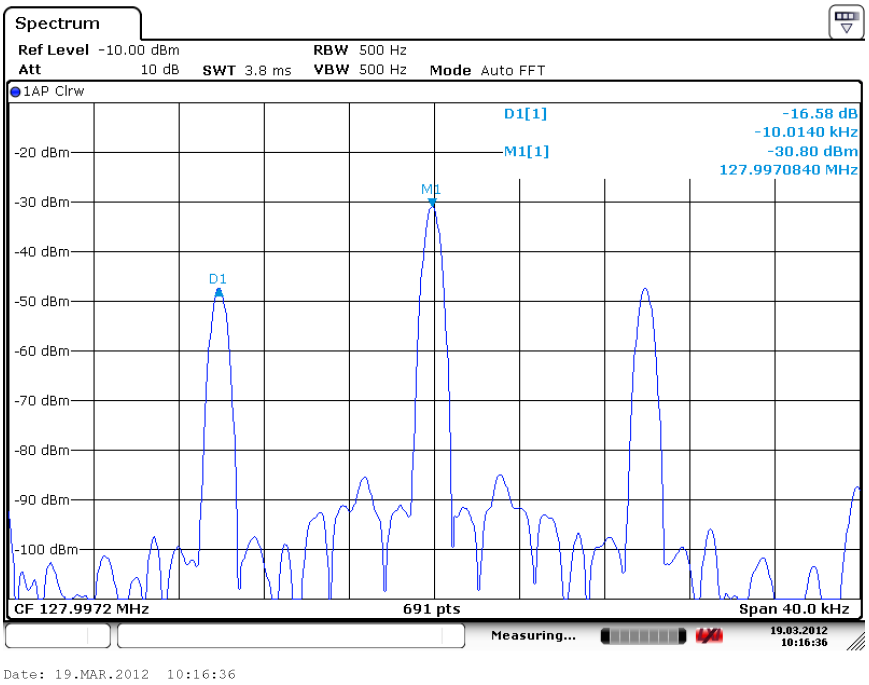


Figure 6: Delta maker at the lower sideband component using the marker delta function

AM RF Signal Measurement	**Amplitude**		**Frequency**	
RF carrier Signal using Marker		dBm		MHz
Lower Sideband Signal, using Δ Marker		dBc		ΔkHz
Upper Sideband Signal, using Δ Marker		dBc		ΔkHz

Table 2: Marker reading

Question 1: Why the unit in Δ Marker is named dBc? Give reason(s) to support your answer.

Question 2: If we want to calculate the amplitude of sideband signals from Table 2, what could the formulae be? Give an example with your answer.

Question 3: How many frequency components in a pure RF carrier sinusoidal signal is/are?

Question 4: How many frequency components are in the AM RF with a sinusoidal modulating signal? What are these components?

LAB 7: Setup the Analog Wireless Communication System

I Objectives

Students will learn:

- What are the components of a wireless communication system?
- The importance of modulation and demodulation in wireless communication systems.
- The effects of bandwidth, signal power, signal to noise ratio in a wireless communication system.

II **Equipment**

R&S FSV3 spectrum analyser

R&S SMB100A RF signal generator

Antennas

III **Introduction**

Set up a communication system using a RF signal generator and a spectrum analyser as shown in the following Figure.

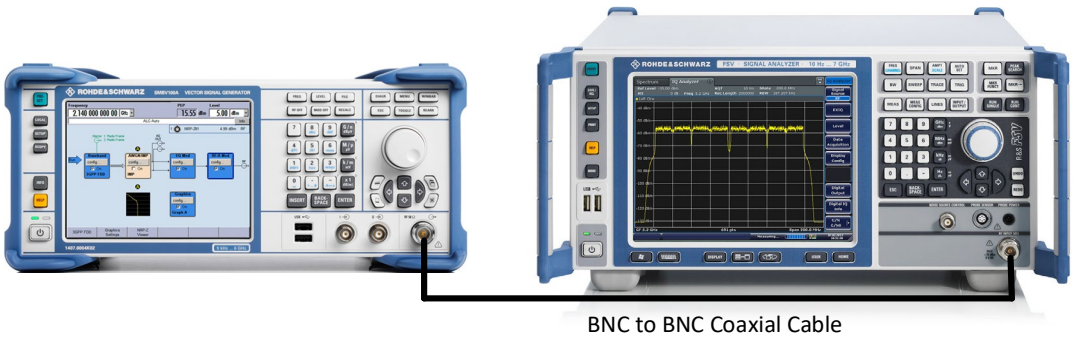
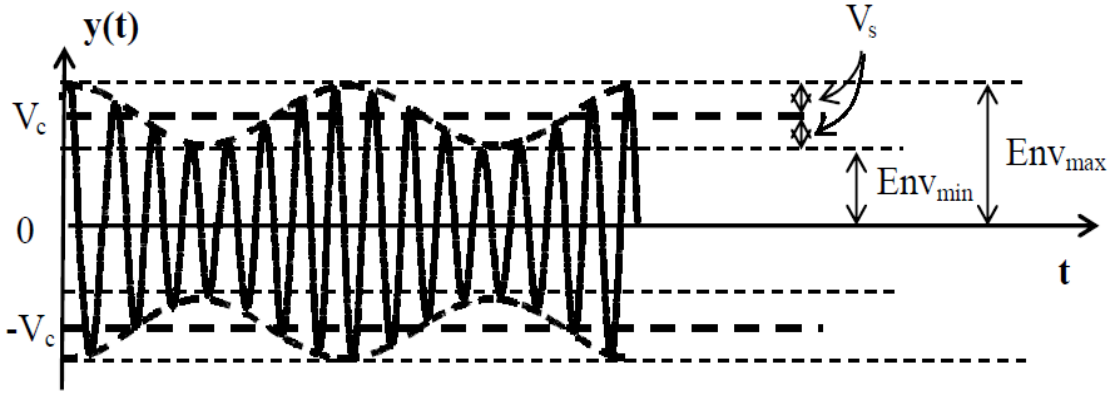


Figure: Basic Set up for a Communication System

IV **AM communication system**

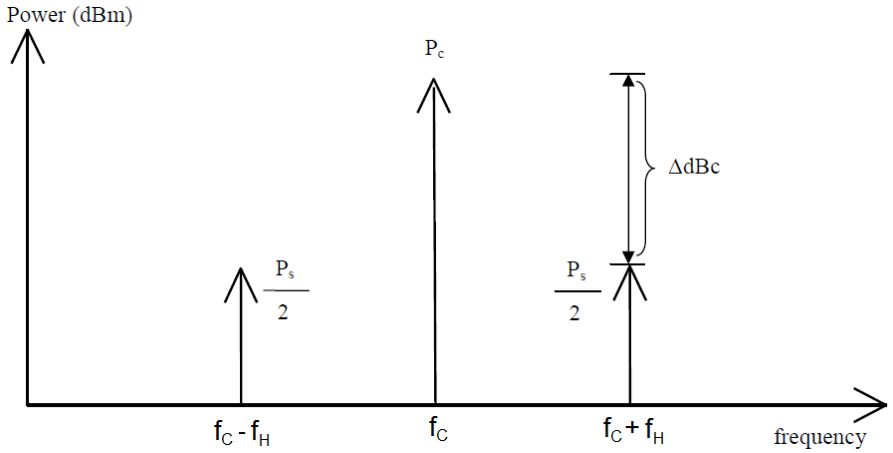
In amplitude modulation, the amplitude of the carrier is varied in accordance with the instantaneous amplitude of the modulating (information) signal as shown in the following Figure.



$Env_{max} = V_c + V_s$ $Env_{min} = V_c - V_s$

Amplitude Modulated Carrier

The spectrum displayed on the spectrum analyser is power spectrum as shown in the following Figure. The power of the sideband component relative to the carrier component is denoted as ΔdBc.



Power spectrum of AM signal

From power spectrum measurement, it is also possible to calculate the modulation index using the following equation.

$$m = 2x10^{\frac{-|\Delta dBc|}{20}}$$

If the frequency of the baseband signal is f_H, the bandwidth (B_{AM}) of the AM signal will be as follows.

$$B_{AM} = (f_C + f_H) - (f_C - f_H) = 2f_H$$

Follow the steps given below to generate an AM signal with the following parameters:

RF output power: -20 dBm

Carrier frequency (f_C): 435 MHz

Modulating signal (f_S): sine wave of 1.2 kHz

Modulation index (m): 10 %

Modulation: on

RF output: on

Procedure

(i) Select the carrier frequency and output amplitude (power) of RF signal generator

Select FREQUENCY hard key➔ 435 ➔ 

Select LEVEL hard key ➔ -20 ➔ 

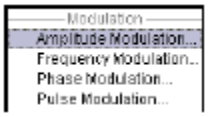
Select 

to turn **on** the RF output.

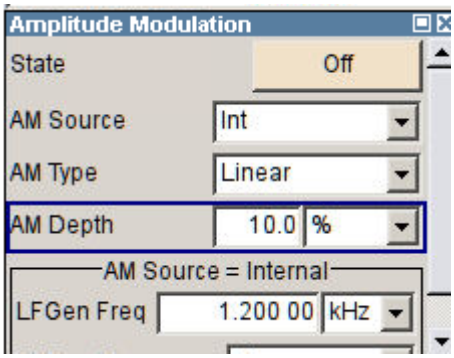
(ii) Set the AM modulation with modulation index of 10%.

Select 

and turn the knob to select the Modulation block. Press the knob and a drop down dialog appeared. Select Amplitude Modulation … to choose AM modulation type



The Amplitude Modulation dialog appeared.



(iii) Turn the knob to select the AM DEPTH and press the knob to key the modulation index value ➔ 10 ➔ 

(iv) Set the modulating signal frequency via turning the knob to select the LFGEN FREQ and press the knob to enter the value ➔ 1.2 ➔ 

(v) Set the State ON

(vi) Set the amplitude, centre frequency and span at the spectrum analyser to display the AM signal.

Amplitude = -10 dBm

Centre frequency = 435 MHz

Span = 4.8 kHz [2 x (Bandwidth which is 2 x 1.2 KHz)]

AMPT ➔ -10 dBm FREQ ➔ CENTER FREQ ➔ 435 MHz ➔ SPAN 4.8 KHz

Sketch the frequency spectrum of this AM signal with all the correct labelling.

Question 1: What are the lower side frequency and upper side frequency?

Question 2: What is the carrier frequency?

Question 3: What is the bandwidth of the AM signal?

Question 4: What is the value of the modulating frequency (f_S or f_H)?

(vii) Keep the centre frequency of the spectrum at 435 MHz and change the SPAN to zero. Turn on the demodulator at the spectrum analyser to demodulate the AM signal as follow:

FREQ ➔ CENTER FREQ ➔ 435 MHz ➔ <Zero SPAN>
Turn on one marker e.g Marker 1 and Press <MKR FUNC>➔ <Marker Demod> , <Mkr Demod ON/ OFF> (so that ON is underlined), and click <AM>. Using the

AF output control to increase the Speaker's volume.

(viii) Change the modulation index to 20%, 50%, 80% and 100%. Investigate the amplitude spectrum of the AM signal at the spectrum analyser and listen the audio output from the speaker.

Question 5: When the modulation index is increase, what happens to the signal to noise signal of the AM signal, higher or lower? Give reason(s) to support your answer.

_____

V FM communication system

Set the RF signal generator to obtain the following FM signal with the parameters given and display its spectrum:

RF output power:	- 30 dBm
Carrier frequency (f_C):	88 MHz
Modulating signal (f_S):	sine wave of 20 kHz
Frequency deviation (Δ_f):	20 kHz
Modulation: on	
RF Output: on	

Note: The modulation index (m_f) of FM signal is:

$$m_f = \frac{\Delta f}{f_s}$$

If $m_f < 0.5$ ➔ narrowband FM (NBFM)

If $m_f \geq 0.5$ ➔ wideband FM (WBFM)

Bandwidth of the narrowband FM,

BW = 2 f_H same a AM

Bandwidth of the wideband FM,

BW = $2(1 + m_f)f_H$

From the given setting, $m_f = \frac{\Delta f}{fs}$ = 20kHz/20kHz = 1 (➔ WBFM)

Therefore, BW = 2 (1 + 1) 20 kHz = 80 kHz

Set the amplitude, centre frequency and span at the spectrum analyser to display the FM signal.

Level = -20 dBm

Centre frequency = 88 MHz

Span = 160 kHz (2 x Bandwidth)

AMPT ➔ -20 dBm FREQ ➔ CENTER FREQ ➔ 435 MHz ➔ SPAN 160 kHz

(i) Sketch the frequency spectrum of this FM signal with all the correct labelling.

(ii) Keep the centre frequency of the spectrum at 88 MHz and change the SPAN to zero. Turn on the demodulator at the spectrum analyser to demodulate the FM signal as follow.
FREQ ➔ CENTER FREQ ➔ 88 MHz ➔ SPAN 0 Hz

(iii) Turn on one marker e.g Marker 1 and Press <MKR FUNC>➔ <Marker Demod> , <Mkr Demod ON/ OFF> (so that ON is underlined), and click <FM>. Using the

AF output control to increase the Speaker's volume.

(iv) Change the frequency deviation to 10 kHz, 30 kHz and 40 kHz. Investigate the amplitude spectrum of the FM signal at the spectrum analyser and listen the audio output from the speaker.

Question 6: When the frequency deviation is increased, what happens to the signal to noise signal of the FM signal, higher or lower? Give reason(s) to support your answer.

Question 7: When the modulation index is increase, what happens to the bandwidth of the FM signal, higher or lower? Give reason(s) to support your answer.

V Demodulating a commercial AM or FM Signal

(i) Connect an antenna to the spectrum analyzer input.

(ii) Select a frequency range on the spectrum analyzer, such as the range AM/FM radio broadcasts. For example, the frequency range for commercial FM broadcasts is 88 MHz for 108 MHz. Press <PRESET>, <FREQ>, START FREQ, 88 <MHz>, STOP FREQ, 108 <MHz>.

(iii) Place a marker on the signal of interest by using <PEAK SEARCH> to place a marker on the highest amplitude signal, or by pressing <MKR>, NORMAL and moving the marker to a signal of interest.

(iv) Press <MKR FUNC>➔ <Marker Demod> , <Mkr Demod ON/ OFF> (so that ON is underlined), and click <FM>. Using the 

AF output control to increase the Speaker's volume.

Question 8: What is the frequency range for commercial AM broadcast?

Question 9: State the AM/FM broadcasting system whether it is a simplex or a duplex wireless communication system.

Question 10: Draw the bock diagram of the above wireless communication systems?

ENGINEERING @ SP

The School of Electrical & Electronic Engineering at Singapore Polytechnic offers the following full-time courses.

1. Diploma in Aerospace Electronics (DASE)

The Diploma in Aerospace Electronics course aims to provide students with a broad-based engineering curriculum to effectively support a wide spectrum of aircraft maintenance repair and overhaul work in the aerospace industry and also to prepare them for further studies with advanced standing in local and overseas universities.

2. Diploma in Computer Engineering (DCPE)

This diploma aims to train technologists who can design, develop, setup and maintain computer systems; and develop software solutions. Students can choose to specialise in two areas of Computer Engineering & Infocomm Technology, which include Computer Applications, Smart City Technologies (IoT, Data Analytics), Cyber Security, and Cloud Computing.

3. Diploma in Electrical & Electronic Engineering (DEEE)

This diploma offers a full range of modules in the electrical and electronic engineering spectrum. Students can choose one of the six available specialisations (Biomedical, Communication, Microelectronics, Power, Rapid Transit Technology and Robotics & Control) for their final year.

4. Diploma in Engineering with Business (DEB)

Diploma in Engineering with Business provides students with the requisite knowledge and skills in engineering principles, technologies, and business fundamentals, supported by a strong grounding in mathematics and communication skills, which is greatly valued in the rapidly changing industrial and commercial environment.

5. Common Engineering Program (DCEP)

In Common Engineering Program, students will get a flavour of electrical, electronic and mechanical engineering in the first semester of their study. They will then choose one of the 7 engineering courses specially selected from the Schools of Electrical & Electronic Engineering and Mechanical & Aeronautical Engineering.

School of Electrical & Electronic Engineering

More than **60** Years of solid foundation	**8** Tech Hubs	Unique **PTN** Scheme	SP-NUS SP-SUTD Programmes	More than **35,000+** Alumni

SP Singapore Polytechnic

Electives offered by SP | SCHOOL OF ELECTRICAL & ELECTRONIC ENGINEERING

All SP students, including EEE students are free to choose electives offered by ANY SP schools, subject to meeting the eligibility criteria.

Like all schools, School of Electrical and Electronic Engineering offers electives for:

- EEE students only
- *and* for all SP students

EEE students are required to complete 3 electives, starting from Year 2 to Year 3 (one elective per semester).

Electives Choices for All SP students

Mod Code	Module Title
EP0400	Unmanned Aircraft Flying and Drone Technologies
EP0401	Python Programming for IoT*
EP0402	Fundamentals of IoT*
EP0403	Creating an IoT Project*
EP0404	AWS Academy Cloud Foundations
EP0405	AWS Academy Cloud Architecting
EP0406	Fundamentals of Intelligent Digital Solutions
EP0407	Technology to Business
EP0408	Cybersecurity Essentials
EP0409	Low Code 5G & AIoT

Certificate in IoT (Internet of Things)

* A certificate in IoT would be awarded if a student completes the 3 modules: EP0401, EP0402 and EP0403

Electives Choices for EEE students

Mod Code	Module Title
EM0400	Commercial Pilot Theory
EM0401	Autonomous Electric Vehicle Design
EM0402	Artificial Intelligence for Autonomous Vehicle
EM0403	Autonomous Mobile Robots
EM0404	Smart Sensors and Actuators
EM0405	Digital Manufacturing Technology
EM0406	Linux Essential
EM0407	Advanced Linux
EM0408	Linux System Administration
EM0409	Rapid Transit System
EM0410	Rapid Transit Signalling System
EM0412	Data Analytics
EM0413	Mobile App Development
EM0414	Client-Server App Development
EM0415	Machine Learning & Artificial Intelligence
EM0416	Solar Photovoltaic System Design
EM0418	Integrated Building Energy Management System
EM0419	Digital Solutioning Skills