Unit 1: Radio Fundamentals

Ref: http://www.asecuritysite.com/wireless/wireless01

1.1 Introduction

As microelectronic has made devices smaller, in such a way that users now have power processing devices in the palm of their hands, there is an increasing requirement for connections to networks to be *wire-less*. Unfortunately many networks rely on cables as they provide a degree of security, as the signals are contained within the cables. They are also fairly robust, and operate error free for many years. Networks have thus grown into vast infrastructures of nodes connected to switches, which are then connected to routers. Each of these connect using a vast array of cables. The physical and logical configuration of the network can thus be well managed, and controlled. For many reasons, such as bandwidth requirements, robustness and security, it is sensible to have fixed networks at the core of any networked system, but the actual connectivity of devices is likely to move away from fixed connections towards mobile ones. This new type of connection is likely to create many new issues, which must be overcome become wireless networking becomes the standard way to connect to a network. The three major ones are:

- **Security**. The signals from a wireless adaptor are available to anyone within the wireless domain, and can thus be subjected to security breaches. There are two main aspects in wireless security: encryption and authentication. In terms of encryption, WEP was one of the first method to be used on modern wireless networks. Unfortunately it was relatively easy to crack, and once cracked, the whole of the wireless network was comprised (as it used a shared encryption key). New methods of encryption included WPA, which has session keys for each connect, and is difficult to crack. Authentication will be covered in a future chapter.
- **Robustness**. Wireless networks tend to be less robust than fixed networks, especially as they tend to be reliant on access points and antennas, which may be subjected to vandalism, or could be affected by other nearby access points.
- **Bandwidth**. It would never be possible for wireless networks to compete in bandwidth performance with fiber optic cables, as radio waves have a limited bandwidth of twice the frequency bandwidth of the system. This is mainly due to the limitation in the available radio system, where, currently, many of the radio bands have been used by other applications, such as satellite TV, and with military devices. Thus, a system which spans from 2GHz to 2.2GHz, has a frequency bandwidth of 200MHz. The actual data rate bandwidth of this type of system is typically twice the frequency bandwidth, which will be 400Mbps. Fiber optic cables support rates of many Gbps.

Most wireless networks use a shared radio environment, where the devices can transmit and received at a distance of up to 450 meters in an open environment. The wireless network implements most of the data link and physical layer functions. Its main functions are to:

1. Provide a path for data to flow.
2. Allow the sharing of the common medium.
3. Allow synchronization and error control to minimize errors on data transmission.
4. Allow routing mechanisms to efficiently determine the best route for the data.
5. Allow a software interface to network-based application software.

The applications of wireless technology is likely to increase over the forthcoming year, especially with the increasing processing power of mobile devices, but typical applications include:

- Environments which have frequently change, such as in a retail environment, or in workplaces which are continually rearranged.
- High security networks. Ethernet has suffered from security problems, thus wireless networks with encryption can overcome this.
- Providing remote access for a corporate network.
- Providing temporary LANs which could be used for special projects.
- Remote access to databases in mobile applications, such as for medical practitioners, or office staff.
- Supporting networks in environments where cable runs are difficult, such as in old buildings, hazardous areas, and in open spaces.
- Support for users who use SOHO (Small Office and Home Office), as it provides a quick access to networks.

1.2 Electromagnetic wave (EM) fundamentals

An electromagnetic wave travels as both an electric field (E) and an associated magnetic field (H), as illustrated in Figure 1.1. The E field is always at right angles to the magnetic field, and the propagation is also a right-angles to both the E field and the H field. This conforms to the right-hand law where E is the middle finger, H is the thumb, and the index finger defines the direction of propagation. The direction in which the E field propagates is important as it often defines the type of antenna used, and on how it is aligned with the EM wave.

In free space an EM wave propagates at the speed of light, with a defined frequency and wavelength (Figure 1.2). These are related as:

$$c=f\lambda \qquad (1.1)$$

where f is the frequency (Hz), and λ is the wavelength of the wave (m). c is defined as the speed of light and is approximately 300,000,000 ($3\text{x}10^8$) m/s. For example if the frequency of the wave if 2.4GHz, then, in free-space its wavelength will be:

$$\lambda = \frac{c}{f} = \frac{3 \times 10^8}{2.4 \times 10^9} = 12.5cm \qquad (1.2)$$

which is a significant wavelength, as we will see later in the module, as it defines the size of the antenna used in the most popular type of wireless system (IEEE 802.11b).

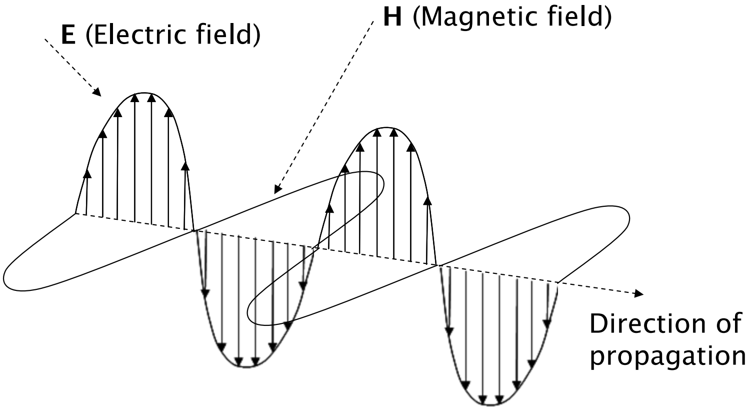


Figure 1.1: EM wave propagation

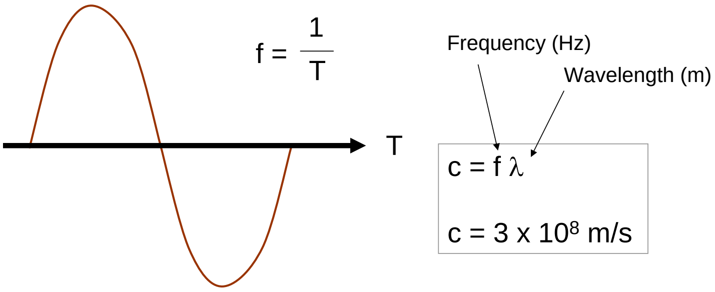


Figure 1.2: Basic formula for EM waves

1.3 EM Spectrum

The EM spectrum covers a number of classifications for the wave. The lowest frequency of EM waves is radio waves which range up to 1GHz, and include AM radio, FM radio, TV and Cell phone technologies. Generally this spectrum is congested with applications, and it has been relatively simple to implement electronic devices which use these applications. The microwave spectrum sits above this spectrum, and has been used for RADAR and microwave oven applications. A small gap exists for IMS (Industrial, Medical and Scientific), which has been allocated for new wireless LAN standards. Figure 1.3 shows the general classifications. The characteristics of each of the wave differs, from example radio wave propagate fairly well in free space, and can travel long distances. Microwaves tend to be used in line-of-sight applications as the wave cannot bend round large objects. Infra-red waves are generally associated with heat radiation and are also used for fibre optic communications, which infrared and ultra-violet can be used for laser-type applications, such as line-of-sight optics, which can be used to transmit high data rates over short distances.

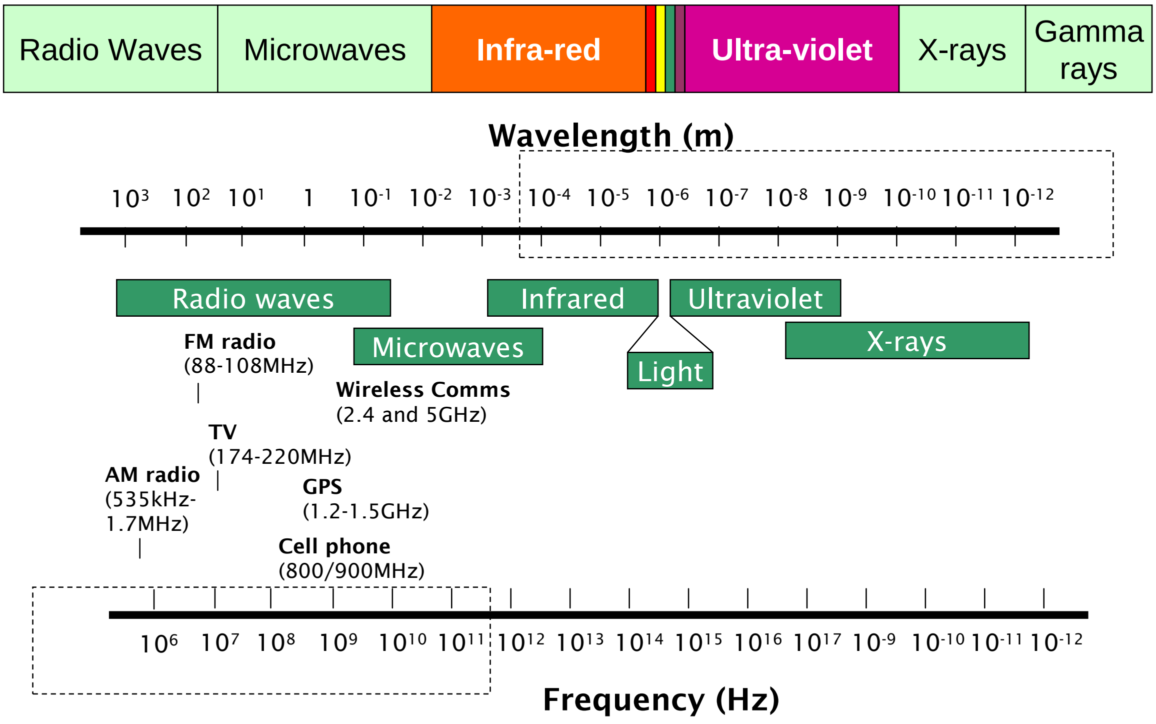


Figure 1.3: EM Spectrum

Generally the higher the frequency of the wave, the higher the available bandwidth capacity there is to transmit data. As an estimate the available bandwidth is:

$$B_{av} = \frac{f}{10} bps \qquad (1.3)$$

Thus, for example, the available bandwidth for a few radio wave are:

Radio Wave (AM)	f=1.7MHz, B_{av}=170kbps.
Radio Wave (TV)	f=200MHz, B_{av} =20Mbps.
Radio Wave (Mobile phone)	f=900MHz, B_{av} =90Mbps.
Microwave (IEEE 802.11b)	f=2.4GHz, B_{av} =240Mbps.
Infra-red	f=10^{13}Hz, B_{av} =1Tbps.

This available bandwidth, though, is often split between different users, which is in IEEE 802.11b there is around 14 channels, thus the available bandwidth is a maximum of 17Mbps. Unfortunately the actual bandwidth depends on other factors, especially noise, where the signal must be much higher than the noise for the communications to be received reliably. The larger the power transmitted, normally the larger the further the signal can be transmitted without it being affected by noise. Figure 1.4 shows some of the EM waves and a typical noise floor. New communication techniques, such as UWB (Ultra wideband) spread their signal across a wide band of frequencies. The power level of UWB does not affect other communications as its power in any of the bands is generally lower than the noise floor.

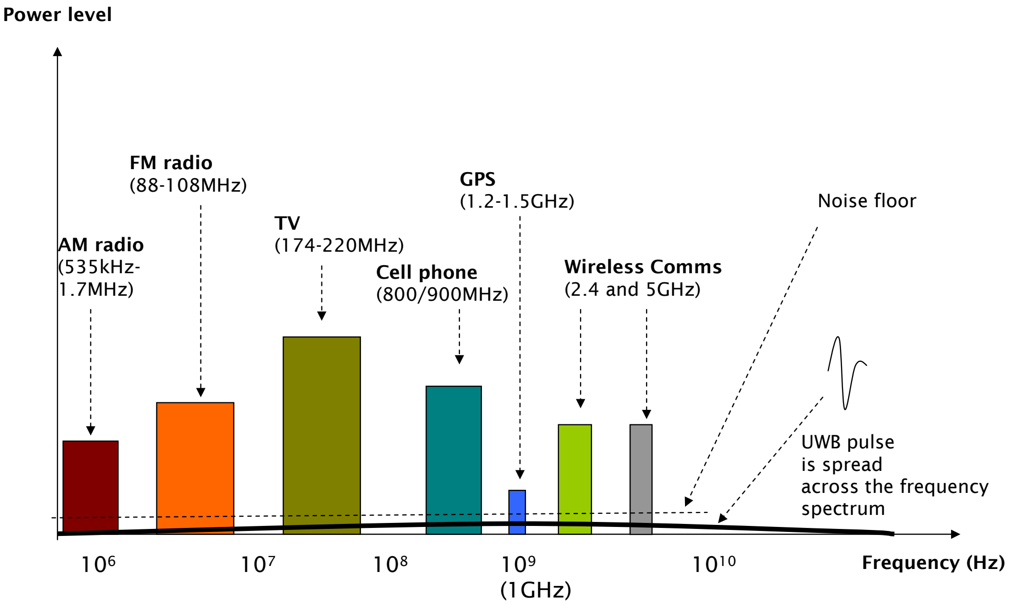


Figure 1.4: Power levels

1.4 Radio Wave problems

Radio wave suffer from many propagation problems, along with their inherent lack of security. Figure 1.5 illustrates three of them. The first major one is **fading**, where the wave loses its strength as it propagates. This could be due to the wave spreading out, or being absorbed, such as by moisture in the air. Along with this radio waves suffer from reflections from metal objects, which causes multipath problems. In Figure 1.6 it can be seen that there can be many ways that a wave can propagate to receive a destination. If the waves arrive, and the phase of the wave has been changed, it is possible for the multipath waves to combine and distort the result. Luckily this type of problem can be overcome by just moving the aerial a small amount, and is used in diversity aerials which are seen on many wireless access points.

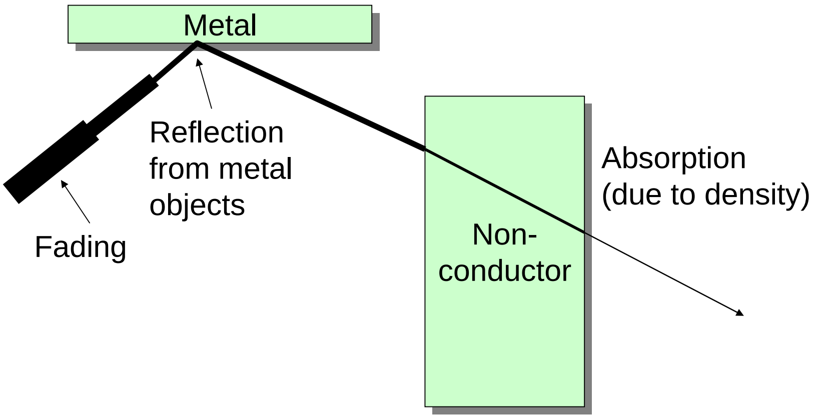


Figure 1.5: Power levels

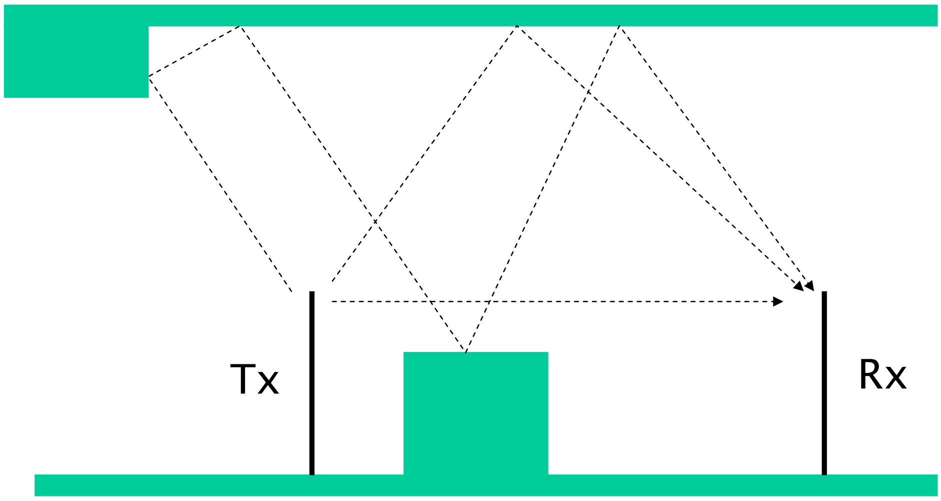


Figure 1.6: Multipath problems

1.5 Radio wave identification

Devices in a wireless network typically tune-into a given frequency band, which allows several frequencies bands to exist, and thus supports multiple simultaneous transmissions. One method is to use a cellular technology in which devices connect to the strongest transmitting device in an area, and connect with its transmission frequency. This concept is illustrated in Figure 1.7, where only three frequencies have to be used, so that they do not overlap. This are identified as 1, 2 and 3. As a device roams it can be handed over from one cell to the next. This is the technique that mobile phones and wireless networks (IEEE 802.11) use to connect devices to a wireless infrastructure.

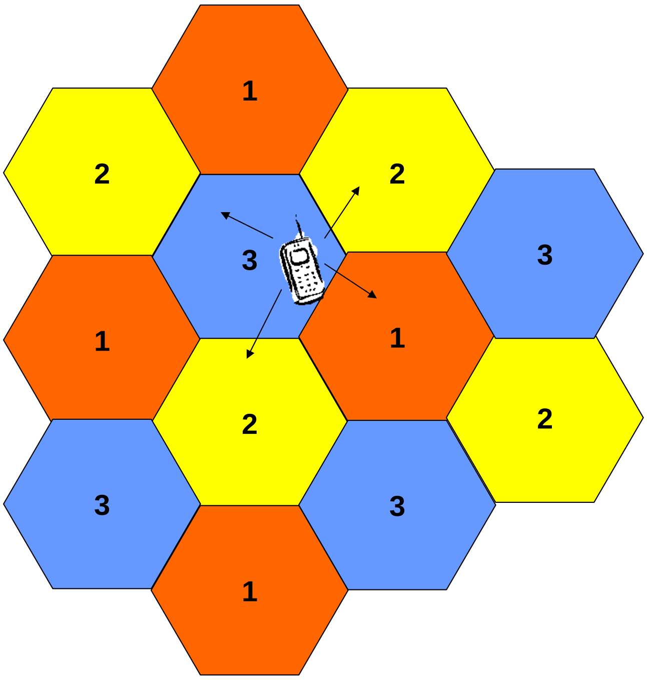


Figure 1.7: Cellular technology

1.6 IEEE 802.11 radio specification

There are two main frequencies which are used in modern wireless LANs. These are IEEE 802.1a, which uses a 5GHz carrier, and IEEE 802.11b/n/g, which uses a 2.5GHz carrier.

1.6.1 IEEE 802.11b/g/n

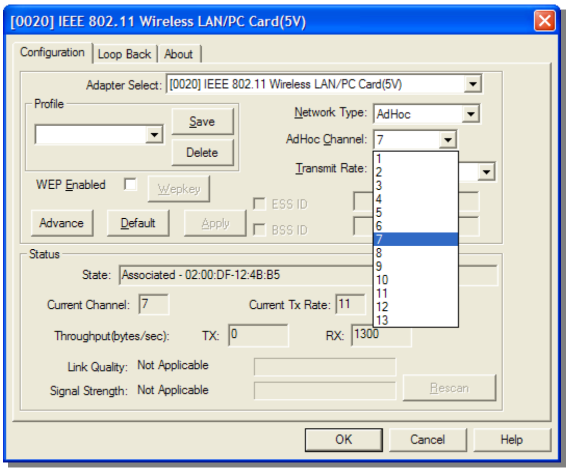
IEEE 802.11b/n/g uses a number of channels in frequency range around 2.4 GHz to 2.45 GHz. This high frequency allows the radio wave to propagate fairly well through building and air. At 11Mbps, the maximum range is around 140 meters, but this reduces when there are obstacles in the way. At 1Mbps, the range increases to 400 meters. The frequencies are split into a number of channels. In Northern America, there are 11 channels, in Japan, there are 14, and in Europe, there are 13 channels (as shown in Figure 1.8).

Operating Channels:	11 for N. America, 14 Japan, 13 Europe (ETSI), 2 Spain, 4 France
Operating Frequency:	2.412-2.462 GHz (North America), 2.412-2.484 GHz (Japan), 2.412-2.472 GHz (Europe ETSI), 2.457-2.462 GHz (Spain), 2.457-2.472 GHz (France)
Data Rate:	1, 2, 5.5 or 11Mbps
Media Access Protocol:	CSMA/CA, 802.11 Compliant
Range:	11Mbps: 140m (460 feet)
	5.5Mbps: 200m (656 feet)
	2Mbps: 270m (885 feet)
	1Mbps: 400m (1311 feet)
RF Technology:	Direct Sequence Spread Spectrum
Modulation:	CCK (11Mps, 5.5Mbps), DQPSK (2Mbps), DBPSK (1Mbps)
Output Power:	13 dBm
Sensitivity:	11Mbps < -83 dBm
	5.5Mbps < -86dBm
	2Mbps < -89dBm
	1Mbps < -91dBm

The concept of dBm will be discussed in the Antenna chapter. The IEEE 802.11g standard improves on IEEE 802.11b, but increases the bit rate to 54Mbps. With IEEE 802.11n, multiple antennas with multiple routes can be used which gives a possible maximum throughput of 150Mbps.

1.6.2 IEEE 802.11a

IEEE 802.11a uses a 5HGz carrier, which gives a smaller antenna size, and provides bits rates of 6, 9, 12, 18, 24, 36, 48, and 54Mbps. It has a possible range of up to 5km.



[0020] IEEE 802.11 Wireless LAN/PC Card(5V)

Adapter Select: [0020] IEEE 802.11 Wireless LAN/PC Card(5V)

Network Type: AdHoc

AdHoc Channel: 7

WEP Enabled □

□ ESS ID

□ BSS ID

Status

State: Associated - 02:00:DF-12:4B:B5

Current Channel: 7

Current Tx Rate: 11

Throughput(bytes/sec): TX: 0 RX: 1300

Link Quality: Not Applicable

Signal Strength: Not Applicable

Figure 1.8: IEEE802.11 channel setting for Europe

1.7 Spread spectrum

To avoid interference in the band, radio LANs (RLANs) use either Frequency Hopping or Direct Sequence Spread Spectrum techniques (FHSS & DSSS). These two methods avoid or lower the potential for interference within the band as shown in the next slide. Spread spectrum technologies work by spreading the actual signal over a wider bandwidth for transmission. Using these methods provides resilience from narrow band interference and also reduces interference to other sources using the ISM band.

Frequency Hopping Spread Spectrum technology works by splitting the ISM band into 79 1MHz channels. Data is transmitted in a sequence over the available channels, spreading the signal across the band according to a hopping pattern, which has been determined between the wireless devices. Each channel can only be occupied for a limited period of time before the system has to hop.

Military systems have been using Spread Spectrum and Frequency Hopping for many years. This is to:

- Avoid jamming on a certain channel.
- Avoid noise on a certain channel.
- Confuse the enemy as the transmitting frequency moves in a way that only the sender and receiver known. Imagine having to move the dial of your radio receiver, each minute to a certain frequency in a give way. Such as Radio 1 is broadcast on 909MHz from 12:00, then 915MHz until 12:01, then 900MHz unit 12:02, and so on.

In the OSI model, the physical layer defines the electrical, mechanical, and procedural specifications. In wireless communications, the spread spectrum process *spreads* a signal's power over a wider band of frequencies sacrificing bandwidth in order to gain signal strength. This opposes the conservation of frequency bandwidth, but the spreading procedure makes the data signal much less vulnerable to electrical noise than conventional radio modulation method. Spread spectrum modulators commonly use one of the two methods to spread the signal over a wider area: frequency hopping or direct sequence.

To avoid interference in the band, radio LANs (RLANs) use either Frequency Hopping or Direct Sequence Spread Spectrum techniques (FHSS & DSSS). These two methods of avoiding and lowering the potential for interference within the band are shown in Figure 1.9. Spread spectrum technologies work by spreading the actual signal over a wider bandwidth for transmission. Using these methods provides resilience from narrow band interference and also reduces interference to other sources using the ISM band.

Frequency Hopping Spread Spectrum technology works by splitting the ISM band into 79 1MHz channels. Data is transmitted in a sequence over the available channels, spreading the signal across the band according to a hopping pattern, which has been determined between the wireless devices. Each channel can only be occupied for a limited period of time before the system has to hop.

Direct Spread Spectrum technology divides the ISM band into 13, 22MHz overlapping channels, three of which are non-overlapping (ch1, ch7 and ch13 as shown in Figure 1.8). Unlike the FHSS system, the channel has to be set prior to communications and is not altered. To spread the signal, each bit of the original signal is modulated by a chip code (a fast repetitive pattern). For example, a 2Mb/s signalling rate modulated by an 11 chips code (the frequency of the code is 11times that of the data stream), results in a signal spread over 22MHz of bandwidth. At the receiver, the whole modulated spread signal is demodulated by the same chip code, resulting in the original data. Current literature suggests that only three non-overlapping channels (**1, 6 and 11**) may be used when using 5.5 or 11Mbps DSSS operation. This is again due to the increased bandwidth requirements of DSSS.

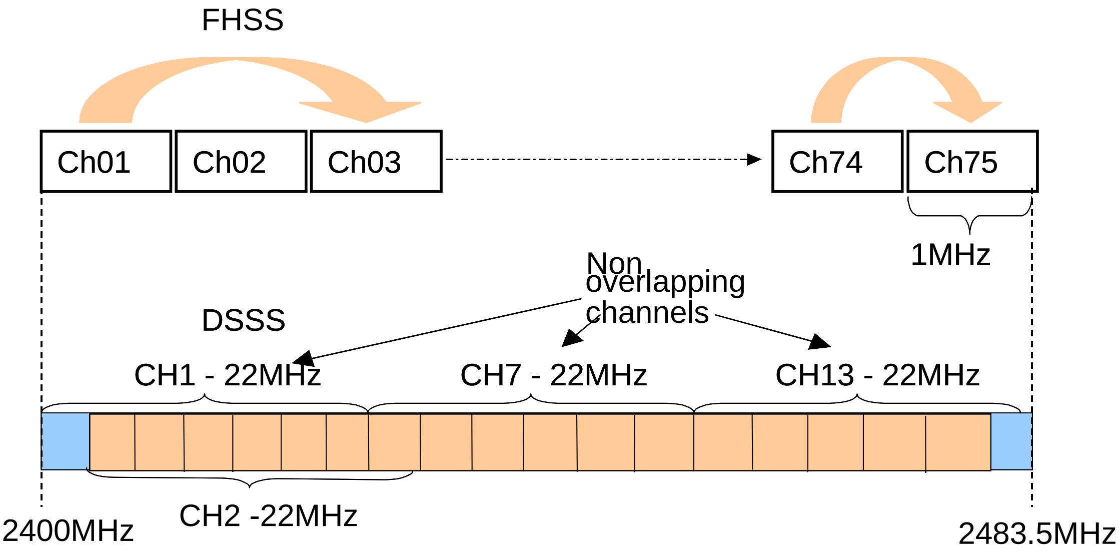


Figure 1.9: IEEE 802.11 frequency spectrum

1.8 Tutorial

- Take the test at http://www.asecuritysite.com/security/information/wireless01
- Run NetworkSims ProfSIMs. Go to **Wireless section**, and select **Wireless**, and undertake the challenges under **Basic Aironet**.