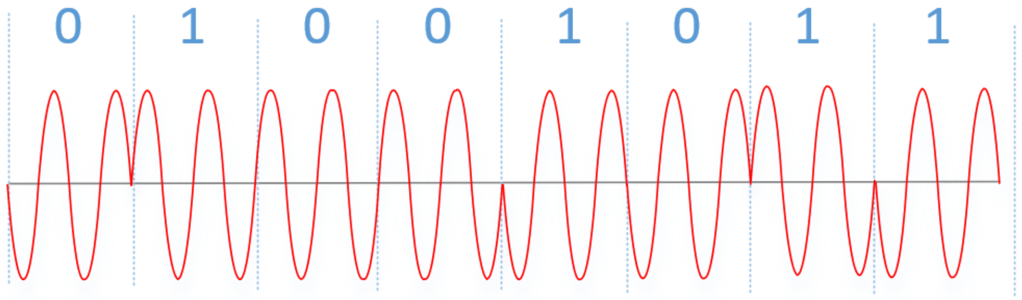
# Wi-Fi



Af: Henrik Thomsen, Mercantec Viborg

# Indhold

## Introduction

In this chapter, you will learn about the following:

- History of WLAN
- Standards organizations
- IEEE – Institute of Electrical and Electronics Engineers
- Wi-Fi Alliance
- Core, distribution, and access
- Communications fundamentals
- Frequency, wavelength and amplitude
- Modulation techniques

## IEEE

IEEE or Institute of Electrical and Electronics Engineers – pronounced I-Triple-E – is a non-profit organization dedicated to advancing technological innovation and excellence. IEEE among other things define standards in IEEE standard committees, among them the IEEE 802 committee, which defines standards for LAN and MAN networks. The IEEE 802 family of standards are defined and maintained by individual working groups, for example:

- IEEE 802.3 working group defines Ethernet LAN standards
- IEEE 802.11 working group defines wireless LAN standards WLAN (This book)
- IEEE 802.15 working group defines wireless PAN standards WPAN, for example Bluetooth
    - Note: PAN = Personal Area Network
- IEEE 802.16 working group defines WiMAX wireless MAN standards WMAN
    - NOTE: MAN = Metropolitan Area network

## History of IEEE 802.11 WLAN

The first version of IEEE 802.11 was released in 1997 and known as IEEE 802.11-1997 defining operating speeds at 1 or 2 Mbps[1]. Some of the most used defined 802.11 protocols are shown in the table below.

| | Released | Frequency GHz | Data rates in Mbps |
|---|---|---|---|
| **IEEE 802.11** | Jun 1997 | 2,4 | 1 and 2 |
| **IEEE 802.11a** | Sep 1999 | 5 | 6 – 9 – 12 – 18 – 24 – 36 – 48 and 54 |
| **IEEE 802.11b** | Sep 1999 | 2,4 | 1 – 2 – 5,5 and 11 |
| **IEEE 802.11g** | Jun 2003 | 2,4 | 6 – 9 – 12 – 18 – 24 – 36 – 48 and 54 |
| **IEEE 802.11n** | Oct 2009 | 2,4 and 5 | 7,2 – 14,4 – 21,7 – 28,9 – 43,3 – 57,8 – 65 and 72,2<br>Or<br>15 – 30 – 45 – 60 – 90 – 120 – 135 and 150 |
| **IEEE 802.11ac** | Dec 2013 | 5 | Up to 866,7 |
| **IEEE 802.11ad** | Dec 2012 | 2,4 – 5 and 60 | Up to 6912 (Almost 7 Gbps) |

As seen in the table there IEEE 802.11 is an evolving standard offering better and better performance as it evolves.

## Standardization organizations

Each of the standards organizations discussed in this chapter help to guide a different aspect of the wireless networking industry.

### Legal frequencies and power levels

ITU-R or “International Telecommunication Union Radio communication sector” is tasked by the United Nations to manage international frequency management. Local entities such as FCC in United States, Post- og teletilsynet in Norway, Post- och telestyrelsen in Sweden and Erhvervsstyrelsen in Denmark controls the national frequency spectrum and legal power levels. In Sweden, Norway and Denmark we follow the recommendations from ETSI – European Telecommunications Standards institute defining the legal frequencies and allowable power for building IEEE 802.11 wireless network.

- ETSI standard EN 300 328 for the 2,4 GHz ISM band
- ETSI standard EN 301 893 for the 5 GHz band

### IETF

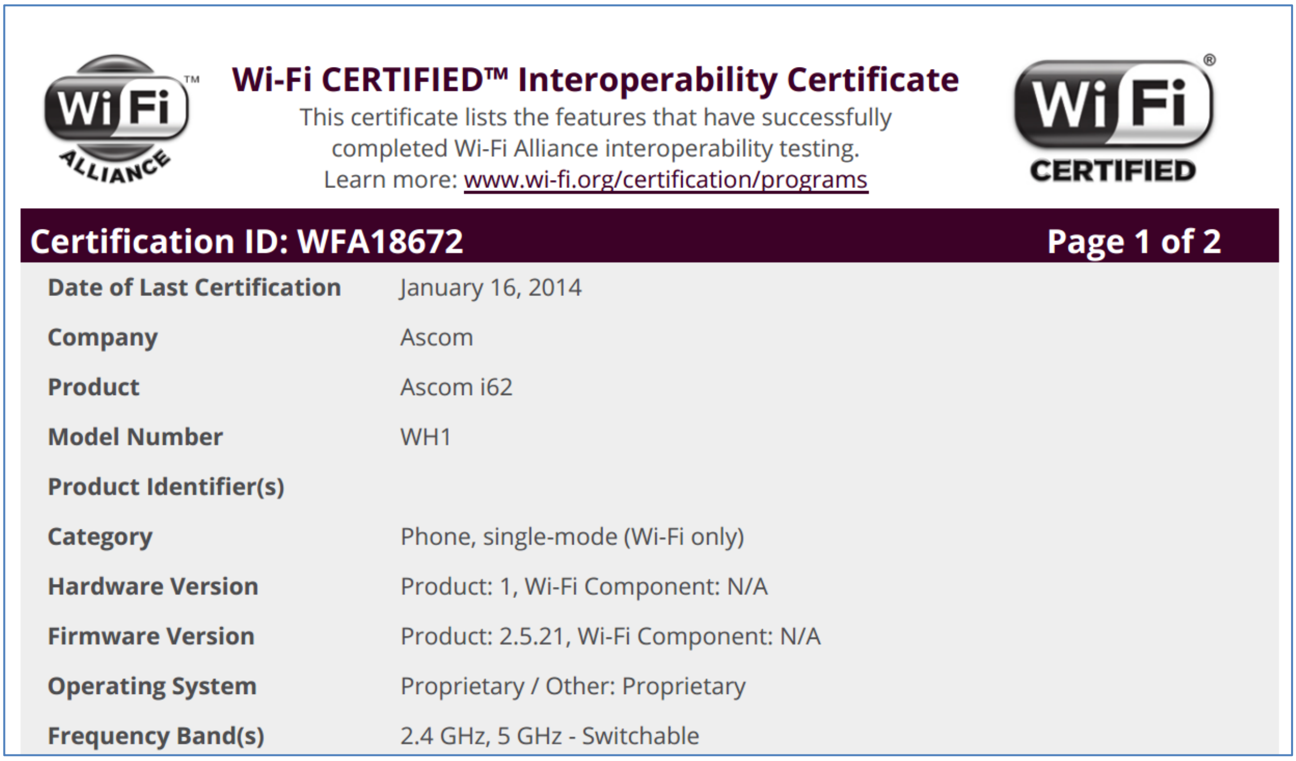
IETF or Internet Engineering task Force – is an open international community of network designers trying to make the internet better by standardizing network protocols such as IP and TCP. The standards are described in RFC’s – Request For Comments and replaced by new RFC’s when obsolete.

[1] Mbps – Megabits per second

## Wi-Fi and Wi-Fi alliance

Often mistakenly assumed that Wi-Fi is an acronym for Wireless Fidelity as hi-fi is short for high fidelity, but Wi-Fi is brand name used to market 802.11 WAN technologies, and has no special meaning.

The Wi-Fi alliance is a trade association that promotes and certify Wi-Fi products, ensuring compatibility between Wi-Fi products and vendors. The Wi-Fi alliance uses the Ying-Yang style Wi-Fi logo to marked products.



Wi-Fi CERTIFIED™ Interoperability Certificate

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing.
Learn more: www.wi-fi.org/certification/programs

**Certification ID: WFA18672** — **Page 1 of 2**

| | |
|---|---|
| **Date of Last Certification** | January 16, 2014 |
| **Company** | Ascom |
| **Product** | Ascom i62 |
| **Model Number** | WH1 |
| **Product Identifier(s)** | |
| **Category** | Phone, single-mode (Wi-Fi only) |
| **Hardware Version** | Product: 1, Wi-Fi Component: N/A |
| **Firmware Version** | Product: 2.5.21, Wi-Fi Component: N/A |
| **Operating System** | Proprietary / Other: Proprietary |
| **Frequency Band(s)** | 2.4 GHz, 5 GHz - Switchable |

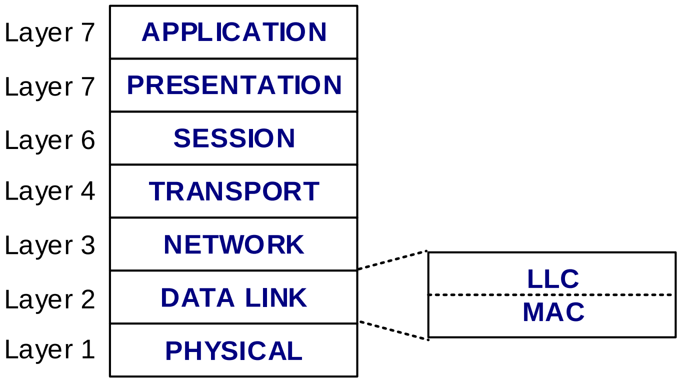
**Figure 1 - Wi-Fi alliance certified product certificate**

The Wi-Fi alliance certificate ensures interoperability between different vendors of IEEE 802.11 network equipment. It should be noted that only the IEEE 802.11 standardized functions are certified – not the vendor specific enhancements introduced by different vendors. Products that are Wi-Fi alliance certified are branded with Wi-Fi alliances certified logo shown below.

Wi Fi ®
CERTIFIED

## ISO

ISO or International Organization for Standardization – is a global nongovernmental organization that defines international standards – such as the size of a credit card. ISO has also defined OSI model or Open Systems Implementation also known as the 7-layer or reference model.



| | |
|---|---|
| Layer 7 | APPLICATION |
| Layer 7 | PRESENTATION |
| Layer 6 | SESSION |
| Layer 4 | TRANSPORT |
| Layer 3 | NETWORK |
| Layer 2 | DATA LINK |
| Layer 1 | PHYSICAL |

The IEEE 802.11-2007 standard defines communication mechanism only at the physical layer and the MAC sublayer from the data-link layer. This course subject is primarily working with these two layers.

## Core, Distribution and Access network architecture

When designing enterprise size network the core, distribution and access design architecture are often used.

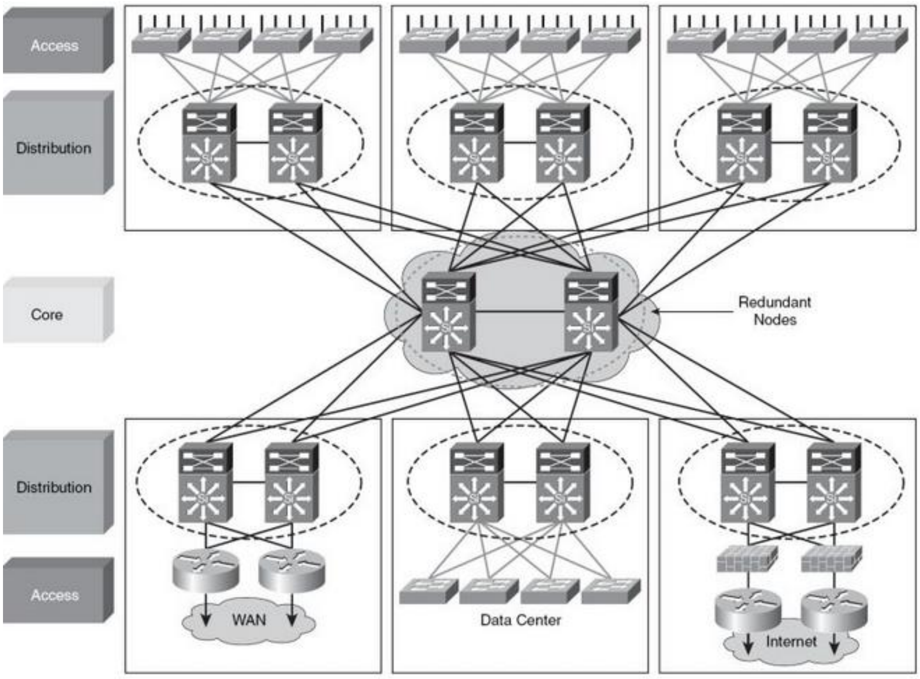


Figure 2 - Core, Distribution and access example

As seen from Figure 2 enterprise size network are build modular with the core layer acting as a fast switching backbone and the distribution layer distributes the communication into different buildings and/or floors. The access layer is the layer where equipment is located such as the user's computers.

Wireless networks are normally implemented in the access layer giving users access to the network. Sometimes a wireless bridge link could give communication to the distribution layer.

As can be seen from Figure 3 a huge building is but a small part of the total network for this enterprise. The building distribution switches are connected to the enterprises core switches – not shown on Figure 3.

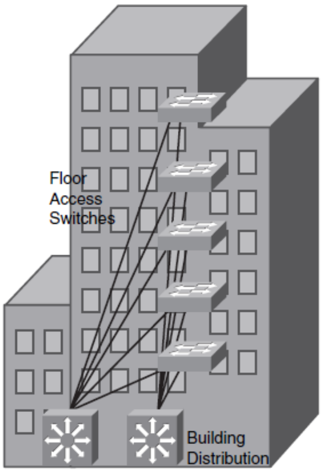


Figure 3 - Building distribution and access

## Communications fundamentals

Most people in the computer industry understand that in data communications bits is transmitted across wire, fibre optics or radio waves. Many of these people have no understanding of what actually is happening in the wire, fibre or the radio waves.

In the following sections, you will review some of the fundamentals in communications principles when working with wireless communication. The more knowledge of radio communication known, the easier it is to troubleshoot and recognize and identify the terms used in wireless community.

### Frequency

Frequency is one of the behaviours of waves. Waves travel away from the source that generated them, and the number of waves travelling away each second is the frequency measured in Hz – hertz. A wave source could be the impact of a stone in a pond or a Wi-Fi transmitter antenna in an access point. By counting the number of waves generated by the stone and measuring the time it is possible to calculate the frequency.

$$\text{Frequency in hertz} = \frac{\text{Number of waves}}{\text{time in seconds}}$$

If 18 waves were counted in 5 seconds the frequency would be

$$\text{Frequency} = \frac{18\ \text{waves}}{5\ \text{seconds}} = 3,6\ Hz$$

Wi-Fi network equipment uses 2.400.000.000 Hz or 2,4 GHz, 5 GHz and latest 60 GHz.

## Amplitude and wavelength

When transmitting an RF signal – radio frequency – the signal leaves the antenna approaching the speed of light nearly 300.000 kilometres per Second. The more signal strength the higher the amplitude. See Figure 4.

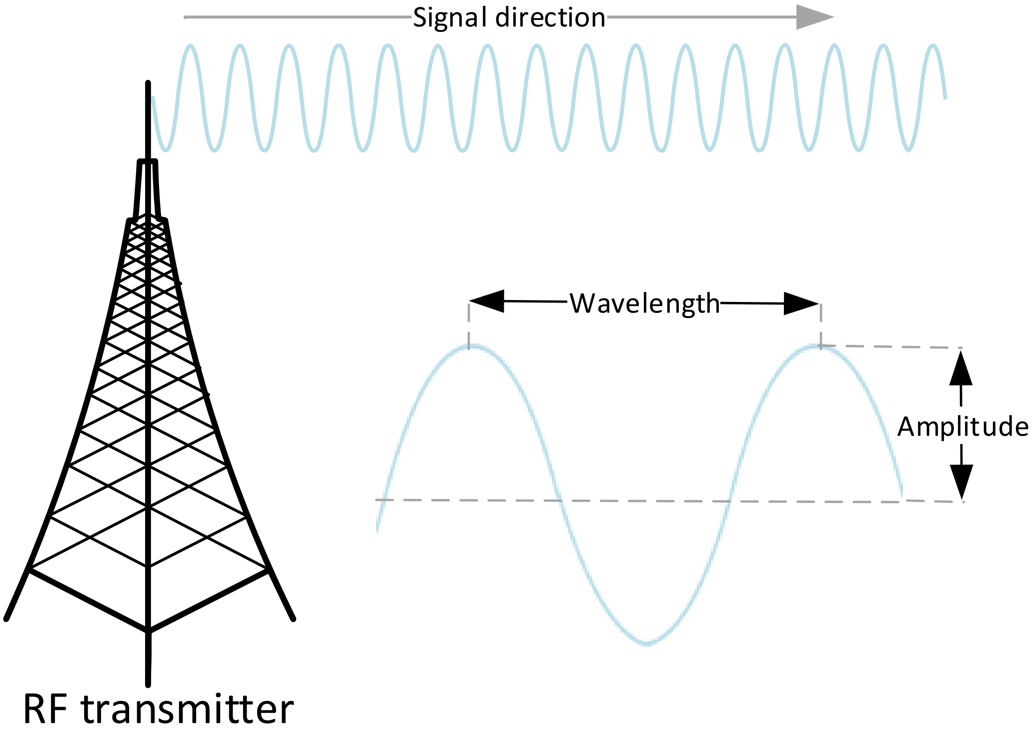


Figure 4 - Wavelength and amplitude

## Wavelength

To calculate the wavelength of a signal it is necessary to know how fast waves travel through the media and the frequency of the waves.

$$\boldsymbol{wavelength\ in\ kilometers\ =\ \frac{wavespeed\ in\ kilometers\ pr\ second}{frequency\ in\ Hz}}$$

The speed of sound through air is approximately 343 metres per second or 0,343 kilometres per second. The wavelength of a 1.000 Hz tone would be

$$\boldsymbol{wavelength\ =\ \frac{0,343\ Km/s}{1.000\ Hz} = 0,000343\ Km = 34\ cm}$$

The wavelength of a 2,4 GHz radio frequency signal – using the speed of light – would be

$$\boldsymbol{wavelength\ =\ \frac{300.000\ Km/s}{2.400.000.000\ Hz} = 0,000125\ Km = 12,5\ cm}$$

## Amplitude and attenuation

The amplitude of the wave is the height of the wave and can often be used as a measure of the signal strength. A signal may lose strength when transmitted on a wire or through the air. The loss of signal is also called attenuation and is best described as decreased amplitude.

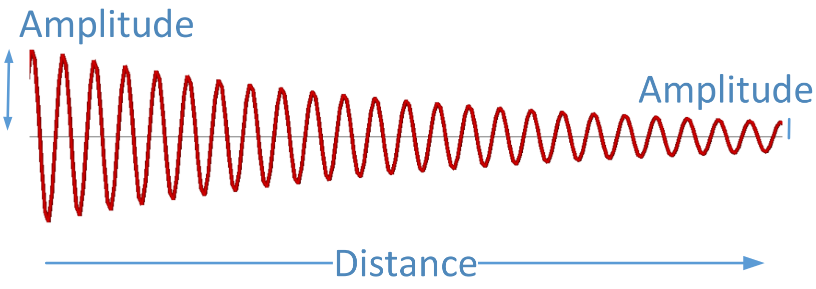


Figure 5 - Signal loss or attenuation

## Absorption

Absorption is a common RF behaviour that occurs when a signal passes through an object. If a signal is not bounce of, pass around or pass through an object then 100 percent absorption has occurred. Most materials absorb an amount of the signal that passes through it. Brick and concrete walls absorb a significant part of the signal. Objects with large water content such as people or fish tanks absorb the signal to a large extent. A human contains between 50% and 65% percent of water, which leads to absorption and loss of signal strength. So a perfectly planned Wi-Fi network could be degraded to function less than desirable in some circumstances.

Absorption is the leading cause of signal attenuation – loss of signal – in most installed Wi-Fi networks.

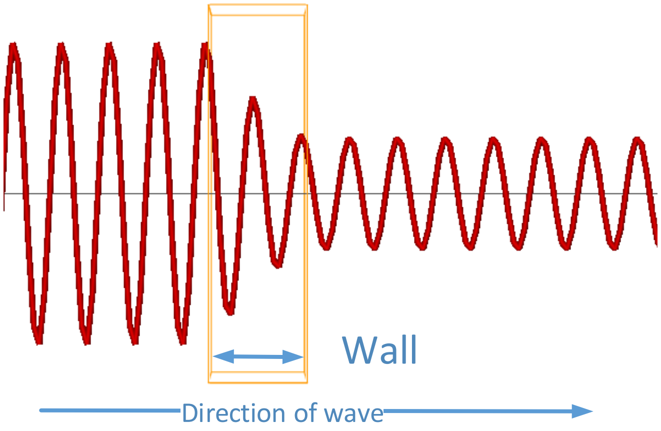


Figure 6 - Absorption of signal in a wall causing attenuation

## Phase

Phase is a relative term used to describe the position in a single cycle of a wave. A wave is divided into 360 degrees – as is a circle. See Figure 7.

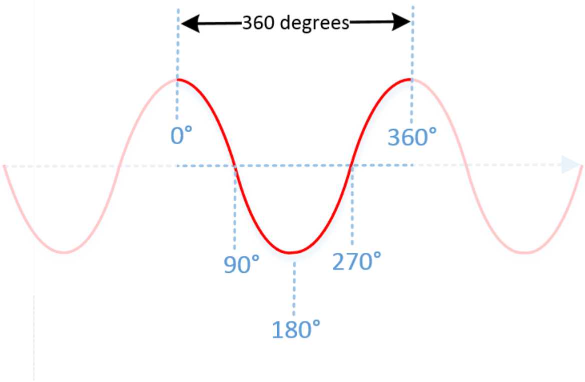


Figure 7 - A wave is divided into 360 degrees

When comparing two waves phase between the two waves are expressed in degrees. In Figure 8 the red and the blue wave are out of phase with each other by 90 degrees.

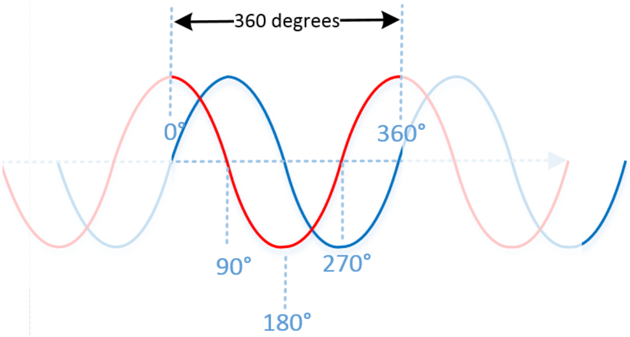


Figure 8 - Two waves 90 degrees out of phase with each other.

## Reflection

As a ball can bounce of a wall, radio waves can bounce of an object. This phenomenon is called reflection and can be quite a challenge when working with Wi-Fi networks. Microwaves such as Wi-Fi RF signals reflects of metal surfaces but also concrete walls, windows and other objects in the building. Outside reflection can occur from buildings and surface water.

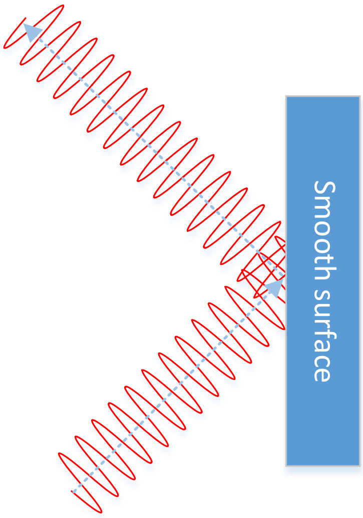


Figure 9 - RF microwavereflection

### Reflection and multipath

When a receiving antenna receives a signal directly from the antenna and simultaneously receives reflected signals there is a multipath between the transmitter and the receiver. As seen from Figure 10 the reflected signal – red – travels a longer distance than the direct – blue – signal. This means that the reflected signal reaches the receiving antenna later and is out of phase with the direct signal. The two signals are mixed together in the antenna which often leads to poor reception.

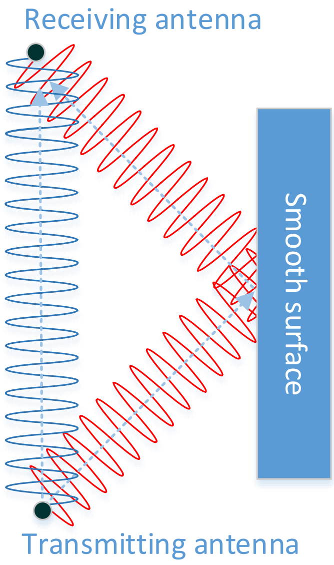


Figure 10 - Multipath

## Carrier signals and modulation

Transmitting and receiving information through RF – radio frequency – signals, either analog music or digital information, require an RF transmitter and one or more RF receivers. By example when you tune your car radio to your favourite FM stations transmitter, enabling you and everybody – in the transmitters range – to listen in on the broadcast. Remember attenuation or signal loss.

The FM broadcast band used by radio stations, differ between different parts of the world. In Europe and Africa, it spans from 87,5 MHz to 108 MHz. The FM broadcast band is highly regulated by each country in contrast to the 2,4 GHz and 5 GHz bands used for Wi-Fi networks, which can be used without license. Power levels and the frequency range however are strictly regulated by each country in the 2,4 and 5 GHz range.

## Amplitude-shift keying

ASK – Amplitude-shift keying – varies the amplitude of the carrier to represent the binary data. As shown in Figure 11 the amplitude changes to represent the data. ASK is highly sensitive to noise and interference, because noise and interference influences the amplitude of the signal. ASK is not used for Wi-Fi.

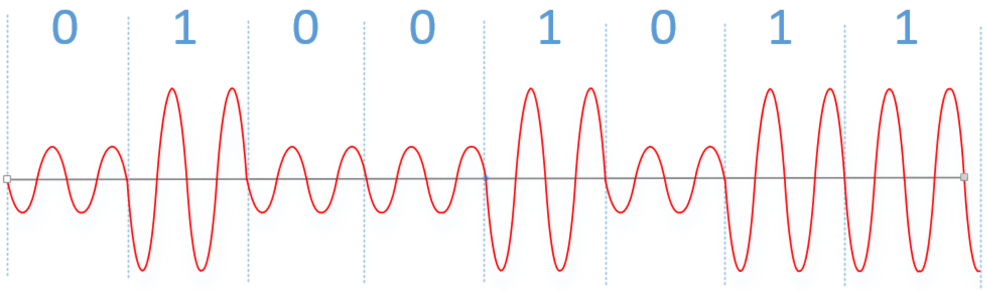


Figure 11 - ASK - Amplitude Shift keying example. 01001011 encoded in the carrier

## Frequency-shift keying

FSK – frequency-shift keying – vary the frequency to represent the binary data. FSK was used initially in Wi-Fi technologies but were impractical when faster communication was the goal.

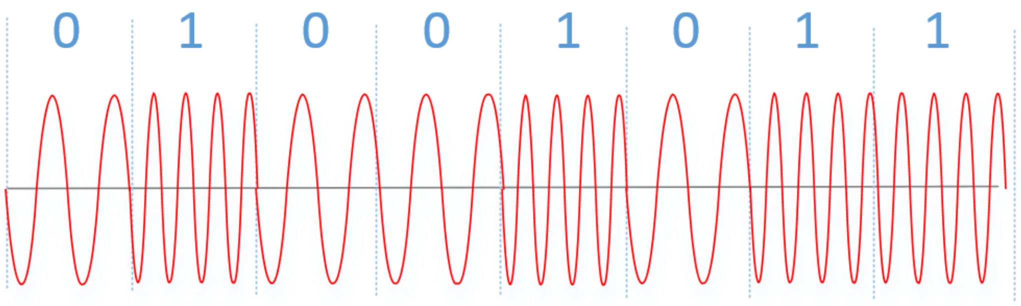


Figure 12 - FSK - Frequency Shift keying example. 01001011 encoded in the signal

## Phase-shift keying BPSK and QPSK

PSK – Phase shift-keying – varies the phase of the carrier to represent the binary data. As seen in the example in Figure 13 there is 180 degrees phase change in the signal when a binary "1" is transmitted and no phase change for a binary "0". This is called BPSK – Binary Phase-Shift Keying.

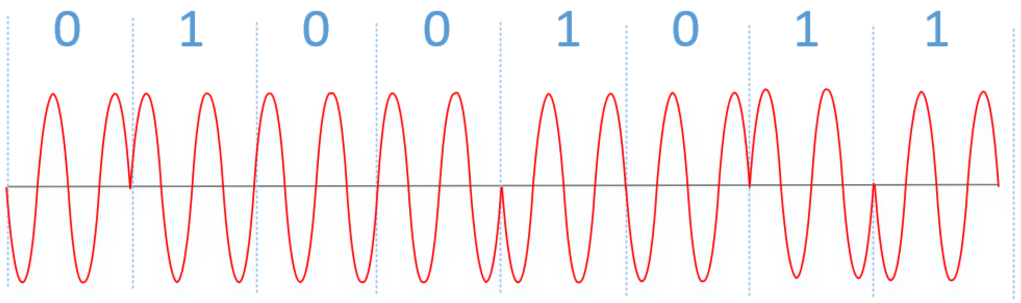
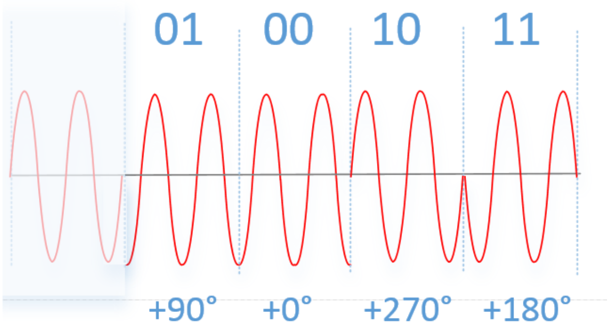


Figure 13 - PSK - Phase Shift keying. 0 degrees phase change equals "0" – 180 degrees phase change equals "1"

Phase shift keying is a highly complex technology and used in all W-Fi standards. Using multiple phase-shifts keying it is possible to increase the data rate. Instead of encoding bits individually the bits are encoded in groups, for example by using four different phase shifts it is possible to transmit two bit simultaneously. This is called QPSK – Quadruple Phase-Shift Keying.

| Bit combination | Signal phase shift |
|---|---|
| 00 | 0° |
| 01 | + 90° |
| 10 | + 180° |
| 11 | + 270° |



The data 01001011 is transmitted twice as fast in Figure 14 than in Figure 13.

Figure 14 - multiple phase shift keying

Multiple phase-shift keying is one of the technologies that increase bandwidth from the original 802.11-1997 to present day gigabit bandwidths. It should be mentioned though, that increasing the number of phase-shifts increase the sensitivity to noise.

## Summary of important abbreviations

| Abb. | Meaning | Explanation |
|---|---|---|
| ASK | Amplitude Shift Keying | Keying 0's and 1's by altering the radio carriers amplitude |
| BPSK | Binary Phase-Shift Keying | Keying 0's and 1's by altering the radio carriers phase 180 degrees |
| FSK | Frequency Shift Keying | Keying 0's and 1's by altering the radio carriers frequency |
| Hz | Hertz | Waves per second in a signal |
| IEEE | Institute of Electrical and Electronics Engineers | Standardization organization responsible for developing IEEE 802.11 standards |
| PSK | Phase Shift Keying | Keying 0's and 1's by altering the radio carriers phase |
| QPSK | Quadruple Phase-Shift Keying. | Keying two bits by altering the radio carriers phase 90 degrees between ‘00’,’01’,’10’ and ‘11’ |
| RF | Radio Frequency | Waves in the range from 3 KHz to 300 GHz |
| Wi-Fi | Wi-Fi | Wi-Fi is a brand name for IEEE 802.11 wireless network equipment |

## RF components

A successful radio transmission consists of a transmitter and a receiver tuned to the same frequency carrier signal and using the same modulation technique.  The purpose of wireless data communication is to move information between computers. The radio system moves bits of information on OSI layer 1 – the physical layer.

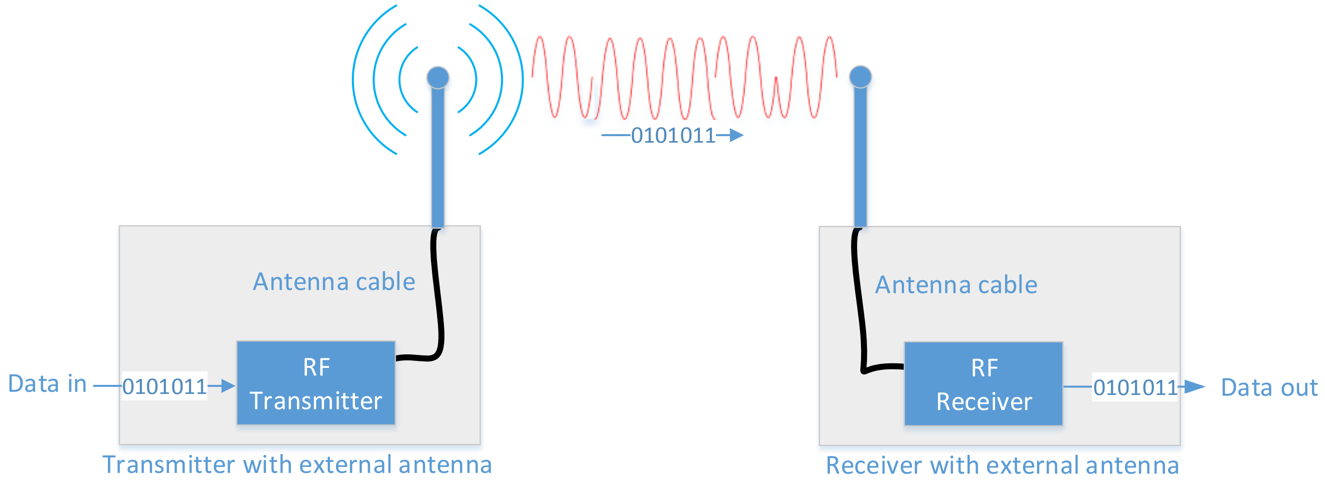


Figure 15 - A successful RF transmission of 0101011

## Transceivers

IEEE 802.11 RF radio systems have a transmitter and a receiver built together, this is called a transceiver. When both participating systems are using the same carrier frequency, it is only possible to transmit in one direction at a time – each system must wait to transmit until the other one finishes. This is called half duplex transmission. IEEE 802.11 describes half duplex RF systems.

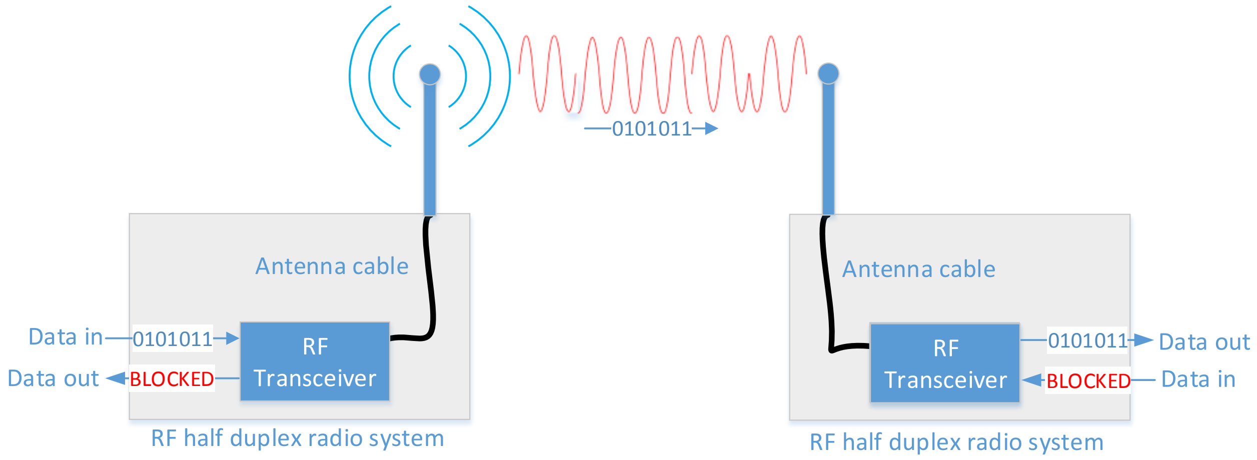


Figure 16 - RF transceiver system showing transmission from left to right

## Units of power and comparison

When designing 802.11 wireless networks, two major subjects are coverage and performance. To understand these, we need to look at some of the terms involved when designing and troubleshooting wireless networks.

### Watt

Watt is the basic unit of power. A typical FM radio station transmits kilowatts – kW – of power whereas a 802.11 network's maximum allowed power, according to regulations, is 0.1 Watt or 100 milliwatt – mW.

### Decibel

Decibel – dB – is used to compare values. Decibels are used to compare power levels when transmitting and receiving microwaves. When comparing the actual power transmitted by a microwave transmitter and the actual power received by the receiver. To calculate the decibel ratio between two signals the following formula is used:

Where $P_1$ is power level 1 and $P_2$ is power level 2.

$$decibels = 10 \times log_{10} \frac{P_1}{P_2}$$

If a transmitter is transmitting 0.1 watt and the receiver is receiving 0.00001 watt the relative difference in power is

$$10 \times log_{10} \frac{0{,}00001}{0{,}1} = -40dB$$

### dBm

A measurement unit which is often used is comparing a power level to 1 mW – 0.001 Watt – and expressing the decibel ratio between the measured signal and 1 mW. This is called dBm (m for milliwatt)

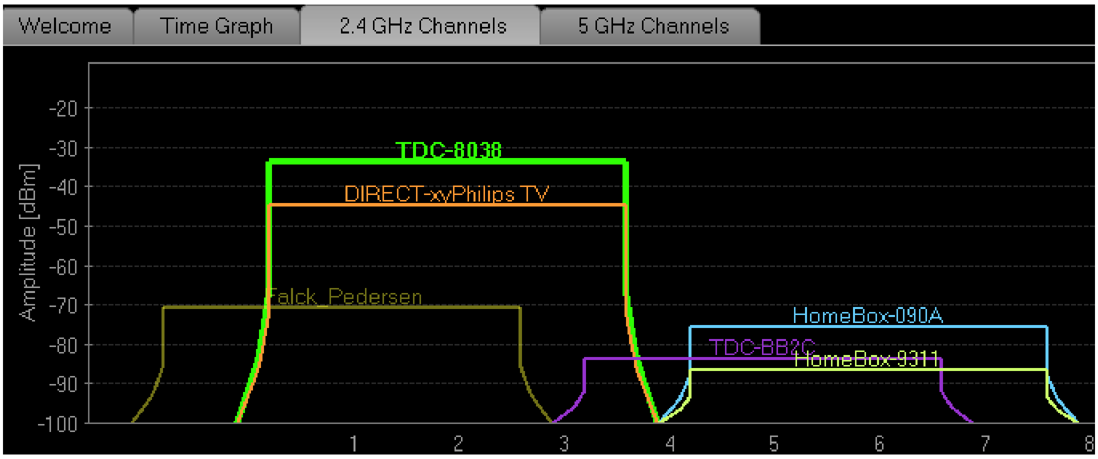


Figure 17 - Visible 2,4 GHz 802.11 network in a location (Recorded with the program inSSIDer)

As seen from Figure 17 my laptop is receiving the 802.11 network SSID TDC-8038 at approximately -33 dBm which corresponds to 0.0005 mW or 500 µW – microwatt.

$$10^{\left(\frac{-33dBm}{10}\right)} = 0{,}0005\ mW$$

The main reason for using decibels and dBm is to make it more convenient to compare very large and very small numbers. The list

| Network SSID | Amplitude [dBm] | Amplitude [mW] |
|---|---|---|
| **TDC-8038** | -33 | 0,0005 |
| **DIRECT-xyPhilips TV** | -44 | 0,00004 |
| **Falck Pedersen** | -71 | 0,00000008 |
| **HomeBox-090A** | -75 | 0,00000003 |
| **TDC-BB2C** | -83 | 0,000000005 |
| **HomeBox-9311** | -87 | 0,000000002 |

The logarithmic dBm scale makes it easier to compare power levels than comparing directly in Watts. Many people though argue that decibels are confusing – but data sheets and troubleshooting tools all use decibel, so a basic knowledge of dB and dBm are necessary.

### dBi

Decibel isotropic – dBi – is used to describe an antenna's gain compared to a perfect theoretical isotropic antenna. Isotropic means the antenna transmits an equal amount of energy in all directions. The sun is an isotropic transmitter, radiating power in all directions.

Often we would want an antenna to radiate more power in a particular direction. Just like the silver parabola in a flashlight directs the light in a particular direction.

Figure 18 - Netgear ANT24D18 antenna

The Netgear ANT24D18 antenna transmits 14 dBi more power in one direction than an isotropic antenna, and that would be a gain of 25 times.

$$10^{\left(\frac{14\ dBi}{10}\right)} = 25\ times$$

## SNR – Signal-to-Noise Ratio

RF background noise is mixed with the signals received making it difficult and sometimes impossible for the receiver to demodulate the data. SNR or signal-to-noise ratio is the ratio between the signal received by a receiver and the background noise expressed in dB. An SNR of 25 dB or better is normally considered a good signal and an SNR below 10 dB or lower is considered a very poor signal.

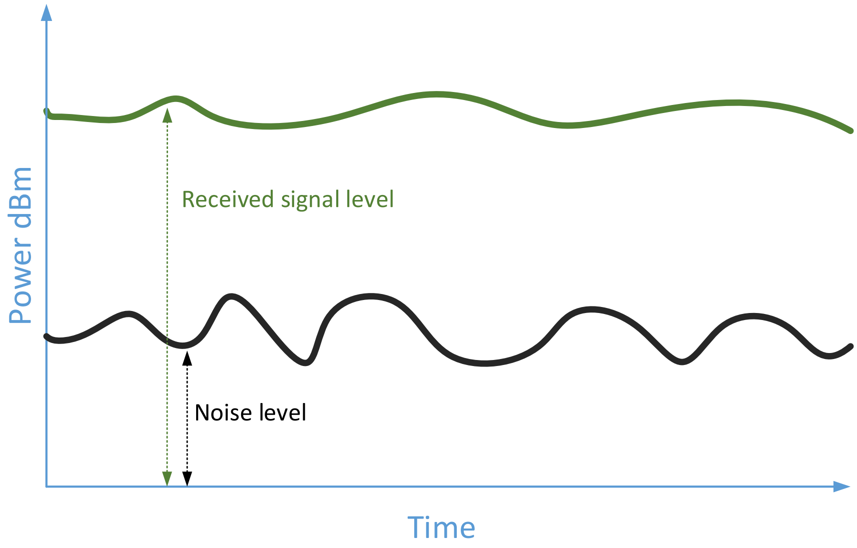


Figure 19 - SNR - Signal-to-Noice Ratio illustration

Many vendors of Wi-Fi equipment define signal quality as the signal-to-noise ratio – SNR.

## RSSI – Received Signal Strength Indicator

| Data Rate | Received signal |
|---|---|
| 54 Mbps | From -50 dBm |
| 48 Mbps | From -55 dBm |
| 36 Mbps | From -61 dBm |
| 24 Mbps | From -64 dBm |
| 18 Mbps | From -70 dBm |
| 12 Mbps | From -75 dBm |
| 9 Mbps | From -80 dB |
| 6 Mbps | From -86 dBm |

A Wi-Fi receiver keeps track of received signal strength to make decisions related to data rate and roaming between access points. The received signal strength indicator or RSSI is implemented differently by different vendors, but have the same function. When a Wi-Fi receiver discovers that the RSSI drops below a certain level it will change the modulation form to a modulation not so prone to errors, which means that the data rate will decrease. See the 802.11g example from the table to the right. When the received signal strength drops, the data rate is dropped allowing for a lower SNR but at the cost of speed.

In networks with multiple access-points a moving receiver can roam between the access-points based on the RSSI. It will connect to the access-point with the strongest signal on-the-fly.

# Antennas

An antenna is a transducer between a guided wave and a radiated wave. The wave is guided to or from the antenna in an electrical conductor like a coaxial cable

An antenna can be used in two ways:

1. When the transmitter sends an electrical RF signal to the antenna, the antenna generates RF waves that travel away from the antenna.
2. When the antenna absorbs incoming RF waves it generates an electrical RF signal to the receiver

Antennas are designed to specific frequency bands for example the 2.4 GHz Wi-Fi bands. There are two ways to increase the power output from an antenna. The first is to increase the power to the antenna, the other is to focus the output from the antenna in a specific direction using a directional antenna.

## Antenna types and antenna patterns

The most common antennas used in Wi-Fi networks are

- **Omnidirectional** antennas radiate RF in almost all directions. They are designed to give general coverage of an area; distributing the power equally.
    - Like a free hanging light bulb.
- **Semi directional** antennas radiate RF in a general direction, focusing the power to cover a specific area.
    - Like a street lamp focuses the light on the road.
- **Highly directional** antennas radiate RF in a specific direction focusing the power in a tight beam.
    - Like a spotlight focusing the light on the performer on stage.

### Omnidirectional antennas

Omnidirectional antennas are used to cover a circular geographical area with the antenna in the middle, and are designed in different qualities and with different gains. The radiation pattern or antenna pattern is a graphical representation of the radiation properties of a specific antenna type. See figure 6. Seen from the top of the antenna the radiation pattern would be donut-like.

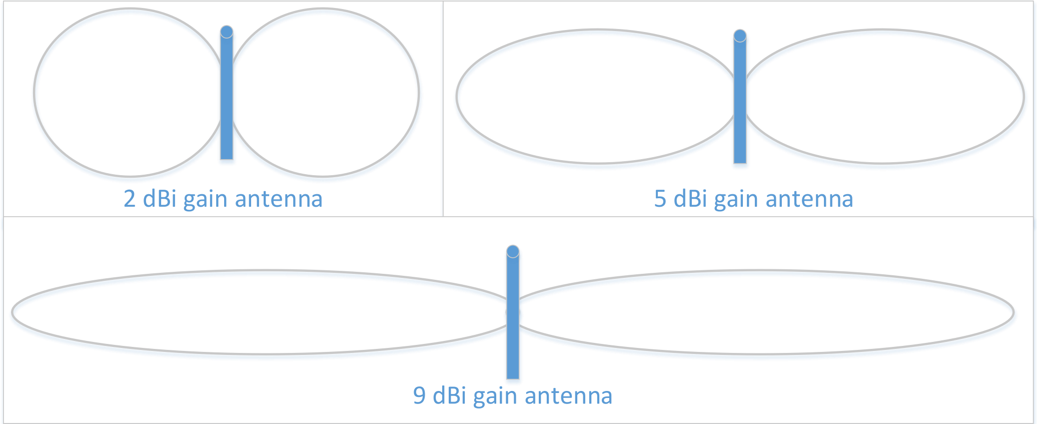


Figure 20 - Vertical view of three different antennas – seen from the side

An example of an actual antenna is the D-Link ANT24-0501C which is a 5 dBi indoor antenna for the 2.4 GHz RF band.

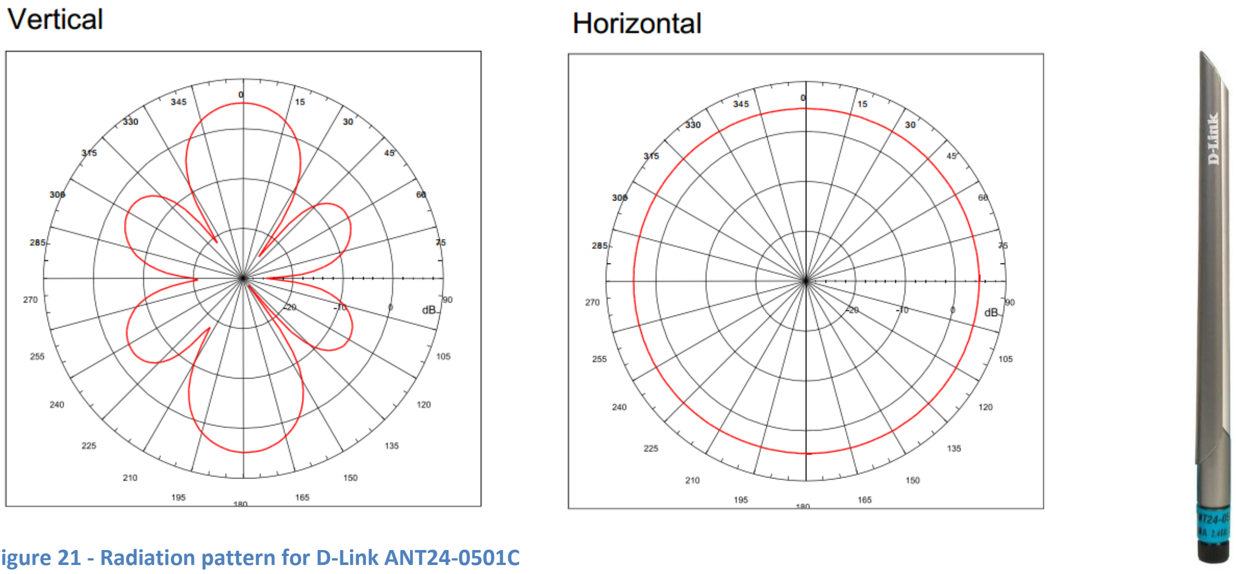
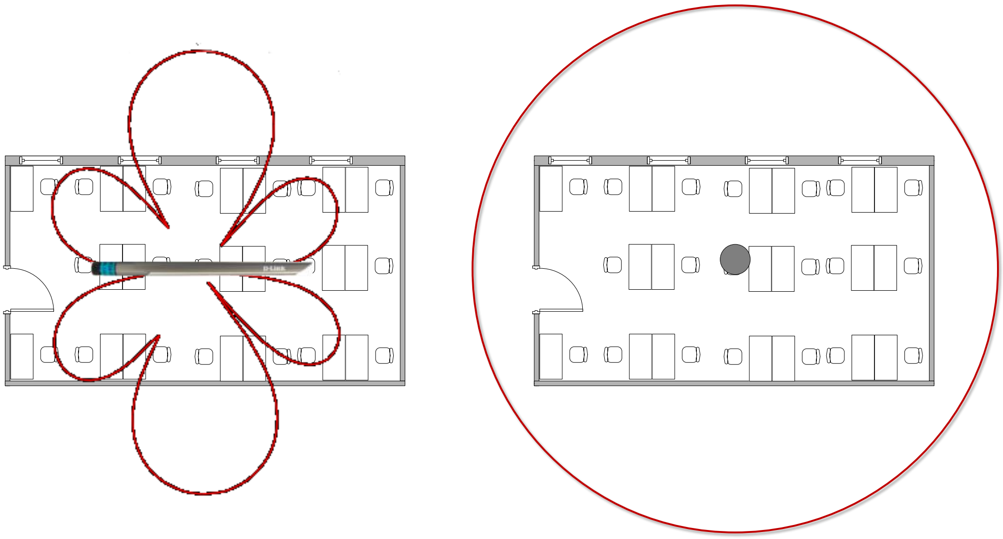


Figure 21 - Radiation pattern for D-Link ANT24-0501C

The vertical radiation pattern is a side view of the antenna showing the main-lobes at 0° and 180° reach 5 dBi. Remember 0 dBi was the perfect isotropic antenna. There are four unwanted side-lobes that reach -4 dBi. Remember decibels are logarithmic meaning that there are 9 dB's difference between the main-lobes and the side-lobes. 9 dB which is almost 8 times more power in the main-lobes.

The horizontal radiation pattern is a top view of the antenna showing an almost perfect circle at +5 dBi.

To cover an area like a big room with this antenna it would be crucial that the antenna was placed in its vertical position – standing up – and placed in the middle of the room – preferably at the same height as the devices to which it should connect. Antenna size exaggerated in Figure 22.



Horizontal – antenna lying down

Vertical – antenna standing up

Figure 22 - Omnidirectional antenna in vertical and horizontal position

## Semi directional antennas

Semi directional antennas radiate RF in a general direction, focusing the power to cover a specific area. Just like a street lamp focuses the light on the road. Several types of semi directional antennas are available. For example the antenna shown in Figure 23 with a gain of 8.8 dBi. As can be seen from Figure 24 in the radiation pattern the main-lobe at 90° is almost at 10 dB and the side-lobes are around -10 dB giving a difference of almost 20 dB which means that almost 100 times more power is radiated out of the main-lobe.

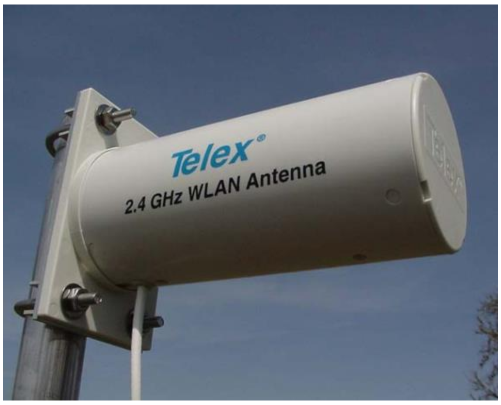


Figure 23 - Yagi antenna from Telex

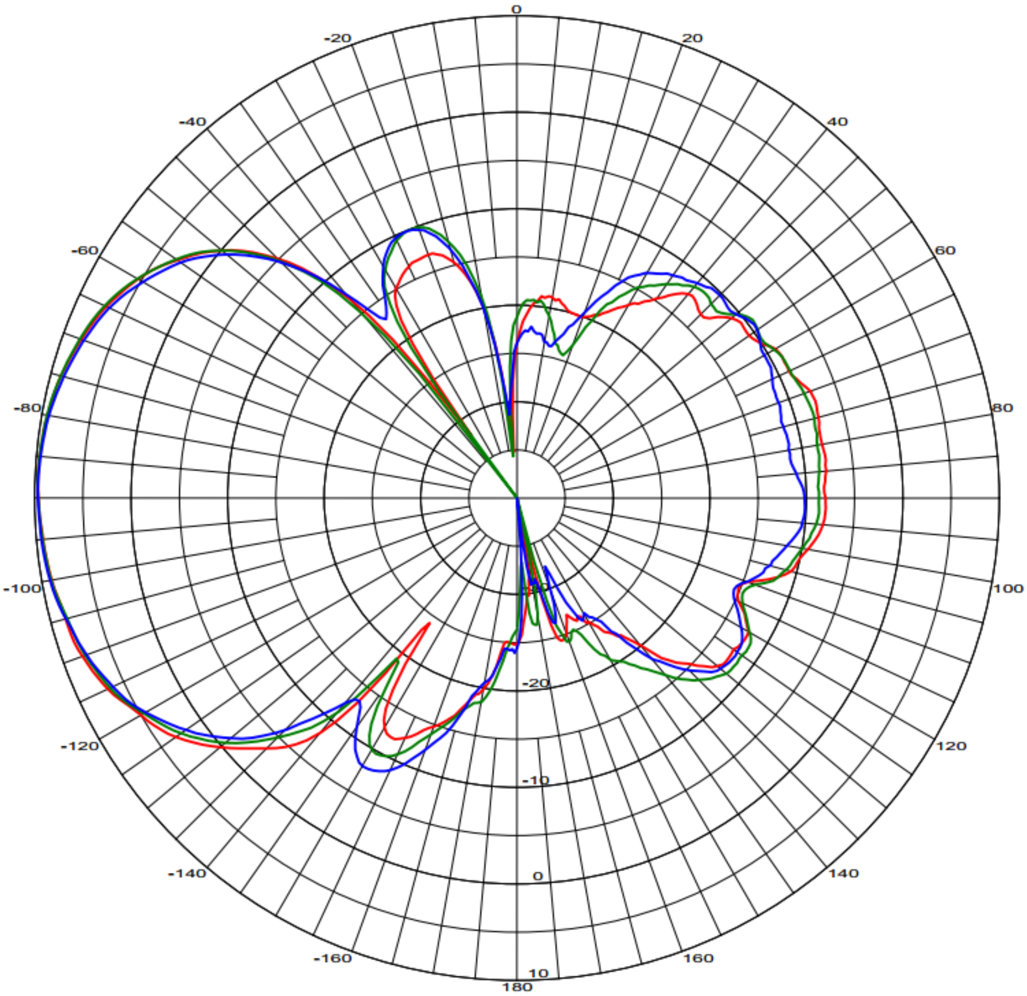


Figure 24 - Vertical radiation pattern from Telex antenna (Colours showing three different 2,4 GHz channels)

Semi directional antennas are often used as point-to-point connections, for example between two buildings

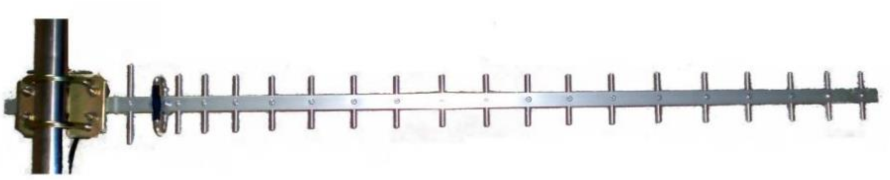


Figure 25 - 2,4 GHz "naked" Yagi antenna

### Highly directional antennas

Highly directional antennas such as parabolic and grid antennas offer higher gains, and are ideal for long-distance point-to-point communication as far as 58 km.

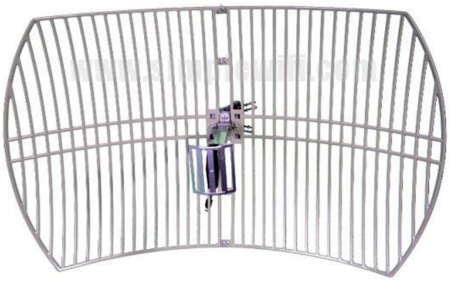


Figure 26 - 24 dBi grid antenna

## Summary of important abbreviations

| Abb. | Meaning | Explanation |
|---|---|---|
| dB | Decibel | Logarithmic unit of measurement in acoustics and electronics |
| dBm | Decibel milliwatt | Power relative to 1 mW |
| dBi | Decibel isotropic | Gain of an antenna compared to an ideal isotropic antenna. (Gain of the antenna) |
| SNR | Signal to noise ratio | The difference between a desired signal and the background noise. Often expressed in decibel |
| RSSI | Received Signal Strength indicator | Measurement of the power in a received radio signal |

# IEEE 802.11 Standards

In this chapter a number of the 802.11 standards will be introduced. They will be covered in depth in later chapters.

As discussed in session 1, ”history of IEEE 802.11 WLAN” numerous 802.11 standards have evolved over time. This section will summarize some of the important standards and their use.

The IEEE 802.11 working group consists of more than 250 wireless companies and has more than 450 active members. Different 802.11 task groups are in charge of revising and developing the original 802.11 standard. Each task group is given a letter from the alphabet adding to the confusion of the 802.11 alphabet soup.

| | Released | Frequency GHz | Data rates in Mbps |
|---|---|---|---|
| **IEEE 802.11** | Jun 1997 | 2,4 | 1 and 2 |
| **IEEE 802.11a** | Sep 1999 | 5 | 6 – 9 – 12 – 18 – 24 – 36 – 48 and 54 |
| **IEEE 802.11b** | Sep 1999 | 2,4 | 1 – 2 – 5,5 and 11 |
| **IEEE 802.11g** | Jun 2003 | 2,4 | 6 – 9 – 12 – 18 – 24 – 36 – 48 and 54 |
| **IEEE 802.11n** | Oct 2009 | 2,4 and 5 | 7,2 – 14,4 – 21,7 – 28,9 – 43,3 – 57,8 – 65 and 72,2<br>Or<br>15 – 30 – 45 – 60 – 90 – 120 – 135 and 150 |
| **IEEE 802.11ac** | Dec 2013 | 5 | Up to 866,7 |
| **IEEE 802.11ad** | Dec 2012 | 2,4 – 5 and 60 | Up to 6912 (Almost 7 Gbps) |

Table 1 – Some of the IEEE 802.11 task groups

At the time of writing the IEEE 802.11 working group had eight active task groups and 29 inactive task groups, giving a total of 37 different alphabet combinations.

## Original IEEE 802.11 standard

The original IEEE 802.11 standard – called IEEE 802.11-1997 – was published in June 1997 and supported 1 and 2 Mbps data rates. The standard defined use of the license-free 2.4 GHz ISM – Industrial, Scientific and Medical band, using two different radio transmitting principles called FHSS and DSSS.

### FHSS –Frequency Hopping Spread Spectrum

FHSS or frequency-hopping spread spectrum is a method – or modulation technique – of transmitting radio signals by rapidly switching between several frequency channels. FHSS will be covered later in this session.

### DSSS – Direct Sequence Spread Spectrum

DSSS or Direct Sequence Spread Spectrum is another radio frequency spread spectrum modulation technique used by IEEE 802.11-1997

## Data rate vs. throughput

Data rate is the speed in bps through the medium and throughput is the actual data transfer speed in bps. WiFi networks are half duplex meaning that there is only communication in one direction at any particular time. The throughput from one WiFi access point is shared between all associated WiFi clients. Experienced throughput is typically one half or less of the available data rate.

## 802.11b

IEEE 802.11b was released in 1999 and offers speeds of up to 11 Mbps as seen in Table 1. 802.11b is backward compatible with older legacy 802.11-1997 devices that use the DSSS modulation technique but not devices that use FHSS modulation. 802.11b operates in the unlicensed 2.4 GHz ISM band like the legacy 802.11-1997 and supports the data rates 1 – 2 – 5.5 and 11 Mbps. The 5.5 and 11 Mbps transmission rates are known as HR-DSSS or High-Rate DSSS.

The 2.4 GHz band is quite crowded with devices such as microwave ovens, cordless phones, Bluetooth devices and many other applications. Interference occurs when two or more devices transmit at the same time using the same frequencies, degrading the throughput.

## 802.11a

In the same year as 802.11b was released 802.11a was released. 802.11a uses three 100 MHz wide bands in the 5 GHz frequency space called the UNII bands or Unlicensed National Information Infrastructure bands. 802.11a offers speeds of up to 54 Mbps. See Table 1. 802.11a uses a modulation technique called OFDM.

The use of the 5 GHz UNII bands offer advantages over the crowded 2.4 GHz ISM band giving less interference with other devices and enabling higher throughput. 802.11a radios are not compatible with radios that use the 2.4 GHz ISM band as they use two different frequency bands.

It is possible to use 2.4 GHz and 5 GHz radios simultaneously in the same physical space without interference because they transmit in different frequency ranges. Most WiFi manufacturers offer dual-frequency equipment with both 2.4 GHz and 5 GHz radios and several 802.11 standards such as 802.11a/b/g/n radios.

### OFDM - Orthogonal Frequency-Division Multiplexing

OFDM or Orthogonal frequency-division multiplexing is a method of encoding the digital data on multiple carrier frequencies simultaneously; transferring the data in several parallel streams and thereby gaining higher data rates.

## 802.11g

IEEE 802.11g was released in 2003 and transmits in the 2.4 GHz ISM frequency band. The main goal of the 802.11g task group was to increase the bandwidth of the 802.11b standard and yet remain backward compatible with the original 2.4 GHz standards in the OSI physical layer called PHY's.

### 802.11g modulation techniques

The mandatory PHY's are ERP-DSSS/CCK and ERP-OFDM. ERP-DSSS/CCK gives backward compatibility with the earlier 2.4 GHz technologies (802.11 legacy and 802.11b) and ERP-OFDM gives date rates up to 54 Mbps.

#### *ERP-OFDM*

ERP-OFDM is the same as OFDM used in 802.11a. The only difference is the transmit frequency, where 802.11a transmits in the 5 GHz frequency band and 802.11g transmits in the 2.4 GHz band. Data rates of 6 – 9 – 12 – 18 – 24 – 36 – 48 and 54 Mbps are possible using this technology. Though IEEE only requires the data rates 6 – 9 -12 and 24 Mbps for a 802.11g radio. The remaining data rates are optional in the standard, but most 802.11g radios support them.

### *ERP-DSSS/CCK*

ERP-DSSS/CCK or Extended Rate Physical DSSS with Complementary Code Keying is the implementation of HR-DSSS from 802.11b for backward compatibility with 802.11 legacy and 802.11b, supporting the data rates of 1 – 2 – 5.5 and 11 Mbps.

### Implementation

With the support of ERP-DSSS/CCK and ERP-OFDM, radio vendors typically allow 802.11g access points to be configured in three main configurations.

### *B-Only mode*

When configured as a B-Only access point, the radio supports DSSS, HR-DSSS and ERP-DSSS/CCK technologies and operates as an 802.11b radio supporting data rates of 1 – 2 – 5.5 and 11 Mbps. The throughput of the access point would be the same as an older 802.11b radio.

### *G-Only mode*

Access points – AP – configured as G-Only will only communicate with clients using ERP-OFDM. Support for DSSS technologies is disabled.  G-Only mode supports data rates from 6 to 54 Mbps.

### *B/G mode*

B/G mode often called mixed mode supports both ERP-DSSS/CCK and ERP-OFDM covering data rates from 1 to 54 Mbps and supports the 802.11 legacy, 802.11b and 802.11g standards.

## 802.11n

The IEEE 802.11n standard allows for data rates up to 600 Mbps. 802.11n operates in both the 2.4 and 5 GHz frequency bands and uses several antennas to gain higher data rates.

### 802.11n modulation techniques

The mandatory PHY is called HT for High Throughput.  This uses OFDM and is backward compatible with 802.11a and 802.11g. 802.11n can also use HR-DSSS for backward compatibility with 802.11b.

802.11n will be covered further in a separate chapter.

## 802.11 legacy,a,b,g comparison

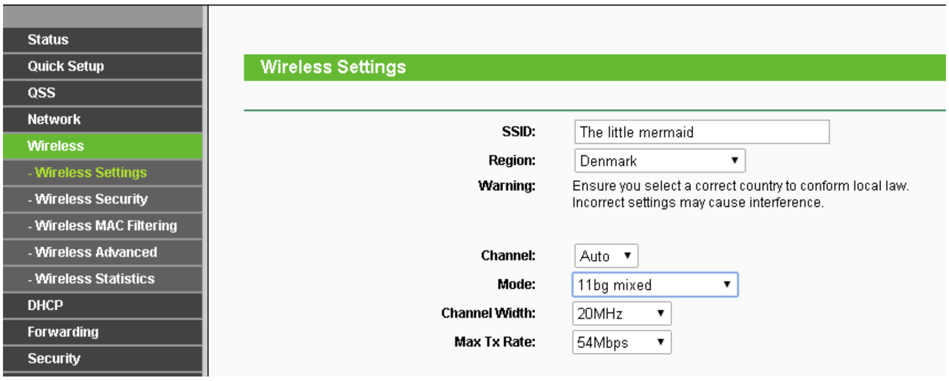
| | 802.11 Legacy | 802.11b | 802.11g | 802.11a | 802.11n |
|---|---|---|---|---|---|
| **Frequency** | 2,4 GHz ISM band | 2,4 GHz ISM band | 2,4 GHz ISM band | 5 GHz UNI-1, UNI-2 and UNI-3 bands | 2,4 GHz and 5 GHz |
| **Spread spectrum technologies** | FHSS or DSSS | HR-DSSS | ERP-OFDM and ERP-DSSS/CCK | OFDM | HT-OFDM 20 MHz and 40 MHz HT channels |
| **Data rates** | 1 and 2 Mbps | DSSS supports 1 and 2 Mbps<br>HR-DSSS supports 5,5 and 11 Mbps | ERP-DSSS/CCK supports 1 – 2 – 5,5 and 11 Mbps<br>ERP-OFDM at 6 – 12 and 24 Mbps are mandatory<br>ERP-OFDM at 9 – 18 – 36 and 48 Mbps are also supported | 6 – 12 and 24 Mbps are mandatory<br>Also supported are 9 – 18 – 36 – 48 and 54 Mbps | 6,5 to 72,2 Mbps are mandatory[2]<br>Also supported Up to 600 Mbps[2] |
| **Backward compatibility** | N/A | 802.11 legacy DSSS only | 802.11 HR-DSSS and 802.11 legacy DSSS | None | 802.11a, 802,11b, and 802.11g |
| **Ratified** | 1997 | 1999 | 2003 | 1999 | 2009 |

## 802.11d

The original 802.11 standard was written for compliance with the regional regulations in Europe, the United States, Japan and Canada. Regulations in other specific countries might define limitations on allowed frequencies and power transmit levels.

Information about country codes is delivered in fields inside frames called beacons and probe responses, allowing 802.11 compliant devices to adapt to regional regulations.

[2] Only bandwidth range shown. To see all data rates see 802.11n chapter



Wireless Settings

SSID: The little mermaid

Region: Denmark

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Channel: Auto

Mode: 11bg mixed

Channel Width: 20MHz

Max Tx Rate: 54Mbps

Figure 27 – WiFi access point set to regional regulations in Denmark

## 802.11e

In the original 802.11 standard, no consideration was made to prioritize traffic from time-sensitive applications such as VoIP – Voice over IP – also known as VoWLAN and VoWiFi– Voice over Wireless LAN and Voice over WiFi. The most used terminology is VoWiFi. 802.11e defines QoS – Quality of Service – for WiFi networks.

Traffic from applications carrying traffic such as voice, audio and video has a low tolerance for latency and jitter and requires higher priority over standard application data traffic, to ensure good voice and video quality.

The IEEE 802.11e amendment defines the layer 2 MAC methods to meet the QoS requirements for time-sensitive applications in WLAN networks.

### Original WiFi without QoS

In the original 802.11 standard two methods of access of the half-duplex medium is defined.

1. The default method called DCF – Distributed Coordination Function – is a random method determining who gets to transmit on the wireless medium next.
2. PCF – Point Coordination Function – where the access point takes control of the medium and polls the clients. This method was never adopted by WLAN vendors.

### WiFi with 802.11e QoS

802.11e defines enhanced medium access methods to support QoS called HCF – Hybrid Coordination Function – which has two different media access methods to provide QoS

1. EDCA – Enhanced Distributed Channel Access – which is an extension to the original DCF where the prioritization is based on the OSI upper-layer protocols such as RTP – Real-time Transport Protocol – carrying voice or video. EDCA ensures that the prioritized packets are transmitted in a timely manner.
2. HCCA – Hybrid Coordination Function Controlled Channel Access – is an extension of the original PCF. HCCA gives the access point the ability to prioritize certain client stations, giving them the chance to transmit before others. Like PCF the HCCA medium access method was never adopted by WLAN vendors.

## Other 802.11 standards

Beyond those standards mentioned there are several more standards. Noteworthy are 802.11ac and 802.11ad; defining VHT – Very High Throughput – offering higher data rates than 802.11n. The 802.11ac will offer data rates up to 1 Gbps and 802.11ad will deliver data rates up to 7 Gbps. 802.11ac is also known as WiGig using the three frequency bands 2.4, 5 and 60 GHz.

Figure 28 - Wifi alliance WiGig symbol

## Summary

There are numerous 802.11 standards, each with their own specific functionality, developed since 1997. The primary standards are covered in this chapter. Each standard will be covered in depth in the remainder of this material. Remember the 802.11 standard only covers the physical and data-link layer of the OSI model, which are called the PHY and MAC layer.

# Wireless networks and Spread Spectrum Technologies

In this chapter you will learn about the following

- Industrial, Scientific and Medical – ISM – bands
- Unlicensed National Information Infrastructure – UNII – bands
- Narrowband and spread spectrum technologies
- Frequency Hopping Spread Spectrum - FHSS
- Direct Sequence Spread Spectrum – DSSS
- Orthogonal Frequency Division Multiplexing – OFDM
- Adjacent, nonadjacent and overlapping channels
- Throughput vs. bandwidth
- Communication resilience

## ISM – Industrial, Scientific and Medical bands

The IEEE 802.11 legacy, 802.11b, 802.11g and 802.11n all define communication in the frequency range between 2.4 GHz and 2.4835 GHz. This frequency range is one of three frequency ranges known as the industrial, scientific and medical bands or ISM bands. The frequency range of the ISM bands is:

- Industrial band: 902 – 928 MHz ( 26 MHz wide )
- Scientific band: 2.4 – 2.5 GHz ( 100 MHz wide )
- Medical band: 5.725 – 5.875 GHz ( 150 MHz wide )

The ISM bands are defined by ITU telecommunication sector ITU-T in the United States. Their usage in other countries may be different due to local regulations. All three bands are license free bands without any restrictions of which kind of equipment is used. It would be perfectly legal to use medical equipment operating in the 2.4 GHz scientific band.

### 900 MHz ISM band

The 900 ISM band is 26 MHz wide and spans from 902 MHz to 928 MHz. This band is not suitable for wireless networks because of the low frequency. The higher the frequency used, the higher the possible bandwidth. The 900 MHz ISM band has been used for wireless home telephones, baby monitors and headphones.

This band is not used in the IEEE 802.11 standards.

### 2.4 GHz ISM band

The 2.4 GHz ISM band is the most common band used for wireless network communication. The 2.4 GHz band is 100 MHz wide and spans from 2.4 GHz to 2.5 GHz. The 2.4 GHz band is the most used and most crowded ISM band. A majority of WiFi networks use the 2.4 GHz ISM band.

- 802.11 legacy using FHSS or DSSS radios
- 802.11b using HR-DSSS radios
- 802.11g using ERP radios
- 802.11n using HT radios.

Beside WiFi the 2.4 GHz ISM band is used for many purposes such as microwave ovens, cordless phones, wireless video cameras, Bluetooth and Zigbee.

### 2,4 GHz channels

The 2.4 GHz IEEE 802.11 band is divided into 14 separate channels, as seen in Figure 29. Although the 2.4 GHz ISM band is divided into 14 channels, local authorities designates which channels are allowed to be used.

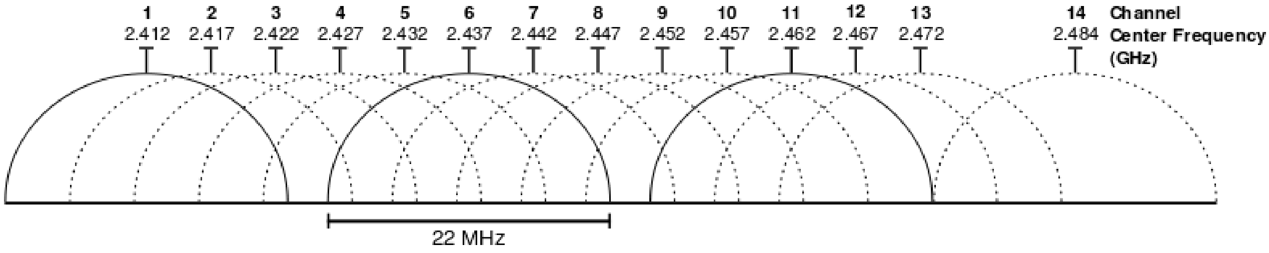


Figure 29 – 2.4 GHz 802.11 WiFi channels

As seen from Figure 29 the channels are overlapping each other. Each channel is 22 MHz wide, but the channels' centre frequencies only differ by 5 MHz. The most used channels are Channel 1, 6 and 11 because they don't overlap, thereby avoiding interference between these channels.

- If two neighbouring access-points in close proximity of each other use the same channel they would interfere with each other, and have to share the frequency, resulting in degraded throughput.
- If one access-point uses Channel 4 and the other access-point uses Channel 6, some of the signal would interfere resulting in degraded throughput.
- If one access-point instead uses Channel 1 and the other access-point uses Channel 6 or 11, the two access-points do not interfere with each other, and each access-point has a higher throughput.

### 5.8 GHz ISM band

The 5.8 GHz ISM band is 150 MHz wide and spans from 5.725 GHz to 5.875 GHz. As with the other ISM bands the 5.8 GHz band is used for a lot of different purposes and consumer products, just like the other ISM bands. The 5.8 GHz ISM band is not used for 802.11 WiFi. The band used for 802.11 5 GHz WiFi is the UNII band.

## UNII – Unlicensed National Information Infrastructure bands

The 802.11a WiFi amendment designated the use of three 5 GHz bands. These frequency bands are known as the UNII bands.

| Band | Name | Frequency | Channels | Channel numbers |
|---|---|---|---|---|
| UNII-1 | Lower | 5,15 – 5,25 GHz | 4 | 36, 40, 44, 48 |
| UNII-2 | Middle | 5,25 – 5,35 GHz | 4 | 52, 56, 60, 64 |
| UNII-2 extended | Extended | 5,470 – 5,725 GHz | 11 | 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 |
| UNII-3 | Upper | 5,725 – 5,825 GHz | 4 | 149, 153, 157, 161 |

The three UNII bands are locally regulated by countries/regions regarding channels, allowed users and maximum power levels. To avoid interference with RADAR's and military applications, the use of DFS – Dynamic Frequency Selection – and TPC – Transmit Power Control – capabilities are used by 802.11 devices.

The 5 GHz channels are non-overlapping, giving more channels than the 2.4 GHz band.

## Narrowband and Spread Spectrum

This section covers two major radio frequency transmission principles: narrowband and spread spectrum.

### Narrowband transmission

Narrowband transmission uses very little frequency bandwidth to transmit a message. See Figure 30. Narrowband transmission is used to transmit information – such as an FM radio station – on a specific frequency. Narrowband transmitters typically use a high power transmitter. Narrowband transmission is susceptible to intentional jamming or unintentional interference. The use of narrowband radio transmission is regulated by local authorities to avoid interference.

### Spread spectrum transmission

Spread spectrum transmission uses more bandwidth than necessary to transmit the data it is carrying. See Figure 30. A spread spectrum radio spreads the data between the frequencies that it is using. This is less susceptible to interference because many frequencies need to be jammed or interfered with to disrupt communication. Spread spectrum radio transmitters – such as WiFi networks – typically use low power transmitters.

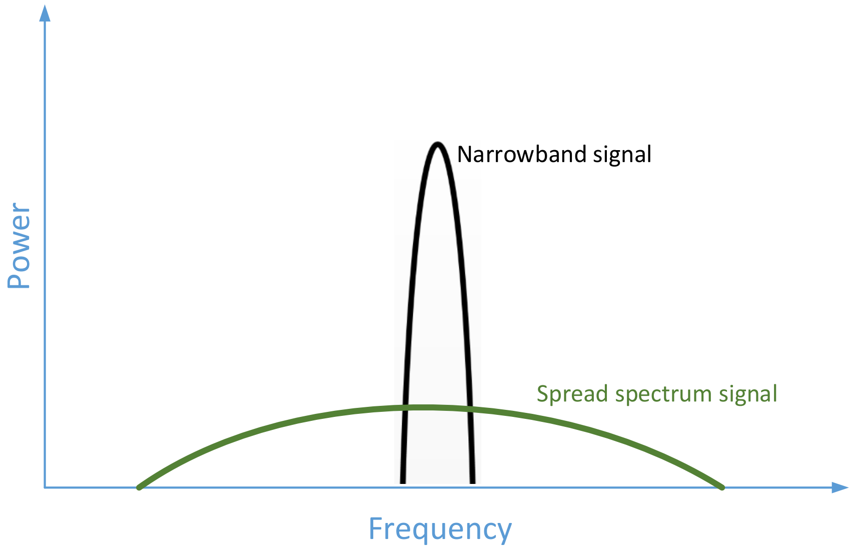


Figure 30 - Narrowband and spread spectrum signal

## Multipath interference

One of the problems with RF communication is multipath interference, where the same signal from the transmitter is reflected one or more times between the transmitter and the receiver. See Figure 31. The same signal from the transmitter is received more than once and the reflected signals are interfering with the direct path signal. Spread spectrum transmission is less susceptible to multipath interference than narrowband transmission, as different frequencies give different interference patterns.

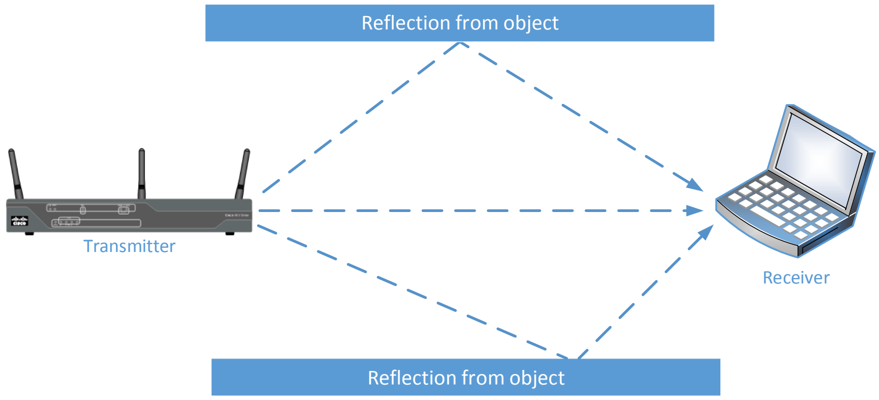


Figure 31 - Multipath interference

When multipath interference disrupts communication in 802.11 networks, longer symbols are used to represent the transmitted data, resulting in lower data rates.

With 802.11n the use of more than one antenna and other technologies explained in Chapter 18, can actually benefit from the effects of multipath.

## Transmission methods

The evolution of IEEE 802.11 technologies since its introduction in 1997 has primarily been increasing the data rates. Different transmission methods have been developed and used in different generations of 802.11 technologies.

| | | Used since | Data rates |
|---|---|---|---|
| **FHSS** | Frequency Hopping Spread Spectrum | 1997 | 1 to 2 Mbps |
| **DSSS** | Direct Sequence Spread Spectrum | 1997 | 1 to 11 Mbps |
| **OFDM** | Orthogonal Frequency Division Multiplexing | 1999 | 1 to 600 Mbps |

## FHSS – Frequency Hopping Spread Spectrum

In FHSS the transmitter transmits a small amount of data on one frequency then hops to another frequency and transmits the next small amount of data. FHSS transmits data using a predefined hopping sequence between a given set of frequencies in a spread spectrum. The hop sequence is repeated again and again. If multipath interference causes one frequency to fail, the next hop frequency would probably be okay.

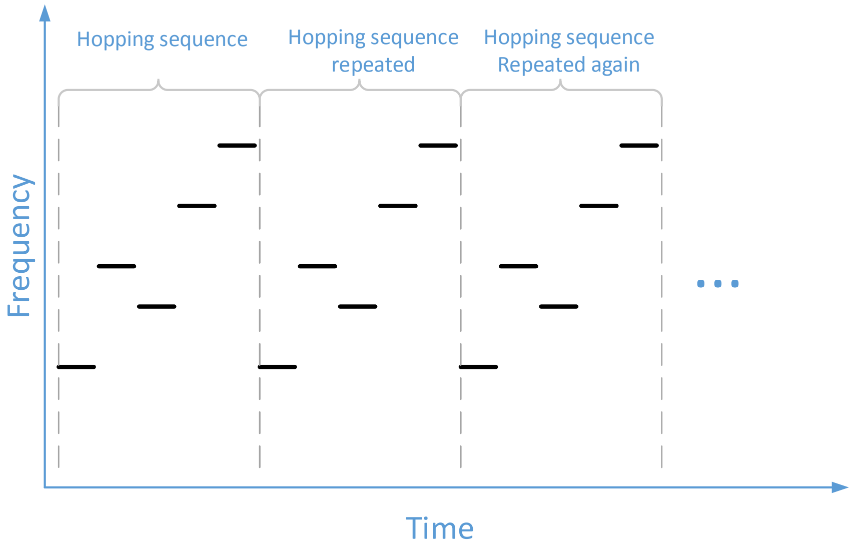


Figure 32 - Illustration of frequency hopping spread spectrum

FHSS is used in 802.11 legacy and is superseded by DSSS and OFDM in newer IEEE standards.

## DSSS – Direct Sequence Spread Spectrum

DSSS transmits on all frequencies in the channel simultaneously where FHSS transmitted on one frequency at a time.  DSSS transmits the same information on a wider frequency spectrum, making the transmission more resilient to interference. The receiver is still able to interpret the received data correctly even though some of the received information in the spectrum is garbled.

## OFDM – Orthogonal Frequency Division Multiplexing

OFDM uses a technique where 52 separate, closely spaced frequencies are used simultaneously to transmit data. OFDM transmits 52 parallel low data rate signals that added together gives high data rates. Because of the low data rates OFDM is more resilient to multipath interference than FHSS and DSSS. Remember that OFDM adds all separate channels data rate which in total gives a high data rate.

## 802.11 Topologies

The main component of an 802.11 wireless network is the radio cards, which are referred to as a station or STA. The radio card – STA – can reside in an access-point or be used in a client. The 802.11-2007 standards define three different 802.11 topologies known as service sets, which describe how these radio cards may be used to communicate with each other. These three service sets are known as BSS – Basic Service Set, ESS – Extended Service Set – and IBSS – Independent Basic Service Set. Radio cards are half duplex devices, allowing only one radio card transmitting at any given time. If more than one radio transmits on the same channel at the same time, the signals would interfere with each other and disrupt communication.

### Access Points

Access points or AP's are often used to build wireless communication networks, and are often compared to switches in cabled Ethernet networks. There are some similarities between Ethernet switches and 802.11 access points, as presented in the following.

Figure 33 - Access point symbol

Often access points are used to connect a wireless network to a wired Ethernet network. See Figure 34.

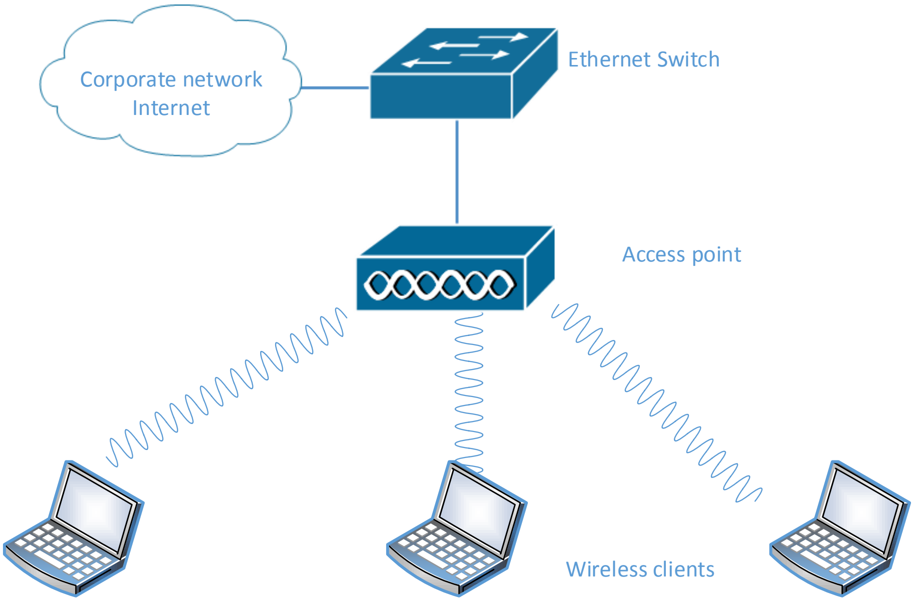
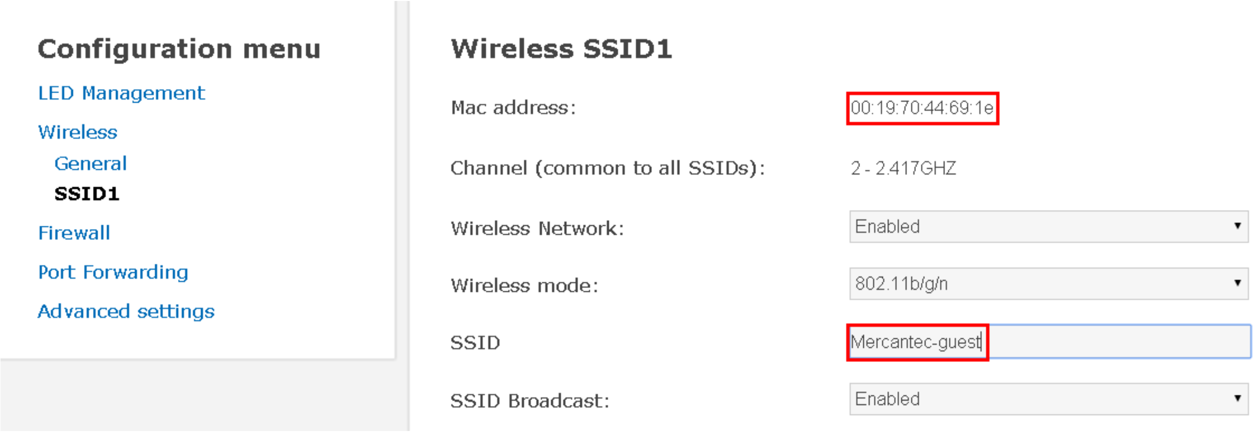


Figure 34 - Access point in corporate network connecting wired and wireless topologies

## SSID – Service Set Identifier

The SSID – Service Set identifier – is a logical name used to identify 802.11 wireless networks. The radio cards use the SSID to identify each other. The SSID is a configurable setting on all radio cards and can consist of 1 to 32 bytes. SSID are often human readable such as "Mercantec-Guest".



Wireless SSID1

Mac address: 00:19:70:44:69:1e

Channel (common to all SSIDs): 2 - 2.417GHZ

Wireless Network: Enabled

Wireless mode: 802.11b/g/n

SSID Mercantec-guest

SSID Broadcast: Enabled

Figure 35 - Access point configured to SSID "Mercantec-guest"

Access points normally broadcast the SSID – which is enabled in Figure 35 – but most access points have the ability to cloak the SSID keeping the SSID hidden from unauthorized users. Hiding the SSID is a weak security attempt, as it is possible for unauthorized users to see the SSID with a network protocol analyser.

## BSSID – Basic Service Set Identifier

Besides the SSID the access point is uniquely identified by its BSSID – Basic Service Set Identifier – which is its unique MAC address. See Figure 35.

The SSID can be seen as the service name users can use to join a wireless network, whereas the BSSID is the physical address clients use to exchange data packets with the access point. See Figure 36.

## BSS – Basic Service Set

The BSS – Basic Service Set – is the most used service set. A BSS consists of one access point with one or more clients called stations. Client stations join the wireless AP – Access Point – and start communicating through the AP. Client stations that are a member of a BSS are called associated.

In BSS mode the client stations can exchange packets with the AP. In order for two client stations to exchange packets, the packets must be transmitted through the AP.

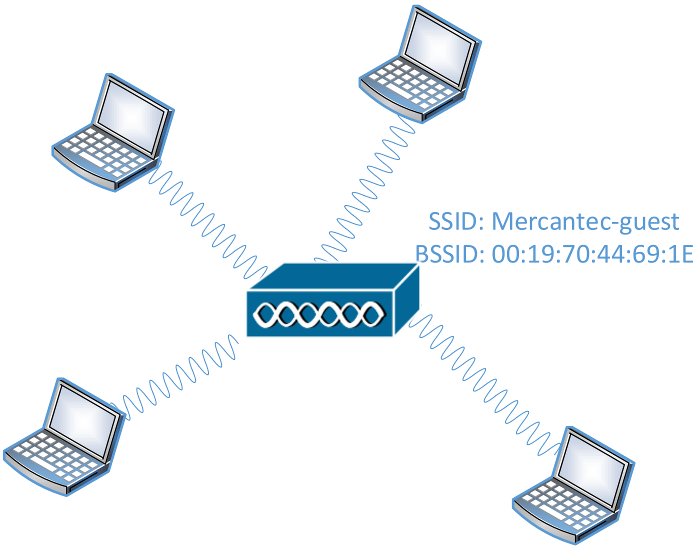


Figure 36 - A Basic Service Set (BSS)

## ESS – Extended Service Set

An ESS – Extended Service Set – is one or more BSS – Basic Service Set – connected by a distribution system, which is typically the corporate Ethernet. Usually an ESS is a collection of access points sharing the same SSID in one or more buildings, covering a large physical area such as a company or a hospital.

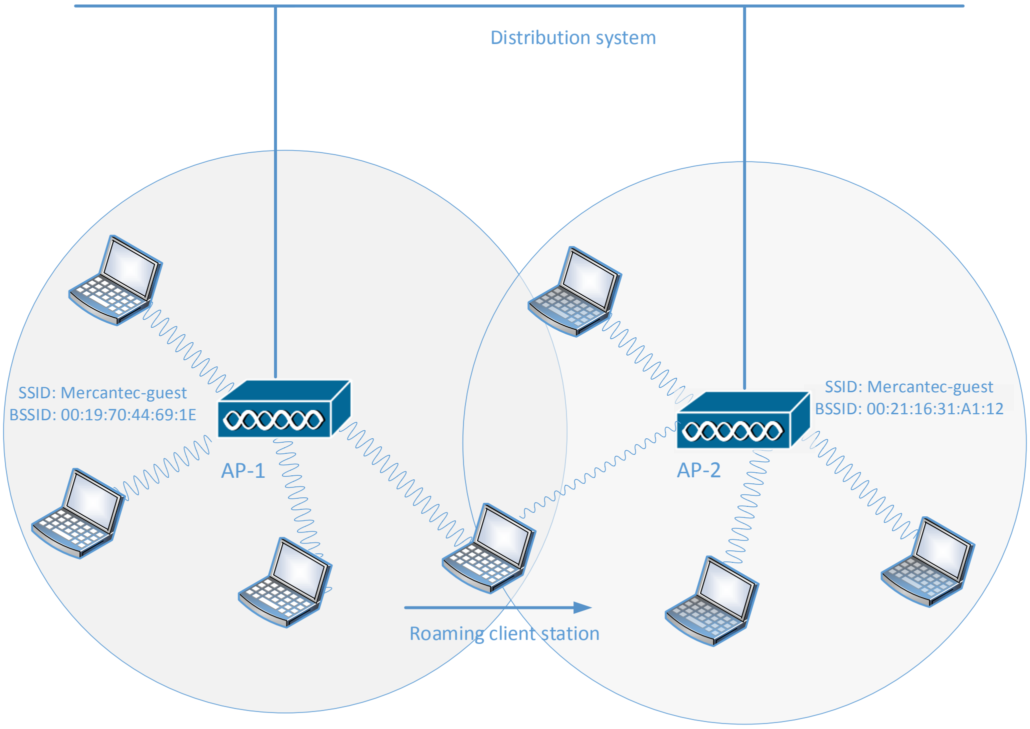


Figure 37 - Extended Service Set (ESS) with client station roaming from AP-1 to AP-2

The roaming client station in Figure 37 is moving away from AP-1 towards AP-2. When the signal strength from AP-2 exceeds the signal strength from AP-1, the client station will try to associate with AP-2. The client station recognizes that AP-1 and AP-2 are two different AP's because they have different BSSID's even though they share the same SSID. The network name of an ESS is called an ESSID - Extended SSID.

## IBSS – Independent Basic Service Set

In IBSS mode there is no access point. The client stations associate to each other. This mode is also called ad-hoc mode, and can be used to connect two or more client stations to each other, when no access point is available.

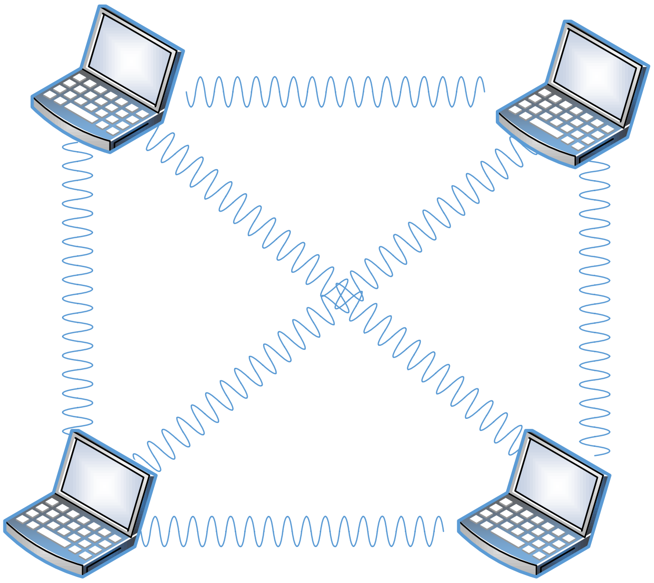


Figure 38 - Independent Basic Service Set (IBSS) - Client stations associate directly with each other

As with the other service sets only one transmitter at a time can be transmitting. The client stations must contend for the half duplex medium, enabling only one transmitting client station at any one time.

### MBSS – Mesh Basic Service Set

The 802.11s-2011 defines a fourth service set known as MBSS – Mesh Basic Service Set. When access points support MBSS it is possible to build a wireless distribution network where wired networks are inaccessible.

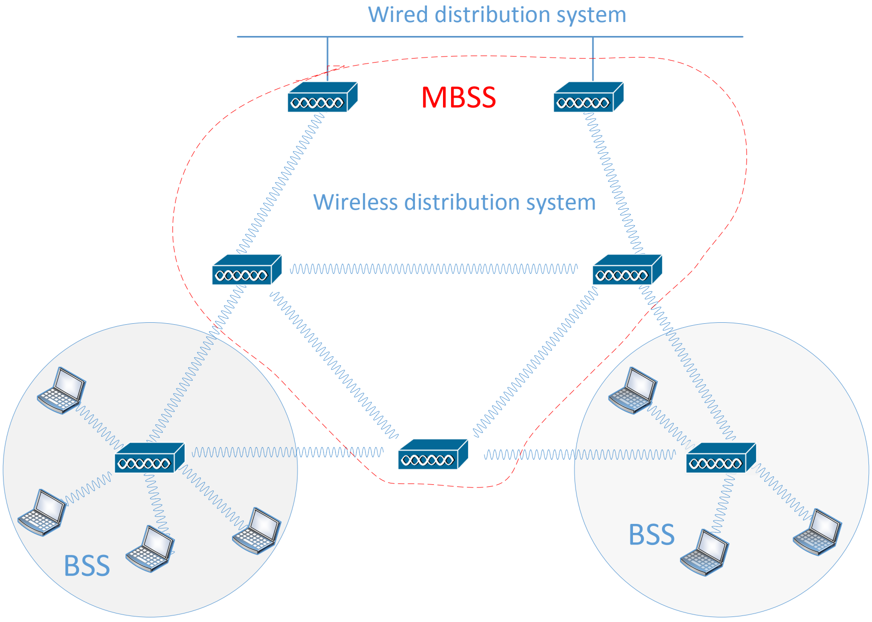


Figure 39 - MBSS network connect two BSS to the wired distribution system

## 802.11 Medium Access

802.11 wireless networks use a MAC – Medium Access Control – called CSMA/CA or Carrier Sense Multiple Access with Collision Avoidance to avoid collisions if more than one radio is transmitting simultaneously.

### CSMA/CA

CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance – defines rules to provide controlled and efficient access to the network medium, the radio waves.

#### CS – Carrier Sense

An 802.11 radio will sense if the medium is busy before it is transmitting. This is called Carrier Sense.

#### MA – Multiple Access

Multiple Access ensures that all radios get a fair chance to transmit.

#### CA – Collision Avoidance

Collision Avoidance means that only one radio will be permitted to transmit at any given time. If two stations transmit simultaneously a collision occurs and the signal will be garbled, and the radio has to retransmit the packet.

### Collision detection

As mentioned 802.11 radios are not capable of receiving while transmitting and cannot detect a collision when it occurs. To guarantee delivery of transmitted unicast frames, a frame is only considered delivered when an acknowledged – ACK – frame is received from the receiver. See example in Figure 40.

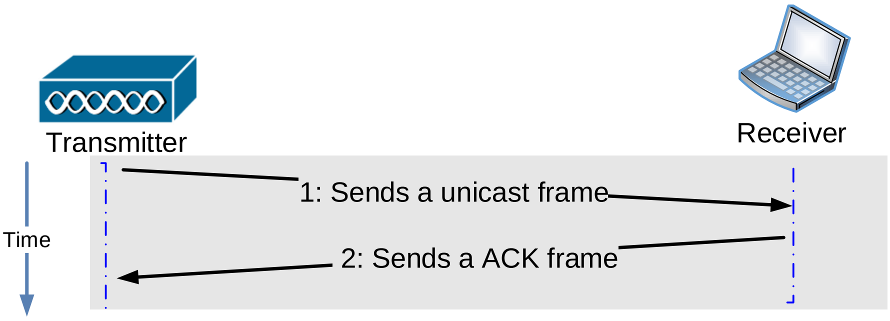


Figure 40 – Example of transmission of unicast frame from Access Point to Client Station

The majority of 802.11 frames must be acknowledged by an ACK frame to ensure successful transmission. If any portion of a frame is corrupted the CRC – Cyclic Redundancy Check – checksum will not match and the receiver will not acknowledge the frame. The transmitter will retransmit the frame if it does not receive an ACK frame.

If no proof of delivery is provided, the original radio card assumes there was a delivery failure and retransmits the frame.

## DCF – Distributed Coordination Function

DCF or Distributed Coordination Function is the fundamental access method of 802.11 communications, and consists among others of IFS – Interframe Space – and a random back-off timer.

The main purpose of DCF is to ensure only one radio is transmitting at any given time, on the half-duplex medium.

### IFS – Interframe space

The interframe space is a time period that exists between transmissions of wireless frames. There are six types of interframe space, each with its own time period. The interframe spaces are listed from shortest to longest, in the table.

| | Name | Priority | Duration |
|---|---|---|---|
| **RIFS** | Reduced Interframe Space | Highest | Shortest |
| **SIFS** | Short Interframe Space | Second | . |
| **PIFS** | PCF Interframe Space | Middle | . |
| **DIFS** | DCF Interframe Space | Lowest | . |
| **AIFS** | Arbitration Interframe Space | Used by QoS stations | . |
| **EIFS** | Extended Interframe Space | Used with retransmissions | Longest |

The actual interframe space time length varies depending on the transmission speed of the network. The two most common interframe spaces are SIFS and DIFS.

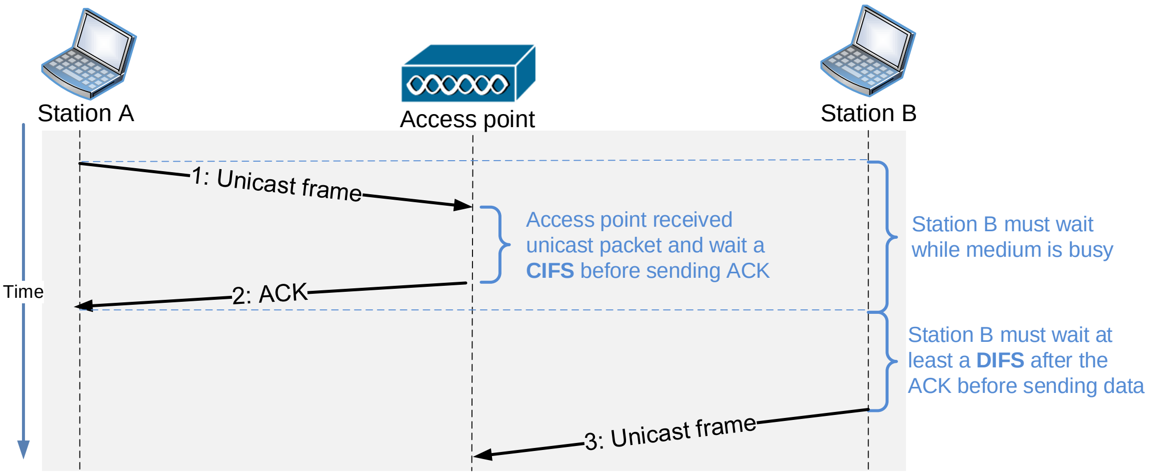

Station A
Access point
Station B
Time
1: Unicast frame
Access point received unicast packet and wait a CIFS before sending ACK
Station B must wait while medium is busy
2: ACK
Station B must wait at least a DIFS after the ACK before sending data
3: Unicast frame

Figure 41 - SIFS and DIFS interframe space.

In Figure 41 station A transmits a unicast data frame to the access point while station B is waiting while the medium is busy. The access point received the frame from station A without errors and acknowledges the reception after waiting a CIFS interframe space, by sending an ACK frame to station A. Station B must wait at least a DIFS interframe space and check the medium is free before transmitting its own unicast data frame.

### Random back-off timer

When more radios contend for the medium they use a random period of time after the DIFS interframe space, before initiating a transmission. The station with the shortest random back-off time will start transmitting if the medium is free.

The random back-off timer minimizes the chance of two or more stations transmitting at the same time, although it does not guarantee against collisions. If the transmitting stations do not receive an ACK frame acknowledging their frame transmission, they start the carrier sense all over and try to transmit the frame again.

The random back-off timer gives all stations a fair chance of getting some air time.

## HCF – Hybrid Coordination Function

The IEEE 802.11e quality of service – QoS – amendment added a new coordination function to 802.11 medium contentions, known as HCF – Hybrid Coordination Function. While the random back-off timer gives all stations a fair chance of getting some air time, there is no priority for stations that have high priority traffic such as voice or video.

Two enhancements are introduced: EDCA – Enhanced Distributed Channel Access – and HCCA – HCF Controlled Channel Access.

### EDCA – Enhanced Distributed Channel Access

EDCA or Enhanced Distributed Channel Access is a wireless media access method that provides differentiated access for stations using eight UP – User Priority – levels.

EDCA defines four access categories based on the UP’s – User Priorities

| UP | Access Category | Used for | Priority |
|---|---|---|---|
| **AC_VO** | Voice | Highest priority such as VoIP | Highest |
| **AC_VI** | Video | High priority traffic such as video | Second highest |
| **AC_BE** | Best Effort | Medium priority such as business critical | Second lowest |
| **AC_BK** | Background | Low priority such as WEB traffic | Lowest |

### *EDCA and priority tags*

When using 802.11e EDCA, traffic entering the queue system is queued based on UP – User Priority – as seen in Figure 42. The scheduler selects the order in which frames are transmitted. The 802.11e amendment does not specify in which order the queues should be emptied, but normal operation would be transmitting all frames in the AC_VO queue before transmitting frames from the AC_VI queue ensuring a good voice quality.

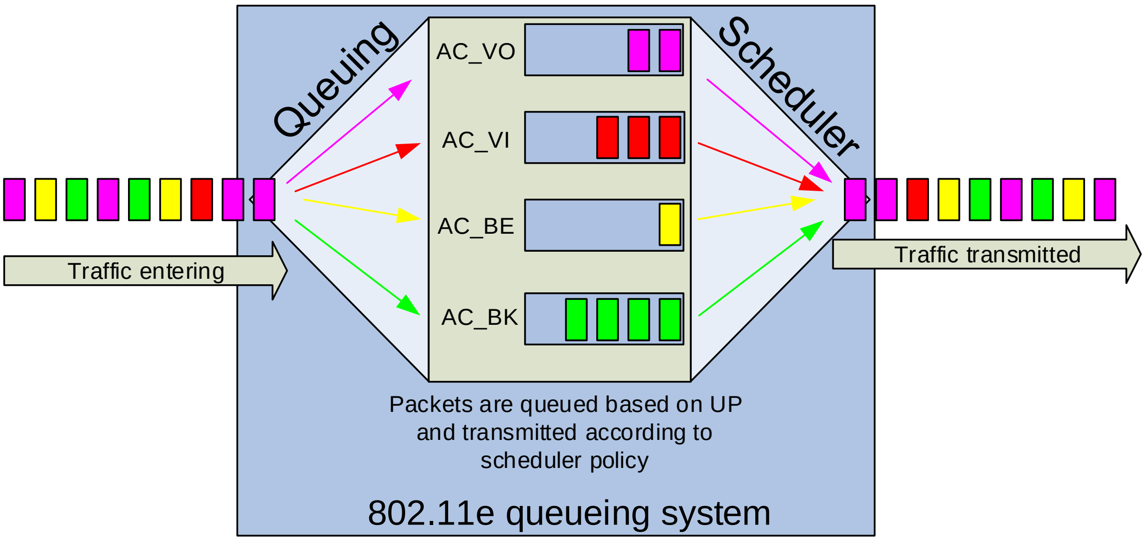


Figure 42 - 802.11e EDCA queueing system

## HCCA – HCF Controlled Channel Access

The second medium access enhancement in 802.11e is called HCCA or HCF Controlled Channel Access, which allows stations to send multiple frames in a block when transmitting over the RF medium. If a station needs to send multiple packets – instead of contending for each frame, the station receives an allotted time period where it can transmit multiple packets with only an SIFS interframe space between. All frames are acknowledged by the receiver using a single ACK frame. See Figure 43.

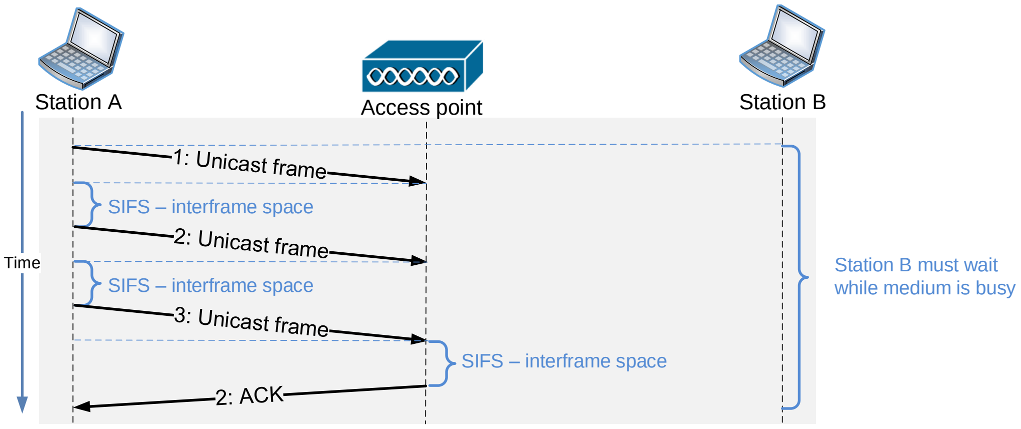
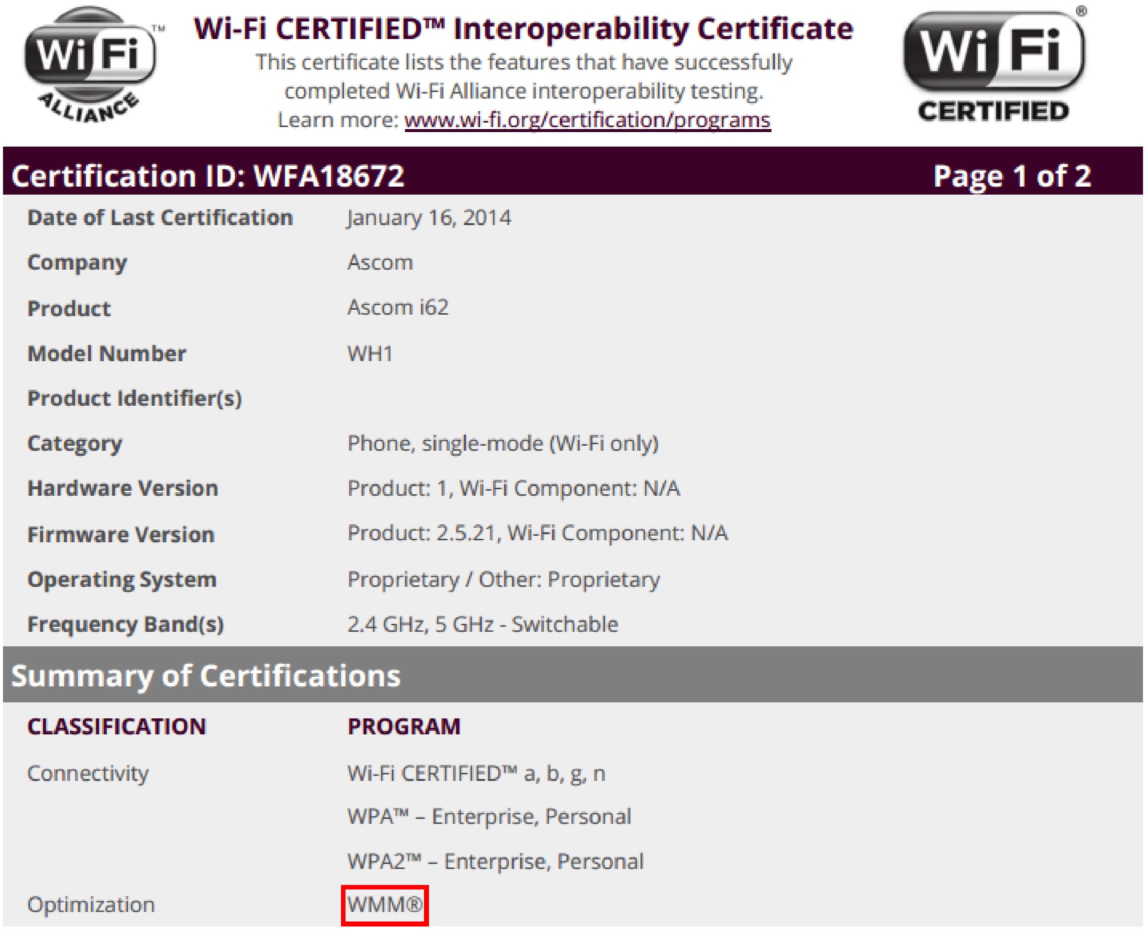


Figure 43 - IEEE 802.11e block transfer with immediate block ACK

### Wi-Fi multimedia certification

Before 802.11e QoS mechanism no method of prioritizing time sensitive applications such as VoWiFi – Voice over Wi-Fi existed. With the amendment of 802.11e the Wi-Fi alliance introduced the WiFi Multimedia certification called the WMM certification, ensuring compatibility between equipment manufactures. See Figure 44 for an example.



**Wi-Fi CERTIFIED™ Interoperability Certificate**

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing.
Learn more: www.wi-fi.org/certification/programs

**Certification ID: WFA18672** — **Page 1 of 2**

| | |
|---|---|
| **Date of Last Certification** | January 16, 2014 |
| **Company** | Ascom |
| **Product** | Ascom i62 |
| **Model Number** | WH1 |
| **Product Identifier(s)** | |
| **Category** | Phone, single-mode (Wi-Fi only) |
| **Hardware Version** | Product: 1, Wi-Fi Component: N/A |
| **Firmware Version** | Product: 2.5.21, Wi-Fi Component: N/A |
| **Operating System** | Proprietary / Other: Proprietary |
| **Frequency Band(s)** | 2.4 GHz, 5 GHz - Switchable |

**Summary of Certifications**

| **CLASSIFICATION** | **PROGRAM** |
|---|---|
| Connectivity | Wi-Fi CERTIFIED™ a, b, g, n |
| | WPA™ – Enterprise, Personal |
| | WPA2™ – Enterprise, Personal |
| Optimization | WMM® |

Figure 44 - Ascom i62 VoWi-Fi phone WMM certificate

### Airtime fairness

One of the important features of 802.11 is its ability to support many different data rates. This allows older technologies to still communicate alongside newer devices, along with enabling devices to maintain communications by shifting to slower data rates as they move away from an access point. The ability to use these slower data rates is paramount to 802.11 communications; however, it can also be a huge hindrance to the overall performance of the network, and to individual devices operating at faster data rates.

Since 802.11 is contention based, each radio must contend for its turn to communicate, then transmit, and then go back to the contention process. As each radio takes its turn transmitting, the other 802.11 radios must wait. If the transmitting radio is using a fast data rate, the other radios do not have to wait long. If the transmitting radio is using a slow data rate, the other radios will have to wait a much longer period of time. When 802.11 radios transmit at very low data rates such as 1 Mbps and 2 Mbps, effectively they cause medium-contention overhead for higher data rate transmitters due to the long wait time while the slower devices are transmitting.

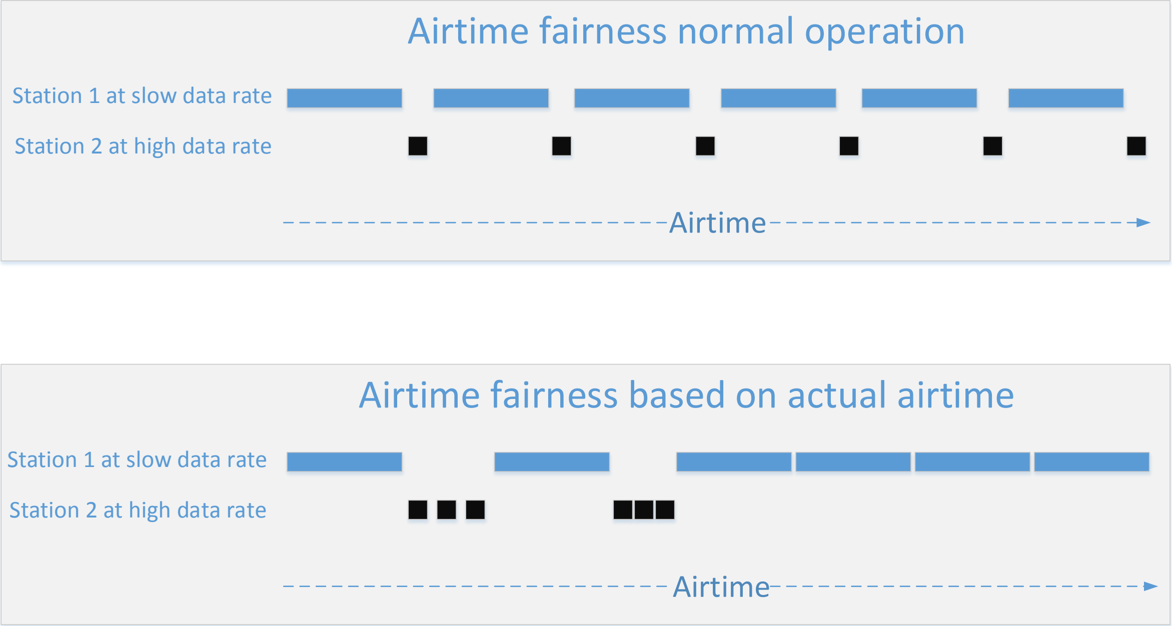

Airtime fairness normal operation
Station 1 at slow data rate
Station 2 at high data rate
Airtime
Airtime fairness based on actual airtime
Station 1 at slow data rate
Station 2 at high data rate
Airtime

**Figure 45 - Airtime fairness principles**

There are currently no 802.11 standards defining airtime fairness besides the default – shown as normal operation in Figure 45, even though different vendors introduce their own version of airtime fairness. Interoperability between vendors is not guaranteed.

## MAC Architecture

In this chapter the components of the 802.11 MAC architecture will be discussed. Remember 802.11 is a communication standard based on OSI layer 1 and OSI layer 2, and the main priority of digital communication is transferring binary 1’s and 0’s between computers. To achieve this in a noisy radio environment at high data rates between multiple units requires control of the half duplex medium as discussed in the previous chapter – 802.11 medium access.

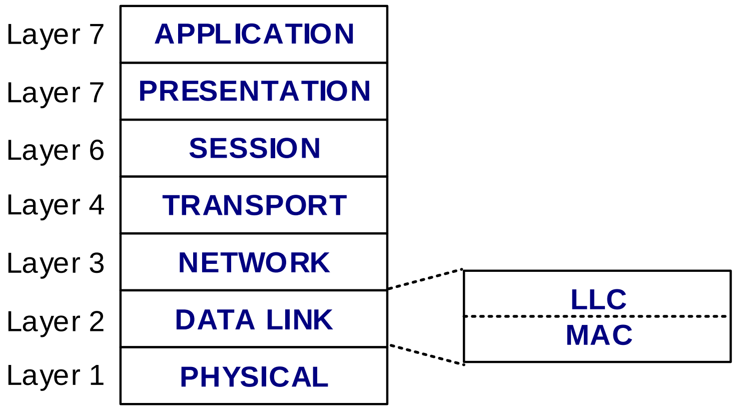


Figure 46 - THe MAC layer is a part of the OSI data link layer.

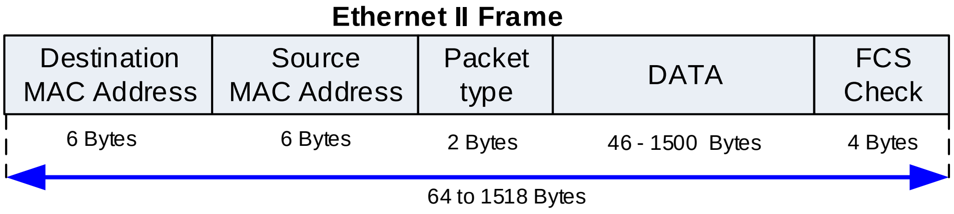
## Data link layer

The 802.11 data link layer is divided into two sublayers. The upper layer LLC – Logical Link Control – which is identical in all 802 based networks, such as 802.3 Ethernet, while the lower part of the data link layer differs between different versions of 802.

802.3 Ethernet and 802.11 Wireless have different MAC – Media Access Control – sublayers.

## The 802.3 Ethernet frame

There is only one type of Ethernet II frame as shown in Figure 47. This frame is used by all types of packets in Ethernet communication. An Ethernet frame includes two MAC addresses – the source and the destination address. As will be seen in the following section, 802.11 Wireless frames differ from Ethernet frames.



Ethernet II Frame

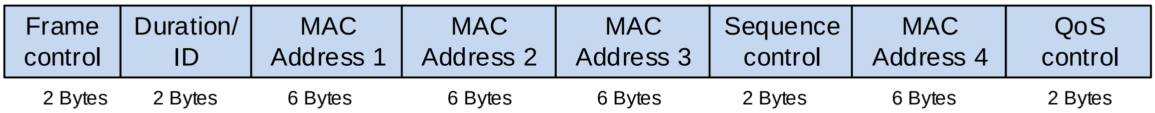
| Destination MAC Address | Source MAC Address | Packet type | DATA | FCS Check |
|---|---|---|---|---|
| 6 Bytes | 6 Bytes | 2 Bytes | 46 - 1500  Bytes | 4 Bytes |

64 to 1518 Bytes

Figure 47 - The Ethernet frame

## 802.11 wireless frame types

802.11 has three major frame types, used for different purposes; a management frame, a control frame and a data frame. The frame includes up to four MAC addresses.  See Figure 48.



| Frame control | Duration/ ID | MAC Address 1 | MAC Address 2 | MAC Address 3 | Sequence control | MAC Address 4 | QoS control |
|---|---|---|---|---|---|---|---|
| 2 Bytes | 2 Bytes | 6 Bytes | 6 Bytes | 6 Bytes | 2 Bytes | 6 Bytes | 2 Bytes |

Figure 48 - 802.11 wireless MAC header

802.3 Ethernet and 802.11 wireless both use the same MAC address format and identify the frame source address (SA) and the destination address (DA). Wireless networks also define the receiver address (RA) and the transmitter address (TA). Under normal circumstances only three MAC addresses are used.

### Use of three MAC addresses

When a Basic Service Set – BSS – system as shown in Figure 49 is used, three MAC addresses are used to identify the collaborating systems.

1. Source Address (SA) identifies the source of the frame
2. Receiver Address (RA) identifies the immediate receiver; in this case access point 1 – AP 1
3. Destination Address (DA) identifies the final recipient of the frame on the LAN

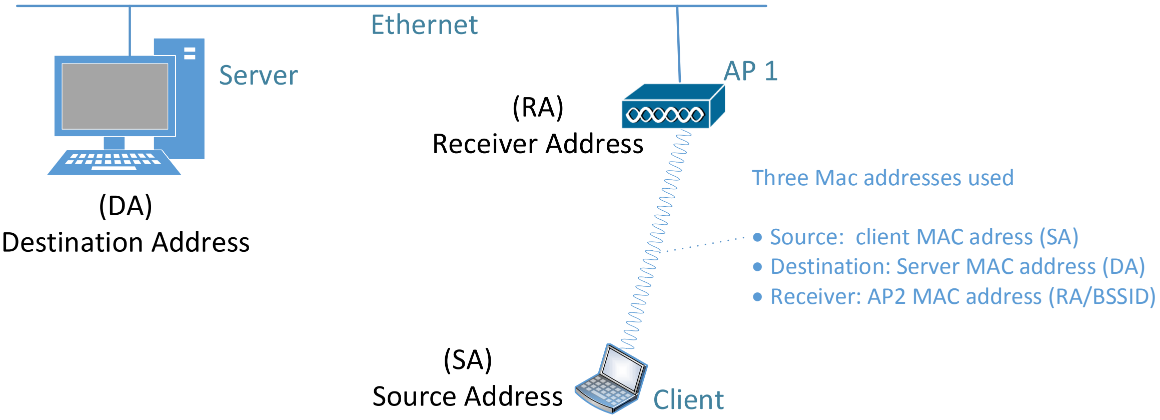

Ethernet
Server
AP 1
(RA)
Receiver Address
(DA)
Destination Address
Three Mac addresses used
• Source:  client MAC adress (SA)
• Destination: Server MAC address (DA)
• Receiver: AP2 MAC address (RA/BSSID)
(SA)
Source Address
Client

Figure 49 - Using the third MAC address - RA - to identify the access point as the link receiver.

### Use of four MAC addresses

When using a Wireless Distribution System, as shown in Figure 50, frames from the client are relayed from access point 1 – AP 1 – to access point 2 –AP 2. In this case four MAC addresses are used to identify the collaborating systems. When looking at packets between AP 1 and AP 2 the 802.11 frame contains

1. Source Address (SA) identifies the source of the frame – The client
2. Receiver Address (RA) identifies the immediate receiver in this case access point 2 – AP 2
3. Transmitter Address (TA) identifies the immediate transmitter in this case access point 1 – AP 1
4. Destination Address (DA) identifies the final recipient of the frame on the LAN

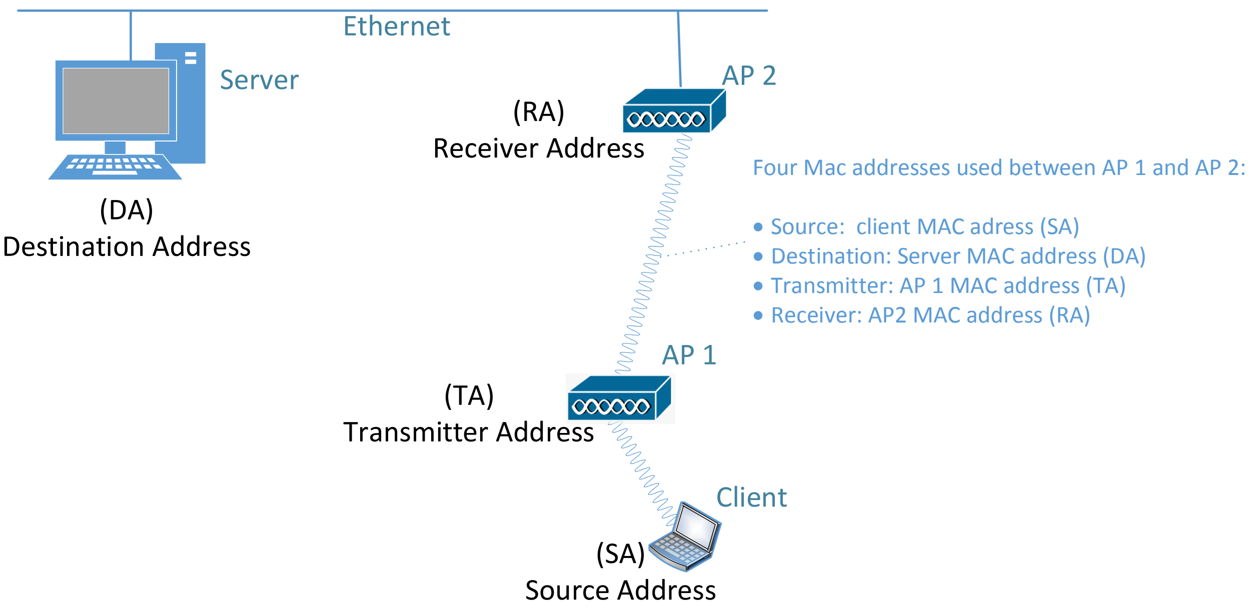

Ethernet
Server
(DA)
Destination Address
AP 2
(RA)
Receiver Address
Four Mac addresses used between AP 1 and AP 2:
• Source:  client MAC adress (SA)
• Destination: Server MAC address (DA)
• Transmitter: AP 1 MAC address (TA)
• Receiver: AP2 MAC address (RA)
AP 1
(TA)
Transmitter Address
Client
(SA)
Source Address

**Figure 50 - Four MAC addresses necessary when using a wireless distribution system**

## Three 802.11 frame types

There are three major 802.11 frame types:

1. Management frames
2. Control frames
3. Data frames

These frame types are further subdivided into several subtypes.

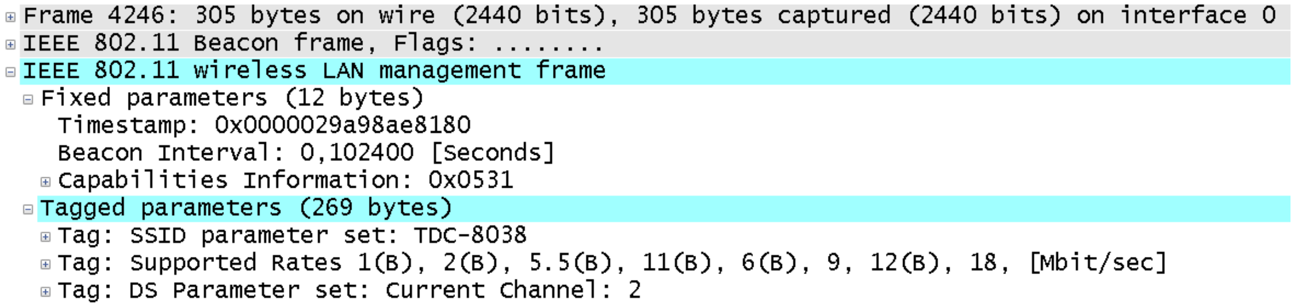
## Management frames

802.11 management frames make up the majority of frame types in a WLAN. Management frames are used to join and leave a BSS – Basic Service Set. Some of the interesting management frames used in a BSS – Basic Service Set – are listed in the table below.

| Management subtypes | Send by | Brief explanation |
|---|---|---|
| Association Request | Client | Send from client who wants to join a AP includes SSID |
| Association Response | AP | Send from AP accepting or rejecting the association req. |
| Disassociation | AP or Client | Terminates a previously made association |
| Reassociation Request | Client | Send from client to new AP it wants to roam to |
| Reassociation Response | AP | Send from AP accepting or rejecting the reassociation |
| Probe Request | Client | Send from client to determine which AP in range |
| Probe Response | AP | Send from AP in response of probe request |
| Beacon | AP | Send periodically from AP to announce its presence |
| Authentication Request | Client | Send by client to AP in authentication process |
| Authentication Response | AP | Send by AP to client in authentication process |
| Deauthentication | AP or Client | Send to terminate secure communication |

### Beacon management frame

Beacon management is one of the most important frame types, often referred to as the beacon. Beacons are basically the heartbeat of a wireless network. The AP of a BSS – Basic Service Set – sends the beacons while the client listens for beacon frames. Each beacon contains a timestamp, which clients use to synchronize their radio clocks with the AP. Synchronization between the stations and the AP is very important for successful communication.



```
⊞ Frame 4246: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface 0
⊞ IEEE 802.11 Beacon frame, Flags: ........
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters (12 bytes)
      Timestamp: 0x0000029a98ae8180
      Beacon Interval: 0,102400 [Seconds]
    ⊞ Capabilities Information: 0x0531
  ⊟ Tagged parameters (269 bytes)
    ⊞ Tag: SSID parameter set: TDC-8038
    ⊞ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    ⊞ Tag: DS Parameter set: Current Channel: 2
```

Figure 51 - Screen dump from Wireshark showing partial beacon frame.

The beacon frame includes information about channel setting, data rates, SSID – if not cloaked, QoS parameters, security and vendor proprietary information.

### Passive and active scanning

When a station wants to connect to an AP it must first discover the AP. This is called scanning. A station can listen for beacon frames, which is called passive scanning or it can transmit probe requests to the APs, which is called active scanning.

### *Passive scanning*

In passive scanning the station listens for beacons containing preconfigured SSIDs and tries to associate to the AP. If the client receives beacons from multiple APs containing the same SSID, the client tries to associate with the AP with the best signal. The client builds a table of SSIDs received in beacons.

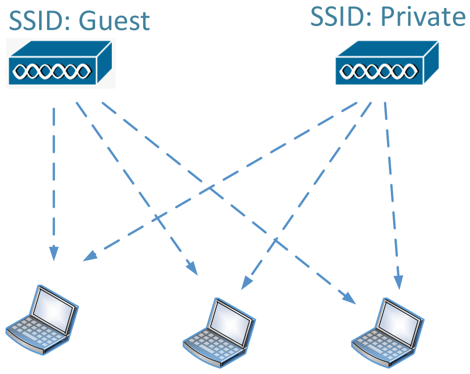


Figure 52 -Passive scanning. Clients listen for beacons.

### *Active scanning*

In addition to passive scanning for APs, the clients can actively search for them. In active scanning the clients transmit probe request frames and the APs return a probe response frame. These probe requests can either contain a specific SSID the client wants to associate with, or the SSID can be an empty field in which case all APs will return probe responses.

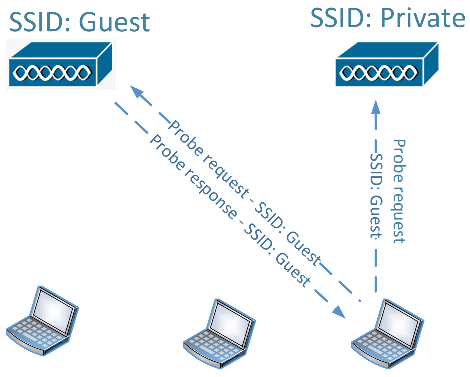


Figure 53 - Active scanning. Client actively asks for AP's with SSID Guest.

A client station can use both passive and active scanning at the same time.

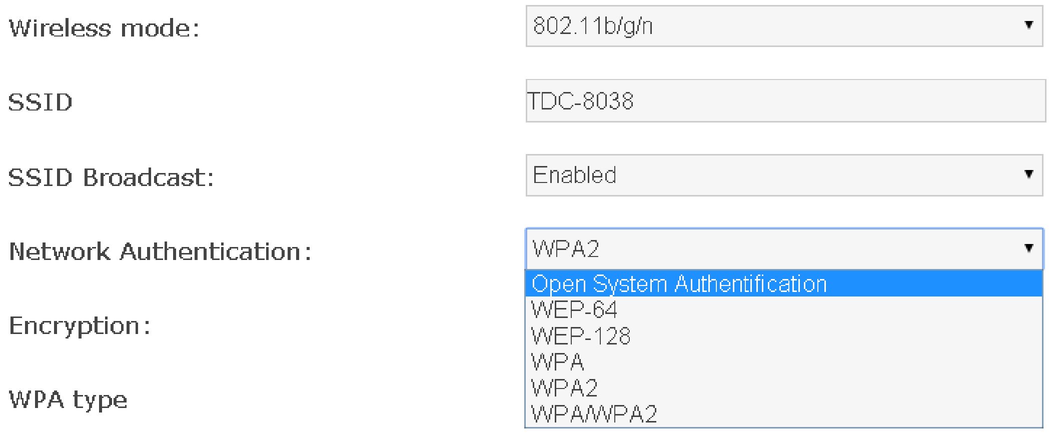
### Authentication

Authentication is the first two steps required to connect to the 802.11 BSS – Basic Service Set. Both authentication and association must occur in that order, before a client station can pass traffic through the AP.

The purpose of 802.11 authentication is to establish an initial connection between the client and the AP. The 802.11-2007 standard defines two authentication methods: Open System Authentication and Shared Key Authentication.

### *Open System Authentication*

Open system authentication is the simpler of the two authentication methods. It provides authentication without performing any type of client verification. The client simply authenticates by exchanging an authentication request with the AP.



Wireless mode: 802.11b/g/n

SSID TDC-8038

SSID Broadcast: Enabled

Network Authentication: WPA2

Encryption:

WPA type

Figure 54 - partial screen dump from AP configuration settings.

Open system authentication can be used with security procedures after the station is authenticated and associated. The different authentication methods will be discussed in chapter 13 – network security architecture.

## *Shared Key Authentication*

Shared key authentication uses WEP – Wired Equivalent Privacy – when authenticating client stations. It requires that a static WEP key is configured on the AP and the client. The client will not be able to authenticate with the AP if the static WEP keys do not match. Shared key authentication is a four way authentication frame exchange, with eight frames transmitted through the air.

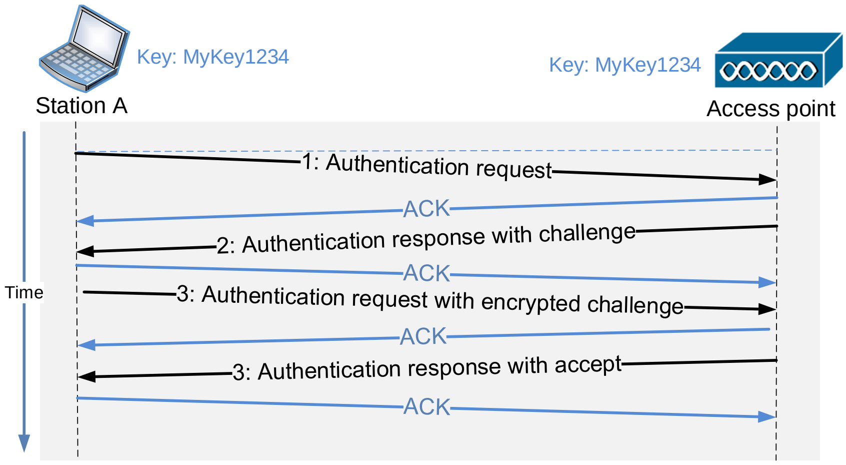
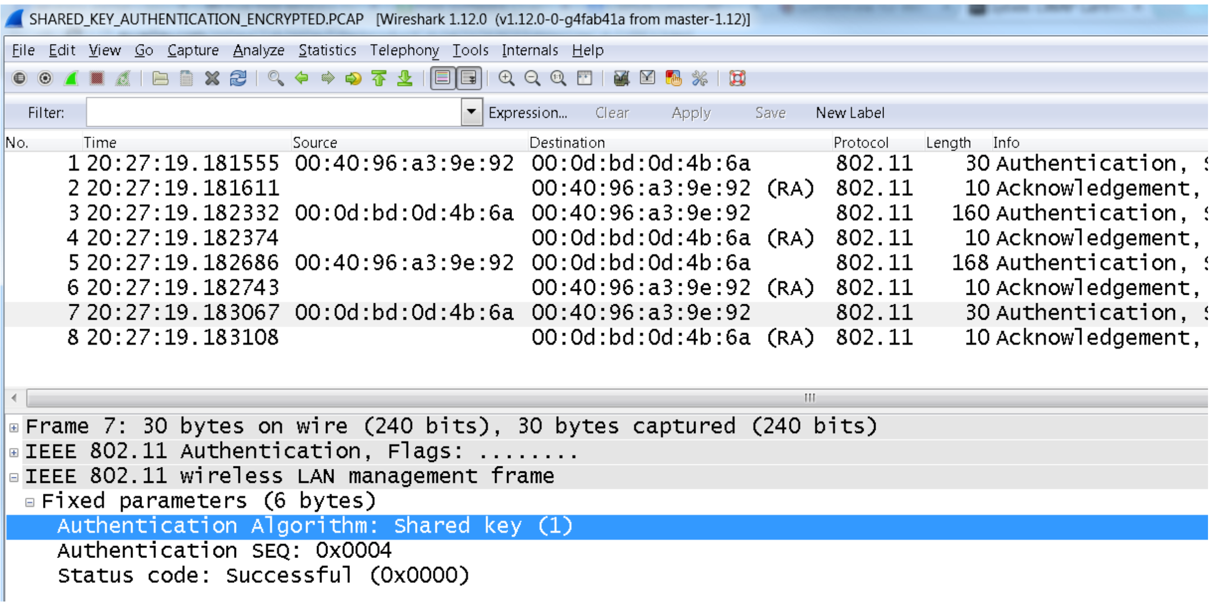

Key: MyKey1234
Station A
Key: MyKey1234
Access point
Time
1: Authentication request
ACK
2: Authentication response with challenge
ACK
3: Authentication request with encrypted challenge
ACK
3: Authentication response with accept
ACK

**Figure 55 – Successful shared key Authentication with WEP.**

WEP authentication is considered insecure and should be avoided. In chapter 13 – Network Security Architecture – recommended security and authentication procedures will be discussed.

### What makes WEP authentication is insecure?

The main reason WEP authentication is insecure, is that it is possible for an intruder to sniff the challenge transmitted by the AP and the encrypted challenge returned from the client. It is possible for the intruder to brute force the secret key with this information.


SHARED_KEY_AUTHENTICATION_ENCRYPTED.PCAP [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save New Label

```
No.  Time              Source             Destination             Protocol  Length  Info
   1 20:27:19.181555  00:40:96:a3:9e:92  00:0d:bd:0d:4b:6a        802.11      30  Authentication,
   2 20:27:19.181611                     00:40:96:a3:9e:92 (RA)   802.11      10  Acknowledgement,
   3 20:27:19.182332  00:0d:bd:0d:4b:6a  00:40:96:a3:9e:92        802.11     160  Authentication,
   4 20:27:19.182374                     00:0d:bd:0d:4b:6a (RA)   802.11      10  Acknowledgement,
   5 20:27:19.182686  00:40:96:a3:9e:92  00:0d:bd:0d:4b:6a        802.11     168  Authentication,
   6 20:27:19.182743                     00:40:96:a3:9e:92 (RA)   802.11      10  Acknowledgement,
   7 20:27:19.183067  00:0d:bd:0d:4b:6a  00:40:96:a3:9e:92        802.11      30  Authentication,
   8 20:27:19.183108                     00:0d:bd:0d:4b:6a (RA)   802.11      10  Acknowledgement,

⊞ Frame 7: 30 bytes on wire (240 bits), 30 bytes captured (240 bits)
⊞ IEEE 802.11 Authentication, Flags: ........
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters (6 bytes)
      Authentication Algorithm: Shared key (1)
      Authentication SEQ: 0x0004
      Status code: Successful (0x0000)
```

**Figure 56 - Captured shared key authentication frame exchange including challenge and encrypted challenge.**

### Association

After the client station has authenticated successfully with the AP, the next step for it is to associate with the AP. When a client station associates with an AP, it becomes a member of a BSS – Basic Service Set. When the client station is associated it can send data through the AP to the distribution system behind the AP – the network.

Typically a client station will try to obtain an IP address from a DHCP server by sending a DHCP discover packet when it is successfully associated with an AP.

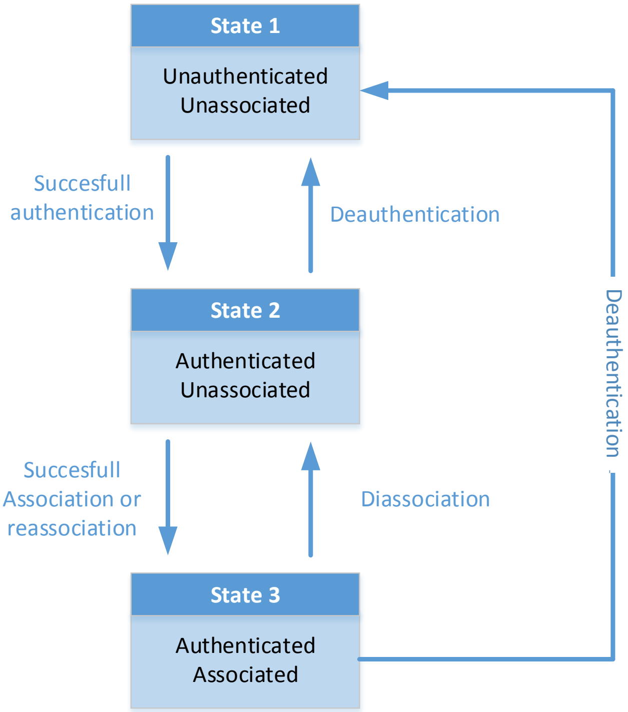
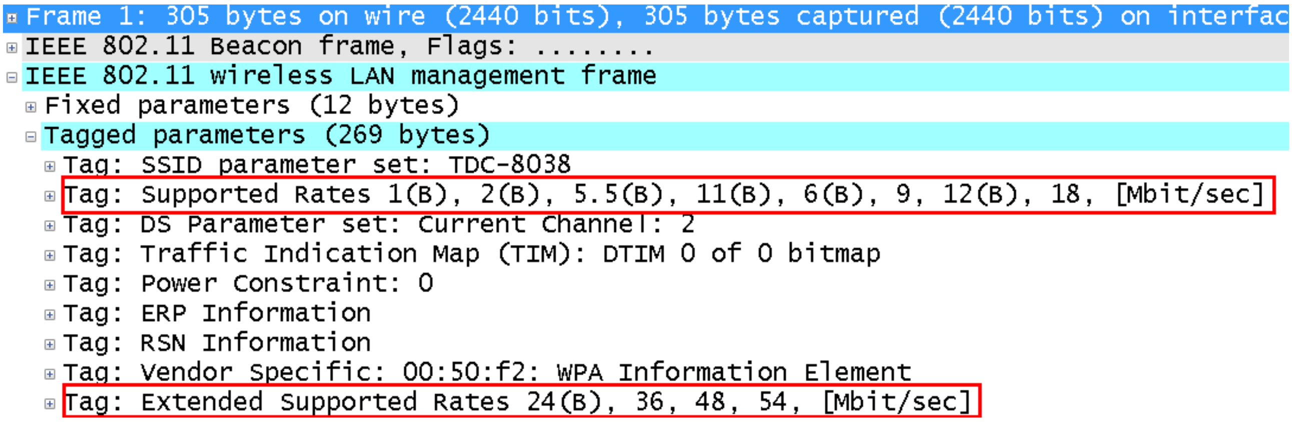


Figure 57 - Authentication and association states.

### *Basic and supported data rates*

As seen in previous chapters 802.11 standards define different data rates and spread spectrum technologies. For example, HR-DSSS (802.11b) radios are capable of supporting data rates of 1, 2, 5.5, and 11 Mbps. ERP (802.11g) radios are capable of supporting the HR-DSSS data rates, but are also capable of supporting ERP-OFDM rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

Access points announce supported data rates in beacon frames and specify which rates are basic rates and which rates are supported rates. To associate to an access point the client station must support the basic rates but not necessarily the supported data rates. Basic rates are also called required rates.



```
⊞ Frame 1: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interfac
⊞ IEEE 802.11 Beacon frame, Flags: ........
⊟ IEEE 802.11 wireless LAN management frame
  ⊞ Fixed parameters (12 bytes)
  ⊟ Tagged parameters (269 bytes)
    ⊞ Tag: SSID parameter set: TDC-8038
    ⊞ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    ⊞ Tag: DS Parameter set: Current Channel: 2
    ⊞ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    ⊞ Tag: Power Constraint: 0
    ⊞ Tag: ERP Information
    ⊞ Tag: RSN Information
    ⊞ Tag: Vendor Specific: 00:50:f2: WPA Information Element
    ⊞ Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```

Figure 58 - Data rates announced by access point. Basic rates marked with (B).

As seen from Figure 58 this access point announces 1 – 2 – 5.5 – 11 – 6 – 12 and 24 Mbps as basic rates and 18 – 36 – 48 and 54 Mbps as additional supported rates. Any client stations, who wish to associate to this access point, must support the basic data rates. On some access points it is possible to configure which data rates are basic and which are supported.

### *Roaming and reassociation*

Roaming is the ability for client stations to transition from one AP to another AP while maintaining connectivity for the upper-layer applications. The decision to roam from one AP to another AP is made by the client station based typically on signal strength (RSSI), noise level (SNR) and bit error rate. The vendor of the radio card decides why and when a client station tries to roam, it is not defined by any 802.11 standards.

A client station will try and authenticate itself to all APs in range, but can at any given time only be associated to one.

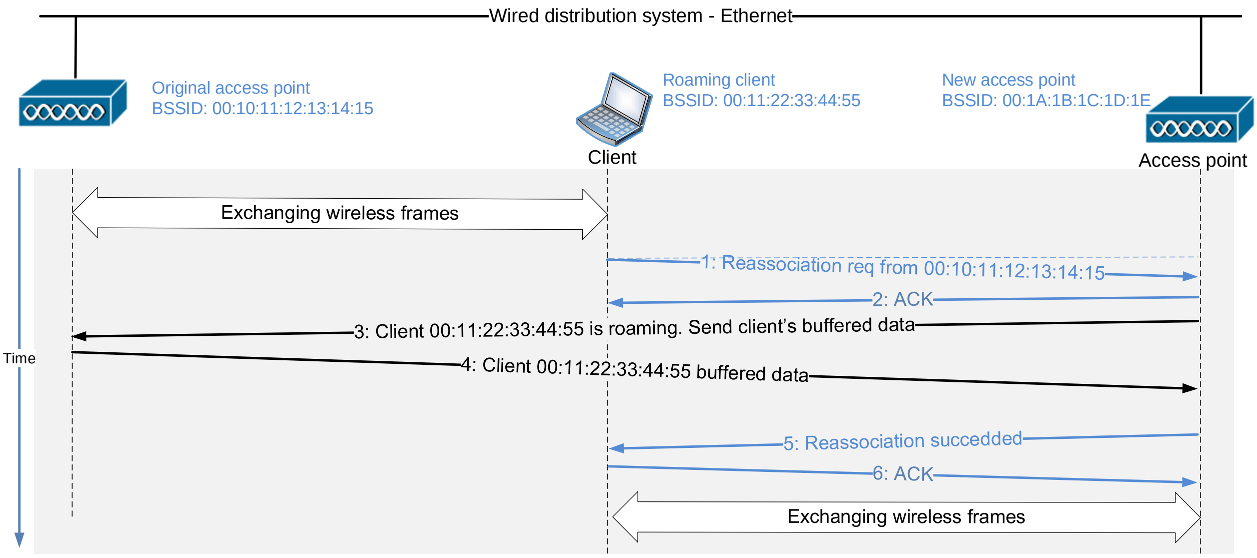

Wired distribution system - Ethernet
Original access point
BSSID: 00:10:11:12:13:14:15
Roaming client
BSSID: 00:11:22:33:44:55
New access point
BSSID: 00:1A:1B:1C:1D:1E
Client
Access point
Time
Exchanging wireless frames
1: Reassociation req from 00:10:11:12:13:14:15
2: ACK
3: Client 00:11:22:33:44:55 is roaming. Send client's buffered data
4: Client 00:11:22:33:44:55 buffered data
5: Reassociation succedded
6: ACK
Exchanging wireless frames

**Figure 59 - Client reassociate with new access point.**

In Figure 59 the client is authenticated with both APs, but is only associated with the original access point and wants to reassociate to the access point based on the signal strength. The six frame reassociation sequence changes the clients association to the new AP.

The exchange of frames between the two APs involved in the roaming sequence should exchange client status through the distribution medium providing a clean handover between the two APs. This handover is not a part of the 802.11 standards and is implemented by vendors, if at all.

### *Disassociation and deauthentication*

*Disassociation* and *deauthentication* are notifications, not requests. If a station wants to disassociate or deauthenticate from an AP, or an AP wants to disassociate or deauthenticate from a station, either device can send a disassociation or a deauthentication frame. This is a polite way of terminating the association or authentication. See Figure 60.

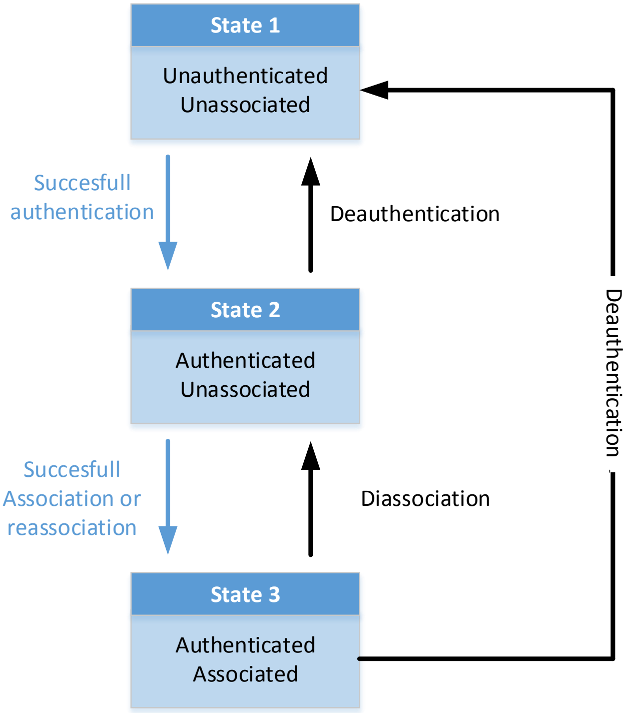


Figure 60 - Disassociation and deauthentication.

## Protection mechanism

When using 802.11b devices together with 802.11g devices, the 802.11g devices need to provide backward compatibility with the slower 802.11b devices. 802.11g devices must also be compatible with even older 802.11 legacy devices.

When 802.11b and 802.11g devices are used in mixed mode legacy 802.11 and 802.11b devices communicate using different spread spectrum technologies and different data rates than 802.11g devices, as seen in the table below.

| | 802.11 Legacy | 802.11b | 802.11g |
|---|---|---|---|
| **Frequency** | 2,4 GHz ISM band | 2,4 GHz ISM band | 2,4 GHz ISM band |
| **Spread spectrum technologies** | FHSS or DSSS | HR-DSSS | ERP-OFDM and ERP-DSSS/CCK |
| **Data rates** | 1 and 2 Mbps | 1 – 2 – 5,5 and 11 Mbps | 6 – 9 – 12 – 18 – 24 – 36 – 48 and 54 Mbps |
| **Backward compatibility** | N/A | 802.11 legacy DSSS only | 802.11 HR-DSSS and 802.11 legacy DSSS |
| **Ratified** | 1997 | 1999 | 2003 |

### 802.11g-Only mode

When an IP is running in 802.11g-only mode it will communicate only with 802.11g devices. Newer 802.11n devices will also be able to communicate with the AP because they are backward compatible. The total throughput on an 802.11g-only AP, will typically be higher than a 802.11b/g mixed mode setting, because the slower 802.11b devices takes more air-time to transmit the same amount of data.

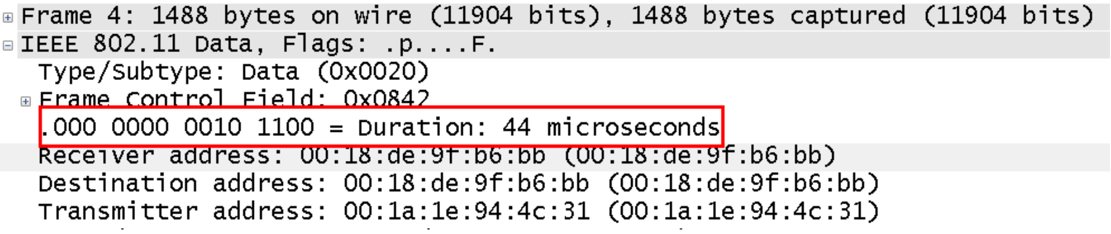
### 802.11b/g Mixed mode

An access point configured to 802.11b/g mixed mode – supporting coexistence between 802.11b and 802.11g devices – uses a protection mechanism called 802.11g protected mode.

Contrary to what some people believe, the 802.11g devices do not simply switch to 802.11b mode and communicate using the lower 802.11b data rates.

Even if all of the wireless devices support 802.11g, the AP will switch to protected mode if it sees one 802.11b adapter. It could be a visitor, an old printer or other devices. If you want the network to always use higher data rates, the AP should be configured to only support the desired data rates. But devices with lower data rates will not be able to connect, and the range of the AP will be reduced as the data rate will be decreased with lower RSSI – signal strengths.

One way of preventing collisions is using a countdown timer called NAV – Network Allocation Vector. A field called Duration transmitted at the beginning of a frame telling other stations the duration the media is busy. This is not possible in mixed mode environments, because 802.11b devices are unable to receive 802.11g frames. This could lead to 802.11b devices transmitting before the duration period times out, causing collisions.



```
⊞ Frame 4: 1488 bytes on wire (11904 bits), 1488 bytes captured (11904 bits)
⊟ IEEE 802.11 Data, Flags: .p....F.
    Type/Subtype: Data (0x0020)
  ⊞ Frame Control Field: 0x0842
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: 00:18:de:9f:b6:bb (00:18:de:9f:b6:bb)
    Destination address: 00:18:de:9f:b6:bb (00:18:de:9f:b6:bb)
    Transmitter address: 00:1a:1e:94:4c:31 (00:1a:1e:94:4c:31)
```

Figure 61 - Duration field in frame. All stations use Duration as a countdown timer.

### RTS/CTS

RTS/CTS is a protection mechanism used in 802.11b/g mixed mode environments when 802.11b devices are present.

RTS – Request To Send – is a small frame transmitted by 802.11g devices at slow rate informing 802.11b of the duration timeout period. CTS Clear To Send – is a small frame returned by the receiving device also including a duration period. See Figure 62.

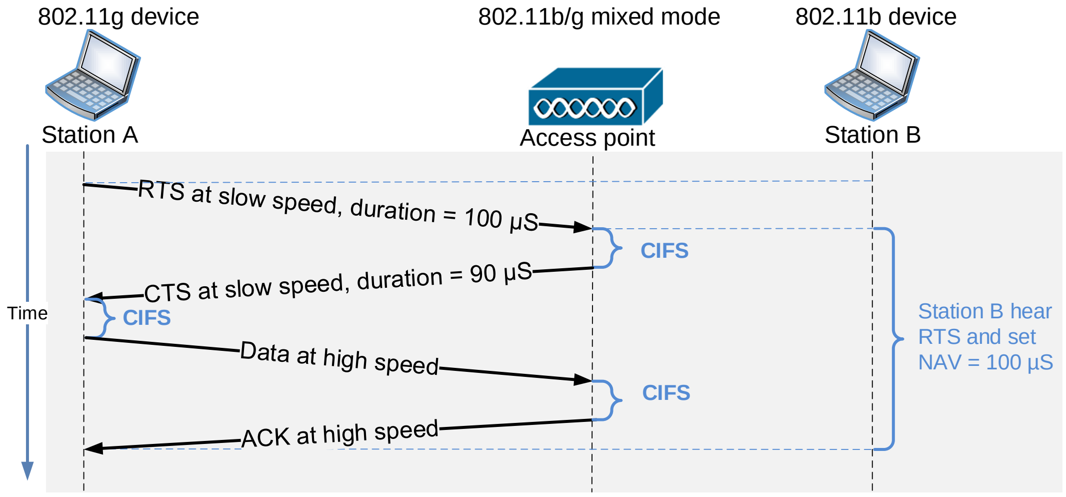


Figure 62 - RTS/CTS mechanism, informing slower devices of medium busy time period

An advantage of using RTS/CTS is resolution of the hidden node problem. The hidden node problem is when two stations are out of range of each other, but both are in range of the AP. See Figure 63.

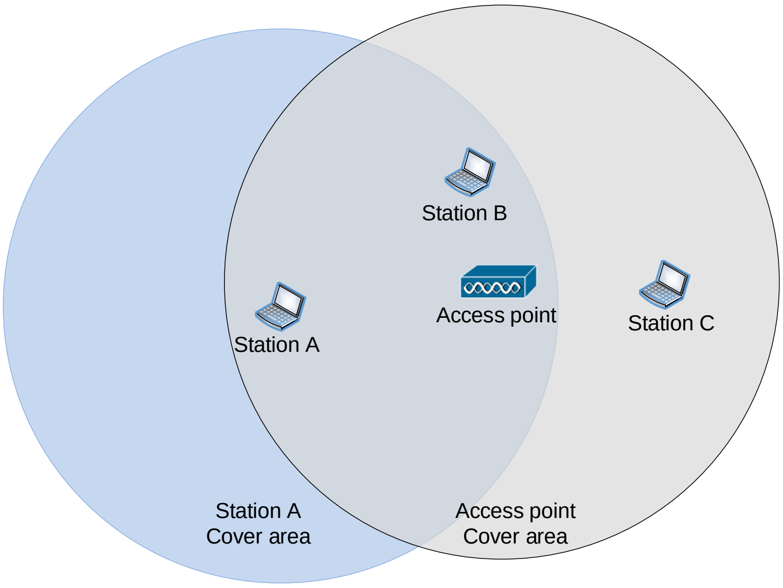


Figure 63 - Hidden node problem. Station C is out of range of station A's transmitter.

As seen from Figure 64 the hidden node station C hears the CTS from the AP, and sets its NAV timer accordingly.  This avoids the problem of station C assuming the media is free, starting transmitting and causing an collision.

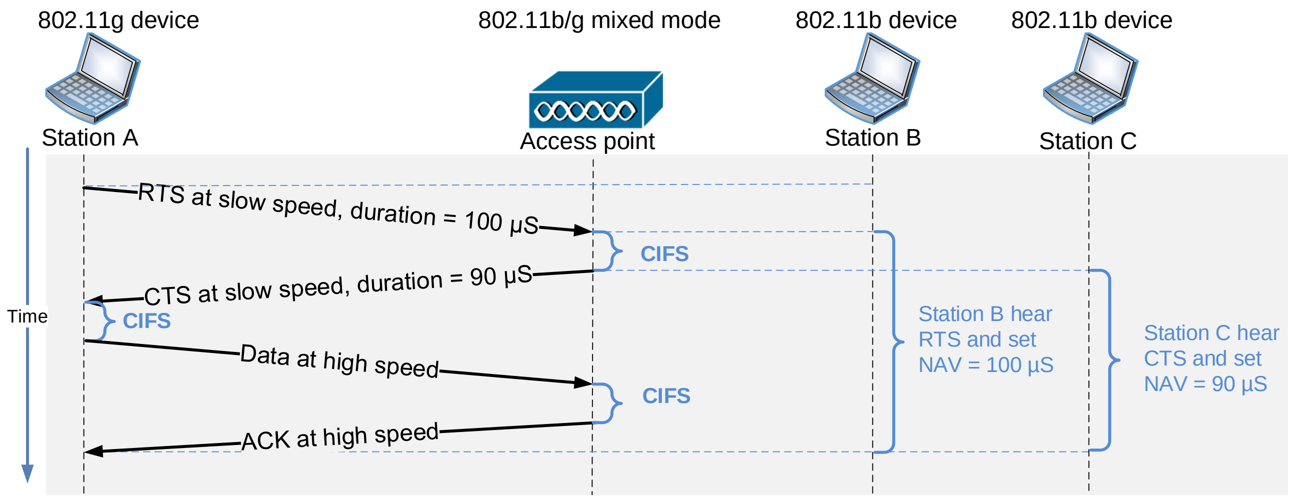


Figure 64 - RTS/CTS solve hidden node problem setting NAV timer on hidden node

## 802.11b/g mixed mode throughput

When an 802.11b device is discovered in an 802.11b/g mixed mode environment the AP will enable the protection mechanism and start using RTS/CTS. A large amount of RTS/CTS frames are added to the overall traffic lowering the throughput of the wireless network.

As a rule of thumb, a wireless network using a data rate of 54 Mbps usually provides about 18 to 20 Mbps aggregate throughput when protection is not enabled. When protection is enabled the added overhead reduces the aggregate throughput to below 13 Mbps and possibly as low as 9 Mbps.

## Power Management

One of the main applications for wireless networking is mobile devices powered by batteries. To increase battery life, power management features are a part of 802.11 standards.

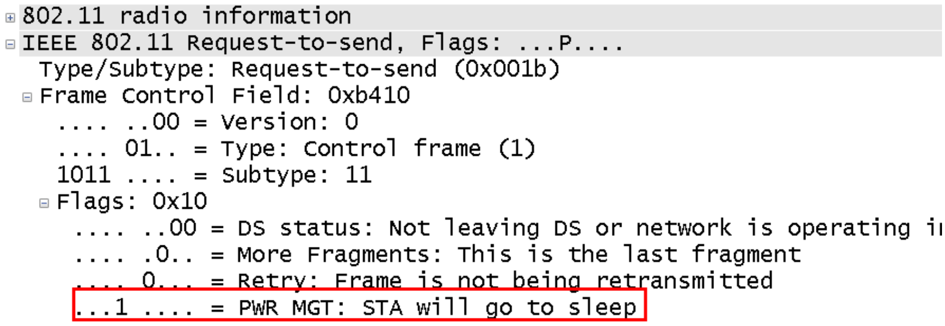
Two legacy power management modes called Active Mode and Power Safe Mode. A client station can set a bit to indicate its power mode to the AP.

### Active mode

Active mode is the default for most 802.11 stations. When in active mode the client station is always ready to receive and transmit frames, and it provides no battery conservation.

### Power Save Mode

When a client station is in power safe mode, it shuts down the radio temporarily to save power. Before the station transitions to power safe mode, it indicates to the AP in a frame that it is going to sleep. See Figure 65.



```
⊞802.11 radio information
⊟IEEE 802.11 Request-to-send, Flags: ...P....
   Type/Subtype: Request-to-send (0x001b)
 ⊟Frame Control Field: 0xb410
    .... ..00 = Version: 0
    .... 01.. = Type: Control frame (1)
    1011 .... = Subtype: 11
  ⊟Flags: 0x10
     .... ..00 = DS status: Not leaving DS or network is operating i
     .... .0.. = More Fragments: This is the last fragment
     .... 0... = Retry: Frame is not being retransmitted
     ...1 .... = PWR MGT: STA will go to sleep
```

Figure 65 - Frame indicating to the AP that the client station is going into power safe mode.

The AP will buffer traffic to the client station while it is in power safe mode. The client station will periodically wake up and listen to the AP's beacon frames. If the AP has buffered any data for the sleeping client station, it will announce it in the beacon frames. The client station can stay in power safe mode, as long as no data is buffered, just periodically listening to the beacon. To leave power safe mode, the client station transmits a management frame to the AP indicating it wants to receive the buffered data.

## Band steering

The 2.4 GHz band is heavily used by 802.11b, 802.11g and 802.11n devices, Bluetooth, cordless phones and many other applications. Most equipment in use is dual band capable; using both the 2.4 GHz and 5 GHz bands. When used in mixed mode, the 2.4 GHz band offers reduced throughput, due to RTS/CTS and slow transmission by 802.11b devices.

When a dual band radio station connects to an AP it will try to connect to the channel offering the strongest signal. Often the 2.4 GHz signal will be stronger because the higher frequency 5 GHz signal naturally attenuates more the 2.4 GHz signal, making the client station connect to the AP's 2.4 GHz radio. Often the 5 GHz band is less saturated by noise and traffic, making it a better decision to connect to the AP's 5 GHz radio. Band steering maens trying to use the less saturated band, when associating to an AP.

# WLAN architecture

## Management, Control and Data planes

Networks are often divided into three logical planes of operation:

1. The management plane, used by administrators to administer and monitor the operation of the network.
2. The control plane, consisting of control and signalling information such as routing protocols used by routers.
3. The data plane, which is the network's actual transfer of user data between clients and servers.

### WLAN Management plane

In the WLAN management plane operations such as configuration of access points, monitoring WLAN operation and AP firmware upgrade management takes place.

### WLAN control plane

In the WLAN control plane more automated processes take place such as:

**Dynamic RF** – coordinated channel and power setting for multiple access points. Most vendors implement some type of dynamic RF capability, enabling access points to minimize interference.

**Roaming** – support for handoff between access points.

**Load balancing** – sharing the load between multiple access points.

### WLAN Data plane

The actual forwarding of user data takes place here. The data plane involves access points forwarding traffic from Wi-Fi to the distribution medium.

## Autonomous WLAN architecture

An autonomous or standalone access point is an access point where all three planes exist in the access point itself. All configuration settings are done in the access point itself.

An autonomous access point contains at least two physical interfaces, such as an 802.11 radio card and an 802.3 Ethernet port. Normally the radio card and the Ethernet port(s) are bridged together.

Figure 66 – Linksys WAP300N autonomous AP

### SOHO Router - Small Office/Home Office

Small wireless access points often used in small offices and home wireless network have an embedded router for connecting the network to the Internet. See **Fejl! Henvisningskilde ikke fundet.**. The wired access network is bridged/switched to the embedded access point sharing the same logical network 192.168.1.0/24 between the wired and the wireless network.

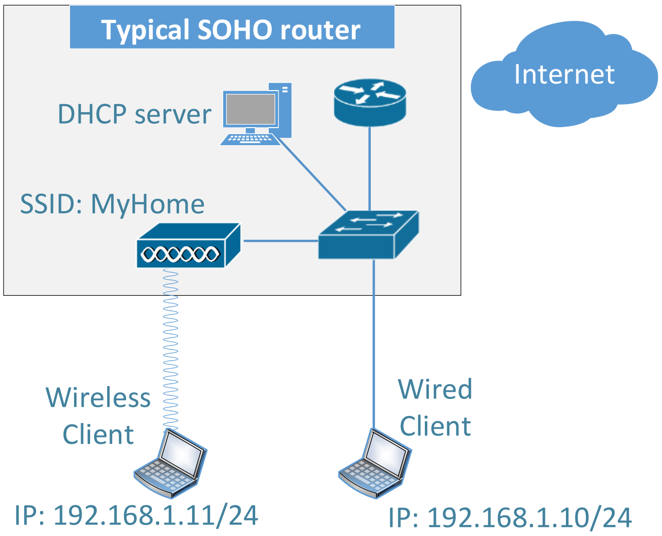


Figure 67 - Typical SOHO router design – note the two clients are on the same logical network 192.168.1.0/24

### Corporate autonomous networks

When using autonomous access points to build wireless networks, spanning buildings and connecting many wireless clients, all the access points need to be configured individually. Each access point handles security on its own. See Figure 68.

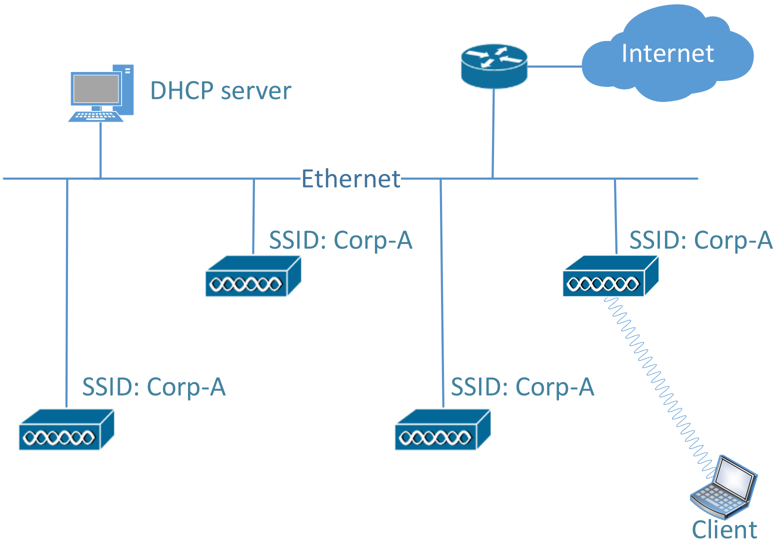
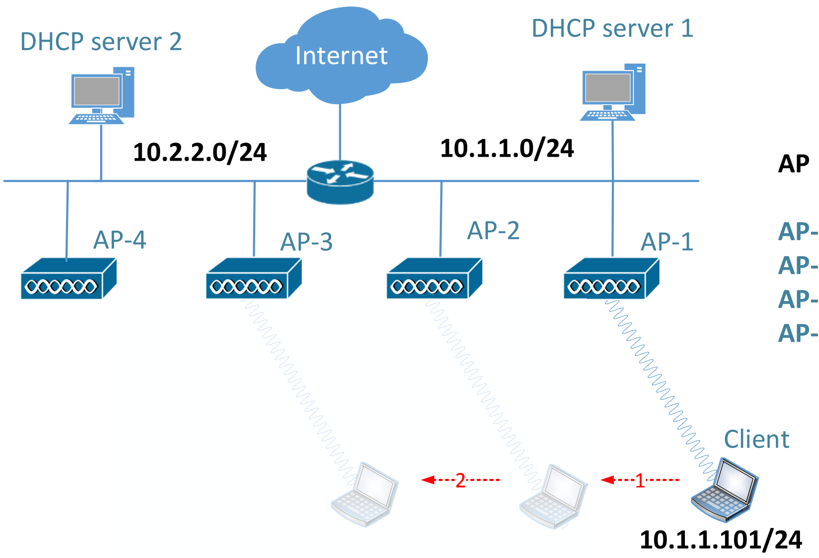


Figure 68 - Simple wireless network using autonomous access points

### Roaming in network with autonomous access points

Roaming with autonomous networks is possible when the client is allowed to keep its IP address before and after roaming. When looking at Figure 69:

1. The client associates with AP-1 using its BSSID
2. The client receives IP address 10.1.1.101 from DHCP server 1
3. The client moves towards AP-2
4. The client receives a stronger signal from AP-2 when approaching
5. The client reassociates to AP-2 using its BSSID
6. The client can use the IP address 10.1.1.101 as AP-2 is on the same logical network
7. The client moves towards AP-3
8. The client receives a stronger signal from AP-3 when approaching
9. The client reassociates to AP-3 using its BSSID
10. The client cannot use the IP address 10.1.1.101 as AP-3 is on the 10.2.2.0 logical network
11. The client loses all active connections and needs to get a new IP address from DHCP server 2



| AP | SSID | BSSID |
|---|---|---|
| AP-1 | Corp-A | 00-10-10-10-10-10 |
| AP-2 | Corp-A | 00-10-10-10-10-11 |
| AP-3 | Corp-A | 00-10-10-10-10-12 |
| AP-4 | Corp-A | 00-10-10-10-10-13 |

**Figure 69 - Roaming with autonomous networks. Client roaming from AP-1 to AP-2 then AP-3**

As seen from Figure 69, it is possible to do a layer-2 roaming, where the client can keep the same IP address. It is not possible to do a layer-3 roaming with autonomous access points, because the client needs an IP address in the new logical network.

## Virtual WLANs

Some autonomous access points are capable of making virtual WLANs. Virtual WLANs are used by access points to announce more than one SSID. As shown in Figure 70 the access point announces two SSIDs. The clients associated with each SSID are separated using VLANs. Clients on the Guest SSID are effectively separated from the Corp-A network. Each virtual SSID is mapped to a virtual BSSID.

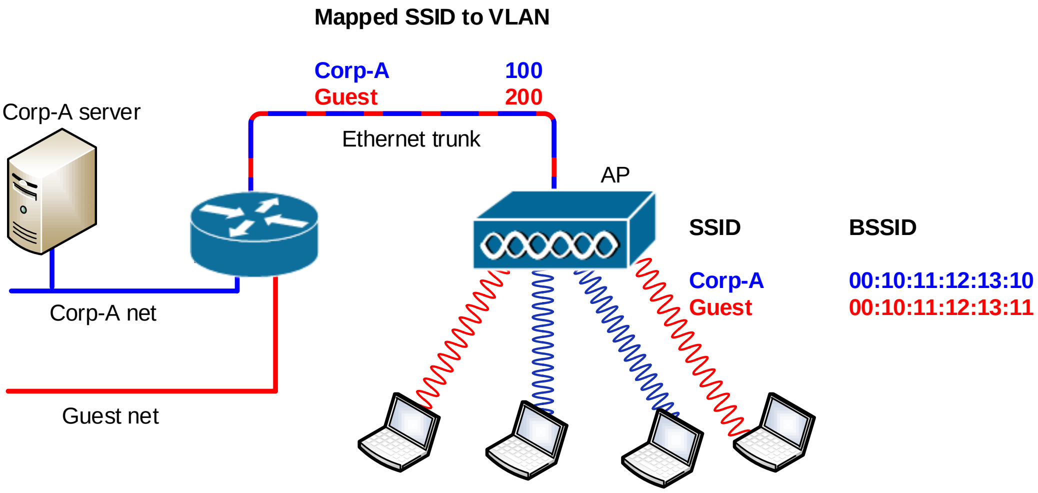


Figure 70 - Virtual 802.11 WLAN's mapped to Ethernet VLAN's

## WNMS – Wireless Network Management System

Some vendors of autonomous access points offer a WNMS – Wireless Network Management System – to centralize device management and a RADIUS server for centralized user management. All user traffic in the data plane is handled by the individual access points, as seen in Figure 68 when the client accesses the Internet.

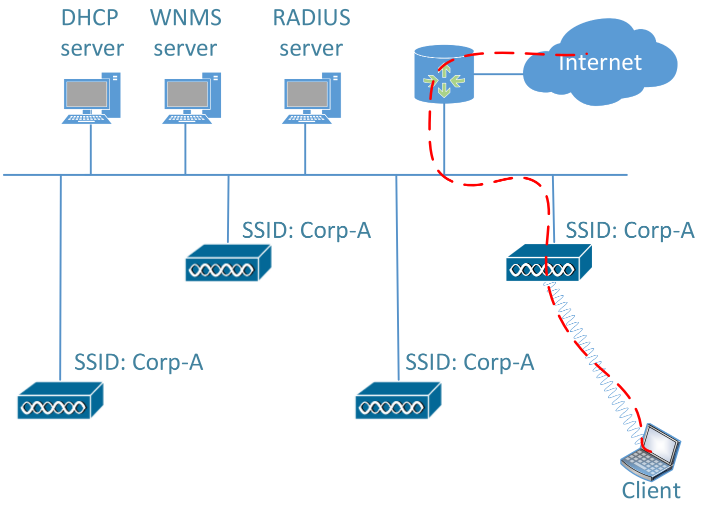


Figure 71 - Centralized management using autonomous access points.

## Centralized WLAN architecture

Instead of using autonomous access points, many corporate wireless networks use a centralized WLAN controller often abbreviated WLC – Wireless LAN Controller. A centralized WLAN controller controls LWAPs – lightweight access points. Unlike autonomous access points all user traffic in the data plane passes through the WLAN controller.  As seen in Figure 72, all client data passes through the WLAN controller.

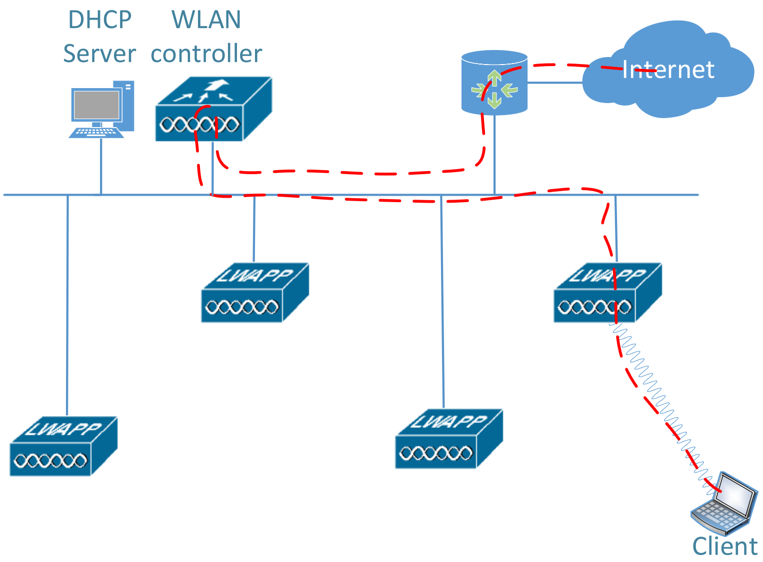


Figure 72 - WLAN controller using lightweight access points.

### AP Management

The WLAN controller controls the configuration and management of the lightweight access points including channel and power settings. Most WLAN controllers also support updating the firmware of the lightweight access points.

### 802.11 traffic tunnelling

All traffic from the wireless clients are tunnelled from the lightweight access point to the WLAN controller, as illustrated in Figure 73.

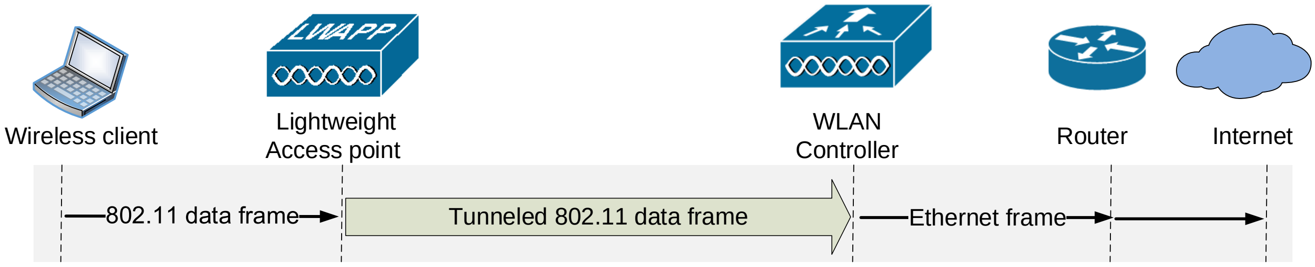
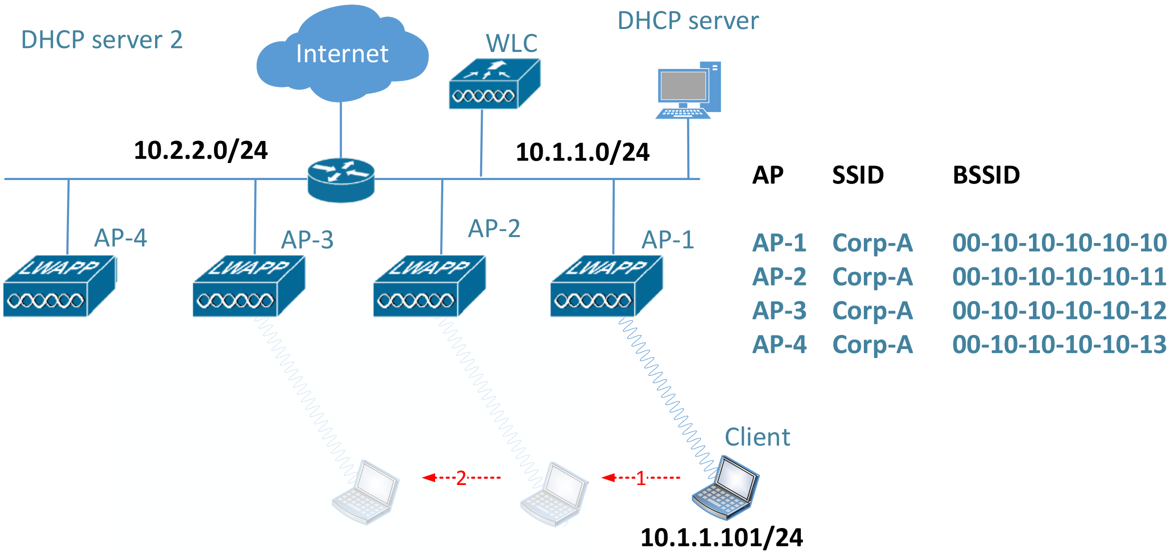


Figure 73 - Tunnel transferring 802.11 frames between lightweight access point and WLAN controller

## Roaming in network with WLAN controller

When using a WLAN controller – WLC – it is possible to make both layer-2 roaming and layer-3 roaming, because the tunnel between the lightweight access point and the WLC carries the 802.11 traffic inside the tunnel. The IP addresses of the lightweight access points are not seen or used by the wireless clients.

1. The client associates with the WLC through AP-1 using its BSSID
2. The client receives IP address 10.1.1.101 from the DHCP server
3. All user traffic from the client are sent from the WLC on the 10.1.1.0/24 network
4. The client moves towards AP-2
5. The client receives stronger signal from AP-2 when approaching
6. The client reassociates with the WLC to AP-2 using its BSSID
7. The client can still use the IP address 10.1.1.101 as the WLC is in the 10.1.1.0/24 network
8. The client moves towards AP-3
9. The client receives stronger signal from AP-3 when approaching
10. The client reassociates with the WLC to AP-3 using its BSSID
11. The client can still use the IP address 10.1.1.101 as the WLC is in the 10.1.1.0/24 network



| AP | SSID | BSSID |
|---|---|---|
| AP-1 | Corp-A | 00-10-10-10-10-10 |
| AP-2 | Corp-A | 00-10-10-10-10-11 |
| AP-3 | Corp-A | 00-10-10-10-10-12 |
| AP-4 | Corp-A | 00-10-10-10-10-13 |

Figure 74 - Successful layer-2 and layer-3 roaming, when using a WLC

### WLAN profiles

WLAN controllers are capable of announcing virtual SSIDs. In Figure 75 an example of a WLC announcing two SSID through its lightweight access points is shown. The traffic from the SSIDs is effectively separated through VLANs to the corporate network. A WLAN profile is basically the mapping of an SSID to a VLAN.

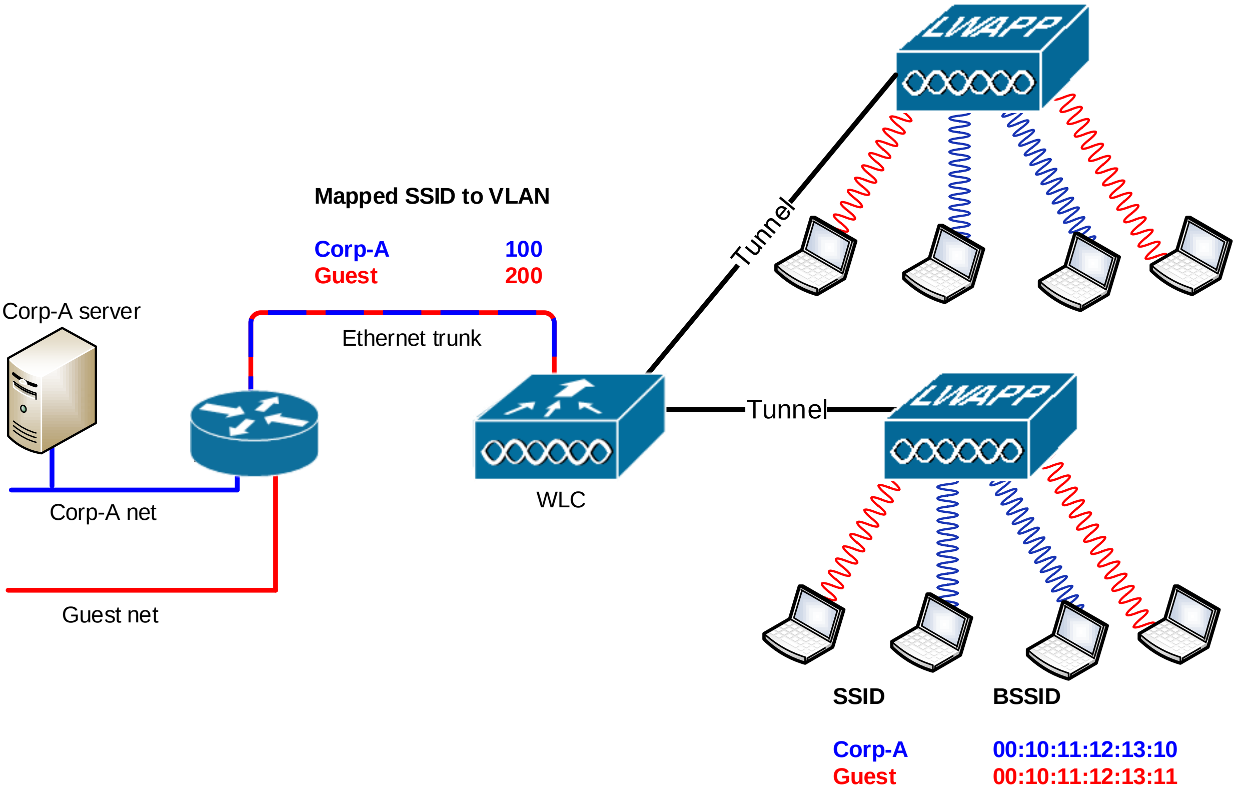
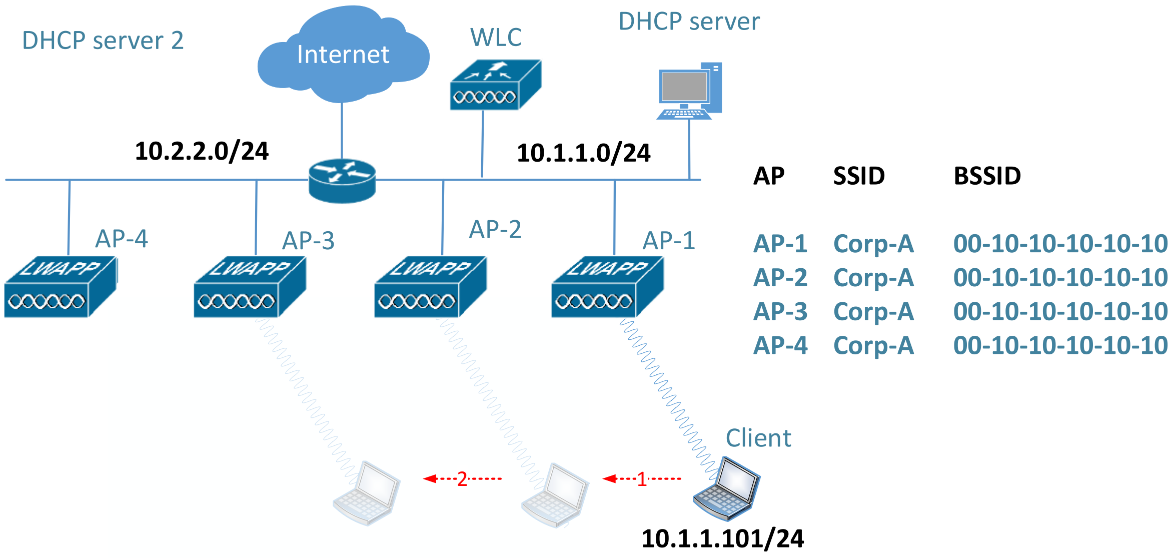


Figure 75 - WLC announcing virtual SSID's through lightweight access points

### Virtual access point system

Several vendors offer solutions known as Virtual access point or virtual AP. A virtual AP system is a system where several APs share the same BSSID. The client sees only one AP, because clients distinguish APs from each other by their normally unique BSSID addresses. The WLC controller receives the client’s signal strength information from the APs, and decides which access point is the most suitable to transmit and receive frames from the client.



| AP | SSID | BSSID |
|---|---|---|
| AP-1 | Corp-A | 00-10-10-10-10-10 |
| AP-2 | Corp-A | 00-10-10-10-10-10 |
| AP-3 | Corp-A | 00-10-10-10-10-10 |
| AP-4 | Corp-A | 00-10-10-10-10-10 |

Figure 76 - Virtual AP system with one SSID and one BSSID

# WLAN deployment and vertical markets

In this chapter we will look at different kind of services used in wireless network deployments. Different considerations need to be taken when handling deployment of services such as data, voice and video.

## Deployment considerations

When deploying wireless services considerations are based on different factors, such as user density, coverage and application service requirements.

### Data

When data-oriented applications such as email and web services are used, the main considerations when deploying Wi-Fi are user density, coverage and bandwidth. Data-oriented applications are not very time sensitive and are forgiving to packet loss and jitter, that is to say varying delay.

### Voice

Voice applications such as Voice over Wi-Fi – VoWiFi – on the other hand – are very sensitive to delay, jitter and packet loss. VoWiFi phones are typically handheld devices that often don't transmit with as much power as a laptop, to conserve battery power.

### Video

Transmission of video through Wi-Fi is generally more complex than voice, demanding streams for video and voice simultaneously. Video streaming is normally more tolerant to packet loss than voice.

### Video conferencing

When using video conferencing the voice stream is often prioritized higher than the video stream. If congestion should occur, small glitches in the video are not as disruptive as in the audio. If there are small glitches in the audio it is often necessary for the listener to ask the speaker to repeat the sentence.

## WLAN Troubleshooting

When troubleshooting in WLAN environments, many of the same methods used in wired networks also apply. Using the OSI model troubleshooting approach as seen in Figure 77, 802.11 WLAN troubleshooting is limited to OSI layer 1 and 2.

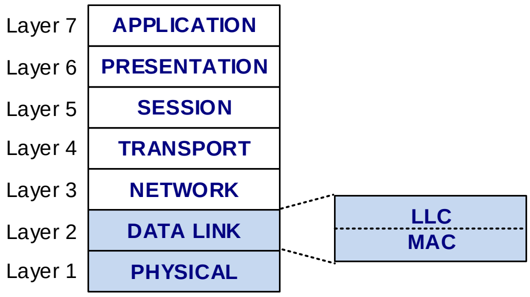


Figure 77 - OSI model with Wi-Fi layers marked

### Layer 2 retransmissions

The number one enemy of WLAN performance is layer 2 retransmissions which occur at the MAC sublayer. All unicast frames must be acknowledged by the receiver transmitting an ACK – acknowledgement frame. If a collision occurs or any part of the unicast frame is corrupted, the CRC – Cyclic Redundancy Check – will fail and the receiving 802.11 radio will not return an ACK frame to the transmitter. The unicast frame has to be retransmitted.

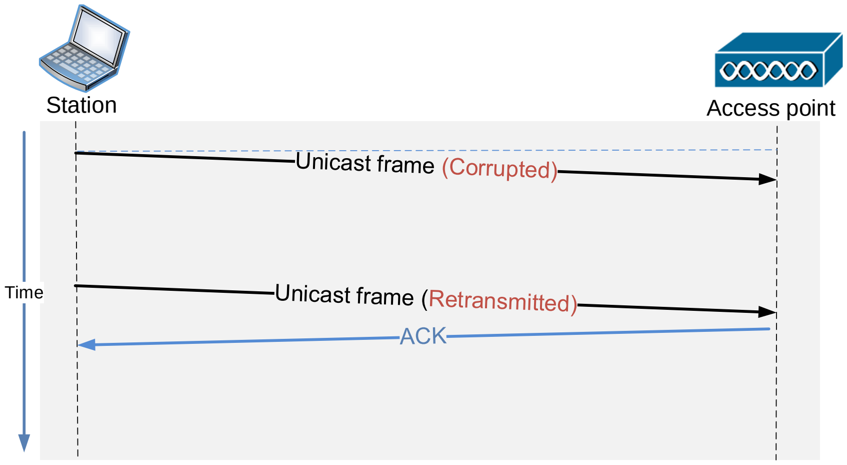
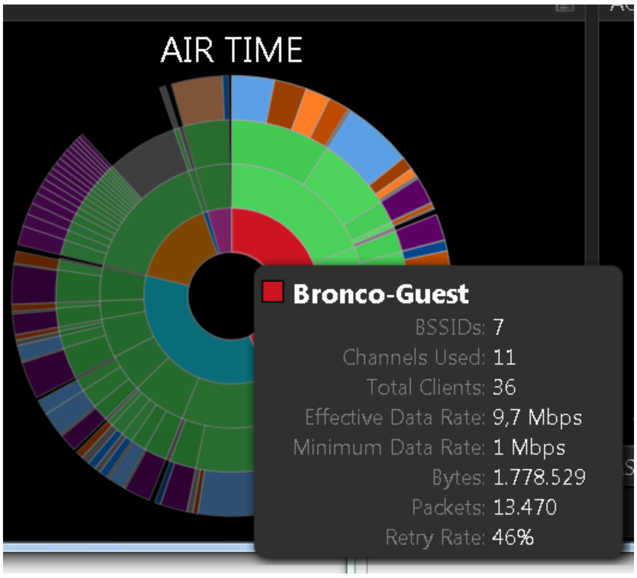


Figure 78 - Retransmission of unicast frames takes up airtime decreasing throughput.

Excessive layer 2 retransmissions can adversely affect the WLAN in two ways:

1. Throughput can decrease significantly if many retransmissions exist
2. Time sensitive services such as VoWiFi can suffer as retransmission of voice frames increases jitter.

Most data applications in WLAN environments handle up to 10% retransmissions without any noticeable performance penalty. Time sensitive applications such as VoWiFi require retransmissions to be less than 5% to ensure a timely and consistent delivery of voice packets.



🟥 **Bronco-Guest**

BSSIDs: 7
Channels Used: 11
Total Clients: 36
Effective Data Rate: 9,7 Mbps
Minimum Data Rate: 1 Mbps
Bytes: 1.778.529
Packets: 13.470
Retry Rate: 46%

Figure 79 - Screendump from MetaGeek Eye P.A. showing a high retry rate

When troubleshooting Wi-Fi networks, tools such as MetaGeeks Eye P.A are necessary to investigate Wi-Fi traffic.

There are many reasons why layer 2 retransmissions occur.

## RF interference

RF interference can reduce Wi-Fi performance significantly or even block traffic. If frames are corrupted due to RF interference, the number of retransmissions will rise reducing the throughput of the network.

Interference can come from several sources and in different forms and can be seen and found using a spectrum analyser. In the example in Figure 80 a possible interference near channel 11 is causing interference with nearby clients. The interfering device turns out to be an RF radiolink between a sound system and the rear speakers. Moving the access point from channel 11 to channel 6 reduced the retransmissions significantly.

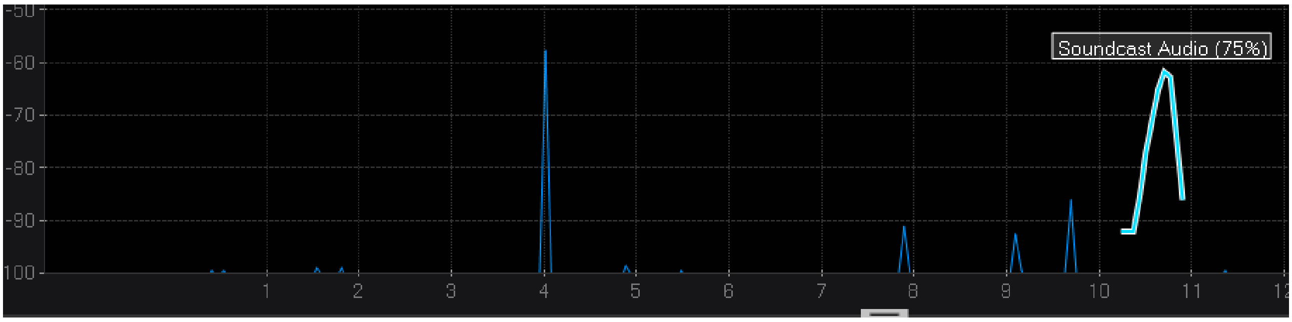


Figure 80 - MetaGeek Chanalyzer spectrum analyser discovered possible interference with sound castaudio device.

### *Channel interference*

If two nearby access points use the same channel, they will use CSMA/CA to avoid transmitting at the same time. When using CSMA/CA, interference between the two access points is reduced to a minimum because they are not transmitting simultaneously.

If two nearby access points use neighbouring channels that overlap each other as seen in Figure 81 the radios don't see each other and start transmitting if their own channel is free. Interference between the two channels will corrupt the frames if both access points transmit simultaneously. It is better to use the same channel instead of overlapping the channels.

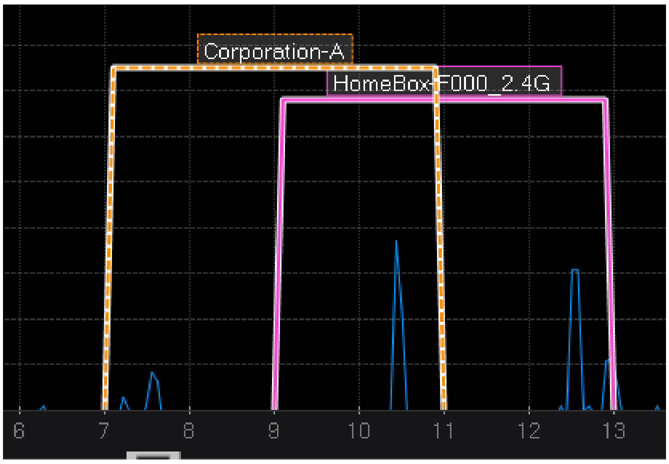


Figure 81 - Two access point overlapping each other's channel

Best of all of course is using non overlapping channels.

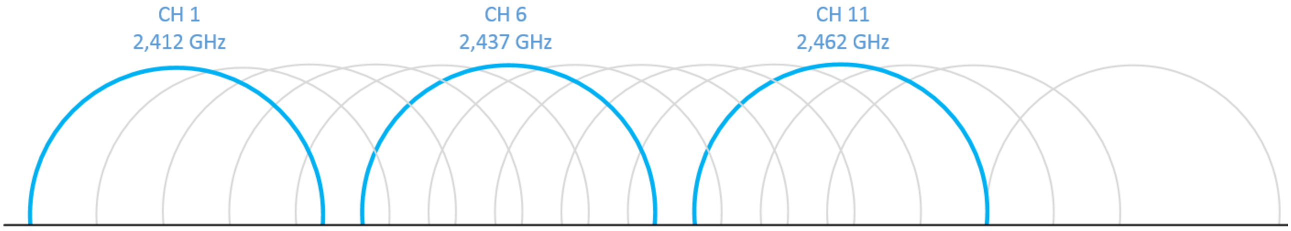


Figure 82 - Non overlapping channels 1, 6 and 11 in the 2.4 GHz band

### Multipath

Multipath can cause interference because of the time difference between the primary radio wave and the reflected radio wave(s) causing interference with each other. Multipath is an issue when legacy 802.11a/b/g networks are used. 802.11n uses multiple antennas using a MIMO technique – multiple-input multiple-output – receiving and transmitting on more than one antenna, reducing the effect of multipath. 802.11n will be discussed in a separate chapter.

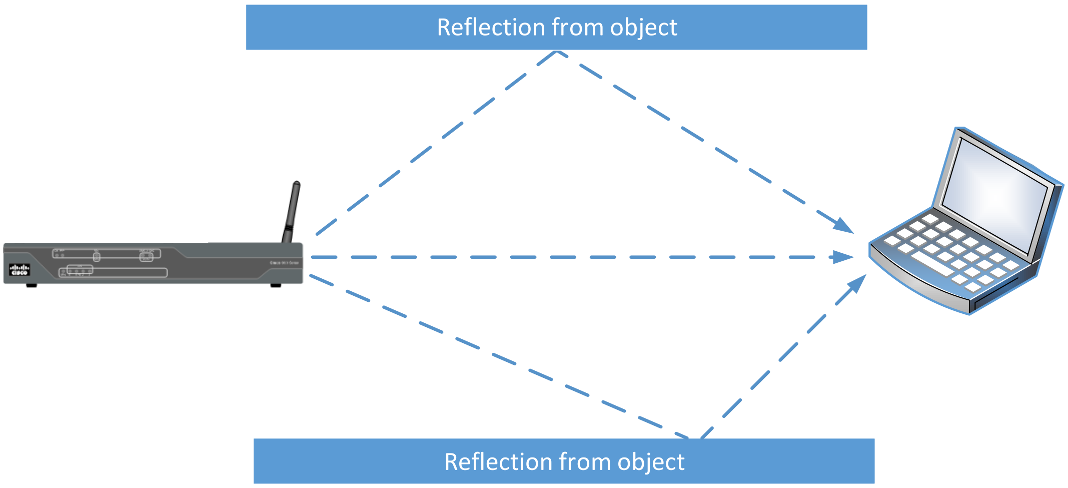


Figure 83 – Multipath can cause interference.

### Low Signal to Noise Ratio – SNR

The signal-to-noise ratio – SNR – is a measure of the quality of the received signal. SNR describes the difference between the received RF signal and the background RF noise floor as depicted in Figure 84. If the noise floor is measured to be -89 dBm and a radio receives a signal of -56 dBm the SNR is 33 dB. The SNR measured in Figure 84 is done with a spectrum analyser measuring the noise floor and WiFi radio measuring the signal strength of SSID 4S2SN.

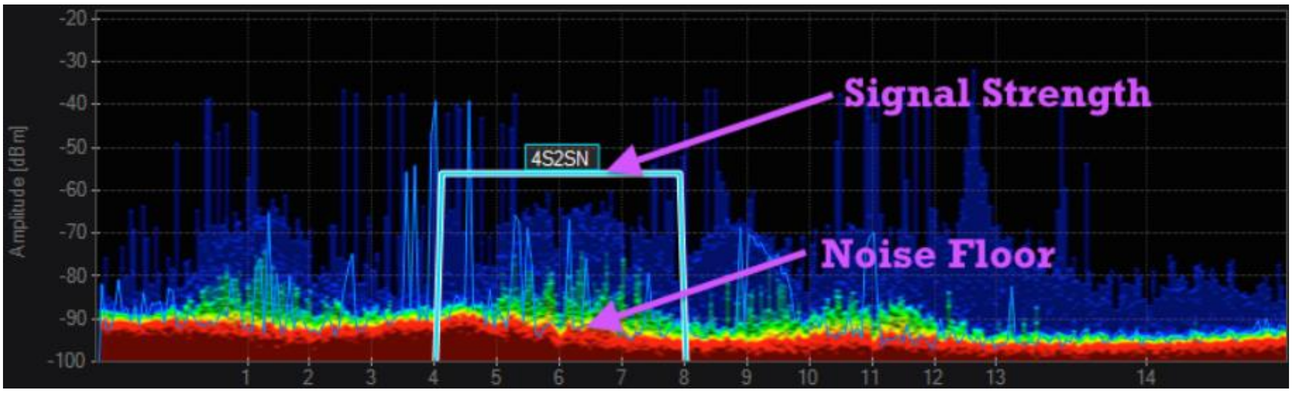


Figure 84 – Measuring SNR using Chanalyzer and a WiFi adapter.

If the SNR drops data corruption occurs in the received frames resulting in layer 2 retransmissions.

### *Hidden node problem*

Before an 802.11 radio starts transmitting it will listen, to determine if the radio channel is free before transmitting using the CSMA/CA access rules.

Station B in Figure 85 would think the radio channel was free even if station A was transmitting because station B is out of reach of station A's cover cell. If station B transmitted while station A transmitted interference would occur at the access point and layer 2 retransmission would be necessary.

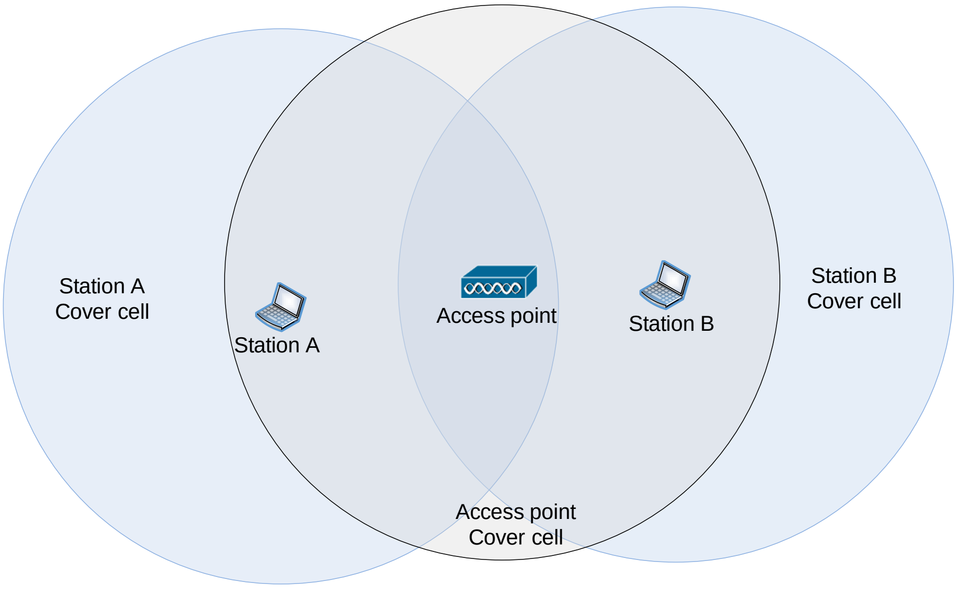


Figure 85 - Hidden node problem. Station A and station B are out of reach of each other

To solve hidden node problems RTS/CTS can be used. When station A wants to transmit, instead of transmitting the data when the channel is free, it transmits a RTS – Request To Send – as seen in Figure 86. The receiver responds with a CTS – Clear To Send – which is heard by station B which sets its NAV timer accordingly, and waits for the duration of the data transmission, thus avoiding interference.

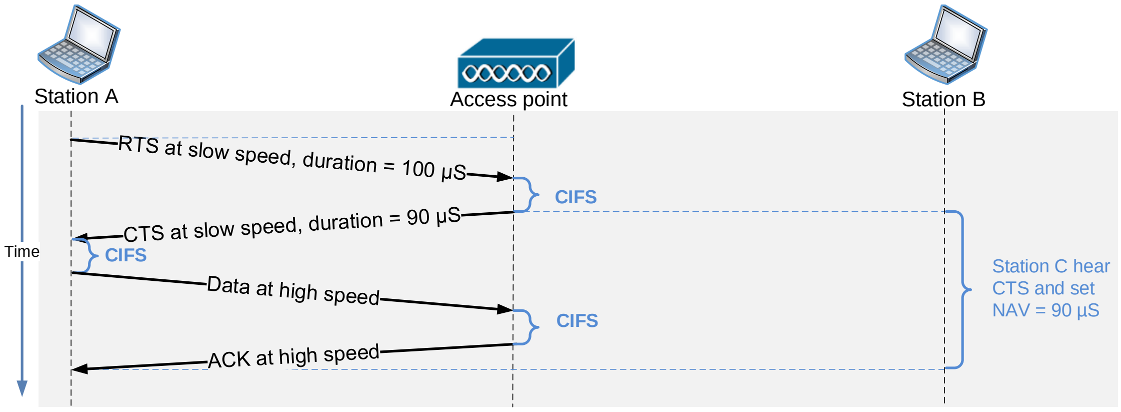


Figure 86 - RTS/CTS operation

RTS/CTS is an 802.11 option, used in mixed mode environments but they can be enabled if hidden node problems occur. RTS/CTS can reduce the throughput of the network, as it adds more protocol overhead. So, it might be a better idea in these situations to add an extra access point.

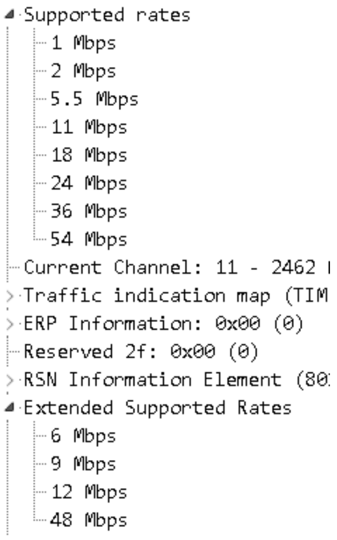
## 802.11 coverage

Providing sufficient coverage and capacity in a WLAN design solves many problems with interference and roaming.

### Dynamic rate switching

DRS or Dynamic Rate Switching is when a client decreases its bandwidth as it’s moved farther away from the access point. Access points support multiple data rates using different kinds of spread spectrum technologies.

As the signal strength gets lower because of the distance, the client and the access point shift to a lower data rate. The lower the data rate the longer time it takes to transmit data, lowering the total throughput of the BSS. It is often recommended to turn off the two lowest data rates 1 and 2 Mbps when designing an 802.11 network.



```
◢ Supported rates
    1 Mbps
    2 Mbps
    5.5 Mbps
    11 Mbps
    18 Mbps
    24 Mbps
    36 Mbps
    54 Mbps
  Current Channel: 11 - 2462 I
> Traffic indication map (TIM
> ERP Information: 0x00 (0)
  Reserved 2f: 0x00 (0)
> RSN Information Element (80
◢ Extended Supported Rates
    6 Mbps
    9 Mbps
    12 Mbps
    48 Mbps
```

Figure 87 – AP Data rates example

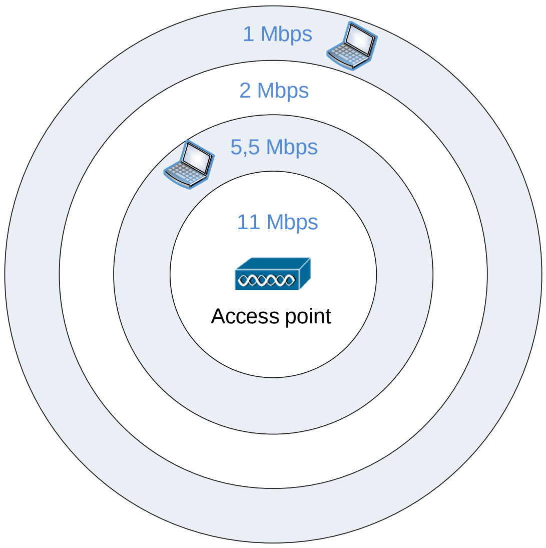


Figure 88 - Data rates based on signal strength/distance to the AP

### Multiple-Channel architecture

When designing coverage for Wi-Fi networks with more than one access point, it is important to ensure overlap between the access points allowing problem free roaming of clients and in the same time avoiding interference between the access points. In the 2.4 GHz ISA band, channels 1, 6 and 11 are not overlapping, making them suitable for coverage. Often the “honeycomb” architecture seen in Figure 89 is used to cover a large physical area, reusing the channels without interference between access points.

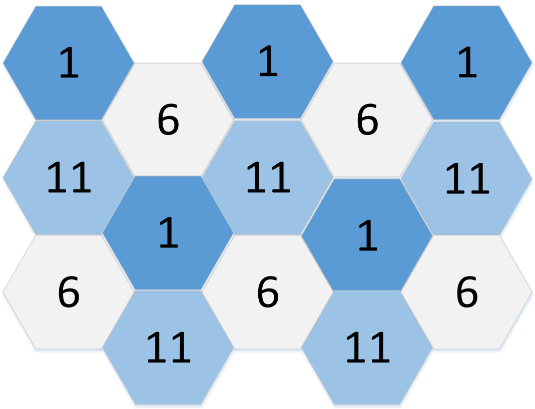


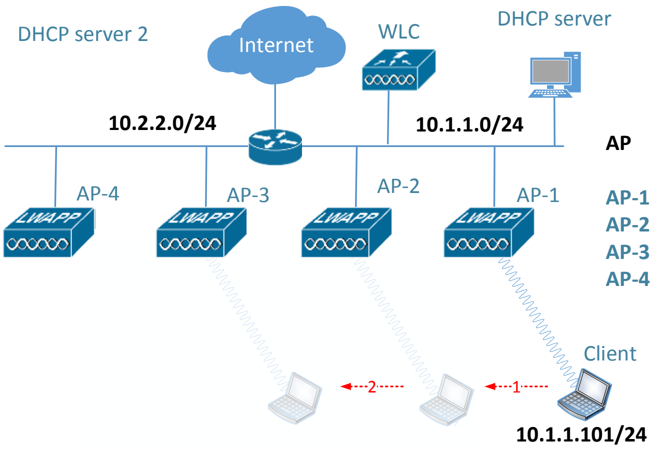
Figure 89 - "honeycomb" multichannel architecture

Channel reuse should also be used in the 5 GHz band, where a total of 24 non overlapping channels are available, making the “channel puzzle” easier.

Designing a network in buildings with multiple floors makes the puzzle three dimensional.

### Single-channel architecture

Instead of using non overlapping channels in adjacent access points, it is possible to use the same channel on neighbouring access points. The vendor Meru’s networks use single channel solutions. In Figure 90 the WLC decides which access point is the most suitable, based on signal strength, to transmit and receive frames from the client. The client will only see one access point as they all share the same SSID, BSSID and channel.



| AP | SSID | BSSID | Channel |
|---|---|---|---|
| AP-1 | Corp-A | 00-10-10-10-10-10 | 6 |
| AP-2 | Corp-A | 00-10-10-10-10-10 | 6 |
| AP-3 | Corp-A | 00-10-10-10-10-10 | 6 |
| AP-4 | Corp-A | 00-10-10-10-10-10 | 6 |

Figure 90 - Single channel single BSSID solution

## Coverage versus capacity

When designing Wi-Fi networks, a compromise between coverage and capacity needs to be considered. When designing for maximum coverage, a minimum number of access points cover as large an area as possible. Each access point transmits with as much power as is legal.

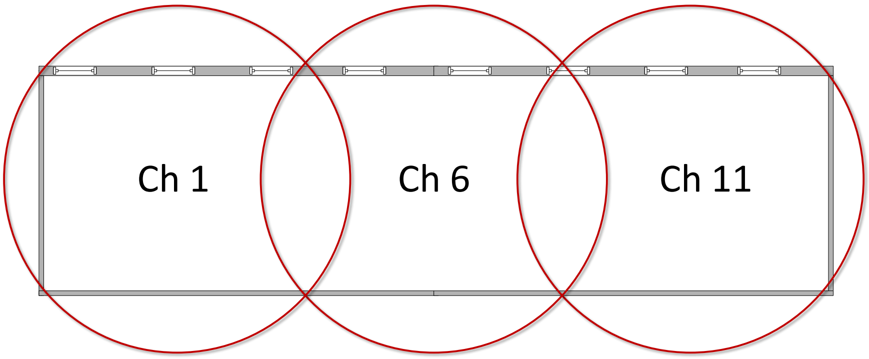


Figure 91 - designing for maximum coverage.

When designing for higher capacity, more access points need to be installed, reducing the power of each access point.

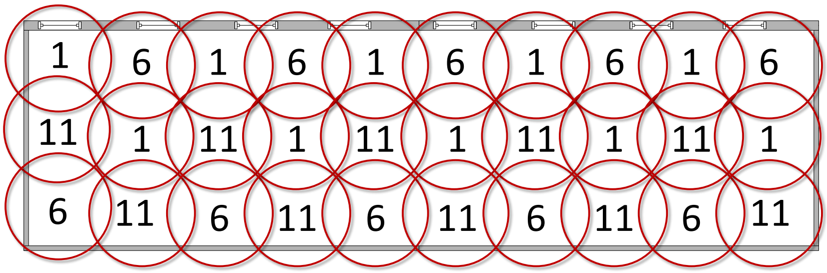


Figure 92 - Designing for maximum capacity

# 802.11 Network security

## 802.11 security basics

There are several issues to consider when implementing wireless network security:

- Authentication, authorization and accounting (AAA)
- Data privacy
- Monitoring
- Segmentation

Because data is transmitted openly through the air and anybody in range can eavesdrop on the transmitted frames, securing the frames using strong encryption is vital. The wireless access must be protected using an authentication solution that protects the network from unauthorized access by intruders.

### Authentication, Authorization and accounting

AAA or Authentication, Authorization and Accounting is a well-known security platform used to protect network resources in wired and wireless network environments.

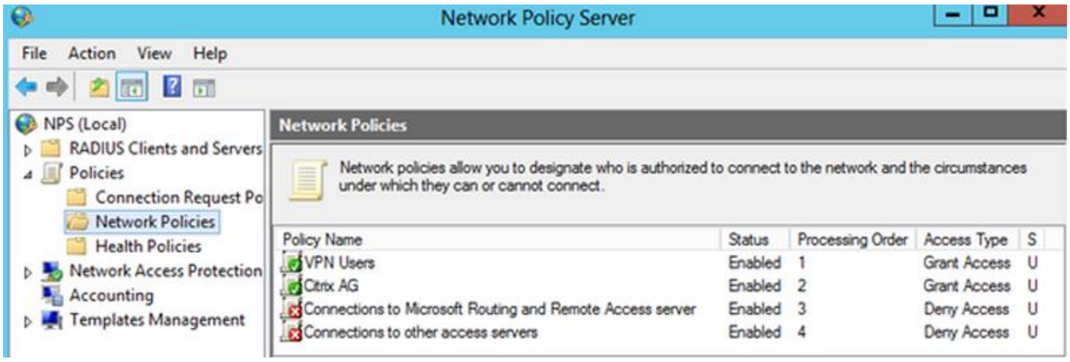
### *Authentication*

Authentication is the verification of user identity and credentials. User verification can include username, password, digital certificate, one-time-passwords or other verification credentials.

Figure 93 - Security token using time synchronized one-time-passwords

### *Authorization*

Authorization grants users access to network resources. When a user is authenticated the user has access only to the network resources to which he or she is authorized.



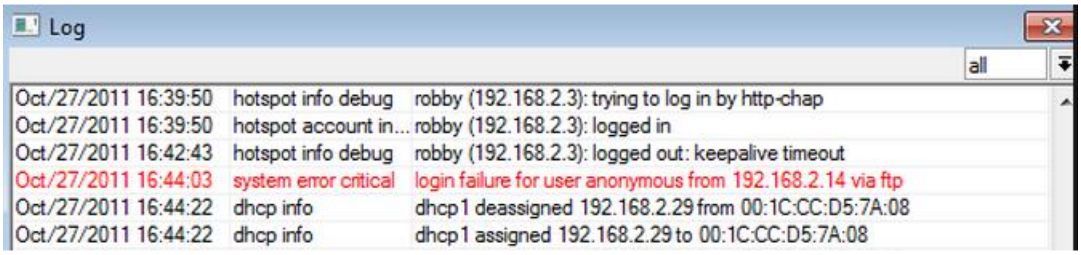
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

| Policy Name | Status | Processing Order | Access Type | S |
|---|---|---|---|---|
| VPN Users | Enabled | 1 | Grant Access | U |
| Citrix AG | Enabled | 2 | Grant Access | U |
| Connections to Microsoft Routing and Remote Access server | Enabled | 3 | Deny Access | U |
| Connections to other access servers | Enabled | 4 | Deny Access | U |

Figure 94 – Authorization of who is granted access to which network

### Accounting

Accounting is the process of logging access to network resources. It is important to log who accessed which resources and when. In some business areas, accounting is dictated by law.



```
Oct/27/2011 16:39:50  hotspot info debug   robby (192.168.2.3): trying to log in by http-chap
Oct/27/2011 16:39:50  hotspot account in... robby (192.168.2.3): logged in
Oct/27/2011 16:42:43  hotspot info debug   robby (192.168.2.3): logged out: keepalive timeout
Oct/27/2011 16:44:03  system error critical login failure for user anonymous from 192.168.2.14 via ftp
Oct/27/2011 16:44:22  dhcp info            dhcp1 deassigned 192.168.2.29 from 00:1C:CC:D5:7A:08
Oct/27/2011 16:44:22  dhcp info            dhcp1 assigned 192.168.2.29 to 00:1C:CC:D5:7A:08
```

Figure 95 - Small log file snippet

### Data privacy

To ensure data privacy, encryption algorithms are used to protect data from eavesdropping in transmissions between the Wi-Fi client and the access points. The traffic is encrypted even if the traffic was encrypted already by the application.

The two most common encryption algorithms in current use are RC4 and AES.

### RC4

RC4 or Rivers Cipher is an encryption cipher often used to protect internet traffic. RC4 is not considered as safe as AES encryption. Companies such as Cisco and Microsoft recommend avoiding RC4 encryption and instead use AES encryption.

### AES

AES or Advanced Encryption Standard is an encryption cipher much stronger than RC4, offering various key sizes. The AES encryption algorithm encrypts data in fixed block sizes with choices of encryption key strength of 128, 192 or 256 bits.

If you assume:

- Every person on the planet owns 10 computers.
- There are 7 billion people on the planet.
- Each of these computers can test 1 billion key combinations per second.
- On average, you can crack the key after testing 50% of the possibilities.

Then the earth's population can crack one 128 bit encryption key in 7.000.000.000.000.000.000.000.000 years!

*Famous technical Paper from Seagate titled "128-bit versus 256-bit AES"*

### *Encrypted frames*

Of the three major 802.11 wireless frames only the upper-layer information inside 802.11 data frames is encrypted. 802.11 management and 802.11 control frames are not encrypted. All radios need to understand the control and management frames but only the transmitting and receiving radio should be able to decrypt the upper layer data.

### Segmentation

Segmenting networks using VLAN's and firewalls to restrict user connections to segments of the network enhances overall security. Separating users into groups and allowing them to access only the needed resources and blocking access to restricted resources.

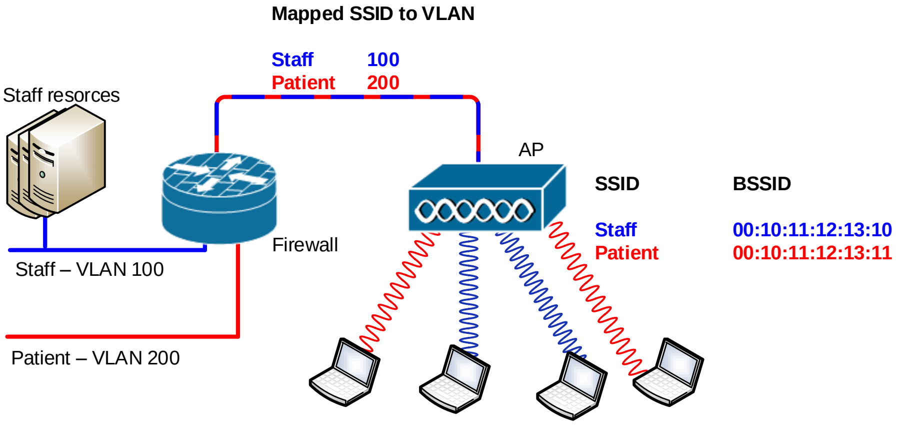


Figure 96 - Segmenting network using VLAN's and firewall in small hospital separating staff and patients traffic.

### Monitoring

Fulltime monitoring of the wireless network is important to protect against possible attacks targeting the WLAN. Systems such as WIDS – WLAN Intrusion Detection Systems – monitor the traffic 24/7 and alert security staff if a suspected attack is in progress.

## Wireless security standards

Security has evolved fast since the introduction of 802.11. The original security standards are all cracked and considered legacy. As seen in Figure 97 the original security standard was WEP – Wired Equivalent Privacy. WPA personal was added later in 2004 and WPA2 in 2007 adding to the confusion.

| Standard | From | Wi-Fi alliance certification | Authentication | Encryption method | Encryption cipher |
|---|---|---|---|---|---|
| 802.11 legacy | 1999 | | Open system or shared key | WEP | RC4 |
| 802.11i | 2004 | WPA personal | Preshared key | TKIP | RC4 |
| | | WPA-Enterprise | 802.1X/EAP | TKIP | RC4 |
| 802.11-2007-RSN | 2007 | WPA2-Personal | WPA2 preshared key | CCMP | AES |
| | | WPA2-enterprise | 802.1X/EAP | CCMP | AES |

Figure 97- Security standards and Wi-Fi alliance certification

The encryption method is the implementation of the encryption cipher and includes frame formats and key exchange between the two radios.

## 802.11 legacy security - Shared Key Authentication

Shared key authentication uses WEP – Wired Equivalent Privacy – when authenticating client stations. It requires that a static WEP key is configured on the AP and the client. The client will not be able to authenticate with the AP if the static WEP keys do not match. Shared key authentication is a four way authentication frame exchange with eight frames transmitted through the air.

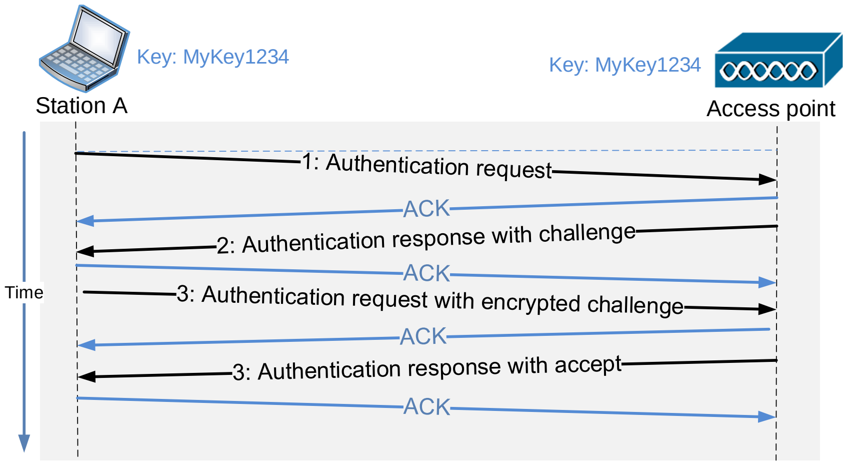
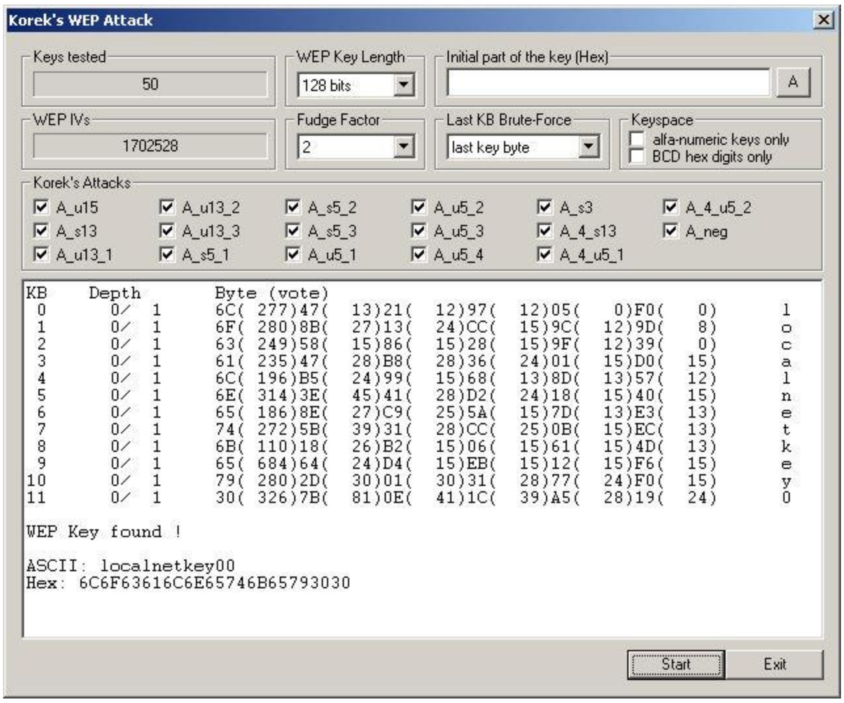

Key: MyKey1234
Station A
Key: MyKey1234
Access point
Time
1: Authentication request
ACK
2: Authentication response with challenge
ACK
3: Authentication request with encrypted challenge
ACK
3: Authentication response with accept
ACK

Figure 98 – Successful shared key Authentication with WEP.

WEP authentication is considered insecure and should be avoided.

### *What makes WEP authentication insecure?*

The main reason WEP authentication is insecure, is that it is possible for an intruder to sniff the challenge transmitted by the AP and the encrypted challenge returned from the client. It is possible for the intruder to brute force the secret key with this information.



Korek's WEP Attack

Keys tested: 50

WEP Key Length: 128 bits

Initial part of the key (Hex):

WEP IVs: 1702528

Fudge Factor: 2

Last KB Brute-Force: last key byte

Keyspace:
☐ alfa-numeric keys only
☐ BCD hex digits only

Korek's Attacks:

☑ A_u15 ☑ A_u13_2 ☑ A_s5_2 ☑ A_u5_2 ☑ A_s3 ☑ A_4_u5_2
☑ A_s13 ☑ A_u13_3 ☑ A_s5_3 ☑ A_u5_3 ☑ A_4_s13 ☑ A_neg
☑ A_u13_1 ☑ A_s5_1 ☑ A_u5_1 ☑ A_u5_4 ☑ A_4_u5_1

```
KB    Depth        Byte (vote)
 0      0/  1      6C( 277)47(  13)21(  12)97(  12)05(   0)F0(   0)      l
 1      0/  1      6F( 280)8B(  27)13(  24)CC(  15)9C(  12)9D(   8)      o
 2      0/  1      63( 249)58(  15)86(  15)28(  15)9F(  12)39(   0)      c
 3      0/  1      61( 235)47(  28)B8(  28)36(  24)01(  15)D0(  15)      a
 4      0/  1      6C( 196)B5(  24)99(  15)68(  13)8D(  13)57(  12)      l
 5      0/  1      6E( 314)3E(  45)41(  28)D2(  24)18(  15)40(  15)      n
 6      0/  1      65( 186)8E(  27)C9(  25)5A(  15)7D(  13)E3(  13)      e
 7      0/  1      74( 272)5B(  39)31(  28)CC(  25)0B(  15)EC(  13)      t
 8      0/  1      6B( 110)18(  26)B2(  15)06(  15)61(  15)4D(  13)      k
 9      0/  1      65( 684)64(  24)D4(  15)EB(  15)12(  15)F6(  15)      e
10      0/  1      79( 280)2D(  30)01(  30)31(  28)77(  24)F0(  15)      y
11      0/  1      30( 326)7B(  81)0E(  41)1C(  39)A5(  28)19(  24)      0

WEP Key found !

ASCII: localnetkey00
Hex: 6C6F63616C6E65746B65793030
```

Figure 99 – One of many WEP attack programs to brute force WEP keys.

## TKIP and CCMP encryption methods

### TKIP – Temporal Key Integrity Protocol

TKIP – Temporal Key Integrity Protocol – defines a method of using RC4 encryption cipher just as WEP, but is more secure as it addresses many of the known weaknesses of WEP.

### CCMP

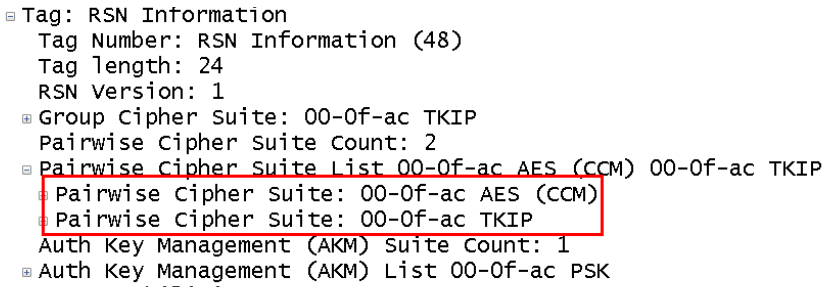
CCMP - Counter Mode Cipher Block Chaining Message Authentication Code Protocol – defines a method of using AES encryption. CCMP/AES uses 128 bit encryption key size and is considered much stronger than TKIP.

## RSN – Robust Security Network

The IEEE 802.11-2007 standard defines RSN – Robust Security Network – and RSNA – Robust Security Network Associations. When two radios authenticate and associate they create dynamic encryption keys that are unique between the two radios.  This association between the two radios is called an RSNA.

When using RSN, implementing CCMP/AES encryption is preferred over TKIP/RC4 when possible.

An RSN – robust security network – is a network that only allows for RSNA's robust security network associations. An RSN network can be identified through the RSN information field in beacon and probe response frames.



```
⊟ Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 24
    RSN Version: 1
  ⊞ Group Cipher Suite: 00-0f-ac TKIP
    Pairwise Cipher Suite Count: 2
  ⊟ Pairwise Cipher Suite List 00-0f-ac AES (CCM) 00-0f-ac TKIP
    ⊞ Pairwise Cipher Suite: 00-0f-ac AES (CCM)
    ⊞ Pairwise Cipher Suite: 00-0f-ac TKIP
    Auth Key Management (AKM) Suite Count: 1
  ⊞ Auth Key Management (AKM) List 00-0f-ac PSK
```

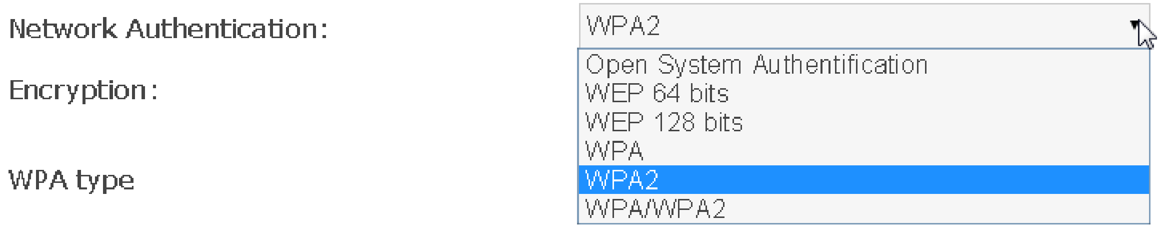
Figure 100 - RSN field in beacon frame indicating support of both TKIP and CCMP. (Screen dump from Wireshark)

## Authentication and authorization

The 802.11-2007 standard defines authentication and key management that can be either a PSK - preshared key – or an EAP protocol – Extensible Authentication Protocol – used during 802.1X authentication. 802.1X/EAP requires a RADIUS server and advanced configuration to operate. A RADIUS – Remote Authentication Dial-In User Service – is a centralized server based database containing authentication and authorization information.

## PSK authentication

WPA-personal and WPA2-personal uses PSK – preshared key – authentication. A preshared key is typically a key shared by all associated radios. PSK with WPA/WPA2-personal is often used in small networks such as home networks where a RADIUS server would be overkill.



Network Authentication: WPA2

Encryption:

WPA type

Figure 101 - Screen dump from small home Wireless router

As seen from Figure 101 it is possible to select either WPA or WPA2, or WPA and WPA2. It is implicit that a preshared key is used and not 802.1X/EAP. The same preshared key is used on all associated radios.

The preshared key called a passphrase is a simple ASC-II string from 8 to 63 characters. It is important to select the key carefully as it could be vulnerable to offline brute force dictionary attacks.

Some vendors have developed their own creative solution using a different key for each associated radio.

## 802.1X/EAP

The IEEE 802.1X standard is not a wireless standard. It is a standard that allows port based access control, allowing or blocking traffic from passing through a port. 802.1X is used in 802.3 Ethernet and 802.11 Wi-Fi environments and secures access to the network based on authentication and authorization.

802.1X implements three roles:

| Role | Function |
|---|---|
| **Supplicant** | Host requesting access to network resources. Each supplicant has unique credentials. |
| **Authenticator** | A device that blocks or allows traffic to pass through it. Authentication traffic is handled by the authenticator |
| **Authentication server** | A server that validates credentials of the supplicant. |

The authenticator in Figure 102 will only allow traffic from the supplicant after it has been successfully validated, and they have exchanged dynamic encryption keys.

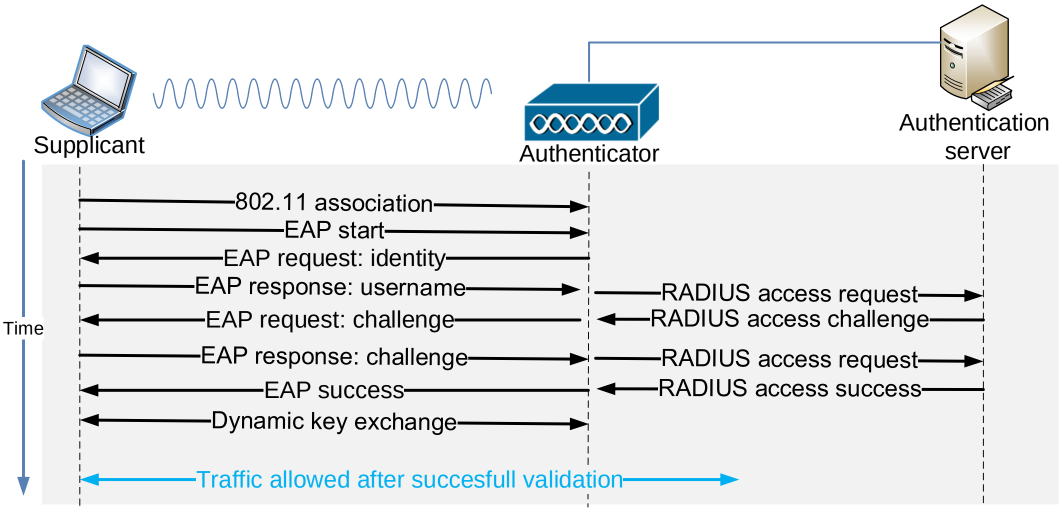


Figure 102 - 802.1X authentication. Authenticator blocks all traffic from the supplicant until validated.

### *EAP and variants*

EAP – Extensible Authentication Protocol – is an authentication framework to exchange authentication information between supplicant and authentication server. EAP is a framework and not a specific authentication transport protocol.

Several versions of transporting EAP – Extensible Authentication Protocol – exist, such as Cisco's LEAP – Lightweight EAP – or PEAP – Protected EAP. PEAP even exists in two different versions. The Wi-Fi alliance supports five different EAP implementations.

| | EAP-TLS | EAP-TTLS | PEAPv0 | PEAPv1 | EAP-FAST |
|---|---|---|---|---|---|
| **IETF** | RFC-5216 | RFC-5281 | draft | draft | RCF 4851 |

| | | | | | |
|---|---|---|---|---|---|
| **Digital certificate client** | Yes | Optional | No | Optional | No |
| **Digital certificate server** | Yes | Yes | Yes | Yes | No |
| **Client password authentication** | No | Yes | Yes | Yes | Yes |

## Wireless attacks

An intruder can use wireless access to attack the wired resources, as the normal operation of an 802.11 WLAN is to connect wireless clients to the wired network. The wireless network and the wireless network resources have to be properly secured.

### Rogue wireless devices

A rogue access point is any unauthorized access point connected to the wired network. Any person could attach an access point to a live Ethernet port and gain wireless access through it. Cheap off-the-shelf SOHO routers are plug-and-play devices that could easily be attached to an Ethernet port by an employee or a visitor.

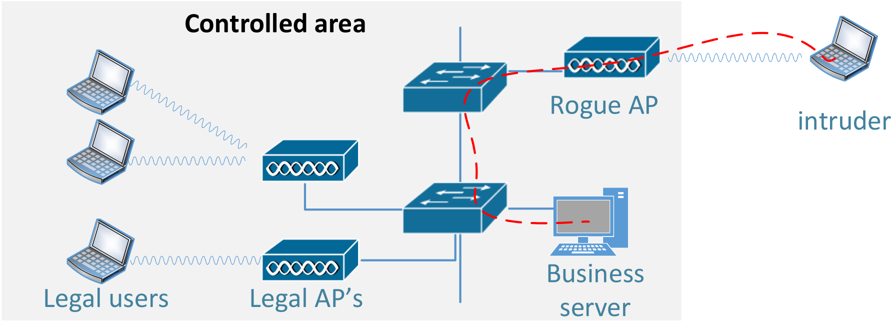


Figure 103 - Intruder gaining access to network resources through rogue access point.

It is possible for an intruder to lure an employee to accept an 802.11 ad hoc connection. As depicted in Figure 104 the intruder gains access through a legal user's Ethernet connection. Many organizations ban ad hoc networks and disable the ability to configure ad hoc networks on the users' laptops.

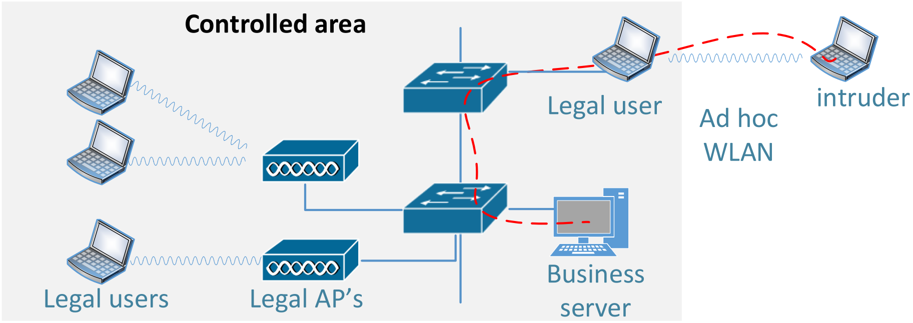
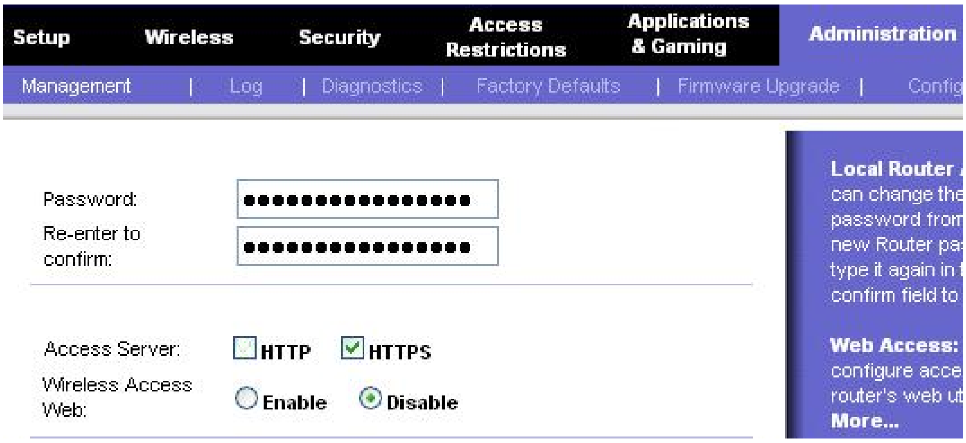


Figure 104 - ad-hoc connection allowing an intruder access through employee Ethernet access.

## Management interface exploits

Most wireless equipment is configured and managed through a management interface. Management interfaces can often be accessed through a web interface, a serial port, telnet or SNMP – Simple Network Management Protocol. It is important to configure strong passwords and disable unused management access interfaces. Default passwords are publicly available and should always be changed.



Password: ●●●●●●●●●●●●●●●●●

Re-enter to confirm: ●●●●●●●●●●●●●●●●●

Access Server: □ HTTP ☑ HTTPS

Wireless Access Web: ○ Enable ● Disable

Figure 105 - Management reachable only through wired access and HTTPS.

## DoS - Denial of Service attack

DoS or Denial of service attacks can temporarily disable a wireless network. Tools are available for any person who wishes to disable – at least temporarily – a wireless network. There are no countermeasures against DoS attacks except locating and disabling the source.

DoS attacks can be performed at OSI layer 1 – the physical layer – by jamming or it could be performed at OSI layer 2 – the 802.11 MAC layer.

## Layer 1 DoS attack

Layer 1 DoS attacks can be intentional or unintentional. A microwave oven can unintentionally cause interference halting wireless traffic. A spectrum analyser is the preferred tool used to locate interfering devices.

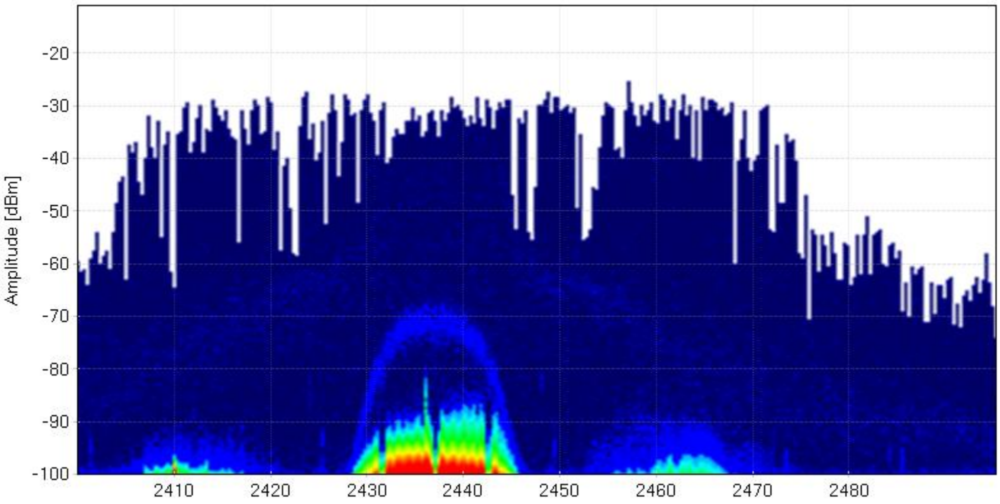
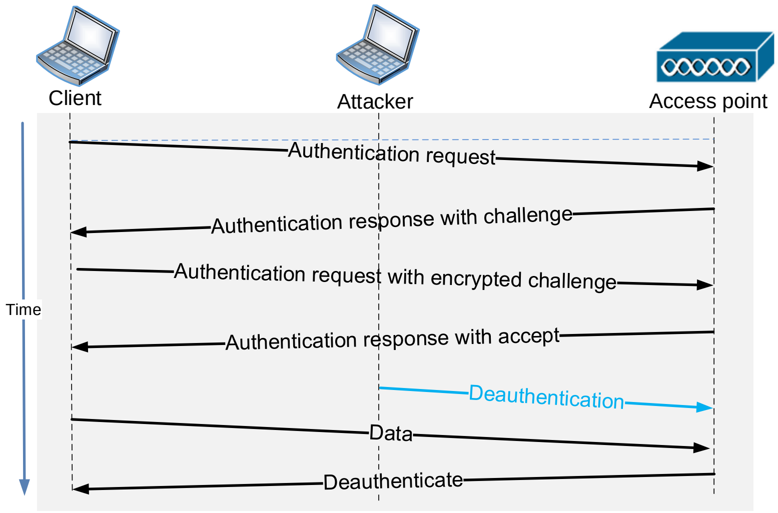


Figure 106 - 2,4 GHz spectrum showing high utilization at channel 6. (2,437 GHz)

In Figure 106 showing the 2.4 GHz spectrum it is noted that there is a high utilization around channel 6 at 2.437 GHz. The red colour means utilization at over 50%, which is high.

## Layer 2 DoS attack

Layer 2 DoS attacks exploit the management frames of an 802.11 network. The most common is to spoof disassociation and deauthentication frames by transmitting spoofed 802.11 frames using the target's MAC address.  Other layer 2 attacks involve association and authentication floods. A WIDS – Wireless Intrusion Detection System – will discover the layer 2 attack and notify the administrator.



Client
Attacker
Access point
Authentication request
Authentication response with challenge
Authentication request with encrypted challenge
Time
Authentication response with accept
Deauthentication
Data
Deauthenticate

Figure 107 - Deauthentication attack. One deauthentication shown.

In Figure 107 the client is deauthenticated by the attacker. The client needs to authenticate and associate to get back on the access point. Only one frame from the attacker is necessary to deauthenticate the client, while the client needs a lot of frames to reassociate.

## WIDS and WIPS

WIDS – Wireless Intrusion Detection Systems and WIPS – Wireless Intrusion Prevention Systems – are used to monitor and detect rogue devices and DoS attacks. A WIPS can also isolate and prevent the intrusion.

An intrusion detection or prevention system will monitor the radio spectrum for the presence of unauthorized access points – intrusion detection, and can automatically take countermeasures – intrusion prevention. A WIDS or WISP uses radio sensors placed strategically throughout the WLAN cover zone. The sensors are the eyes and ears of the system.

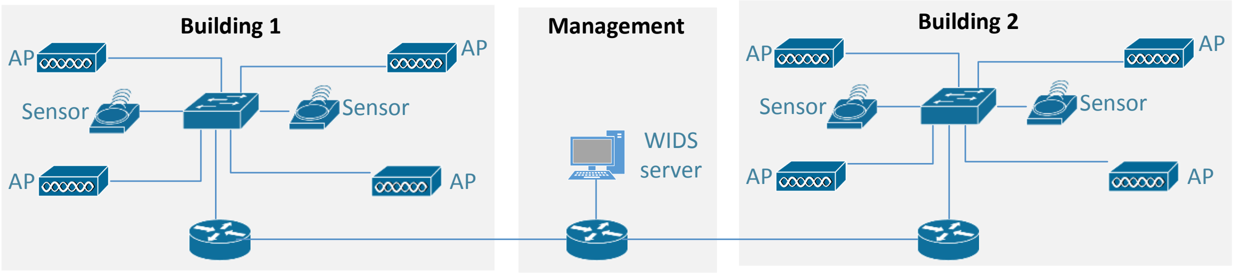


Figure 108 - WIDS server collects information from all sensors.

## Site survey

A site survey is the process of planning and designing a wireless network, to provide a wireless solution that will deliver the required wireless coverage, data rates, network capacity, roaming capability and Quality of Service (QoS).

The survey usually involves a site visit to test for RF interference, and to identify optimum installation locations for access points.

There is a huge difference between performing a site survey in a two-room restaurant and a 16 floor hospital.

### WLAN site survey interview

Before the actual site survey is conducted, a site survey interview with the customer should be performed. The interview is used to determine the purpose of the wireless network and the expectations the customer has for the new wireless network. The interview should answer questions such as:

| | |
|---|---|
| **Coverage** | Physical locations where wireless coverage is wanted |
| **Applications** | Which applications do the users use? VoWiFi, a lot of streaming video, etc. |
| **Capacity** | How many users should be planned for? Where are they located, are there special requirements regarding guests, meeting rooms, outside locations etc. |

### Capacity and coverage

Before actually planning how many access points are needed and where they should be located, a thorough understanding of the customers' expected wireless capacity and coverage should be prepared. With a copy of the floor plan of the coverage area it is possible to get an overview of the planned capacity, as discussed during the site survey interview. Questions such as where the users are located are necessary to plan for the access point's cell size. Smaller cell sizes give more capacity but increase the number of necessary access points. Consideration of using the crowded 2.4 GHz band or using the less crowded 5 GHz band or both should be considered, as 5 GHz access points have a smaller cell size due to the operating frequency.

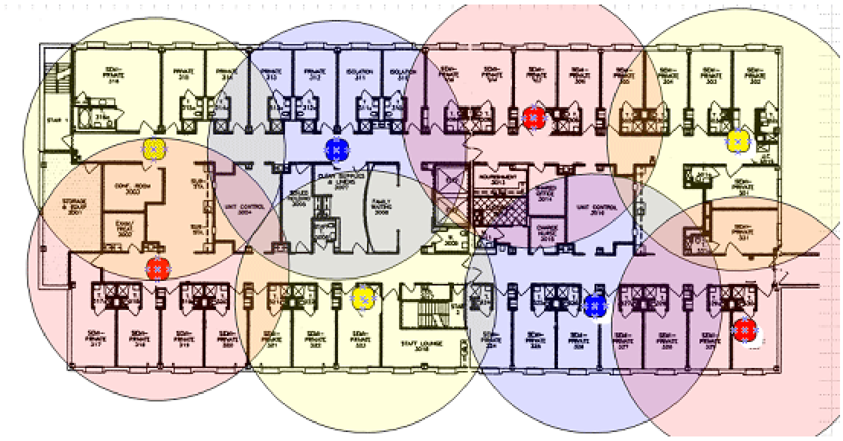


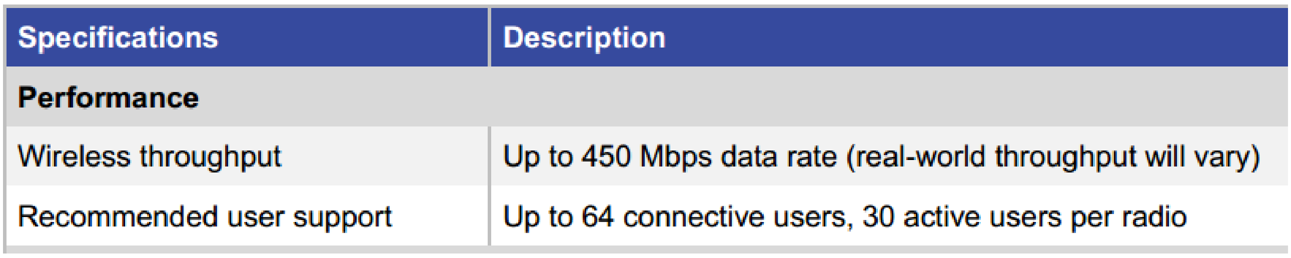
Figure 109 – Floor plan with a preliminary plan of cell size vs. capacity

Before actually planning where the access points should be located, a physical site survey should be performed using proper site survey tools, such as spectrum analysers and determining the actual 802.11 RF coverage in the physical area of the network.

### Planning for wireless traffic

The type of applications used by the users has an important impact in estimating how many users can be associated to each access point.

In an 802.11a/b/g/n network, 30 to 35 users is an often quoted figure.



| Specifications | Description |
|---|---|
| **Performance** | |
| Wireless throughput | Up to 450 Mbps data rate (real-world throughput will vary) |
| Recommended user support | Up to 64 connective users, 30 active users per radio |

Figure 110 - Extract from Cisco data sheet from Small Business 500 series access point.

### Planning for VoWiFi

When planning for voice over Wi-Fi – VoWiFi – a number of considerations come into account. How many calls can an access point handle? It depends on the access point but recommendations of between seven and twelve are often mentioned. Handover time when roaming between access points is crucial when dealing with VoWiFi and handover performance is dependent on the chosen authentication process as seen in the table below. Note the shown handover times are estimations and should be measured in the live network, as they can vary depending on encryption type, network load and other factors.

| Authentication | Encryption type | Handover time |
|---|---|---|
| **Open** | None | ~ 11 mS |
| **Open** | WEP | ~ 12 mS |
| **WPA-PSK** | TKIP | ~ 35 mS |
| **WPA2-PSK** | AES-CCMP | ~ 28 mS |
| **LEAP** | WEP | ~ 37 mS |
| **LEAP** | TKIP | ~ 45 mS |
| **LEAP with CCKM** | TKIP | ~ 12 mS |
| **PEAP** | AES-CCMP | ~ 30 mS |

### User density

Estimating user density is very important when planning access point cell sizes. Use the floor plan together with the customer to estimate how many users there are in each area. Remember to ask the customer if there are peak hours, where the user density is higher. Locations such as conference halls, dining rooms, parking lots, lecture rooms, bath rooms and staircases should be taken into account when talking to the customer. How many users may need wireless coverage in the future?

Figure 111 - Lecture hall at York University[3].

### Backward compatibility

If there are any requirements for backward compatibility to legacy clients, the 802.11 protection mechanism will have an impact on throughput. Many VoWiFi phones, older laptops and other specialized equipment require backward compatibility.

## Existing wireless network

Fixing problems in an existing wireless network often requires a site survey to reveal any problems. Issues such as sources of unwanted RF interference, changes in user density and changes in the user data pattern should be considered during a site survey. If a prior site survey has been conducted, getting access to the documentation of the old survey will be helpful when troubleshooting.

## Distribution network

The access points of the new design must be connected to the customer's distribution network allowing the wireless clients access to network resources. Understanding of the existing distribution network's topology

[3] Picture from Wikimedia commons, under GNU Free Documentation License

is important when planning the wireless network. Issues such as roaming performance, security and physical location of switches, where access points are connected, should be considered when planning the wireless network.

## Documents and reports

During the site survey proper documentation should be created. Most companies working with WLAN site survey use their own documentation standard and checklists to ensure proper documentation. The documentation often includes on-site measurements of signal strengths, interference, and channel overlap and spectrum analysis documentation.

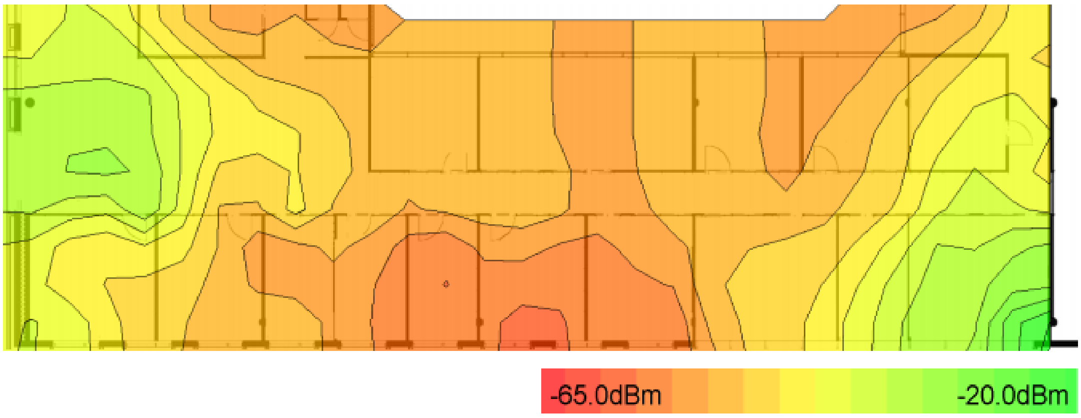
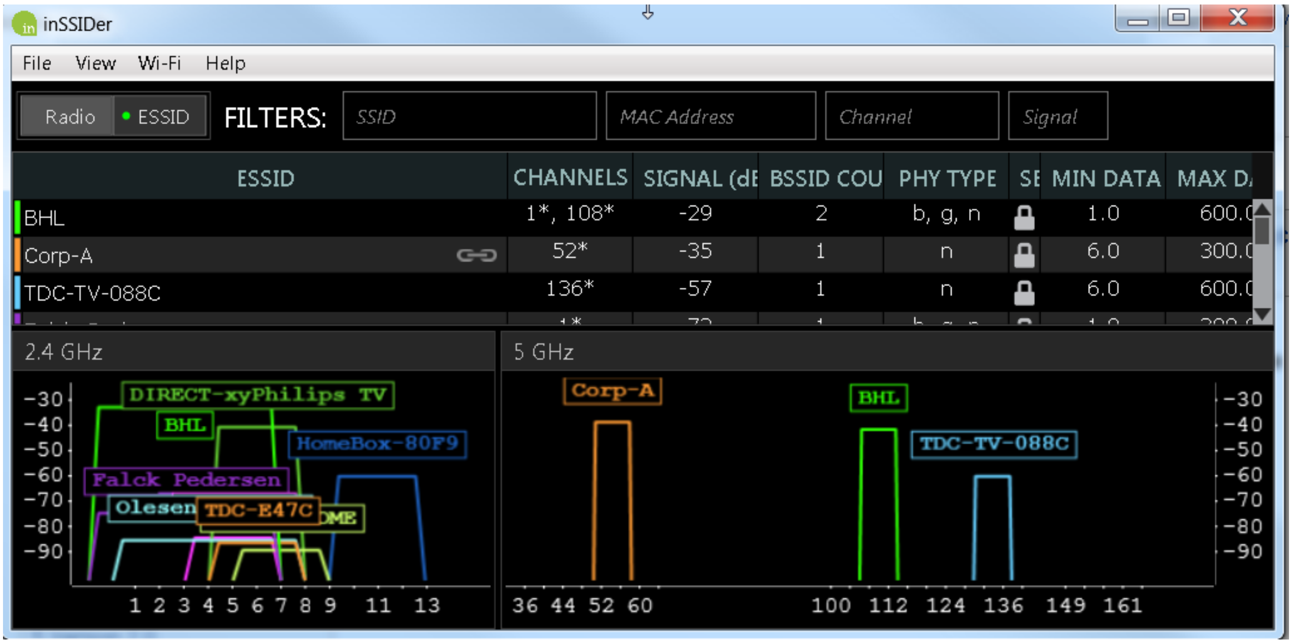


Figure 112 - Partial signal strength measurement example.

# Site survey systems and devices

## Wi-Fi network scanner

A Wi-Fi network scanner is a tool to discover nearby Wi-Fi networks. Typically information such as SSID, BSSID, channel, available data rates, security types and signal strength are obtained.



| ESSID | CHANNELS | SIGNAL (dI | BSSID COU | PHY TYPE | SE | MIN DATA | MAX D/ |
|---|---|---|---|---|---|---|---|
| BHL | 1*, 108* | -29 | 2 | b, g, n | 🔒 | 1.0 | 600.( |
| Corp-A | 52* | -35 | 1 | n | 🔒 | 6.0 | 300.( |
| TDC-TV-088C | 136* | -57 | 1 | n | 🔒 | 6.0 | 600.( |

Figure 113 - inSSIDer a popular network scanner from Metageek.

## Spectrum analysers

A spectrum analyser is a tool to measure signal strength in a specified frequency range. When troubleshooting and conducting site surveys for IEEE 802.11 wireless networks, a spectrum analyser measuring the ISM – 2.4 GHz – band and UNII-1 to UNII-3 – 5 GHz – bands are a powerful tool.

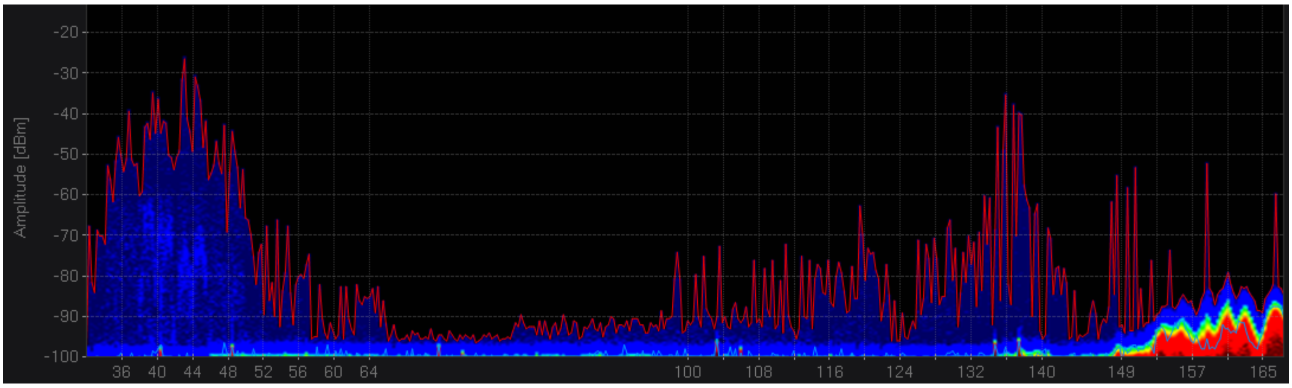
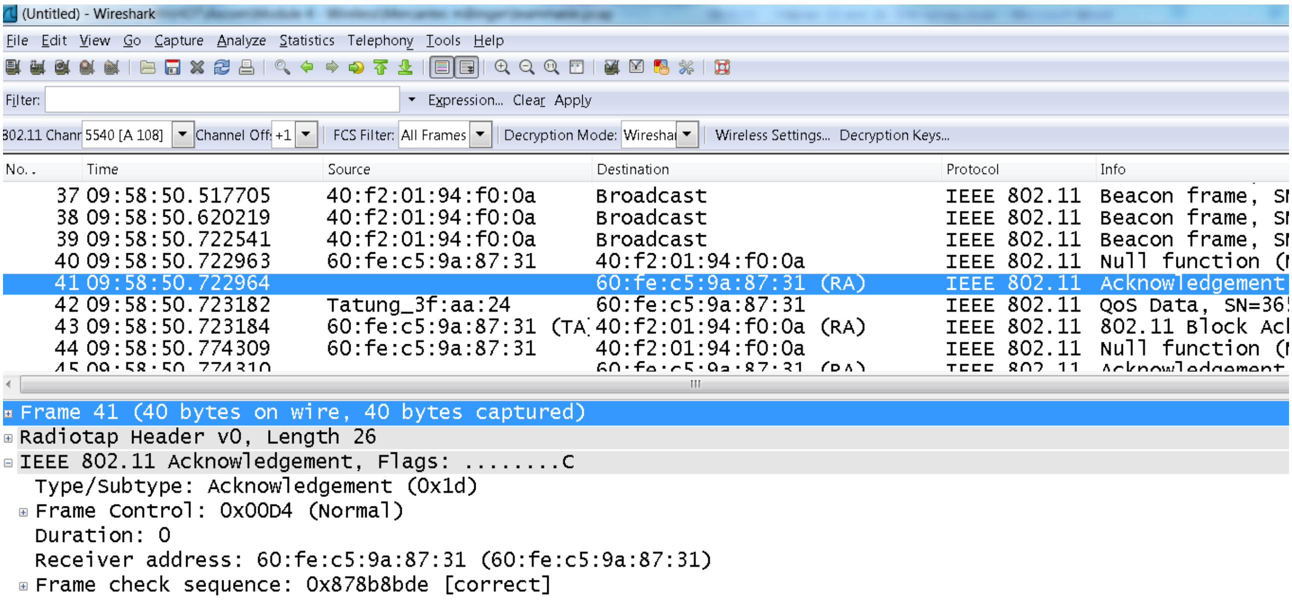


Figure 114 - Wi-Fi Spectrum analyser showing signal levels in UNII-1 to UNII-3 bands.

## Protocol analysis

Wi-Fi based protocol analysers can examine captured 802.11 frames. Even if data is encrypted, a lot can be seen and learned from the captured control and management frames.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply
Wireless Settings... Decryption Keys...

Filter:

802.11 Chann 5540 [A 108] Channel Off: +1 FCS Filter: All Frames Decryption Mode: Wiresha

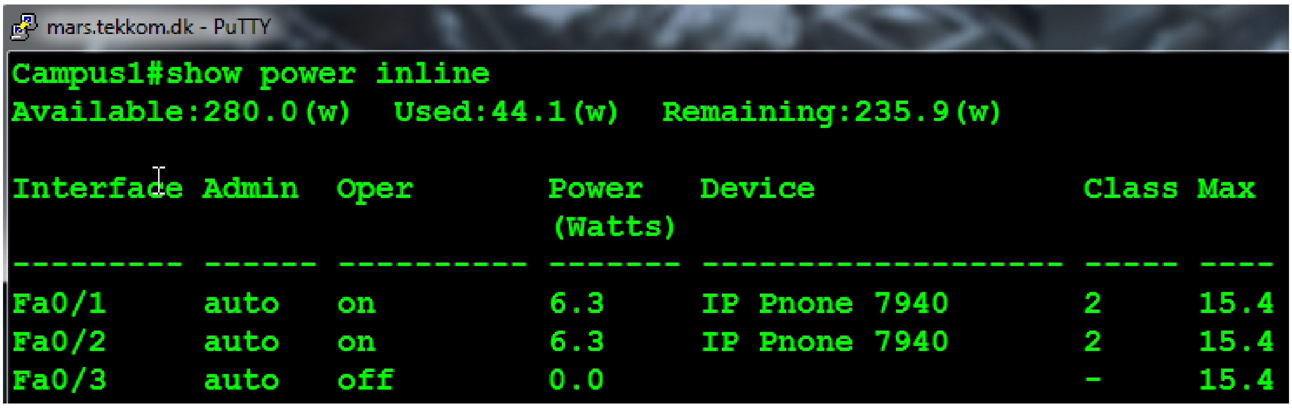
```
No. .  Time               Source                       Destination                Protocol     Info
    37 09:58:50.517705    40:f2:01:94:f0:0a            Broadcast                  IEEE 802.11  Beacon frame, SI
    38 09:58:50.620219    40:f2:01:94:f0:0a            Broadcast                  IEEE 802.11  Beacon frame, SI
    39 09:58:50.722541    40:f2:01:94:f0:0a            Broadcast                  IEEE 802.11  Beacon frame, SI
    40 09:58:50.722963    60:fe:c5:9a:87:31            40:f2:01:94:f0:0a          IEEE 802.11  Null function (I
    41 09:58:50.722964                                 60:fe:c5:9a:87:31 (RA)     IEEE 802.11  Acknowledgement
    42 09:58:50.723182    Tatung_3f:aa:24              60:fe:c5:9a:87:31          IEEE 802.11  QoS Data, SN=36
    43 09:58:50.723184    60:fe:c5:9a:87:31 (TA        40:f2:01:94:f0:0a (RA)     IEEE 802.11  802.11 Block Ack
    44 09:58:50.774309    60:fe:c5:9a:87:31            40:f2:01:94:f0:0a          IEEE 802.11  Null function (I
    45 09:58:50.774310                                 60:fe:c5:9a:87:31 (RA)     IEEE 802.11  Acknowledgement
```

```
⊞ Frame 41 (40 bytes on wire, 40 bytes captured)
⊞ Radiotap Header v0, Length 26
⊟ IEEE 802.11 Acknowledgement, Flags: ........C
    Type/Subtype: Acknowledgement (0x1d)
  ⊞ Frame Control: 0x00D4 (Normal)
    Duration: 0
    Receiver address: 60:fe:c5:9a:87:31 (60:fe:c5:9a:87:31)
  ⊞ Frame check sequence: 0x878b8bde [correct]
```

Figure 115 - Detailed view of captured 802.11 control frame using Wireshark.

## PoE – Power over Ethernet

PoE – Power over Ethernet – is a technology where power is delivered to Ethernet devices through RJ45 Ethernet connectors. Several versions of PoE exist.



mars.tekkom.dk - PuTTY

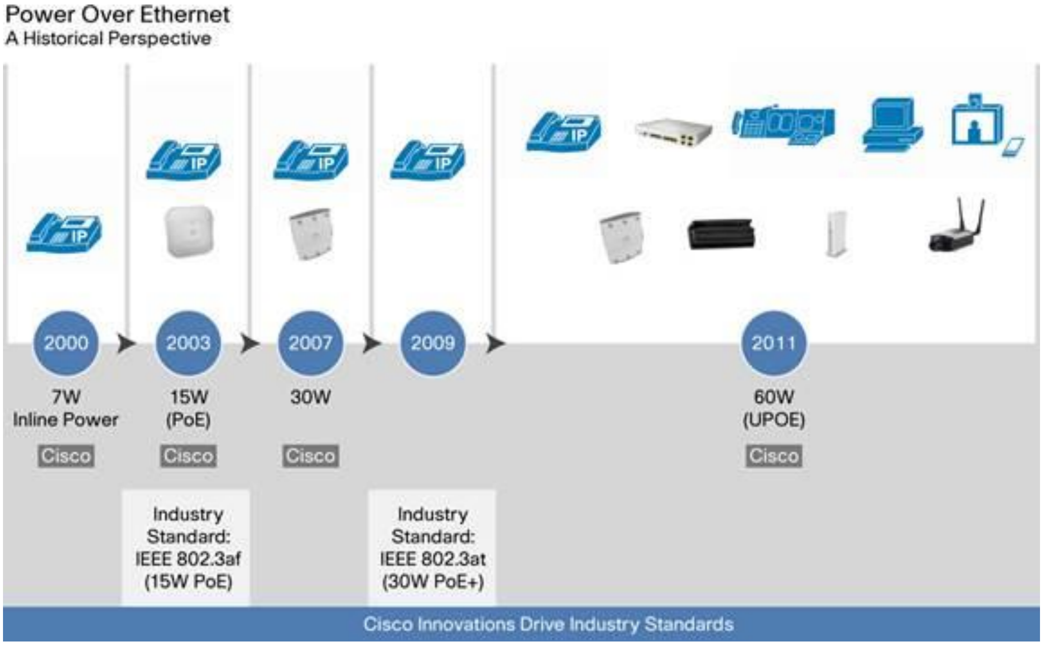
```
Campus1#show power inline
Available:280.0(w)  Used:44.1(w)  Remaining:235.9(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Fa0/1     auto   on         6.3     IP Pnone 7940       2     15.4
Fa0/2     auto   on         6.3     IP Pnone 7940       2     15.4
Fa0/3     auto   off        0.0                         -     15.4
```

Figure 116 - Cisco PoE capable switch delivering power to devices

### Nonstandard PoE

Proprietary Power over Ethernet solutions was created before IEEE standardized PoE in 2003. Proprietary PoE solutions often use different voltages, and mixing proprietary solutions could damage equipment.



Power Over Ethernet
A Historical Perspective
2000
7W
Inline Power
Cisco
2003
15W
(PoE)
Cisco
2007
30W
Cisco
2009
2011
60W
(UPOE)
Cisco
Industry Standard: IEEE 802.3af (15W PoE)
Industry Standard: IEEE 802.3at (30W PoE+)
Cisco Innovations Drive Industry Standards

Figure 117 - Cisco proprietary PoE solutions compared to IEEE standards.

### IEEE 802.3af – PoE

In 2003 the first IEEE PoE standard was approved, and defined how to provide power over 10BaseT - Ethernet, 100BaseT – Fast Ethernet and 1000BaseT – Gigabit Ethernet devices. IEEE 802.3af delivers up to 15.4 Watts to the powered device. The maximum power available for the powered device is 12.95 Watts as some power is dissipated by the cable.

## IEEE 802.3at – PoE+

In 2009 IEEE 802.3at known as PoE+ or PoE plus was approved. PoE+ extends the capabilities of 802.3af PoE but remains backward compatible. PoE+ delivers up to 30 Watts, with the maximum power available for the powered device being 25.5 Watts. The extra power that can be delivered by PoE+ makes it possible to power devices such 802.11n access points with multiple radios, which require more power.

IEEE 802.3at defines PoE devices as either Type 1 or Type 2 devices. Devices capable of supporting PoE+ higher power are defined as Type 2 devices and devices not capable of supporting the high power as Type 1 devices.

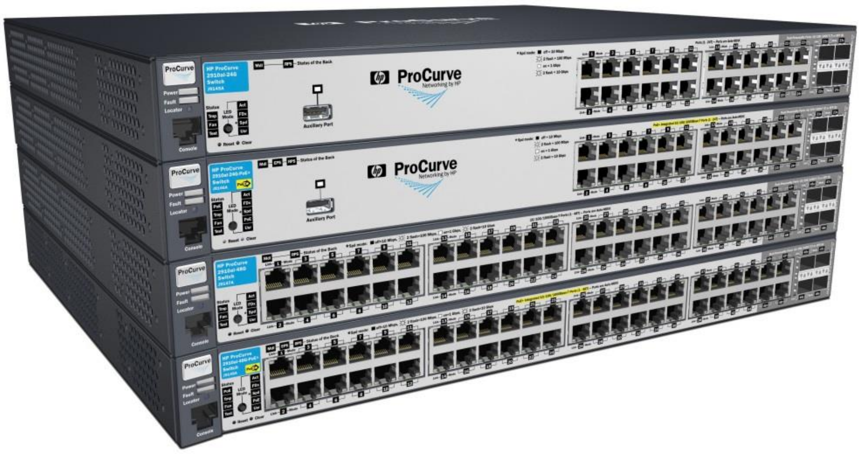


Figure 118 - Stack of PoE / PoE+ capable switches from HP.

## PoE devices

There are two kinds of PoE devices – PD or Powered Device and PSE – Power-Sourcing Equipment. The PSE detects the PD and supplies power to the PD.

### PD – Powered Device

The powered device requests and then draws power from the power-sourcing equipment. The power is delivered through the normal RJ45 Ethernet connection in the same or separate copper pairs.

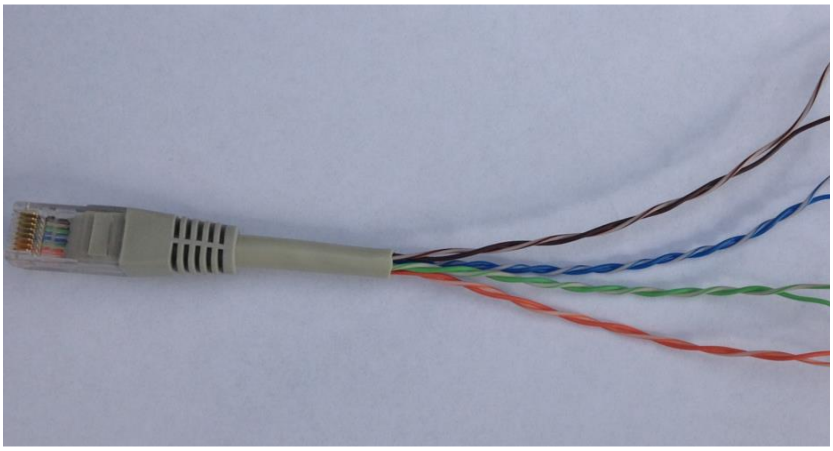
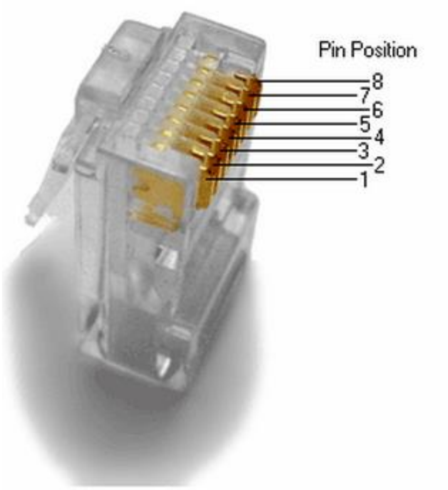


Figure 119 - Category 5E cable contains four pairs of two copper wires.



The powered device should be able to withstand voltages as high as 57 Volts, and accept power with either polarity from the power-sourcing equipment. The polarity of the DC supply may reverse if a crossover cable is used. The power is delivered in two copper pairs in mode A or mode B. In mode A the power is delivered on pins 1, 2, 3 and 6 and in mode B the power is delivered on pins 4, 5, 7 and 8, as in the table below.

| RJ45 | T568A | T568B | Mode A | Mode B |
|---|---|---|---|---|
| 1 | ⬜🟩 | ⬜🟧 | | DC + |
| 2 | 🟩 | 🟧 | | DC + |
| 3 | ⬜🟧 | ⬜🟩 | | DC - |
| 4 | 🟦 | 🟦 | DC + | |
| 5 | ⬜🟦 | ⬜🟦 | DC + | |
| 6 | 🟧 | 🟩 | | DC - |
| 7 | ⬜🟫 | ⬜🟫 | DC - | |
| 8 | 🟫 | 🟫 | DC - | |

The polarities shown in the table above may be reversed depending on the cable and power-sourcing equipment used. The power-sourcing equipment may provide power in mode A or in mode B.

## PD classification

The powered device signals to the power-sourcing equipment that is IEEE PoE compliant by placing a 25 KΩ resistor between the powered pairs. If the power-sourcing equipment fails to recognize a 25 KΩ resistor it delivers no power, thereby protecting non PoE equipment. When the power-sourcing equipment detects a PoE capable device it tries to classify the equipment by applying a voltage between 14.5 and 20.5 Volts for a short period of time. Depending on the current the powered device draws in this short period, the power-sourcing equipment classifies the powered device.

| PoE classification | Class 0 | Class 1 | Class 2 | Class 3 | Class 4 |
|---|---|---|---|---|---|
| Current drawn by PD | 0 to 4 mA | 9 to 12 mA | 17 to 20 mA | 26 to 30 mA | 36 to 44 mA |
| PoE type | 1 – PoE | 1 – PoE | 1 – PoE | 1 – PoE | 2 – PoE+ |

The classification is used to enable the powered device to tell the power-sourcing device how much power it needs.

| PoE classification | Class 0 | Class 1 | Class 2 | Class 3 | Class 4 |
|---|---|---|---|---|---|
| **Description** | Default | Very low pwr | Low power | Mid power | High power |
| **Power range (watt)** | 0.44 to 12.95 | 0.44 to 3.84 | 3.84 to 6.49 | 6.49 to 12.95 | 12.95 to 25.5 |
| **PoE type** | 1 – PoE | 1 – PoE | 1 – PoE | 1 – PoE | 2 – PoE+ |

## 802.11n and High Throughput

The main objective of 802.11n was to increase the data rate and the throughput in both the 2.4 GHz and 5 GHz frequency bands. 802.11n defines a new operation called HT – High Throughput – which provides data rates potentially up to 600 Mbps.

Figure 120 - Motorola AP7131 IEEE 802.11n dual frequency assess point.

## HT – High Throughput

The high throughput technology uses a technology called MIMO – Multiple-input Multiple-output - which together with OFDM – Orthogonal Frequency Division Multiplexing – gives higher throughput and greater range.

802.11n is backwards compatible and a dual frequency 802.11n radio is referred to as an 802.11a/b/g/n radio. 802.11n radios can use the single frequencies 2.4 GHz or 5 GHz or use dual frequency and use both 2.4 GHz and 5 GHz.

## Wi-Fi alliance certification

A Wi-Fi alliance 802.11n certified product must support a range of baseline requirements. Some of the most noteworthy are listed in the table below.

| Feature | Explanation | Type |
|---|---|---|
| Support for two spatial streams | Access points are required to transmit and receive at least two spatial streams.<br>Client stations are required to transmit and receive at least one spatial stream. | Mandatory |
| WMM QoS | Multimedia Quality and Service | Mandatory |
| WPA/WPA2 security | Strong security mechanism | Mandatory |
| 2.4 GHz frequency band<br>5 GHz frequency band | Devices can be 2.4 GHz only, 5 GHz only or dual band. | At least one band |
| 40 MHz wide channels in 5 GHz | Bonding of two 20 MHz channels creating a 40 MHz channel with twice the bandwidth | Optional |
| 40 MHz wide channels in 2.4 GHz | Bonding of two 20 MHz channels creating a 40 MHz channel with twice the bandwidth. Must be capable of communicating with 20 MHz only radios. | Optional |
| Short GI – Guard Interval | Short GI is 400 nS versus normal GI of 800nS. Improves data rate with 10%. | Optional |
| HT duplicate mode | Allows transmission of the same data simultaneously  on each 20 MHz channel in a bonded 40 MHz channel | Optional |

## MIMO – Multiple-Input Multiple-Output

The primary enhancement of 802.11n is that multiple signals are transmitted on the same channel at the same time using a method called spatial multiplexing. To achieve this, the transmitter transmits using multiple radios and antennas as shown in Figure 121. This is called multiple-output. The receiver receives using multiple radios and antennas. This is called multiple-input.

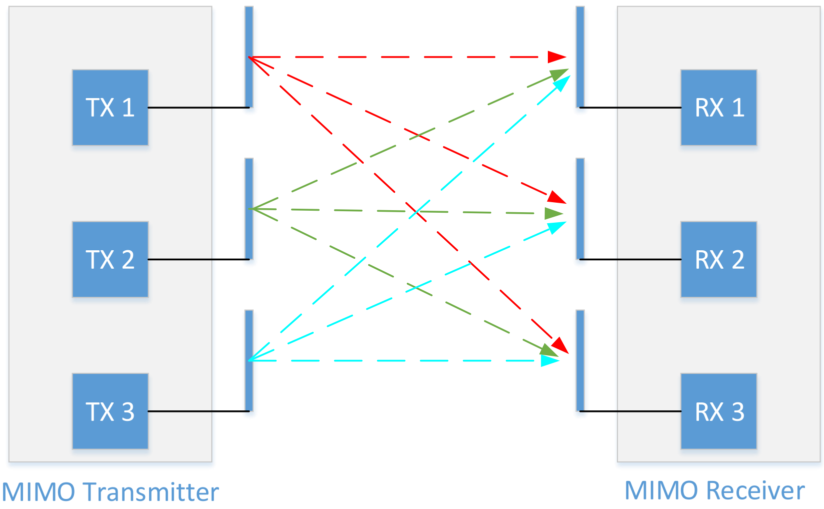


Figure 121 - MIMO - Multiple-Input Multiple-Output principle.

MIMO radios transmit multiple radio signals at the same time to take advantage of multipath. In pre 802.11n technologies multipath radio signals caused problems because reflected radio waves could cause interference.

MIMO technology takes advantage of multipath and can even benefit from it.

## Spatial multiplexing

It is possible for MIMO radios to transmit multiple signals each carrying its own independent information. They are transmitted at the same time and the same channel using a spatial multiplexing technology. Each independent data stream called a spatial stream requires its own transmitter and antenna.

With two transmitters and antennas it is possible to double the data rate and even triple or quadruple it with three or four. The receiver must have an antenna for each spatial stream it receives.

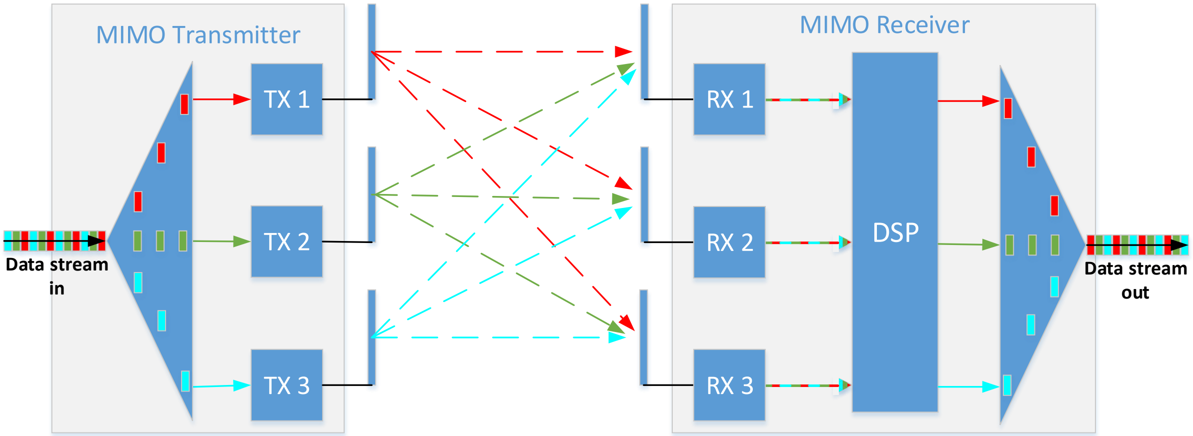


Figure 122 - MIMO system with three spatial streams.

The signals from each individual stream – called spatial streams – arrive at the receiver's antennas at slightly different times. A DSP – Digital Signal Processor – using advanced mathematics, sorts out the original streams from the received signals, as shown in Figure 122. A high multipath environment actually helps the receiver differentiate between each individual stream of RF signals.

### The notation for MIMO systems

Most vendors use a three digit notation form to indicate the number of transmitters, receivers and spatial streams. For example a 3x3:2 access point would have three transmitters and three receivers but would only be able to use two spatial streams. A 3x3:3 system would be able to utilize three spatial streams.

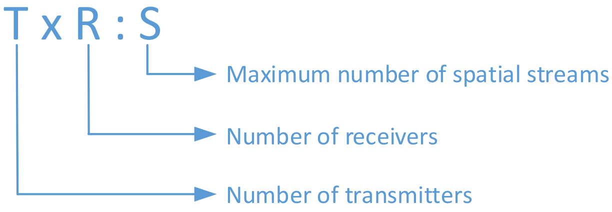


Figure 123 - IEEE 802.11n radio notation

The 802.11n standard allows radio configurations from 1x1:1 to 4x4:4 which allows for a maximum of four spatial streams. In the table below the maximum bandwidths with one to four spatial streams are shown. The table shows bandwidths using a default 20 MHz channel width and a 40 MHz channel width when bonding two 20 MHz channels.

| **Streams** | **20 MHz channel width** | | **40 MHz channel width** | |
|---|---|---|---|---|
| | 800 nS GI | 400 nS GI | 800 nS GI | 400 nS GI |
| **1** | 65 Mbps | 72.2 Mbps | 135 Mbps | 150 Mbps |
| **2** | 130 Mbps | 144.4 Mbps | 270 Mbps | 300 Mbps |
| **3** | 195 Mbps | 216.7 Mbps | 405 Mbps | 450 Mbps |
| **4** | 260 Mbps | 288.8 Mbps | 540 Mbps | 600 Mbps |

GI or guard interval is a small break between transmitting two OFDM symbols. The shorter the break the faster the data rate, but the chance of inter-symbol interference increases with lower guard interval.

## STBC – Space Time Block Coding

STBC or Space Time Block Coding is a method where the same information is transmitted on two or more antennas. STBC can be used when the number of transmitters exceeds the number of spatial streams. STBC does not increase the data rate, but the signal strength increases the signal to noise ratio – SNR – which gives the radio the ability to use a higher data rate than otherwise possible.

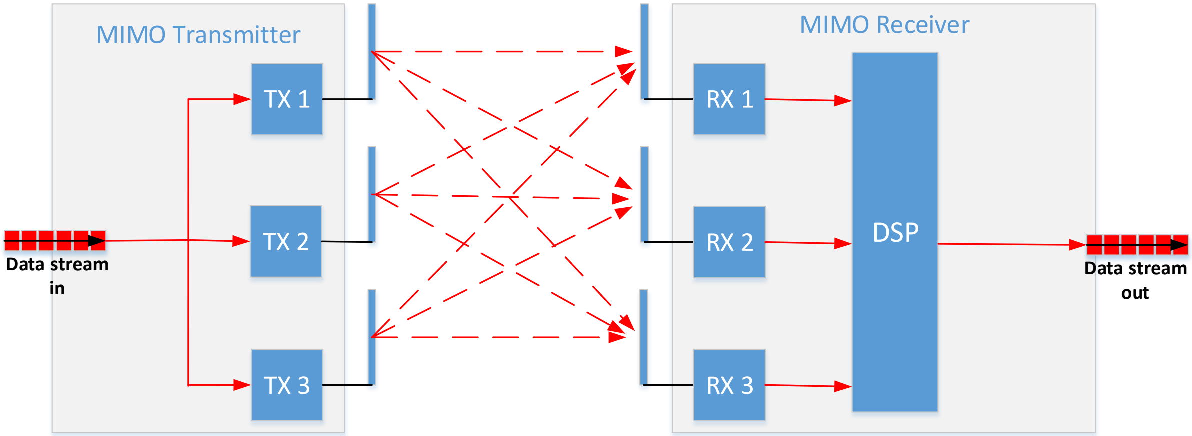


Figure 124 - STBC - Single stream transmitted in 3x3:1 radio system increasing signal to noise ratio (SNR)

## HT – High Throughput Channels

High throughput channels use 20 MHz bandwidth channels as non-HT channels, as with 802.11a/g.

Non-HT OFDM 802.11a/g uses 20 MHz wide channels with 52 subcarriers of which 48 carry data and 4 are pilot subcarriers, which are used for dynamic calibration between the transmitter and the receiver.

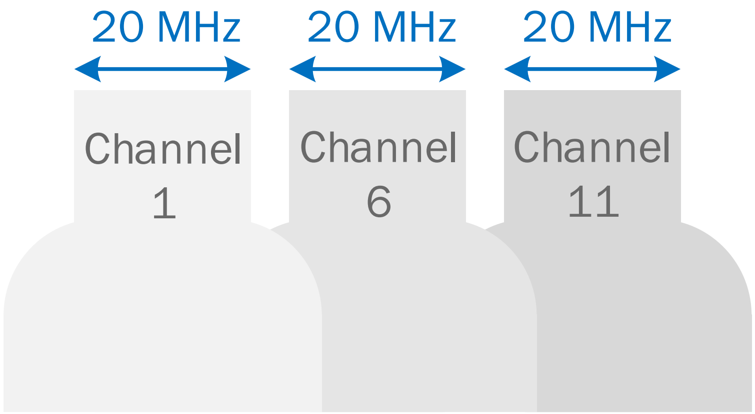


Figure 125 – 2.4 GHz ISM band showing 20 MHz wide channels.

802.11n also uses OFDM and 20 MHz wide channels but has 56 subcarriers and has the ability to bond two 20 MHz channels into one channel with 40 MHz channel width.

### 20 MHz HT channels

802.11n has the ability to use the well-known channels in the 2.4 GHz and 5 GHz bands.

The OFDM channels used by 802.11n radios divide the 20 MHz channels in the 2.4 GHz and 5 GHz bands into 56 subcarriers. 52 subcarriers carry data and 4 pilot subcarriers are used as dynamic calibration between the transmitter and the receiver.

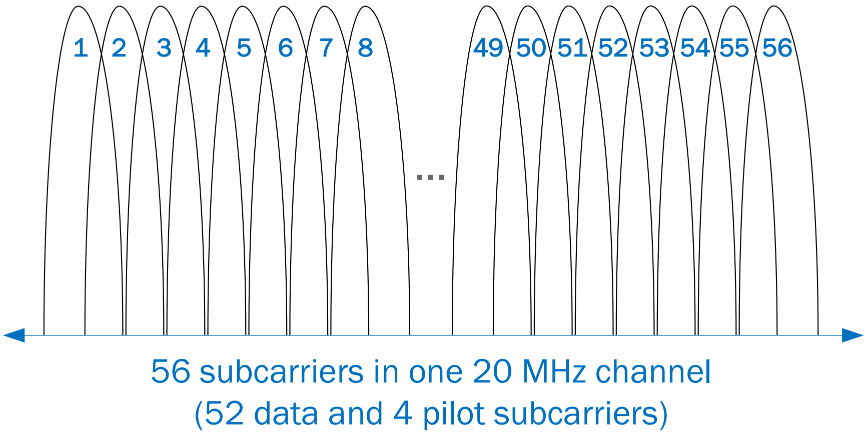

1
2
3
4
5
6
7
8
...
49
50
51
52
53
54
55
56
56 subcarriers in one 20 MHz channel
(52 data and 4 pilot subcarriers)

Figure 126 - one 20 MHz channel is divided into 56 subcarriers.

When using channels with a 20 MHz width it is possible to use the same channels as pre 802.11n. In the 2.4 GHz band, channel 1, 6 and 11 are non-overlapping.

### 40 MHz HT channels

802.11n HT channels have the ability to bond two neighbouring 20 MHz channels into one 40 MHz wide channel. This a little more than doubles the data rate that can be carried by the channel. A standard 20 MHz wide channel reserves some frequency bandwidth in the top and bottom of the channel to avoid interference with neighbouring channels. When bonding two channels, there is no need to reserve bandwidth between the two channels, adding a little extra bandwidth.

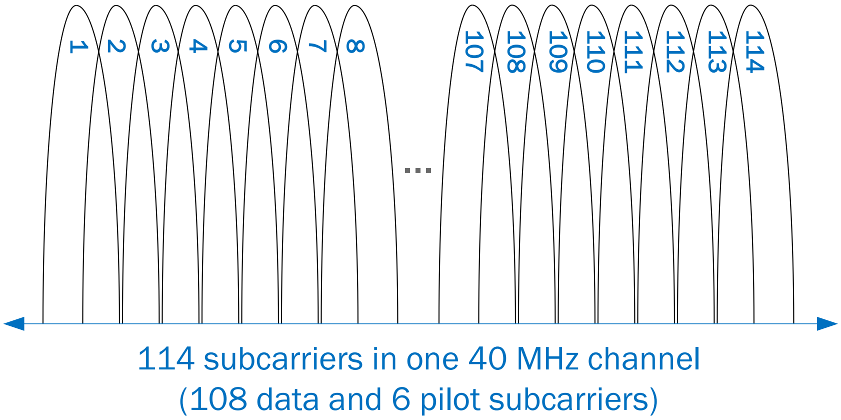

1
2
3
4
5
6
7
8
...
107
108
109
110
111
112
113
114
114 subcarriers in one 40 MHz channel
(108 data and 6 pilot subcarriers)

Figure 127 - A 40 MHz channel is divided into 114 subcarriers.

Using 40 MHz wide channels in the 2.4 GHz ISM band does not scale well, as only channels 1, 6 and 11 are non-overlapping. If two channels are bonded together as shown in Figure 128 , there will only be one 20 MHz wide channel and one 40 MHz wide channel, and the possibility to reuse channels in a pattern is essentially impossible.

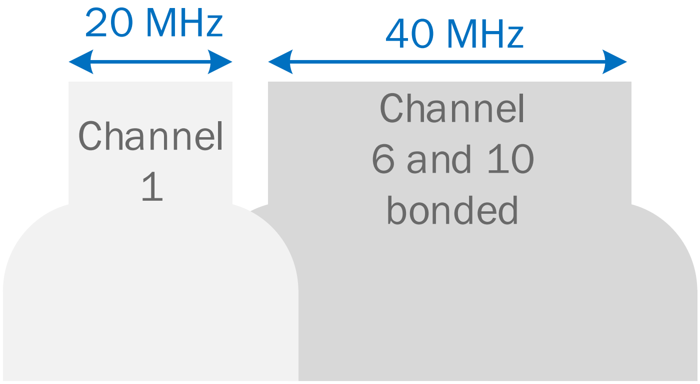
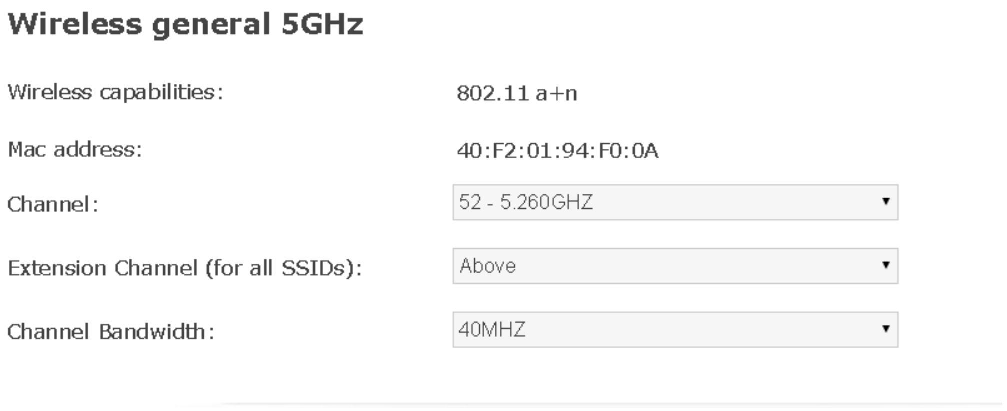


Figure 128 - Only one 40 MHz channel available in the 2.4 GHz ISM band.

Channel bonding in the 5 GHz UNII bands makes more sense as there are a total of twenty-four 20 MHz channels that can be bonded into pairs. When bonding two 20 MHz channels into one 40 MHz channel, one of the channels is the primary channel and the other is the secondary channel. The secondary channel must be above or below the primary channel.



Wireless general 5GHz

| | |
|---|---|
| Wireless capabilities: | 802.11 a+n |
| Mac address: | 40:F2:01:94:F0:0A |
| Channel: | 52 - 5.260GHZ ▾ |
| Extension Channel (for all SSIDs): | Above ▾ |
| Channel Bandwidth: | 40MHZ ▾ |

Figure 129 - 40 MHz channel bonding with primary channel on channel 52 and secondary above channel 52

### 20 MHz and 40 MHz interoperability

802.11a/g stations, which only support 20 MHz channel width, transmit and receive in the primary 20 MHz wide channel. Only 802.11n clients supporting 40 MHz channel width utilize the bonded channels.

## MCS – Modulation and Coding Scheme

802.11n data rates are defined in a MCS – Modulation and Coding Scheme Matrix.

There are 77 different modulation and coding schemes defined based on number of spatial streams, channel size, guard interval and coding method.

| | |
|---|---|
| **Spatial streams** | Up to four spatial streams can be transmitted simultaneously quadrupling the data rate. 802.11n radios use configurations spanning 1x1:1 to 4x4:4 (4x4:4 – 4 transmitters and 4 receivers up to four spatial streams) |
| **Channel size** | 20 MHz or 40 MHz channel width. |
| **Guard interval** | A small break between transmitting two OFDM symbols. The shorter the break the faster the data rate, but the chance of inter-symbol interference increases with lower guard interval. |
| **Coding method** | Modulation and coding method used. For example PSK – Phase shift keying – and QPSK – Quadruple phase shift keying) |

In the table below all MCS index possibilities for 1 spatial stream are shown. These are MCS index 1 through 7. Only one MCS index is shown in the table below, for two to four spatial streams.  MCS index numbers range from 0 to 31.

| **MCS** | **Streams** | **20 MHz channel width** | | **40 MHz channel width** | |
|---|---|---|---|---|---|
| | | 800 nS GI | 400 nS GI | 800 nS GI | 400 nS GI |
| **0** | 1 | 6.5 Mbps | 7.2 Mbps | 13.5 Mbps | 15 Mbps |
| **1** | 1 | 13 Mbps | 14,4 Mbps | 27 Mbps | 30 Mbps |
| **2** | 1 | 19.5 Mbps | 21.7 Mbps | 40.5 Mbps | 45 Mbps |
| **3** | 1 | 26 Mbps | 28,9 Mbps | 54 Mbps | 60 Mbps |
| **4** | 1 | 39 Mbps | 43.3 Mbps | 81 Mbps | 90 Mbps |
| **5** | 1 | 52 Mbps | 57.8 Mbps | 108 Mbps | 120 Mbps |
| **6** | 1 | 58.5 Mbps | 65 Mbps | 121.5 Mbps | 135 Mbps |
| **7** | 1 | 65 Mbps | 72.2 Mbps | 135 Mbps | 150 Mbps |
| **15** | 2 | 130 Mbps | 144.4 Mbps | 270 Mbps | 300 Mbps |
| **23** | 3 | 195 Mbps | 216.7 Mbps | 405 Mbps | 450 Mbps |
| **31** | 4 | 260 Mbps | 288.8 Mbps | 540 Mbps | 600 Mbps |