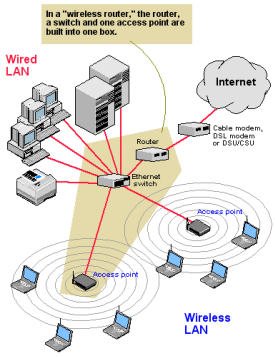
CoNeT Mobile Lab
Wireless Communication

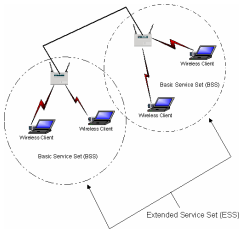


(Version 2)

CoNeT Mobile Lab
Wireless Communication

PART 1: Theoretical Aspects of Wireless Communication

Content Theoretical Aspects



1. Differentiating Between Wireless Technologies

1.1 WLAN vs. WPAN vs. WWAN

WLAN (Wireless Local Area Network)

WLAN transmits data over a short distance, normally 100 meters or so. In terms of transmission technology, WLAN uses spread-spectrum or OFDM (orthogonal frequency-division multiplexing) modulation technology to provide the convenience of exchanging data without the limitation of cables.

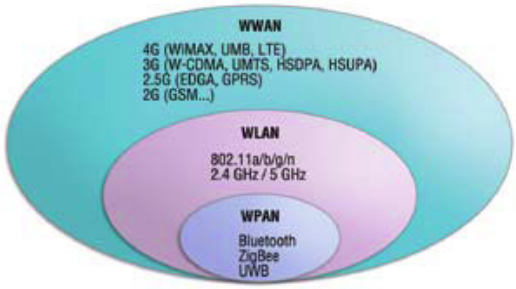
Today's WLANs are based on IEEE 802.11 standards and are referred to as Wi-Fi networks. The 802.11b standard, which operates around the 2.4 GHz frequency band at 11 Mbps, was the first commercialized wireless technology.

Advances in wireless technology have made a higher transmission rate of 54 Mbps possible with 802.11g, which also operates around 2.4 GHz, and 802.11a, which operates around the 5 GHz frequency band. It is now very common to see dual-band Wi-Fi access points and client network adaptors that support a mixture of 802.11a, b, and g standards.

More bandwidth means that it is possible to use wireless to replace traditional wired solutions to transmit larger data such as video.

1. Differentiating between Wireless Technology

- WWAN vs. WLAN vs. WPAN
  - ✓ WWAN (Wireless Wide Area Network)
  - ✓ WLAN (Wireless Local Area Network)
  - ✓ WPAN (Wireless Personal Area Network)



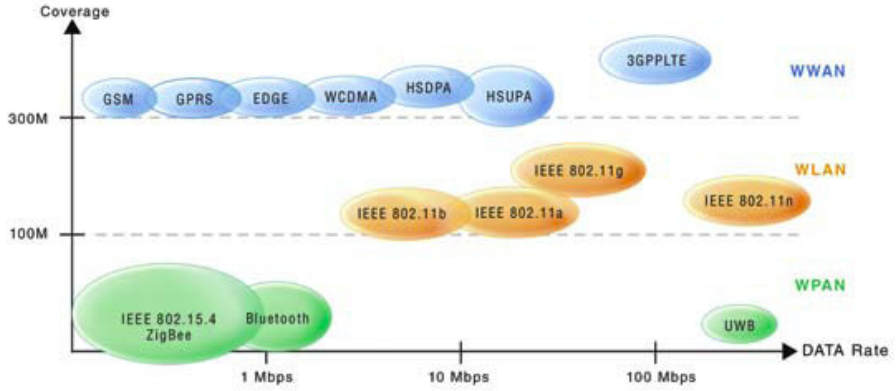
WWAN (Wireless Wide Area Network)

A WWAN utilizes mobile communication networks such as cellular, UMTS, GPRS, CDMA2000, GSM, CDPD, Mobitex, HSDPA, 3G, and WiMax. All of these networks offer wide service coverage and are normally used for citywide, nationwide, or even global digital data exchange.

In cellular communication, GSM (Global System for Mobile Communication) is the leader with over 80% market share, followed by CDMA (Code Division Multiple Access).

The biggest issues regarding data exchange over a WWAN are the associated costs, bandwidth, and IP management. However, as technologies improve and costs drop, WWAN is predicted to replace traditional microwave, RF (radio frequency), and satellite communication due to its lower infrastructure costs.

The industrial Wireless Technology Landscape



WPAN (Wireless Personal Area Network)

A WPAN is a short-range peer-to-peer or ad hoc network built around a person's working area. Normally the distance is no more than 10 meters.

Their limited transmission range is the reason that WPANs are used mainly as cable replacement solutions for data synchronization and data transmission for personal electronic devices such as PDAs or smart phones.

Bluetooth is the most common WPAN technology in use today. It allows devices such as phones, mice, headsets, and other personal devices to connect wirelessly within a range of 10 meters.

The shorter communication distances also mean lower power consumption.

Bluetooth is an ideal solution for short-range data transmission.

1.2 Mayor involved bodies

1.2.1 Main Standardization committees involved in WLANS

- ✓ ITU – The International Telecommunication Union
- ✓ ETSI - European Telecommunications Standards Institute
- ✓ IEEE - Institute of Electrical and Electronic Engineers

1.2.2 Supervisory bodies and standardization bodies

- ✓ US: FCC
- ✓ Europe CEPT, ETSI
- ✓ Japan:MKK
- ✓ IEEE802.1x LAN standards
- ✓ WIFI (Wireless Fidelity) alliance

1.2 Mayor Involved bodies

1.2.1 Main Standardization committees involved in WLANS

The Telecommunication Standardization Sector coordinates standards for telecommunications on behalf of the International Telecommunication Union (ITU) and is based in Geneva, Switzerland.

The European Telecommunications Standards Institute (ETSI) produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio and internet technologies.

The Institute of Electrical and Electronics Engineers or IEEE is an international non-profit, professional organization for the advancement of technology related to electricity. It has the most members of any technical professional organization in the world, with more than 395,000 members in around 150 countries.

1.2.2 Supervisory bodies and standardization bodies

The European Conference of Postal and Telecommunications Administrations (CEPT) was established on June 26, 1959 as a coordinating body for European state telecommunications and postal organizations. The acronym comes from the French version of its name Conférence Européenne des administrations des Postes et des Télécommunications.

CEPT was responsible for the creation of the European Telecommunications Standards Institute (ETSI) in 1988.

The FCC (Federal Communications Commission) regulates the usable frequency bands and the maximum allowable power in these frequency bands for the United States.

Wi-Fi is a trademark of the Wi-Fi Alliance that manufacturers may use to brand certified products that belong to a class of wireless local area network (WLAN) devices based on the IEEE 802.11 standards.

802.11 is the most widely used WLAN technology. Because of the close relationship with the 802.11 standards, the term Wi-Fi is often used as a synonym for IEEE 802.11 technology.

Not every IEEE 802.11-compliant device is submitted for certification to the Wi-Fi Alliance. The lack of Wi-Fi certification does not necessarily imply a device is incompatible with Wi-Fi devices.

2. IEEE 802.11x standards (1)

2.1 IEEE 802.11x evolving and evolution standards (1)

IEEE 802. 11	2 Mbps, 2.4 GHz band, 1997, MAC/Physical Standard
IEEE 802. 11a	54 Mbps, 5 GHz band, 1999, MAC/Physical Standard
IEEE 802. 11b	11 Mbps, 2.4 GHz Band, 1999, MAC/Physical Standard
IEEE 802. 11c	MAC Layer Bridging to support IEEE802.1D
IEEE 802. 11d	Automatic settings for different countries
IEEE 802. 11e	Quality of Service (QoS)
IEEE 802. 11f	IAPP, Inter-Access Point Protocol, cancelled by IEEE after February, 2006
IEEE 802. 11g	54 Mbps, 2.4 GHz Band, 2003, MAC/Physical Standard
IEEE 802. 11h	Support more channels on 5GHz spectrum, 2004
IEEE 802. 11i	Wireless security, 2004

2. IEEE 802.11 Standards

2.1 IEEE 802.11x evolving and evolution standards

With the advent and development of local area networks (LAN), IEEE 802.3 has been widely adopted in many different kinds of communication applications. The continued prevalence of wired communication has also contributed to the growing demand for wireless communication.

In 1997, IEEE released the IEEE 802.11 standards that define the Physical Layer and Data Link Layer of TCP/IP, allowing wireless communication based on these protocols to be extended and used with greater flexibility.

For the Physical Layer, IEEE 802.11 utilizes non-licensed ISM (Industrial, Scientific and Medical) bands that operate between 2.4 GHz and 5 GHz.

IEEE 802.11x evolving and evolution standards (2)

IEEE 802. 11j	Japanese Standard upgrade, 2004
IEEE 802. 11k	Define measurement items and protocol
IEEE 802. 11l	Reserved
IEEE 802. 11m	Maintenance Standard
IEEE 802. 11n	Draft version at this moment, using MIMO (Multi-input Multi Output) Technology to increase transmission speed to 300–600Mbps
IEEE 802. 11r	Define implementations of WLAN roaming, enables 802.11 able to be applied to mobile and VoIP applications
IEEE 802. 11s	Standard for Mesh under standard architecture

IEEE 802.11n

In January 2004, IEEE announced it was forming a new task force to develop new standards for the IEEE 802.11 standard. The goal of this task force was to allow wireless communication speed to reach a theoretical number of 300 Mbps. Since the theoretical speed of this new standard, now called IEEE 802.11n, needs to reach 300 Mbps, the Physical Layer also needs to support a higher transmission speed that is at least 50 times faster than IEEE 802.11b and 10 times faster than IEEE 802.11g.

IEEE 802.11s

An 802.11s mesh network device is referred to as a mesh station (mesh STA). Mesh STAs form mesh links with one another, over which mesh paths can be established using a routing protocol. 802.11s defines a default mandatory routing protocol, or HWMP, yet allows vendors to operate using alternate protocols. HWMP is inspired by a combination of AODV (RFC 3561[1]) and tree-based routing.

Mesh STAs are individual devices using mesh services to communicate with other devices in the network.

2.2 Basic features IEEE 802.11x and WLAN Modes

Protocol	Release Date	Spectrum	Max. Speed	Typical Range (indoor)	Typical Range (outdoor)
802.11	1997	2.4–2.5 GHz	2 Mbps	---	---
802.11a	1999	5.15–5.35/5.47–5.725/ 5.725–5.875 GHz	54 Mbps	30 m	---
802.11b	1999	2.4–2.5 GHz	11 Mbps	30 m	100 m
802.11g	2003	2.4–2.5 GHz	54 Mbps	30 m	100 m
802.11n	2008	2.4 GHz or 5 GHz bands	600 Mbps	50 m	125 m

2.2 Basic features IEEE 802.11x and WLAN Modes

Common usage of the WLAN limits its distance to under 100 meters. Now with advanced technologies it is also possible to extend the distance up to 10 kilometers for multi-point connections or 20 kilometers for point-to-point connections.

The IEEE 802.11 standard is designed for high-speed data transmission. However, it is also vulnerable to outside interferences. **This is unacceptable for some industrial applications where control elements are often involved.**

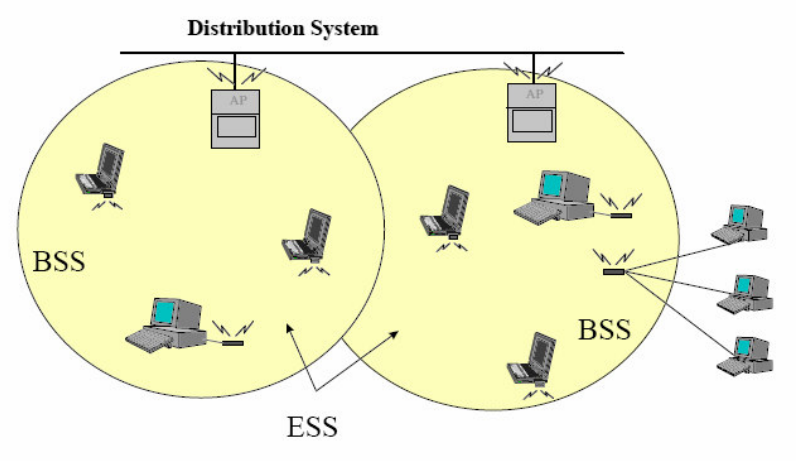
It is a basic control requirement that communication must not be interrupted. To meet this requirement, there are some proprietary 2.4GHz band wireless devices that use FHSS spread spectrum technologies to meet the needs for higher noise resistance. In summary, FHSS sacrifices throughput and communication range for more stability.

FHSS utilizes Frequency Hopping Spread Spectrum technologies to avoid signal interference. Bluetooth is one example that uses this technology. In the early days, IEEE 802.11 also used FHSS but has since adopted DSSS (Direct Sequence Spread Spectrum) out of security concerns.

802.11a, 801.11g, and 802.11n adopt OFDM (Orthogonal Frequency Division Multiplexing) to increase their resistance to external interferences.

3. IEEE 802.11 Architecture

3.1 Architecture Components



3. IEEE 802.11 Architecture

3.1 Architecture Components

An 802.11 LAN is based on a cellular architecture where the system is subdivided into cells, where each cell (called Basic Service Set (BSS) in the 802.11 nomenclature) is controlled by a Base Station, called Access Point (AP).

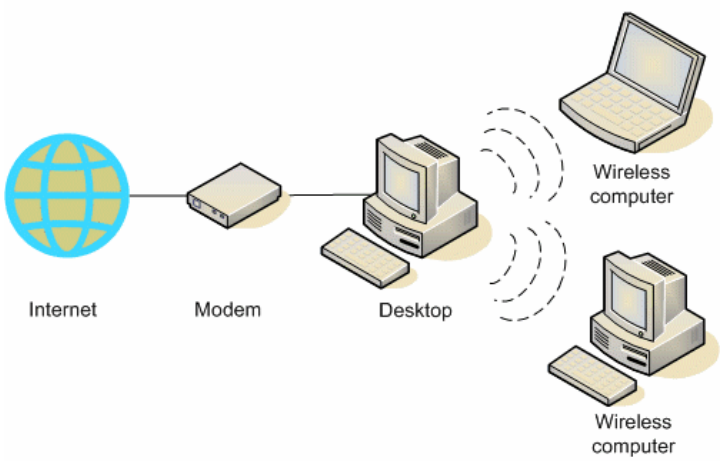
If a wireless LAN can be formed by a single cell, with a single Access Point. It can also work without an Access Point.

Most installations will be formed by several cells, where the Access Points are connected through some kind of backbone called Distribution System (DS), typically Ethernet, and in some cases wireless itself.

The whole interconnected Wireless LAN including the different cells, their respective Access Points and the Distribution System, is seen in the upper layers of the OSI model, as a single 802 network, and is called in the Standard as Extended Service Set (ESS).

The standard also defines the concept of a Portal. A Portal is a device that interconnects an 802.11 and another 802 LAN. This concept is an abstract description of part of the functionality of a “translation bridge”.

3.2 Ad-Hoc operating mode



3.2 Ad Hoc Mode (Peer-to-Peer Workgroup)

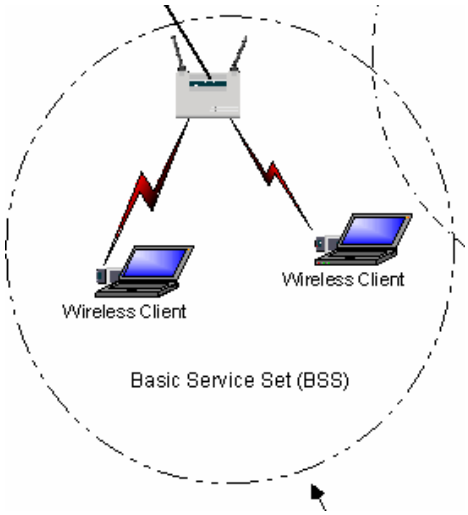
In an ad hoc network each node can be set up to communicate with any other node. No access point is involved in this configuration. This mode enables one to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers in the various Windows based operating systems.

Some vendors also refer to ad hoc networking as peer-to-peer group networking. In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations.

This is the easiest and least expensive way to set up a wireless network as long as the stations are within range of one another.

In an ad hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used.

3.3 Infrastructure operating mode



3.3 Infrastructure operating mode

With a wireless access point, the wireless LAN can operate in the infrastructure mode. This mode lets you connect wirelessly to wireless network devices within a fixed range or area of coverage. The access point has one or more antennas that allow you to interact with wireless nodes.

In infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients.

Connecting multiple access points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one access point domain to another and still maintain seamless network connection.

Network Name: Extended Service Set Identification (ESSID)

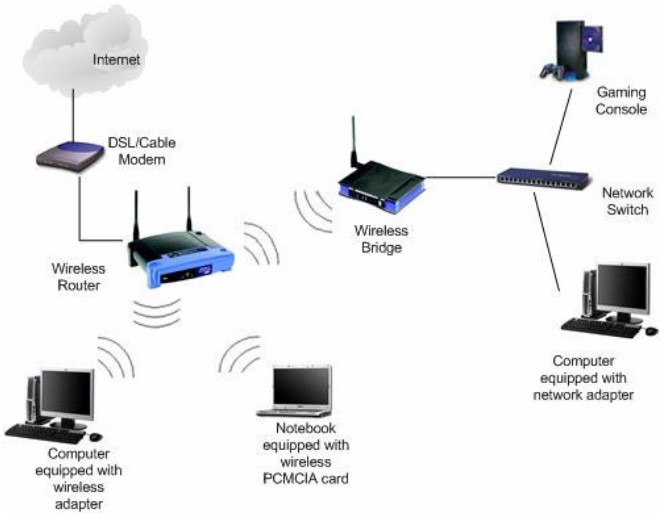
The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID).

In an infrastructure wireless network that includes an access point, the ESSID is used, but may still be referred to as SSID.

An SSID is a 32-character (maximum) alphanumeric key identifying the name of the wireless local area network. Some vendors refer to the SSID as the network name.

For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

3.4 Bridge operating mode



3.4 Bridge operating mode

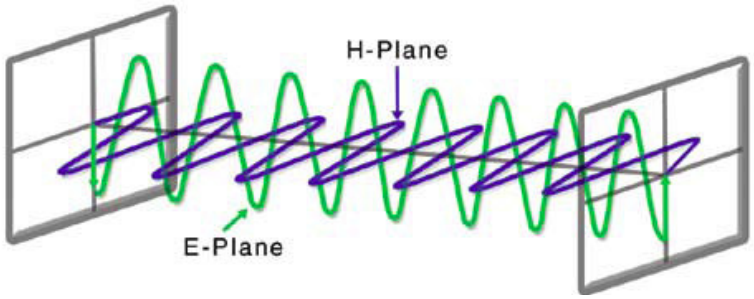
Wireless Bridging is used to connect two LAN segments via a wireless link. The two segments will be in the same subnet and look like two Ethernet switches connected by a cable to all computers on the subnet.

Since the computers are on the same subnet, broadcasts will reach all machines, allowing DHCP clients in one segment to get their addresses from a DHCP server in a different segment.

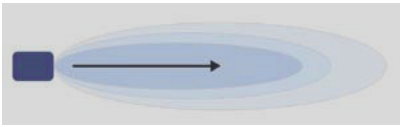
A Wireless Bridge is using to transparently connect computer(s) in one room to computer(s) in a different room without an Ethernet cable between the rooms.

3.5 IEEE802.11 Radio Basics

3.5.1. Electromagnetics waves



Antenna



3.5 IEEE 802.11 Radio Basics

3.5.1 Electromagnetic waves

In a wireless environment, the communication medium is the air. Radio waves carrying data propagate from point to point through free space.

To understand how energy is transferred through the air, we need to review basic electromagnetic theories.

Electromagnetic (EM) waves are formed by alternating current rapidly changing direction on a conductive material. The rapid oscillation of electric and magnetic fields around the conductor produces electromagnetic waves into the air (see the figure). In order to radiate power (AC current) in the air in the form of electromagnetic waves a few factors are critical: the length of the conductor and the frequency of the AC current. Higher frequency reduces the requirement for conductor length.

The conductors are called antennas. Antennas transform electric energy into EM waves during transmission and turn EM waves into electric energy during reception. The size and length of the antenna is directly proportional to its desired transmission/reception frequency. As shown in the figure, electromagnetic waves are radiated from a directional antenna in a parabolic shape.

3.5.1. Electromagnetics waves

- **Diffraction (Shadow Fading)**

- **Scattering**

- **Reflection**

Diffraction (Shadow Fading)

Signal strength is reduced after experiencing diffraction. Obstacles causing diffraction usually possess sharp edges such as the edges of buildings. When EM waves encounter an obstacle with sharp edges that cannot be penetrated, the EM waves wrap around the obstacle to reach the receiver.

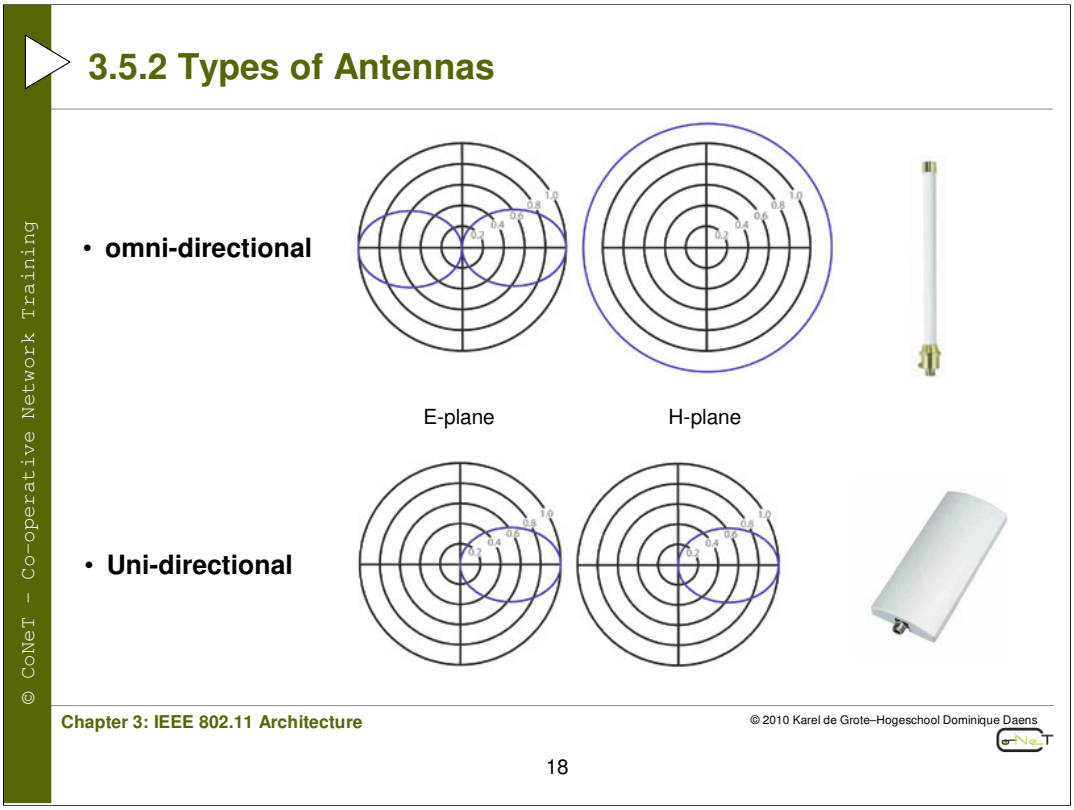
Scattering

When EM waves encounter many small obstacles (smaller than wave length), the EM waves scatter into many small reflective waves and damage the main signal, causing low quality or even broken links. Such obstacles include rough surfaces, rocks/sand/dust, tree leaves, street lights, etc.

Reflection

When EM waves run into large obstacles such as the ground, walls, or buildings, they reflect and change their direction and phase. If the reflected surface is smooth, the reflected signal will likely represent the initial signal and not be scattered.

All of these phenomena result in multipath propagation so not all signals arrive at the receiver antenna at the same time due to obstacles that change the signal paths. In outdoor or indoor applications, multipath propogation can severely affect the received signal quality because the delayed signals are destructive to the main signal. The multipath issue can usually be compensated by antenna diversity at the RF level and/or by OFDM at the baseband level.



3.5.2 Types of Antennas

An antenna is a transducer that is designed to transmit or receive electromagnetic waves. It is like a converter that converts electromagnetic waves and electrical currents back and forth.

Different wireless devices use different antennas to operate in different frequencies and to achieve, for example, a desired range. The most important parameter of an antenna is its working frequency.

There are two basic types of antennas, omni-directional and (Uni)-directional. The two types are categorized by the direction in which they beam radio signals.

Omni-directional antennas are designed to radiate signals equally in all directions. They have very limited vertical spread, which determines the antenna gain. This type of antenna is mostly used to transmit from a central node, such as an access point, to users scattered all around the area and are typically located in the center of open spaces or larger offices to provide even coverage to all clients..

Uni-directional antennas provide a more focused signal than omni-directional antennas. Signals are typically transmitted in an oval-shaped pattern with a beam width of only a few degrees. With higher gain, directional antennas can also be used outdoors to extend point-to-point links over a longer transmission distance, or to form a point-to-multipoint network. Uni-directional antennas are mainly used on rooftops or masts for establishing point-to-point links that interconnect areas of a network that are separated by a distance.

3.5.3 Antenna Specifications

- Connector types

N-type (male) N-type (female) RP-SMA (male) RP-SMA (female) SMA (female) SMA (male)

- Half-Power Beam Width (HPBW)
- Antenna Polarity
- Frequency

3.5.3 Antenna Specifications

• **Connector types**

Before you purchase an antenna for your wireless device, you should check the type of antenna connector that your device uses. You will need to buy an antenna with a matching connector. There are several types of antenna connectors. On WLAN devices, the most commonly used antenna connector is PRSMA and N-type for IEEE 802.11 wireless applications.

• **Half-Power Beam Width (HPBW)**

This parameter is measured from the antenna's radiation pattern, and refers to the beam width at which the antenna's radiation drops to half of its peak value. It also refers to the antenna's effective coverage area. Once you get outside the half-power beam width, the signal typically drops off very quickly. A very high-gain antenna has a very narrow angled half-power beam width, which makes the directionality high as well.

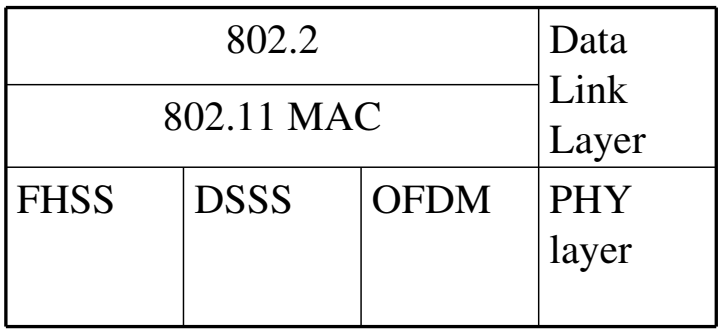
• **Antenna Polarity**

Polarization refers to the direction in which the electromagnetic field lines point as energy radiates away from the antenna. The simplest and most common type is linear polarization. When power is sent from transmitter to receiver, only that portion of the beam with the same polarization can be received. An improper antenna installation may decrease performance.

• **Frequency**

Different wireless applications use different frequencies to achieve their purposes. To make sure your wireless devices work as expected, users need to choose the right antenna with the right frequency. For example, using a 5 GHz IEEE 802.11a application with a 2.4 GHz antenna can weaken or even completely wipe out the signal.

4. IEEE 802.11 Layers Description



4. IEEE 802.11 Layers Description

WLAN largely use the Industrial, Medical & Scientific (ISM) band between 2400 and 2483.5 MHz. To use this frequency band, equipment must be compliant to the European Telecommunication Standard (ETS) 300 328. This standard defines the technical requirements on equipment using the 2400-2483.5 MHz frequency band. Since the 2400-2483.5 MHz frequency band is used by other types of equipment, such as micro wave ovens, techniques to avoid interference have to be used. The ETS 300 328 standard stipulates that frequency spreading must be used.

As any 802.x protocol, the 802.11 protocol covers the MAC and Physical Layer, the Standard currently defines a single MAC which interacts with three PHYs :

• Frequency Hopping Spread Spectrum in the 2.4 GHz Band

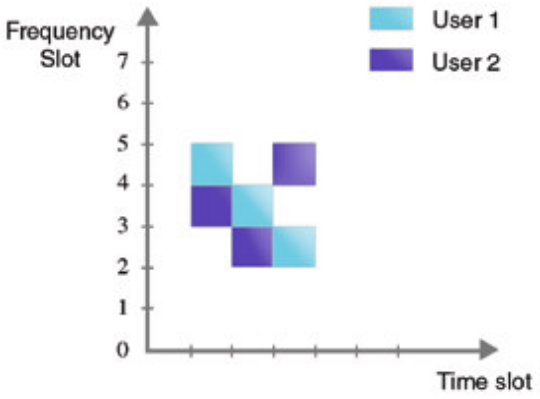
• Direct Sequence Spread Spectrum in the 2.4 GHz Band, and

• Orthoganal Frequency Division Multiplex (OFDM)

Beyond the standard functionality usually performed by MAC Layers, the 802.11 MAC performs other functions that are typically related to upper layer protocols, such as Fragmentation, Packet Retransmitions, and Acknowledgement.

4.1. Modulation Technologies (1)

4.1.1 Frequency Hopping Spread Spectrum (FHSS)



4.1 Modulation Technologies

4.1.1 Frequency Hopping Spread Spectrum (FHSS)

This modulation technique is one of the techniques used in spread spectrum signal transmission. It is also known as Frequency-Hopping Code Division Multiple Access (FH-CDMA).

Spread spectrum enables a signal to be transmitted across a frequency band that is much wider than the minimum bandwidth required by the information signal. The transmitter “spreads” the energy, originally concentrated in narrowband, across a number of frequency band channels on a wider electromagnetic spectrum.

Some of the advantages include:

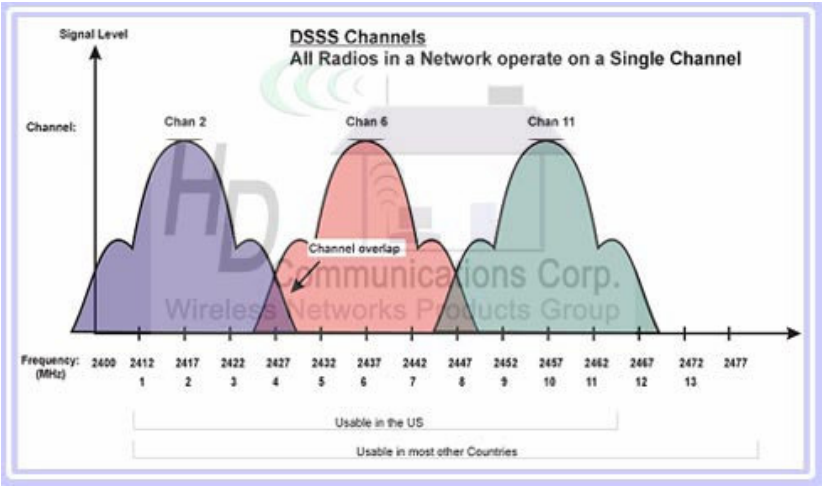
• Improved privacy

• Decreased narrowband interference

• Increased signal capacity

4.1. Modulation Technologies (2)

4.1.2 Direct Sequence Spread Spectrum (DSSS)



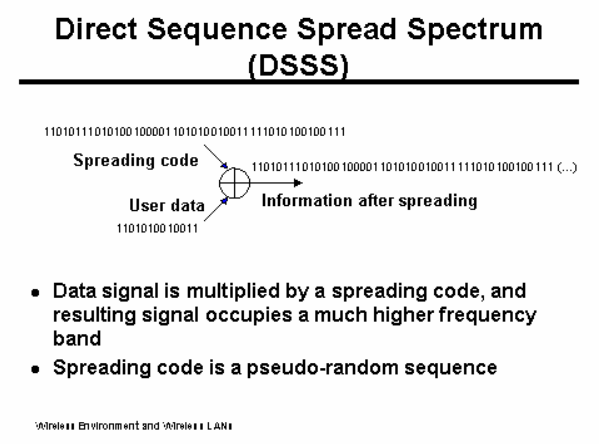
4.1.2 Direct Sequence Spread Spectrum (DSSS)

DSSS divides a stream of information to be transmitted into small pieces, each of which is allocated to a frequency channel across the spectrum. DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code).

Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission.

Direct Sequence Spread Spectrum is also known as Direct Sequence Code Division Multiple Access (DS-CDMA). This modulation technique is officially accepted and used by the IEEE 802.11b and IEEE 802.11g standards.

➢ Principle DSSS

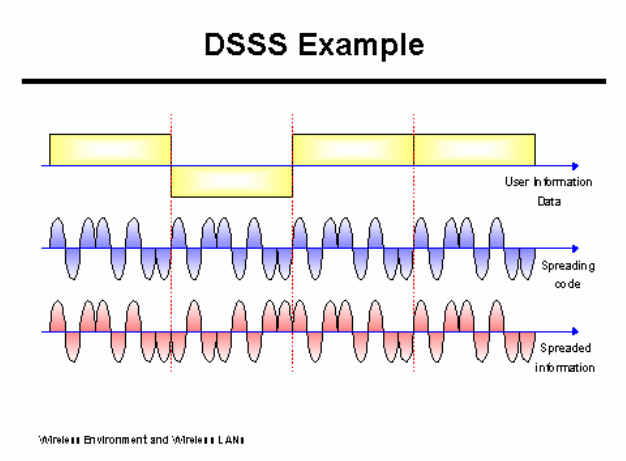


Wireless Channels IEEE 802.11g/b wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart.

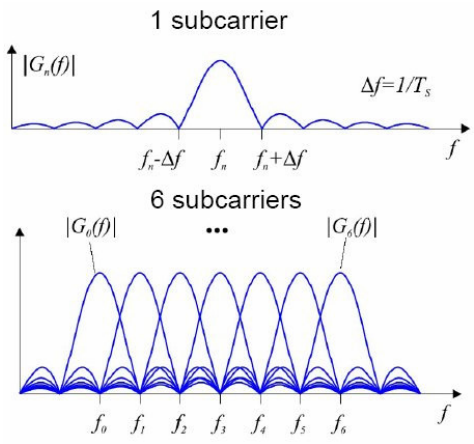
However, due to the spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other.

Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk.

➢ Example DSSS



4.1.3 OFDM (Orthogonal Frequency Division Multiplexing)



4.1.3 OFDM (Orthogonal Frequency Division Multiplexing)

Frequency division multiplexing (FDM) is a technology that transmits multiple signals simultaneously over a single transmission path, such as a cable or wireless system. Each signal travels within its own unique frequency range (carrier), which is modulated by the data (text, voice, video, etc.).

OFDM is a modulation system that divides a single digital signal across more signal carriers simultaneously.

The signals are sent at right angles (orthogonal) to each other so they do not interfere with each other. Orthogonal means that the frequencies into which the carrier is divided are chosen such that the peak of one subcarrier occurs when other subcarriers are at zero. OFDM has the ability to overcome multi-path effects by using multiple carriers to transmit the same signal.

OFDM is commonly used in IEEE 802.11a and 802.11g standards.

4.1.4 Summary modulation techniques

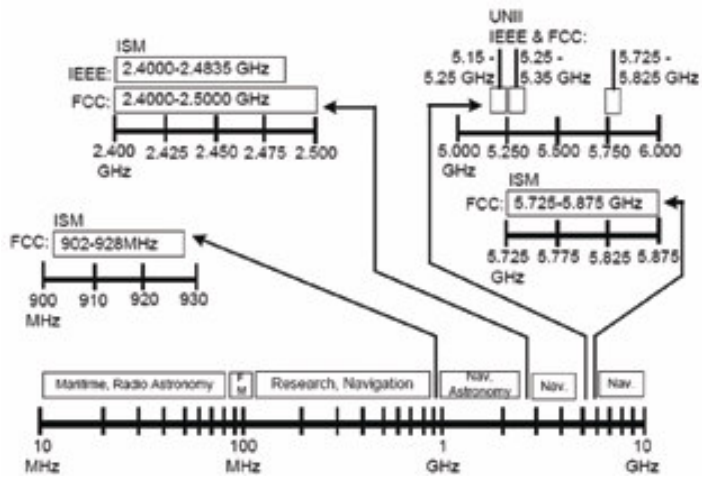
Modulation Technique	DSSS	FHSS	OFDM
Narrowband Interference	Less resistance (22 MHz wide contiguous bands)	more resistance (79 MHz wide contiguous	Much less (multicarrier modulation)
Interference susceptibility	Medium	High	Low
Compatibility	802.11b (WiFi Alliance)	None	802.11a, 802.11g
Implementation Cost	Comparatively less	Comparatively more	High
Throughput	5 – 6 Mbps	2 Mbps for 802.11	25 Mbps

4.1.4 Summary modulation techniques

FHSS utilizes frequency hopping to avoid signal interference. Bluetooth is one example that uses this technology. In the early days, IEEE 802.11 also used FHSS but has since adopted DSSS (Direct Sequence Spread Spectrum) out of security concerns.

802.11a, 801.11g, and 802.11n adopt OFDM to increase their resistance to external interferences.

4.1.5 Un-licensed bands ISM and UNII



4.1.5 Un-licensed bands ISM and UNII

The FCC (Federal Communications Commission) regulates the usable frequency bands and the maximum allowable power in these frequency bands for the United States. WLAN devices are allowed to use the ISM (Industrial/Scientific/Medical) band by the FCC.

The ISM band consists of 3 different sub-bands: 902-826 MHz, 2.4 GHz and 5.7-5.8 GHz.

The FCC has also further defined the UNII (Unlicensed National Information Infrastructure) band for WLAN usage.

ISM and UNII are both un-licensed bands which means anyone can transmit in these bands without a license from the FCC. It is the opening of these un-licensed bands that has allowed the WLAN business to grow in small businesses and homes. The freedom of these license-free bands also means a great number of un-licensed users may share the bandwidth with you.

In the frame of these lectures the discussion only includes the 2.4 GHz ISM band and 5 GHz UNII band because these 2 frequency bands are the most commonly used in WLAN applications.

The diagram shows the spectrum overview of the ISM and UNII bands.

The 5 GHz UNII band consists of 3 parts, each 100 MHz wide. The 802.11a standard uses this band. Each part of the UNII band includes 4 non-overlapping channels with 5 MHz of guard band between them. The FCC states that the lower band (UNII-1) can only be used indoors, the middle band (UNII-2) can be used indoors or outdoors, and the higher band (UNII-3) should only be used outdoors. Since UNII-1 and UNII-2 can be used indoors, the maximum number of non-overlapping channels in an indoor environment is 8.

• 2.4 GHz ISM Band/country

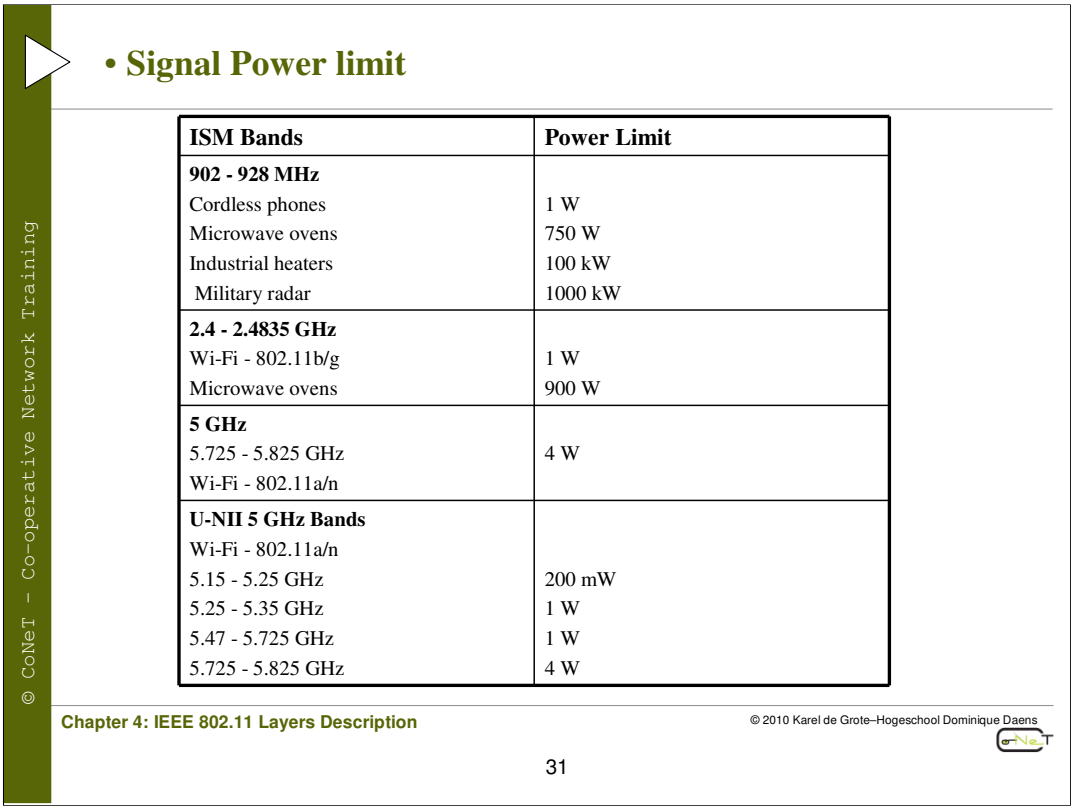
Channel	Center Frequency	Eu, M. East, Asia	USA	Japan
1	2.412 GHz	Y	Y	Y
2	2.417 GHz	Y	Y	Y
3	2.422 GHz	Y	Y	Y
4	2.427 GHz	Y	Y	Y
5	2.432 GHz	Y	Y	Y
6	2.437 GHz	Y	Y	Y
7	2.442 GHz	Y	Y	Y
8	2.447 GHz	Y	Y	Y
9	2.452 GHz	Y	Y	Y
10	2.457 GHz	Y	Y	Y
11	2.462 GHz	Y	Y	Y
12	2.467 GHz	Y		Y
13	2.472 GHz	Y		Y
14	2.484 GHz			Y

• 2.4 GHz ISM/country Band

802.11b/g is the most commonly used WLAN standard today.

The 2.4 GHz ISM band is supported by almost every country worldwide. Not every country supports the same channels in the 2.4 GHz ISM band. So you need to make sure the wireless AP matches the standard used by your country.

The slide shows channels supported in the 2.4 GHz ISM band for different countries/continents.



• Signal Power Limit

WLAN devices are allowed to use the ISM (Industrial/Scientific/Medical) band by the FCC. The ISM band consists of 3 different sub-bands: 902-826 MHz, 2.4 GHz and 5.7-5.8 GHz, which were initially used for machines that emitted radio frequencies, such as RF welders, industrial heaters and microwave ovens, but not for radio communications.

In 1985, the FCC Rules (Part 15.247) opened up the ISM bands for wireless LANs and mobile communications. In 1997, it added additional bands in the 5 GHz range under Part 15.407, known as the Unlicensed National Information Infrastructure (U-NII). Europe's HIPERLAN wireless LANs use the same 5 GHz bands, which are entitled the "Broadband Radio Access Network."

Numerous applications use the ISM/U-NII bands, including cordless phones, wireless garage door openers, wireless microphones, vehicle tracking and amateur radio.

Radio signals are transmitted with a certain power level. Power is measured in watts. However, a watt is a rather large amount of power in WLAN. Therefore, power is usually measured in milliwatts (mW), which is one thousandth of a watt.

A typical wireless AP transmits between 30 to 100 mW of power, and about 50 mW for wireless adaptors (clients). Certain applications will require higher transmit (Tx) power and may attempt to use power boosters or customized high power modules to amplify the transmission power. However, such attempts may cause the system to exceed the radio emission regulations of one's country.

4.2 MAC layer in WLAN

3 different MAC mechanisms:

- DCF (Direct or Distribution Coordination Function)
  - ✓Must be supported
  - ✓Uses CSMA/CA
  - ✓For Asynchronous data transfer
- DCF (CSMA/CA) with RTS/CTS
  - ✓Optional
  - ✓Introduced to solve the hidden node problem
  - ✓Reduces the number of collisions
- PCF (Point Coordination Function)
  - ✓Optional
  - ✓Based on DCF+RTS/CTS
  - ✓For Infrastructure mode (AP)
  - ✓Combines polling with asynchronous data transfer

4.2 MAC Layer in WLAN

The MAC Layer defines three different access methods:

• The Direct or Distributed Coordination Function (DCF): this is a two-way handshaking technique called Basic Access Mechanism

• DCF with RTSS/CTS: this is an optional four way handshaking technique, known as request-to-send/clear-to-send (RTS/CTS) mechanism

• The Point Coordination Function (PCF): generates time-sensitive traffic flows by beacon frames

4.2.1 DCF (Direct or Distribution Coordination Function)

4.2.1.1 CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

- Channel access mechanism (is the part of the protocol which specifies how the node uses the medium: when to listen, when to transmit..) used by most wireless LANs in the ISM bands
- The basic principles of CSMA/CA are listen before talk and contention: This is an asynchronous message passing mechanism (connectionless), delivering a best effort service, but no bandwidth and latency guarantee.
- Main advantages:
    - suited for network protocols such as TCP/IP
    - adapts quite well to variable traffic conditions
    - quite robust against interferences
- CSMA/CA is fundamentally different from the channel access mechanism used by cellular phone systems
- CSMA/CA is derived from CSMA/CD (Collision Detection), which is the basis of Ethernet. The main difference is collision avoidance: the protocol can't directly detect collisions (Ethernet protocols can) and only tries to avoid them.

4.2.1 DCF (Direct or Distribution Coordination Function)

4.2.1.1 CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)

The basic access mechanism, called Distributed Coordination Function, is basically a Carrier Sense Multiple Access with Collision Avoidance mechanism (usually known as CSMA/CA).

CSMA/CA is derived from CSMA/CD (Collision Detection), which is the basis of Ethernet. The main difference is collision avoidance: on a wire, the transceiver has the ability to listen while transmitting and so to detect collisions (with a wire all transmissions have approximately the same strength). But, even if a radio node could listen on the channel while transmitting, the strength of its own transmissions would mask all other signals on the air. So, the protocol can't directly detect collisions (Ethernet protocols can) and only tries to avoid them.

The basic principles of CSMA/CA are listen before talk and contention. This is an asynchronous message passing mechanism (connectionless), delivering a best effort service, but offers no bandwidth and latency guarantee. Its main advantages are that it is suited for network protocols such as TCP/IP, adapts quite well to variable traffic conditions and is quite robust against interferences.

How a CSMA (Carrier Sense Multiple Access) works

A CSMA protocol works as follows:

• A station desiring to transmit senses the medium,

• if the medium is busy (ie some other station is transmitting) then the station will defer its transmission to a later time

• if the medium is sensed free then the station is allowed to transmit.

• How a CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) works

A CSMA protocol works as follows:

➢ A station desiring to transmit senses the medium

➢ If the medium is **busy** (ie some other station is transmitting) then the station will defer its transmission to a later time.

➢ If the medium is sensed **free** then the station is allowed to transmit.

These kind of protocols are very effective when the medium is not heavily loaded, since it allows stations to transmit with minimum delay.

Principle of CD (Collision Detection)

- CSMA is very effective when the medium is not heavily loaded, since it allows stations to transmit with minimum delay
- But there is always a chance of stations transmitting at the same time (collision), caused by the fact that the stations sensed the medium free and decided to transmit at once.
- These collision situations must be identified, so the MAC layer can retransmit the packet by itself and not through upper layers, which would cause significant delay.
- In the 'wired' Ethernet case this collision is recognized by the transmitting stations which go to a retransmission phase based on an exponential random backoff algorithm.

Collision Detection mechanisms are a good idea on a wired LAN, but they cannot be used in a Wireless LAN environment

• Collision Detection (CD)

But there is always a chance of stations transmitting at the same time (collision) caused by the fact that the stations sensed the medium was free and decided to transmit at once.

These collision situations must be identified, so the MAC layer can retransmit the packet by itself and not by upper layers, which would cause significant delay.

In the 'wired' Ethernet case this collision is recognized by the transmitting stations which go to a retransmission phase based on an exponential random backoff algorithm.

Why CD is not possible in WLAN

CD cannot be used on a Wireless LAN environment, for two main reasons:

- Implementing a CD mechanism would require the implementation of a Full Duplex radio, capable of transmitting and receiving at once, an approach that would increase the price significantly.
- In a Wireless environment we cannot assume that all stations hear each other (which is the basic assumption of the CD), and the fact that a station is willing to transmit and senses the medium free, doesn't necessarily mean that the medium is free around the receiver area.

The 802.11 uses a Collision Avoidance (CA) mechanism together with a Positive Acknowledge scheme

• Why is CD not possible in WLAN?

CD cannot be used on a Wireless LAN environment, for two main reasons:

➢ Implementing a CD mechanism would require the implementation of a Full Duplex radio, capable of transmitting and receiving at once, an approach that would increase the radio price significantly.

➢ In a Wireless environment we cannot assume that all stations hear each other (which is the basic assumption of the CD), and the fact that a station is willing to transmit senses the medium free, doesn't necessarily mean that the medium is free around the receiver area.

4.2.1.2 DCF = CSMA/CA with Positive Acknowledgement (ACK)

A station willing to transmit senses the medium:

- If the medium is busy then it defers
- If the medium is free for a specified time (called DIFS, Distributed Inter Frame Space, in the standard) then the station is allowed to transmit
- The receiving station will check the CRC of the received packet and send an acknowledgment packet (ACK)
- Receipt of the ACK will indicate to the transmitter that no collision occurred.
- If the sender does not receive the ACK then it will retransmit the fragment until it is acknowledged or discard it after a given number of retransmissions

4.2.1.2 DCF = CSMA/CA with Positive Acknowledgement (ACK)

A station willing to transmit senses the medium:

• If the medium is busy then it defers

• If the medium is free for a specified time (called DIFS, Distributed Inter Frame Space, in the standard) then the station is allowed to transmit

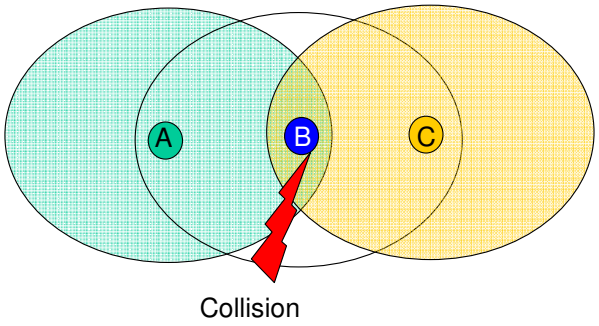
• The receiving station will check the CRC of the received packet and send an acknowledgment packet (ACK)

• Receipt of the ACK will indicate to the transmitter that no collision occurred.

• If the sender does not receive the ACK then it will retransmit the fragment until it is acknowledged or discard the fragment after a given number of retransmissions

Hidden Node problem

- Station A senses the channel (CS) and transmits to station B when channel is idle
- Station C cannot detect the transmission of station A and think s the channel is idle (CS fails)
- Station C transmits and a collision occurs at station B
- Station A does not detect the collision because Sation A is hidden from C



Hidden Node problem

The main effect of transmission on radio waves is the attenuation of the signal. Because of this attenuation the problem of hidden nodes is very common.

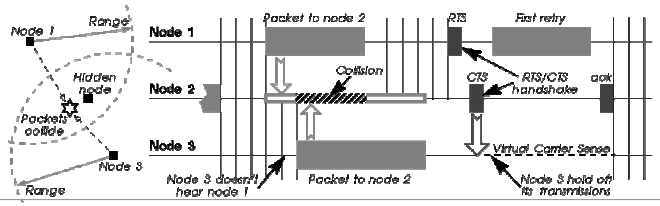
The hidden node problem comes from the fact that all nodes may not hear each other because the attenuation is too strong between them. Because transmissions are based on the carrier sense mechanism, those nodes ignore each other and may transmit at the same time. Usually, this is a good thing because it allows frequency reuse (they are effectively in different cells).

But, for a node placed in between, these simultaneous transmissions have a comparable strength and so collide (in its receiver). This node could be impossible to reach because of these collisions.

The fundamental problem with carrier sense only is that the transmitter tries to estimate if the channel is free at the receiver with only local information. The situation might be quite different between those two locations.

4.2.2 DCF with RTS/CTS ‚Virtual Carrier Sense‘

- In order to reduce the probability of two stations colliding because they cannot hear each other, the standard defines a ‘Virtual Carrier Sense mechanism:
- A station willing to transmit a packet will first transmit a short control packet called RTS (Request To Send), which will include the source, destination, and the duration of the following transaction (ie the packet and the respective ACK)
- The destination station will respond (if the medium is free) with a response control Packet called CTS (Clear to Send), which will include the same duration information.
- All stations receiving either the RTS and/or the CTS, will set their Virtual Carrier Sense indicator (called NAV, for Network Allocation Vector), for the given duration, and will use this information together with the Physical Carrier Sense when sensing the medium.

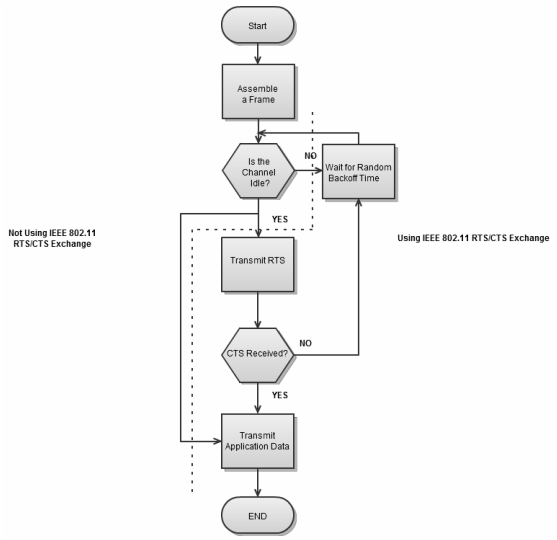


4.2.2 DCF with RTS/CTS ‚Virtual Carrier Sense‘

A simple and elegant solution to the ‘Hidden’ problem (proposed by Phil Karn in his MACA protocol for AX.25) is to use RTS/CTS (Request To Send/Clear To Send). RTS/CTS is a handshaking: before sending a packet, the transmitter sends a RTS and waits for a CTS from the receiver (see figure below). The reception of a CTS indicates that the receiver is able to receive the RTS (the channel is clear in its area). So the transmission is sent.

At the same time, every node in the range of the receiver hears the CTS (even if it doesn't hear the RTS), so understands that a transmission is going on. The nodes hearing the CTS are the nodes that could potentially create collisions in the receiver (assuming a symmetric channel). Because these nodes may not hear the data transmission, the RTS and CTS messages contain the size of the expected transmission (to know how long the transmission will last). This is the collision avoidance feature of the RTS/CTS mechanism (also called virtual carrier sense, also called NAV (Network Allocation Vector)): all nodes avoid accessing the channel after hearing the CTS even if their carrier sense indicate that the medium is free.

DCF (CSMA/CA) without/with RTS/CTS schematic

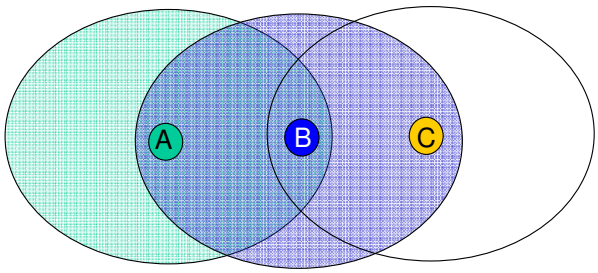


RTS/CTS has another advantage: it reduces the chance of a collision on the medium (collisions are much shorter in time). If two nodes attempt to transmit in the same slot of the contention window, their RTS collide and they don't receive any CTS, so they lose only a RTS, whereas in the normal scenario they would have lost a whole packet.

Because the RTS/CTS handshaking adds a significant overhead, usually it is not used for small packets or lightly loaded networks.

RTS/CTS/NAV mechanism (Solution ‚Hidden nodes')

- Station A senses the channel (CS) and transmits RTS to station B when channel is idle (RTS contains duration of the transmission)
- On reception of RTS, station B transmits CTS to A
- Station C also receives this CTS (C is not hidden for B) and knows now the channel is busy for a while and must wait



RTS/CTS/NAV mechanism (Solution ‚Hidden nodes')

RTS can be thought of as a reservation request sent by a device on the network. CTS is a response to this message, informing the device making the request that its request has been received, and that it is OK to send its packet.

In its traditional mode RTS/CTS was used in the following way. When there are devices on the network that cannot hear other devices on the network (so-called 'hidden node problem') those devices do not transmit their data to the AP immediately when they sense that the channel is quiet. Rather, they send an RTS message to the AP. If the AP receives that RTS message, it sends the CTS, which will be heard by all of the devices on the network, even those that the RTS-sending device may not be able to hear.

By definition, there are no devices in an infrastructure-based network that cannot be heard by the AP. All the devices hearing the CTS will know to cease transmissions for a period of time (defined by the CTS) and this will result in fewer collisions.

Diagram of the RTS/CTS/NAV mechanism

- The following diagram shows a transaction between two stations A (Src) and B (Dest), and the NAV setting of their neighbours (Other)
- On reception of RTS, station B transmits CTS to A
- Station C (Other) also receives this CTS (C is not hidden from B) and knows now the channel is busy for a while and must wait
- The NAV State is combined with the physical carrier sense to indicate the busy state of the medium.

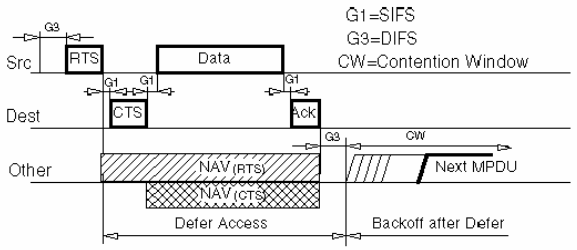


Diagram of the RTS/CTS/NAV mechanism

• **SIFS (Short Inter Frame Space)** is used to separate transmissions belonging to a single dialog (eg Fragment-Ack), and is the minimum Inter Frame Space. There is always at most one single station to transmit at this given time, hence having priority over all other stations.

This value is a fixed value per PHY and is calculated in such a way that the transmitting station will be able to switch back to receive mode and be capable of decoding the incomming packet, on the 802.11 FH PHY. This value is set to 28 microseconds

• **PIFS (Point Coordination IFS)** is used by the Access Point (or Point Coordinator, as it is called in this case), to gain access to the medium before any other station.

This value is SIFS plus a Slot Time; ie 78 microseconds.

• **DIFS (Distributed IFS)** is the Inter Frame Space used for a station willing to start a new transmission, which is calculated as PIFS plus one slot time; ie 128 microseconds

Advantages DCF with RTS/CTS

- Reduces the probability of a collision on the receiver area by a station that is “hidden” from the transmitter, to the short duration of the RTS transmission, because the station will hear the CTS and “reserve” the medium as busy until the end of the transaction
- The duration information on the RTS also protects the transmitter area from collisions during the ACK (by stations that are out of range of the acknowledging station)
- RTS and CTS are short frames. This also reduces the possibility of collisions, since these are recognized faster than they would be if the whole packet were transmitted, (this is true if the packet is significantly bigger than the RTS, so the standard allows for short packets to be transmitted without the RTS/CTS transaction, and this is controlled per station by a parameter called RTSThreshold).

Advantages DCF with RTS/CTS

• Reduces the probability of a collision on the receiver area by a station that is “hidden” from the transmitter, to the short duration of the RTS transmission, because the station will hear the CTS and “reserve” the medium as busy until the end of the transaction

• The duration information on the RTS also protects the transmitter area from collisions during the ACK (by stations that are out of range from the acknowledging station)

• RTS and CTS are short frames. This also reduces the possibility of collisions, since these are recognized faster than they would be if the whole packet were transmitted. This is true if the packet is significantly bigger than the RTS. So the standard allows for short packets to be transmitted without the RTS/CTS transaction and this is controlled per station by a parameter called RTSThreshold.

4.2.3 PCF (Point Coordination Function)

- Point Coordination Function (PCF) supports time-sensitive traffic flows
- Wireless access points periodically send beacon frames to communicate network identification and management parameters specific to the wireless network.
- Between the sending of beacon frames, PCF splits the time into a contention-free period and a contention period. With PCF enabled, a station can transmit data during contention-free polling periods.
- However, PCF hasn't been implemented widely because the technology's transmission times are unpredictable.

4.2.3 PCF (Point Coordination Function)

Point Coordination Function (PCF) supports time-sensitive traffic flows.

Wireless access points periodically send beacon frames to communicate network identification and management parameters specific to the wireless network.

Between the sending of beacon frames, PCF splits the time into a contention-free period and a contention period. With PCF enabled, a station can transmit data during contention-free polling periods. However, PCF hasn't been implemented widely because the technology's transmission times are unpredictable.

4.3 Roaming

4.3.1 What is Roaming?

- Roaming is the process of moving from one cell (or BSS) to another without losing connection.
- Slow roaming speed between mobile network's access points sometimes hinders the performance of industrial applications.
- 'High speed roaming' may be the solution

  Two principles:

  ✓Roaming by Signal

  ✓Roaming by Channel

4.3 Roaming

4.3.1 What is Roaming?

Roaming is the process of moving from one cell (or BSS) to another without losing connection.

In mobile applications that involve multiple access points (APs), roaming (also called handover) refers to when a client moves between two or more access points, and the speed of the mechanism used to effect the roaming mechanism can be crucial to a project's success.

As the client physically moves from one AP to another, the signal strength of the first AP will drop while the signal strength of the second AP will increase. When the signal strength of the first AP drops below the signal strength of the second AP, we say that the client has roamed to the second AP.

Factors that affect the smoothness of roaming include the topology of the access points, the gain and coverage of the antennas, and the roaming threshold settings of the client. To ensure smooth roaming, we first need to take into consideration the route of the moving object, and carefully plan the wireless AP deployment configuration.

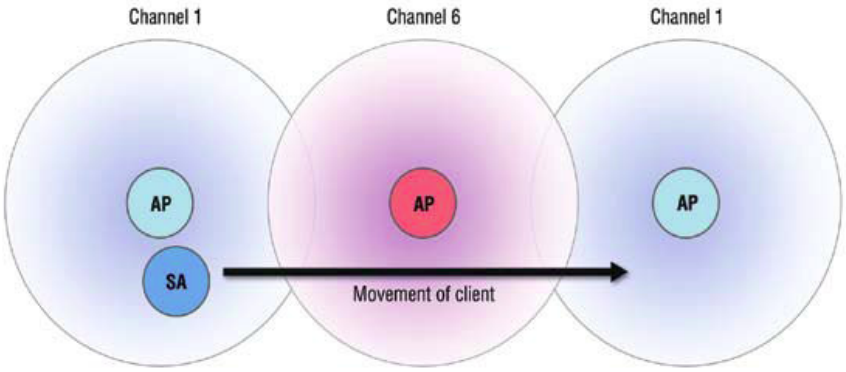
This function is similar to the cellular phones handover, with two main differences:

• On a LAN system which is packet based, the transition from cell to cell may be performed between packet transmissions, as opposed to telephony where the transition may occur during a phone conversation, this makes the LAN roaming a little easier, but

• On a voice system a temporary disconnection may not affect the conversation, while on a packet based environment it will reduce significantly the performance because retransmission would be performed by the upper layer protocols.

The 802.11 standard does not define how the roaming should be performed, but defines the basic tools for that, this includes the active/passive scanning, and a re-association process, where a station which is roaming from one Access Point to another will become associated with the new one

4.3.2 Basic Roaming (Slow Roaming)



4.3.2 Basic Roaming (Slow Roaming)

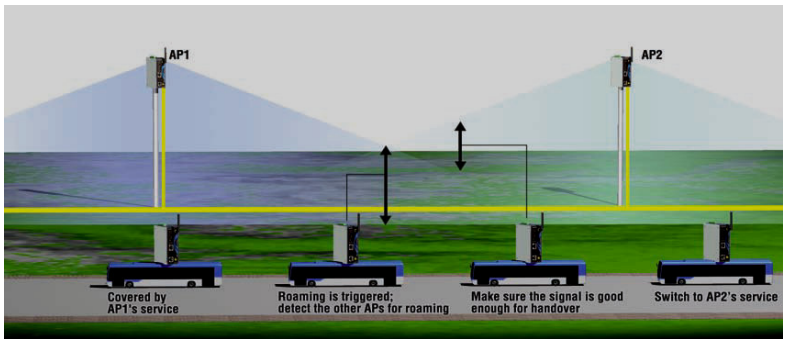
The diagram illustrates a client moving from left to right through regions governed by three different APs. As the client moves, the signal strength of the first AP drops and the signal strength of the second AP increases.

Most commercial wireless clients only consider communication quality when making roaming decisions. This means, when the signal strength of the first AP drops and frames cannot be transmitted, the client in an IEEE 802.11b application will first reduce the communication speed from 11 Mbps to 5.5 Mbps, and then to 2 Mbps, and finally to 1 Mbps. If the communication quality is still poor and frame transmission continues to fail, the client will decide that it's time to roam from the first AP to the second AP.

A roaming mechanism of this sort might be able to satisfy many non-critical applications.

4.3.3 High Speed Roaming

➢ Roaming by Signal



- Roaming by Signal allows roaming only when the current AP's signal drops below a certain threshold and roaming to another AP will improve transmission quality and provide a stronger signal.

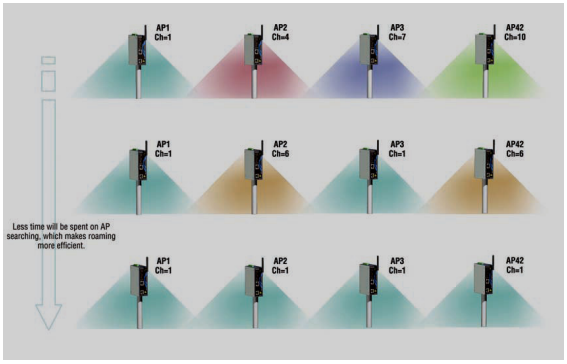
4.3.3 High Speed Roaming

Roaming by signal

Roaming by Signal allows roaming only when the current AP's signal drops below a certain threshold and roaming to another AP will improve transmission quality and provide a stronger signal.

4.3.3 High Speed Roaming

➢ Roaming by Channel



- Roaming by Channel unifies AP channels to avoid wasting channel hopping time during roaming.

Roaming by Channel

Roaming by Channel unifies AP channels to avoid wasting channel hopping time during roaming. However, a unified channel selection can also cause interference. Therefore it is necessary to properly separate channels between roaming APs to reduce interference.

5. Power Management (PSM)

5.1 PSM in Wireless LANs

- PSM is based on a synchronous sleep scheduling policy, in which wireless nodes (stations) are able to alternate between an active mode and a sleep mode.
- As a wireless station using PSM first joins an infrastructure based WLAN, it must notify its access point that it has PSM enabled. The access point then synchronizes with the PSM station allowing it to begin running its synchronous sleep schedule.
- When packets arrive for each of these PSM stations, the access point buffers them until their active period comes around again. At the beginning of each active period, a beacon message is sent from the access point to each wireless station in order to notify them of these buffered packets. PSM stations then request these packets and they are forwarded from the access point. Once all buffered frames have been received, a PSM station resumes with its sleep schedule wherever it left off. Whenever a PSM station has data to send, it simply wakes up, sends its packet, and then resumes its sleep schedule protocol as appropriate.
- The throughput achieved with these techniques is significantly less than with them disabled.
- While PSM may significantly reduce the energy consumed by a wireless station, many users prefer to sacrifice these power savings for an increase in performance.

5. Power Management (PSM)

5.1 PSM in Wireless LANs

Power Saving

Wireless LANs are typically related to mobile applications, and in this type of application battery power is a scare resource.

This is the reason why the 802.11 standard directly addresses the issue of Power Saving and defines a whole mechanism to allow stations to go into sleep mode for long periods of time without losing information.

The main idea behind the Power Saving Mechanism is that the AP maintains an updated record of the stations currently working in Power Saving mode, and buffers the packets addressed to these stations until either the stations specifically require getting the packets by sending a polling request, or until they change their operation mode.

The AP also transmits periodically (as part of its Beacon Frames) information about which Power Saving Stations have frames buffered at the AP, so these stations should wake up in order to receive one of these Beacon Frames.

If there is an indication that there is a frame stored at the AP waiting for delivery, then the station should stay awake and send a Poll message to the AP to get these frames.

Multicasts and Broadcasts are stored by the AP, and transmitted at a pre-known time (each DTIM), where all Power Saving stations which wish to receive this kind of frame should be awake. A DTIM interval, also known as a Data Beacon Rate, is the frequency at which an access point's beacon will include a DTIM (Delivery Traffic Indication Message).

5.2 PSM in Wireless PANs (Bluetooth)

- Wireless nodes in a Bluetooth network are organized into groups known as piconets, with one node dedicated as the master node and all others as slave nodes.
- Up to seven active nodes can exist in a piconet at any given time, with up to 256 potential members (249 inactive).
- All nodes operate using a synchronous sleep scheduling policy in order to exchange data. A beacon messaging system similar to the one for 802.11 based networks is used to exchange messages between slave nodes and their master.
- All nodes are able to communicate with all other nodes within the Piconet, but messages between slaves must be sent exclusively through the master node.
- Bluetooth defines eight different operational states, 3 of which are dedicated to low power operations. These three low power states are known as Sniff, Hold, and Park.
- While in the Sniff state, an active bluetooth device simply lowers its duty cycle and listens to the piconet at a reduced rate.
- When switching to the Hold state, a device will shut down all communication capabilities it has with a piconet, but remain "active" in the sense that it does not give up its access to one of the seven active slots available for devices within the piconet.
- Devices in the Park state disable all communication with the piconet just as in the Hold state, except that they also relinquish their active node status.

5.2 PSM in Wireless PANs (Bluetooth)

6. WLAN Security

The Evolution of Wireless Encryption

6.1 Basic Aspects

- AUTHENTICATION:
  to check a user's credentials and determine if the user should be given access to the data and resources provided by the protected network

- ENCRYPTION:
  encodes the data so that anyone who does not have the secret "key" will not be able to read the data

6. WLAN Security: The Evolution of Wireless Encryption

6.1 Basic Aspects

Security

Security is one of the first concerns of people deploying a Wireless LAN, the 802.11 committee has addressed the issue by providing what is called WEP (Wired Equivalent Privacy).

The main concerns of users are that an intruder would not be able to:

• Access the Network resources by using similar Wireless LAN equipment, and

• capture the Wireless LAN traffic (eavesdropping)

The purpose of WLAN security techniques is to render the connection unusable and the data unreadable by anyone except or you and the person (or machine) you're communicating with.

Although most people do not need in-depth knowledge of WLAN security, understanding the basics can make it easier to find the right product for protecting a given application.

There are two basic aspects to wireless security: **authentication and encryption**. A system uses authentication to check a user's credentials and determine if the user should be given access to the data and resources provided by the protected network. Encryption encodes the data so that anyone who does not have the secret "key" will not be able to read the data.

Eavesdropping is prevented by the use of the WEP algorithm which is a Pseudo Random Number Generator (PRNG) initialized by a shared secret key. This PRNG outputs a key sequence of pseudo-random bits equal in length to the largest possible packet which is combined with the outgoing/incoming packet producing the packet transmitted in the air.

The WEP algorithm is a simple algorithm based on RSA's RC4 algorithm which has the following properties:

• Reasonably strong: Brute-force attack to this algorithm is difficult because of the fact that every frame is sent with an Initialization Vector which restarts the PRNG for each frame.

• Self Synchronizing : The algorithm synchronizes again for each message, this is needed in order to work in a connectionless environment, where packets may get lost (as any LAN).

6.2 Authentication

- The 802.1X standard dictates how authentication on wired and wireless LANs is carried out.
- 802.1X is an authentication method that prevents unauthorized users from entering the network. It is used with WPA to form a complete WLAN security system.
- On many wireless systems, users either log into individual access points, or can freely enter the wireless network but cannot get further without additional authentication.
- 802.1X makes users authenticate to the wireless network itself, not an individual AP or another level like a VPN. This is more secure, as unauthorized traffic can be denied right at the AP.
- 802.1X authentication uses port-based access control, which means that the various entities involved in the authentication process gain access to each other's resources by connecting through "ports." In effect, the authentication procedure involves placing a "guard" at each port to prevent unauthorized users from gaining access to protected data.

6.2 Authentication

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods, Open System and Shared Key.

With **Open System authentication**, a wireless computer can join any network and receive any messages that are not encrypted.

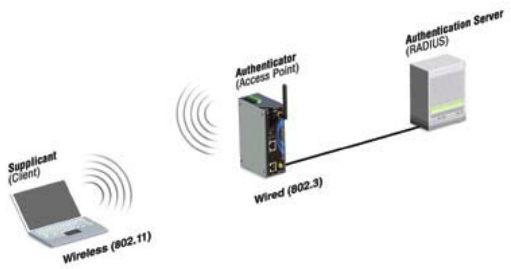
With **Shared Key authentication**, only those computers that possess the correct authentication key can join the network.

By default, IEEE 802.11 wireless devices operate in an Open System network.

➢ Authentication procedure

The 802.1X authentication procedure involves three basic players:

- The supplicant is the client (PC or laptop computer, for example) who would like to gain access to network resources through the wireless network.
- The authenticator, which is usually an access point (AP) for a wireless network and plays the role of gatekeeper.
- The authentication server, which connects to the AP over a wired network and handles the authentication procedure.



Authentication procedure

The 802.1X standard dictates how authentication on wired and wireless LANs is carried out. 802.1X authentication uses port-based access control, which means that the various entities involved in the authentication process gain access to each other's resources by connecting through "ports." In effect, the authentication procedure involves placing a "guard" at each port to prevent unauthorized users from gaining access to protected data.

In effect, the authenticator and authentication server work as a team to verify the identity of the supplicant. The authentication server also takes responsibility for computing the "keys" that the encryption algorithm will use. Although the details of authentication may be complex, the overall procedure is easy to describe:

STEP 1: The Authenticator relays authentication messages between the WLAN and the Ethernet.

STEP 2: The Authentication Server and Supplicant establish a secure tunnel that is used to pass encrypted messages.

STEP 3: The Authenticator performs the authentication check based on the agreed method (TLS, PEAP-MSCHAP-V2, TTL, etc.).

Authentication procedure WEP (Wired Equivalent Privacy)

- WEP provides a basic level of security to prevent unauthorized access to the network and protect wireless data.
- The IEEE 802.11 standard defines two types of WEP authentication: Open System and Shared Key
- Static shared keys (fixed length alphanumeric/hexadecimal strings) are used to encrypt data and are manually distributed to all wireless stations that want to use the wireless network.
- WEP has been found to have serious flaws
- WEP is not recommended for networks that require a high level of security.

WEP (Wired Equivalent Privacy) Authentication

The 802.11 standard defines several services that govern how two 802.11 devices communicate. The following events must occur before an 802.11 station can communicate with an Ethernet network through an access point:

1. Turn on the wireless station.

2. The station listens for messages from any access points that are in range.

3. The station finds a message from an access point that has a matching SSID.

4. The station sends an authentication request to the access point.

5. The access point authenticates the station.

6. The station sends an association request to the access point.

7. The access point associates with the station.

8. The station can now communicate with the Ethernet network through the access point. An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11 standard defines two types of WEP authentication: Open System and Shared Key.

6.2.1. WEP Open System Authentication

- The following steps occur when two devices use Open System Authentication:
  1. The station sends an authentication request to the access point.
  2. The access point authenticates the station.
  3. The station associates with the access point and joins the network.

6.2.1 WEP Open System Authentication

Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the "ANY" SSID option to associate with any available access point within range, regardless of its SSID.

6.2.2 WEP Shared Key Authentication

- The following steps occur when two devices use Shared Key Authentication:
  1. The station sends an authentication request to the access point.
  2. The access point sends challenge text to the station.
  3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and it sends the encrypted text to the access point.
  4. The access point decrypts the encrypted text using its configured WEP key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP key, and the access point authenticates the station.
  5. The station connects to the network. If the decrypted text does not match the original challenge text (that is, the access point and station do not share the same WEP key), then the access point will refuse to authenticate the station, and the station will be unable to communicate with either the 802.11 network or the Ethernet network.

6.2.2 WEP Shared Key Authentication

Shared Key Authentication requires that the station and the access point have the same WEP key to authenticate.

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit. The 64-bit WEP data encryption method allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40- bit WEP data encryption because the user-configurable portion of the encryption key is 40 bits wide. The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the 40-bit WEP data encryption method, the remaining 24 bits are factory-set and not user-configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry. The 128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside the United States due to U.S. export regulations.

When configured for 40-bit encryption, 802.11 products typically support up to four WEP keys. Each 40-bit WEP key is expressed as five sets of two hexadecimal digits (0–9 and A–F). For example, “12 34 56 78 90” is a 40-bit WEP key. When configured for 128-bit encryption, 802.11g products typically support four WEP keys, but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0–9 and A–F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP key. Typically, 802.11 access points can store up to four 128-bit WEP keys, but some 802.11 client adapters can only store one. Therefore, make sure that your 802.11 access and client adapters’ configurations match. Whatever keys you enter for an access point, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, etc.

6.3 Encryption

- The science of encryption or the making and breaking of codes, is one of the most crucial aspects of WLAN technology. This is because the radio waves used to transmit data packets between your computer and the wireless access point can pass through walls, floors, and other barriers.
- People who use laptops that have a wireless LAN card will know this first-hand, since it is often possible to pick up signals from wireless access points located in nearby apartments.
- Using a password to restrict entry to your network may not provide enough protection, since a reasonably clever person can still intercept your data packets.
- In fact, if the person intercepting the wireless data is more than reasonably clever, he or she may also be able to download and read the contents of the packets.

6.3 Encryption

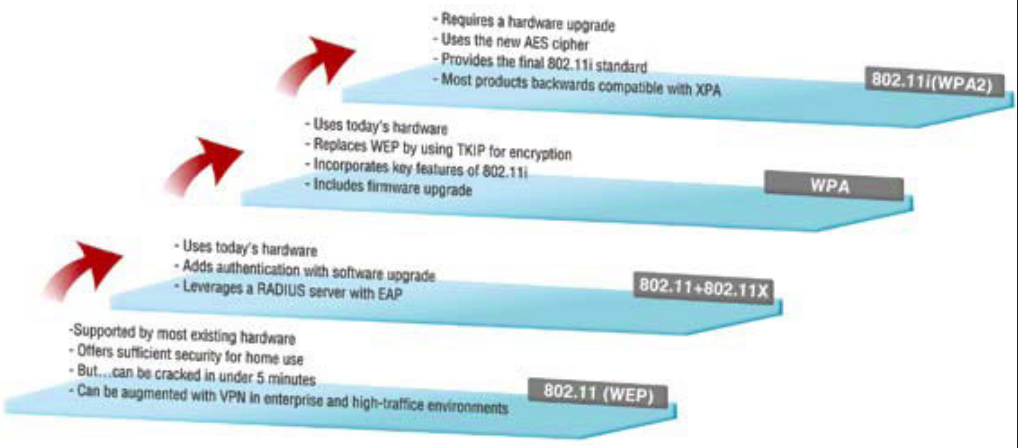
The science of encryption or the making and breaking of codes, is one of the most crucial aspects of WLAN technology. This is because the radio waves used to transmit data packets between your computer and the wireless access point can pass through walls, floors, and other barriers.

People who use laptops that have a wireless LAN card will know this first-hand, since it is often possible to pick up signals from wireless access points located in nearby apartments.

Using a password to restrict entry to your network may not provide enough protection, since a reasonably clever person can still intercept your data packets.

In fact, if the person intercepting the wireless data is more than reasonably clever, he or she may also be able to download and read the contents of the packets.

Evolution of methods of Encryption



6.3.1 WPA (Wi-Fi Protected Access)

- WPA is a stronger security method that was created in response to the flaws discovered in WEP.
- WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption
- It was intended as an intermediate measure until further 802.11i security measures were developed.
- When implemented with authentication methods such as RADIUS, WPA is considered secure enough for all but the most sensitive enterprise applications.
- For most home and small business use, an effective level of security can be obtained by using WPA with a pre-shared key (PSK) that is shared by all users.

6.3.1 WPA (Wi-Fi Protected Access)

WPA is a stronger security method that was created in response to the flaws discovered in WEP.

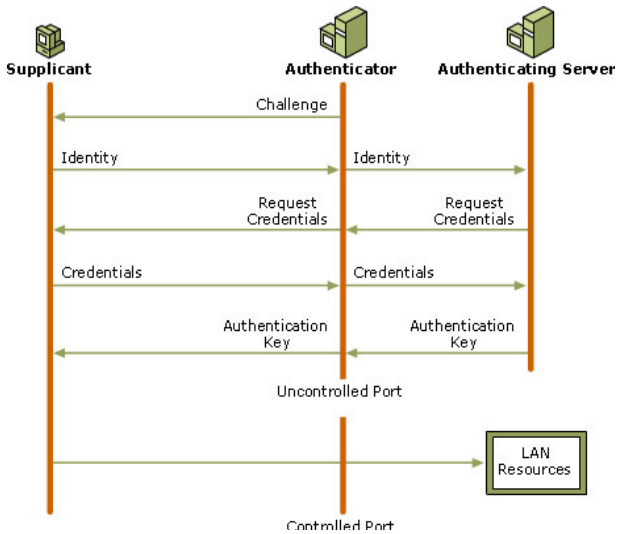
WPA uses Temporal Key Integrity Protocol (TKIP) for data encryption.

It was intended as an intermediate measure until further 802.11i security measures were developed.

When implemented with authentication methods such as RADIUS, WPA is considered secure enough for all but the most sensitive enterprise applications.

For most home and small business use, an effective level of security can be obtained by using WPA with a pre-shared key (PSK) that is shared by all users.

WPA (Wi-Fi Protected Access)



6.3.2 WPA2 (Wi-Fi Protected Access 2nd generation)

- WPA2 is the second generation of WPA.
- The primary difference between WPA and WPA2 is the technology used for data encryption.
- WPA2 uses Advanced Encryption Standard (AES), a stronger encryption technology suitable for industries that require highly secure networks.

6.3.2 WPA2 (Wi-Fi Protected Access 2nd generation)

WPA2 is the second generation of WPA.

The primary difference between WPA and WPA2 is the technology used for data encryption.

WPA2 uses Advanced Encryption Standard (AES), a stronger encryption technology suitable for industries that require highly secure networks.

6.4 Firewall as additional Safeguard

- One of the most basic aspects of maintaining the security of your network involves using a firewall to filter out unwanted traffic.
- To protect a private LAN from unwanted traffic originating outside the LAN, firewall software often runs on a gateway that connects the LAN to the Internet.
- The firewall is configured to filter out traffic based on various characteristics of the incoming packets, such as IP address, MAC address (MAC Address Authentication), type of protocol, etc.
- Even if your private LAN does not connect to a public network, once you allow access to the LAN through a wireless AP, you open the network to possible external attack. As an added safeguard, some manufacturers include firewall software on the access point to filter out traffic accessing the network through the AP.
- Most APs support the encryption technology (WEP, WAP, WAP2) and allows system managers to filter traffic by MAC address, SSID Disable broadcast, IP, as well as TCP/UDP filtering options.

6.4 Firewall as additional Safeguard

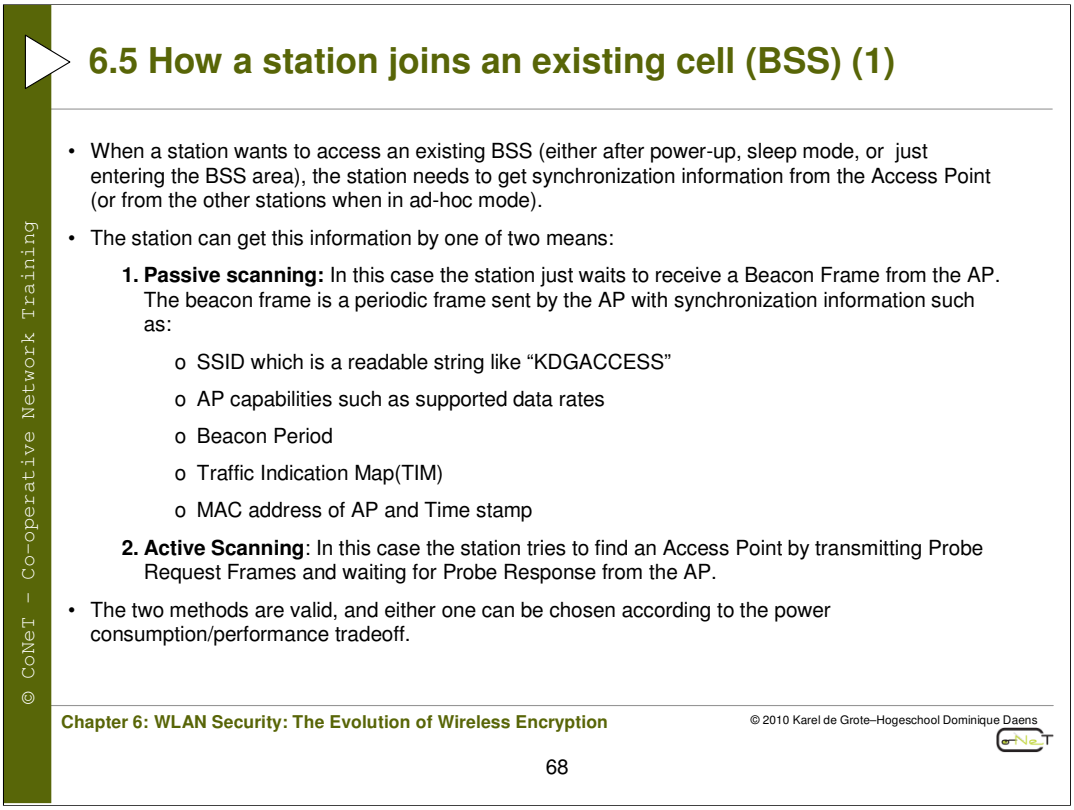
One of the most basic aspects of maintaining the security of your network involves using a firewall to filter out unwanted traffic.

To protect a private LAN from unwanted traffic originating outside the LAN, firewall software often runs on a gateway that connects the LAN to the Internet.

The firewall is configured to filter out traffic based on various characteristics of the incoming packets, such as IP address, MAC address (MAC Address Authentication), type of protocol, etc.

Even if your private LAN does not connect to a public network, once you allow access to the LAN through a wireless AP, you open the network to possible external attack. As an added safeguard, some manufacturers include firewall software on the access point to filter out traffic accessing the network through the AP.

Most APs support the encryption technology (WEP, WAP, WAP2) and allows system managers to filter traffic by MAC address, SSID Disable broadcast, IP, as well as TCP/UDP filtering options.



6.5 How does a station join an existing cell (BSS)?

When a station wants to access an existing BSS (either after power-up, sleep mode, or just entering the BSS area), the station needs to get synchronization information from the Access Point (or from the other stations when in ad-hoc mode).

The station can get this information by one of two means:

• **Passive scanning**: In this case the station just waits to receive a Beacon Frame from the AP. The beacon frame is a periodic frame sent by the AP with synchronization information such as:

- ✓ SSID which is a readable string like “KDGACCESS”
- ✓ AP capabilities such as supported data rates
- ✓ Beacon Period
- ✓ Traffic Indication Map(TIM)
- ✓ MAC address of AP and Time stamp

• **Active Scanning**: In this case the station tries to find an Access Point by transmitting Probe Request Frames and waiting for Probe Response from the AP.

The two methods are valid, and either one can be chosen according to the power consumption/performance tradeoff.

How a station joins an existing cell (BSS) (2)

The Authentication Process

- Once the station has found an Access Point and decided to join its BSS it will go through the ***Authentication Process***
  - ✓ This is the interchange of information between the AP and the station, where each side proves it knows a given password.

The Association Process

- When the station is authenticated it will start the ***Association Process***
  - ✓ This is the exchange of information about the stations and BSS capabilities and which allows the DSS (the set of APs) to know about the current position of the station.

- A station is capable of transmitting and receiving data frames only after the association process is completed!

The Authentication Process

Once the station has found an Access Point and decided to join its BSS it will go through the Authentication Process.

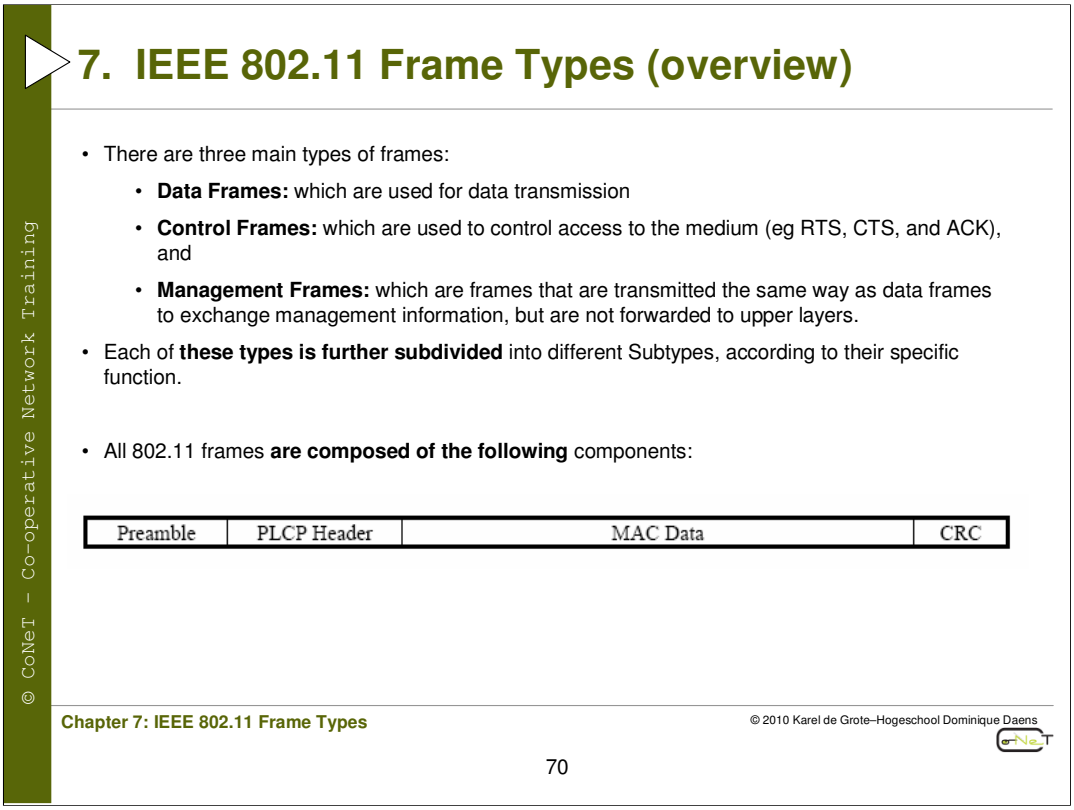
This is the interchange of information between the AP and the station, where each side proves it knows a given password.

The Association Process

When the station is authenticated it will start the Association Process.

This is the exchange of information about the stations and BSS capabilities and which allows the DSS (the set of APs) to know about the current position of the station.

A station is capable of transmitting and receiving data frames only after the association process is completed.



7. IEEE 802.11 Frame Types

Preamble

This is PHY dependent, and includes:

• *Synch* : An 80-bit sequence of alternating zeros and ones, which is used by the PHY circuitry to select the appropriate antenna (if diversity is used), and to reach steady-state frequency offset correction and synchronization with the received packet timing, and

• *SFD* : A Start Frame delimiter which consists of the 16-bit binary pattern 0000 1100 1011 1101, which is used to define the frame timing.

PLCP Header

The PLCP Header is always transmitted at 1 Mbit/s and contains Logical information that will be used by the PHY Layer to decode the frame, and consists of:

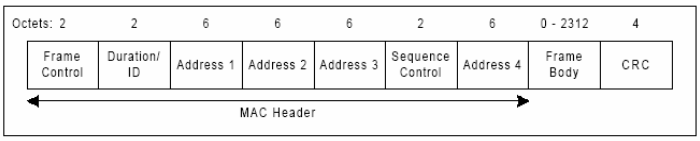
• *PLCP_PDU Length Word* : which represents the number of bytes contained in the packet, this is useful for the PHY to correctly detect the end of packet

• *PLCP Signaling Field* : which currently contains only the rate information, encoded in 0.5 MBps increments from 1 Mbit/s to 4.5 Mbit/s

• *Header Error Check Field*: Which is a 16 Bit CRC error detection field

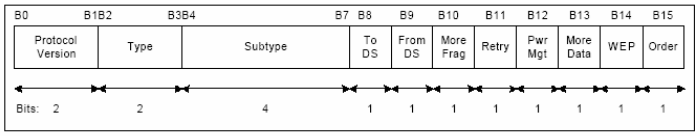
• MAC Data Frame with the Frame Control Field

The following figure shows the general MAC Data Frame



Frame Control Field

The Frame Control Field contains the following Information:



MAC Data

Type and Subtype

These 6 bits define the Type (Management, Control or Data) and SubType (ACK, RTS, CTS...)

ToDS

This bit is set to 1 when the frame is addressed to the AP for forwarding it to the Distribution System (including the case where the destination station is in the same BSS, and the AP is to relay the frame). The Bit is set to 0 in all other frames.

FromDS

This bit is set to 1 when the frame is comming from the Distribution System.

More Fragments

This bit is set to 1 when there are more fragments belonging to the same frame following this current fragment.

Retry

This bit indicates that this fragment is a retransmission of a previously transmitted fragment, this will be used by the receiver station to recognize duplicate transmissions of frames that may occur when an Acknowledgment packet is lost.

Power Management Power Management

This bit indicates the Power Management mode that the station will be in after the transmission of this frame. This is used by stations which are changing state either from Power Save to Active or viceversa.

More Data

This bit is also used for Power Management and it is used by the AP to indicate that there are more frames buffered to this station. The station may decide to use this information to continue polling or even changing mode to Active.

WEP

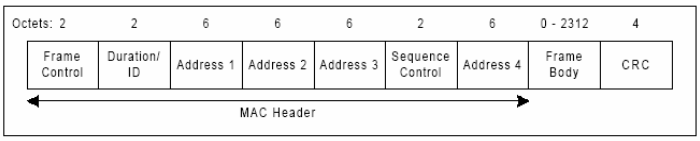
This bit indicates that the frame body is encrypted according to the WEP algorithm

Order

This bit indicates that this frame is being sent using the Strictly-Ordered service class.

• Address Fields in MAC Data Frame

The following figure shows the general MAC Data Frame



Address Fields

A frame may contain up to 4 Addresses depending on the ToDS and FromDS bits defined in the Control Field, as follows:

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Address Fields

A frame may contain up to 4 Addresses depending on the ToDS and FromDS bits defined in the Control Field, as follows:

Address-1 is always the Recipient Address (ie the station on the BSS which is the immediate recipient of the packet). If ToDS is set this is the Address of the AP. If ToDS is not set then this is the address of the end-station.

Address-2 is always the Transmitter Address (ie the station which is physically transmitting the packet). If FromDS is set this is the address of the AP. If it is not set then it is the address of the Station.

Address-3 is in most cases the remaining, missing address, on a frame with FromDS set to 1, then the Address-3 is the original Source Address, if the frame has the ToDS set then Address 3 is the destination Address.

Address-4 is used in the special case where a Wireless Distribution System is used, and the frame is being transmitted from one Access Point to another, in this case both the ToDS and FromDS bits are set, so both the original Destination and the original Source Addresses are missing.