Wireless Local Area Network (WLAN) Technology Fundamentals

Agilent Technologies
Goals and Objectives - WLAN Technology Fundamentals

• The primary goal of this course is to provide an overview of the WLAN technology.

• At the end of this course you will be able to:
  • Know the trends and driving force behind wireless networking technology
  • Describe the IEEE802.11a/b System Level Architecture
  • Understand the Physical Layer of the IEEE802.11a/b standard
  • Understand the MAC Layer of the IEEE802.11a/b standard
  • Describe the timing, power management and security techniques for IEEE802.11 WLAN systems.
Agenda - WLAN Technology Fundamentals

- Introduction - Objectives and Agenda
- Overview of Wireless Networking Technologies
  - Why Wireless Networking?
  - Wireless Networking Trends
  - Wireless Networking Standards and Comparison
- Understanding How Wireless LAN Works
  - Advantages of Wireless LAN
  - Wireless LAN Applications
  - Wireless LAN Topologies
  - Wireless LAN Architecture (Physical and Medium Access Control Layer)
  - Wireless LAN Standards and Comparison
- Standardization of Wireless LAN
  - Why Standardize Wireless LAN
Agenda - WLAN Technology Fundamentals cont’d

- IEEE 802.11 Wireless LAN Standard
  - IEEE 802.11 Wireless LAN Architecture
  - IEEE 802.11 Medium Access Control Layer protocol
  - IEEE 802.11b Medium Access Control Layer Services
    - Synchronization
    - Authentication
    - Security and Privacy
    - Association/Re-association
    - Data Transfer
    - Power Management
  - IEEE 802.11 Physical Layer (Modulation Formats)
- Conclusions and Summary
- References for Additional Information
Overview of Wireless Networking Technologies

The first section of this training covers an overview of the different wireless networking technologies. The driving force behind wireless networking and the current trends will also be discussed.
Why Wireless Networking? - Driving Force

- Global Internet Explosion
- Rapid growth for mobile data communications needs
- Broadband data access at fast data rates
- Growing usage of handheld devices (laptop, palmtop etc)
- Greatly reduces cost of the last 50 Meters
- No wires to pull

Why Wireless Networking? - Driving Force

Wireless Networking technologies enable two or more computers to communicate without physical network cables using existing standard network protocols. The key question here is what are the driving forces behind wireless networking? The global Internet explosion is one of the main driving forces behind wireless networking. The rapid growth of mobile data communications needs for both businesses and private individuals are also fueling wireless networking demands. Today, mobile internet data is access using either an analog fixed line, a company WAN (wired or wireless) or a mobile phone. Although mobile phones allow the user to connect to the network easily, its primitive user interface and its inability to access to large files at a fast data rates really hinders its usefulness. Mobile broadband data access using hand-held-devices like laptops, PDA’s, etc will drive the trend toward future growth. Wireless Modems provide substantial installation cost savings over hard wired Internet access, plus greater office layout flexibility.

Let us now take a look at the market penetration of mobile data services and key trends which are the driving forces behind wireless networking.
Wireless Networking Trends

Wireless Networking Systems are evolving toward providing broadband capability with the performance comparable to that of high-bandwidth fixed networks.

- Higher data rates
- More complex multiple-access and modulation techniques
- Higher frequencies

Wireless Networking Trends

All Wireless systems, including wireless networking are evolving to provide broadband services anywhere. The performance of these services must be comparable with high-bandwidth fixed networks. Wireless LAN users are not willing to trade off data rates for mobility. The demand for much higher data rates has already given rise to standards like the IEEE802.11a where the data rates can go as high as 54Mbps. To meet the needs of higher data rates and larger user-capacity, wireless LAN systems have already moved to more complex multiple-access techniques and modulation schemes (e.g. OFDM 64QAM). The big challenge in the wireless world today is the scarcity of available spectrum which can pose serious obstacles to the development of a new broadband systems. To meet this challenge, the allocated spectrum is moving to the higher frequencies. For example, the IEEE802.11a is deployed in the 5GHz (U-NII band) band which will offers three times the operating bandwidth over the available spectrum in the 2.4GHz band.
Wireless Networking Alternatives - Wireless Local Area Network (WLAN)

- Provide all functionality of a wired LAN system but without a physical wire.
- Carries high-speed traffic (e.g. IEEE802.11a max data rate = 54Mbps)
- Does not support real time voice traffic well
- Coverage area is in order of 50 meters (small cell-size)
- Low-speed mobility
- No user fee required

Different forms of Wireless Networking - Wireless LAN

Wireless Local Area Network (WLAN) is a two-way communication network that serves as an extension to, or as an alternative for a wired LAN. It carries high speed traffic (as high as 54Mbps for IEEE802.11a) and usually utilizes a random access technique such as Carrier Sense Multiple Access (CSMA), so it does not support real time voice information well. The voice traffic is more suitable in an circuit-switched network where the bandwidth is guarantee, not one where the access times can vary over a large range and can cause packets to get lost or arrive out of order. Wireless LAN is operated over a limited geographic area, usually limited to a distance of around 100 meters. With a limited cell-size, the wireless LAN network support only low speed mobility application (pedestrian speed). Wireless LAN require no usage fees. More of Wireless LAN will be covered in this course.
Wireless Networking Alternatives
-Wireless Wide Area Network (WWAN)

• Comes in many forms: - Cellular, Packet radio, Satellite etc.
• Costly infrastructures required i.e. Base Stations
• Carries lower-speed traffic compared to wireless LAN
• Coverage- much larger cell-size than wireless LAN
• High-speed mobility
• User fees required

Wireless Networking - Wireless WAN

Wireless Wide Area Network (WWAN) provides two way network communication using different formats and mediums. The most popular medium being transmission over the cellular network or via packet radio services. The various formats of wireless WAN has different applicability for different kinds of user traffic. For example, cellular carries voice well and data fairly well, Packet radio is ideal for data traffic and Satellite networks carries data and voice very well but at a much higher cost. A costly infrastructure is required to support wireless WAN services. Wireless WAN provides much lower data rates as compared to wireless LAN but over a much larger geographical area (National level) . Wireless WAN supports high-speed mobility but user have to pay for bandwidth on a time or usage basic.
Wireless Networking Alternatives - Wireless Personal Area Network (WPAN)

• Serves as an alternative to cable.

• Coverage is only limited to a few meters.

• Data rates are on the order of a few Mbps

• No user fees required

Wireless Networking - Wireless PAN

Wireless Personal Area Network (WPAN) main functions as an alternative to cable. Wireless PAN may co-exist with wireless LAN, addressing different user needs. For example, wireless PAN can be used to synchronize two computers and transfer files between them. A wireless PAN typically covers only a few meters surrounding a user’s workspace. The data rates are on the order of a few Mbps. Like the wireless LAN system, wireless PAN does not require the user to pay for its usage. One of the most talk about WPAN technology today is Bluetooth, which is a cable-replacement technology. Bluetooth is operating in the same 2.4GHz Industrial, Scientific, Medical (ISM) band as IEEE802.11b. This has caused a lot of concern for the IEEE802.11b camp, because Bluetooth frequency hopping signals will poise interference threat to the IEEE802.11b direct sequence signals.
Wireless Networking Standards – Comparison

Here is a comparison chart of the different wireless networking standards in terms of coverage area, typical throughput, application and user fee. The WPAN is more suitable for short range application where the WLAN technology provides a larger coverage area, usually within a building or campus premises. In terms of throughput, the WLAN is capable of providing a maximum of 54Mbps (IEEE802.11a, 802.11g and HIPERLAN 2) where the WPAN and WWAN provides much lower maximum data rate at 4Mbps and 32Kbps respectively. WPAN (Bluetooth) is designed to provide as a replacement/alternative to cables, such as synchronization of PDAs, wireless printers etc. Unlike the WWWAN, both WLAN and WPAN do not require user fees.
Understanding How Wireless LAN Works

Before we take a deeper look at the IEEE802.11 standard, let us first understand how generally Wireless LAN works. This section will discuss the advantages and applications of Wireless LAN. Different Wireless LAN topologies will be introduced as well. The Physical and Medium Access Control (MAC) layers in the protocol stack defines the Wireless LAN functionality. We will learn under this section, the different implementation options for the Physical layer and also the core mechanism in the Medium Access Control (MAC) layer.
What Is Wireless Local Area Network?

A Wireless Local Area Network (WLAN) is a high bandwidth, two-way data communications network.

It operates over a limited geographic area using radio as the transmission medium, rather than optical fiber or copper twisted pair or coaxial cable.

It serves as an extension to, or as an alternative for, a wired LAN.

It combines data connectivity with user mobility.

What is Wireless Local Area Network?

Wireless Local Area Network technologies emerged in the 1980s as a high bandwidth, two-way data communications network operating over a limited geographical area. By using radio as the transmission medium, Wireless LAN serves as an extension to, or as an alternative for, a wired LAN. It combines data connectivity with user mobility. By using wireless LAN, users can access shared information without having to look for a place to plug in.
Advantages of Wireless LAN

- Mobility
- Scalability
- Greatly reduced installation Cost
- Simpler and faster installation - Last 50 meters
- Installation flexibility
- Reduced cost of ownership

Advantages of Wireless LAN

Wireless LAN allow user to access share information without having to get connected to the network using wires. For the network managers, they can set up or augment networks without installing or moving wires. Wireless LAN provides users with a flexible data communication system with mobility. The lists a few of the advantages that Wireless LAN can provide. The main advantages are productivity, convenience, and much lower installation cost. These advantages over the traditional wired networks are the key reasons why Wireless LAN is gaining popularity in a number of markets, including manufacturing, retail, warehousing, academia, etc.

Hardware costs for Wireless is substantially less than hard wired systems

Wireless LAN is simpler and faster to install and it also eliminates the cost of pulling cables. Last 50 meters from network node to user.

Wireless LAN provides combines data connectivity with user Mobility. It can provide user with access to real-time information when they are on the move. This mobility supports productivity and service opportunities not possible with wired networks.

The scalability characteristic of a Wireless LAN system allows the infrastructure to be changed easily to suit the different environment and application. For example, if the network is to support a small number of users, then a peer-to-peer network can be configured instead of a full infrastructure network that is suitable for thousands of users roaming over a broad area.

Wireless LAN, not only benefits the laptop users in terms of moving from one location to another, there are benefits for users of fixed position computers as well. Take for example, in an environment where it is too costly or impossible to build a wired network, Wireless LAN offers a cost effective alternative to these environments. Wireless LAN offers excellent installation flexibility in places where wire cannot exist.

In dynamic environments where frequent moves and changes are required, Wireless LAN offers much better long-term cost benefits. The Wireless LAN systems offer a reduced cost of ownership in terms of overall installation expenses and life-cycle costs.
Application for Wireless LAN

- **Mobile access to central databases** in real-time, e.g. Medical staff, Warehouse workers, Students.

- **Instant network** for small groups in temporary location, e.g. consulting or accounting audit teams, trade show booth, or employee hot-desking.

- **Network management in dynamic environments**, e.g. minimize the overhead caused by moves, extensions to networks, and other changes.

- **Network management in “difficult” environments**, e.g. networking computers in older buildings.

With a large number of advantages that the Wireless LAN systems can offer, Wireless LANs have gained strong popularity in a number of vertical markets. The slide lists a few of the applications made practical via the power and flexibility of Wireless LANs.

Professionals like medical staff, or warehouse workers can be provided with inexpensive mobile access to central databases in real-time, increasing productivity. Students on campus can also make use of wireless connectivity for easier access to information and learning materials. Wireless LAN also offers instant networking for small groups in temporary locations. Take for example, consulting or accounting and audit teams can increase productivity with instant network setup. Trade show and employee hot-desking can minimize setup requirements using the instant network offer by Wireless LANs. Wireless LANs can provide network management in dynamic environments. This has the advantage of minimizing the overhead caused by moves, extensions to networks, and other changes. Wireless LAN can also provide network management in “difficult” environments, for example installing networked computers in older buildings.
What Is a Good Wireless LAN Solutions?

A Wireless LAN Wish List

- Low cost
- Interoperability
- Minimal susceptibility to interference
- Minimal battery consumption
- Minimal form factor (PCMCIA)
- Throughput/high data-rate
- Good coverage
- Robust security
- Built-in antenna
- Easy installation and maintenance
- User Friendly interface

What s a Good Wireless LAN Solutions? - Wireless LAN Wish List

Above is a Wireless LAN wish list, beyond the technical and spectrum limitations. The deployment success of a Wireless LAN systems is limited by how low the cost can go and how fast the data rate can go. The throughput of Wireless LAN systems are currently targeted at data rates between 1Mbps to 54Mbps. Physical limitations and limited bandwidth are the two keys factors that prevent the capacity of Wireless LAN from approaching that of wired LANs. Spread spectrum is usually employed to support multiple users simultaneously. Interoperability is defined as the ability of equipment from different vendors to work together. Industry standards are developed to ensure interoperability among different Wireless LAN products. A good Wireless LAN solution must also provide good coverage for the end-users, wherever the users are throughout a building or located on campus. WLAN must have minimal susceptibility to interference, whether it is from an adjacent user or from completely different systems (e.g Bluetooth and/or microwave ovens) to ensure a robust and reliable links between the network and the users’ computer or hand-held devices.

The two main causes of interference are a simultaneous transmissions from other devices and multi-path fading. Wireless LAN, security is another issue to be given carefully consideration. Techniques such as encryption and authentication should be used to provide a robust security Wireless LAN systems. Wireless LAN solutions are typically integrated into portable device which are battery powered. This means that power consumption has to be carefully considered. Power saving modes such as sleep and awake modes are used to conserve energy and thus increase battery stand-by time. Other items on the wish list includes easy installation and maintenance, smallest practical form factor (e.g PCMCIA) and an easy-to-use user interface.
Wireless LAN Topologies

Let us now take a look at the different possible Wireless LAN topologies. The topology of a Wireless LAN system can be as simple as involving just two PCs equipped with Wireless LAN adapter cards. This type of topology is usually called a peer-to-peer network or an ad-hoc network. In most cases, a Wireless LAN topology will involved an access point, which act as an interface between the wireless network and the wired network. Installing an access point can extend the range of a peer-to-peer network, effectively doubling the range at which the devices can communicate. In an environment which requires a large coverage area, multiple access point can be installed. The ability to roam will allow users to move seamlessly among a cluster of access points without breaking connectivity. An extension point (repeater) can be used in an environment where a large coverage area is required. But repeaters should only be considered when some constraints prevents the use of an access point linked to the wired network. The function of the extension point is similar to that of an access point, but they are not tethered to the wired network as are the access point. The ideal Wireless LAN topology deployed would depend primarily on users organizational requirements and geography.
Wireless LAN Access Point and Terminal End

The Slide above show a typical IEEE802.11b Wireless LAN Access Point (AP) and a IEEE802.11b Terminal End (PCMCIA card). The terminal end is sometimes known as the network interface card.

The characteristics of the terminal end and the access point

Terminal End:
- Typically a PCMCIA card or small package with (usually) built-in antenna (over air testing)
- No test access point between the baseband and RF sections.
- All digital communications via PCMCIA connector or I/O (USB) connection.

Access Point:
- Typically a small package (4” x 6” x 2”) with built-in antenna (over air or connector based testing?).
- May have test access point between the baseband and RF sections.
- May have a digital I/O test port under the covers.
- All digital communications via LAN connections (10/100 BaseT) may move to RF in later years.
Wireless LAN Architecture

The diagram above illustrates the logical architecture of a wireless LAN. The Physical layer and the Medium Access Control layer are Wireless LAN functions. The Physical layer provides for the transmission of information bits through a communication medium by defining electrical, mechanical and procedural specifications. The Data Link layer ensures error correction and synchronization between two entities. The Data Link Layer consists of the Medium Access Control (MAC) and Logical Link Control (LLC) layer. MAC, which is part of a Data Link layer in a radio-based Wireless LAN has the function of enabling multiple appliances to share a common transmission medium via a carrier sense protocol similar to Ethernet. MAC layer enables a group of wireless computers to share the same frequency and space. The LLC layer for Wireless LAN is similar in many respects to other link layers in common use. The LLC is responsible for the transmission of a link-level Packet data Unit (PDU). Logical Link Control (LLC) specifications provides the mechanisms for addressing stations across the medium and for controlling the exchange of data between two users.
The Physical Layer of Wireless LAN can be implemented using the following technology:

- **Narrowband Radio Technology**
- **Spread Spectrum Technology**
  - Frequency-Hopping Spread Spectrum (FHSS)
  - Direct Sequence Spread Spectrum (DSSS)
- **Infrared (IR) Technology**
- **Orthogonal Frequency Division Multiplexing (OFDM)**

The slide lists the different medium technologies that can be used to transport data and is referred to as the Physical layer in Wireless LAN. The data transport via narrowband Radio Frequencies (RF) systems as well as infrared technologies can be employed. Each set of technologies have their own set of advantages and limitations. The RF technologies are suitable for applications where communications are not “line of sight” and/or must cover longer distances. RF signals can travel through walls and communicate where there is no direct path between stations. In Wireless LAN, two RF technologies are proposed; Narrowband Radio technology and Spread Spectrum technology. For Infrared technology, the communication is carried by light in the invisible part of the spectrum. Infrared technology is primarily used for very short distance communications, typically 3 to 6 feet and where there is a line of sight connection. The infrared technology has the limitation of not being able to penetrate any solid material.
Physical Layer – Spread Spectrum Technology

- Spread Spectrum was derived from military radio applications.
- Spread Spectrum uses a modulation technique that occupies more bandwidth than that needed for transmission.
- To achieve a larger bandwidth, Spread Spectrum uses a code in the transmitter that must be known by the receiver.
- The two Spread Spectrum techniques used in Wireless LAN are:
  - Direct Sequence Spread Spectrum (DSSS)
  - Frequency Hopping Spread Spectrum (FHSS)

Spread Spectrum technology was developed for military application such as secure battlefield communications and has been used for many many years. Spread Spectrum made it much more difficult to “jam” (interfere) with and greatly improved security. The Spread Spectrum signal appears to be broadband uncorrelated noise to other receivers and is much harder to intercept and demodulate. In recent years, Spread Spectrum has received wide commercial and industrial usage, especially in the 2.4GHz ISM band. Applications such as PCS phones, cordless telephones, bar code scanners, and other handheld portable appliances have used Spread Spectrum as the modulation technique.

A disadvantage of Spread Spectrum systems is they use a much larger bandwidth than the minimum necessary to send the information bits. In order to achieve a larger bandwidth, Spread Spectrum uses a code in the transmitter, independent of the data, to spread the modulation. This code must be known by the receiver to enable the message to be despread and demodulated. A receiver without the code would be unable to decode the transmitted bits, and the signal appears as broadband uncorrelated noise to the receiver. There are three Spread Spectrum techniques that are commonly used; (1) Direct Sequence Spread Spectrum, (2) Frequency Hopping Spread Spectrum and (3) Time Hopping Spread Spectrum. The first two techniques are being used in Wireless LAN.
Advantages of Spread Spectrum Technology

Why do we spread the signal?

- Overcrowded Frequency Spectrum!

Advantages of Spread Spectrum

- Low power spectral density
- Protection against multipath interference
- Interference resistant
- Better security and privacy
- Facilitates the use of Code Division Multiple Access
- Attenuates interference

You might ask with today’s overcrowded frequency spectrum, why would anyone want to spread the signal bandwidth?. Wouldn’t taking up more precious frequency spectrum be the wrong way to go. The answer to this question will be evident is you consider the advantages of Spread Spectrum techniques.

The key advantages of the Spread Spectrum techniques are its low power spectral density characteristics and its resistance to interference. The low power spectral density characteristics is the result of spreading the signal over a broader frequency-bandwidth, thus making the power density (W/Hz) much smaller. With its low power spectral density, spread spectrum signals are difficult to detect and thus it a lower probability of interception and is suitable for covert operation. To recover the spread spectrum signal, both the transmitter and receiver must use the same code, thus multipath signal, which are time offset version of the desired code will be rejected in the receiver since they do not correlate. Spread Spectrum rejects interference because cross-correlating the code signal with a narrowband signal will spread the power of the narrowband signal thereby reducing the interfering power in the information bandwidth. Spread Spectrum techniques also provides better security and privacy since the transmitted signal can only be de-spread and the data recovered if the code is known to the receiver. Spread Spectrum techniques make Code Division Multiple Access (CDMA) possible. Multiple users can transmit spread spectrum signals at the same time, the receiver is still able to distinguish between the users. Each user has a unique code that does not correlation with other codes.
Direct Sequence Spread Spectrum

- Direct sequence spread spectrum signal is generated by multiplying narrowband user data with a well-defined wideband pseudo-random sequence.

- Recovering the narrowband user data is achieved by multiplying the received signal by an identical, accurately timed pseudo-random sequence.

Direct Sequence Spread Spectrum

Direct Sequence Spread Spectrum signal is generated by multiplying the narrowband user data by a higher rate pseudo-random bit sequence signal. The user energy will be spread to occupy a bandwidth a little wider than the clock rate of the pseudo-random source (PRS). A pseudo-random sequence generator is clocked at a higher data rate (termed the chipping rate) than the users data rate.

In order for the receiver to recover the original signal, a process called de-spreading is used. Despreading is achieved by multiplying the received signal by the identical, accurately timed pseudo-random bit sequence. Despreading is a correlation process that has the effect of reversing the spreading action in the transmitter. Despreading will work properly only if the same pseudo-random sequence, which is timed aligned with the original spreading bit sequence is used in the receiver.
Direct Sequence Spread Spectrum

The slide above shows the spreading (direct multiplication) process of the user data signal by the higher chip rate code signal. When the data signal is a "1", the output of the spreader will be a replica of the PRS code signal. When the data signal is "-1", the output of the spreader will be the inverse of the PRS code signal. Therefore to recover the original user data, “1” or “-1”, the spreader output (Data Signal X Code Signal) is multiplied by the same code in the receiver. In the example above, the code chip rate is 10 times the information bit rate. This means that 10 code symbols per data symbol are transmitted, and the occupied bandwidth increases by a factor of 10 as well. In practice, the spreading factor will be much larger, usually in the order of $10^2$ to $10^3$. The despreading process also improves the signal to noise ratio on the receiver side. The term processing gain refers to the signal to noise improvement available. Processing gain is defined as the ratio between the code signal chip rate and the user information bit rate.

The despreading process is used to recover our encoded data bits. The spread sequence used in the transmitter is also used in the receiver. The received chip is multiplied by the same time aligned pseudo random sequence. The chip sequence is squared, all positive, and what remains is the original data bit sequence. Uncorrelated narrow band signals are spread out in the receiver as well as other uncorrelated Spread Spectrum signals.
DSSS wrong Despread code

A received signal transmitted with a different Barker sequence will also be uncorrelated. Noise and Interference effects will also integrate out in the auto-correlation calculation. Despreading a DSSS modulated signal and recovering the data under adverse conditions is referred to as conversion gain.

The slide above shows the spreading (direct multiplication) process of the user data signal by the higher chip rate 11 bit Barker Sequence code signal. In the example above, the code chip rate is 11 times the information bit rate. This means that 11 code symbols per data symbol are transmitted, and the occupied bandwidth increases by a factor of 11 as well. In practice, the spreading factor of 10 will prove a 10 dB improvement in Signal to Noise. Despreading improves the signal to noise ratio on the receiver side via integration of the received signal over the 11 chip Barker Sequence. Uncorrelated narrow band signals have a “0” mean and integrate to 0 in the receiver as well as other uncorrelated Spread Spectrum signals.

The term processing gain refers to the signal to noise improvement available. Processing gain is defined as the ratio between the code signal chip rate and the user information bit rate.

The 11 bit despreading process used to recover our encoded data bits 10 Log11/1 processing gain.
Direct Sequence Spread Spectrum

What happens if received codes and locally generated codes are not synchronized or uncorrelated?

When the received codes and the locally generated codes are time synchronized, product will be a positive value. A direct multiplication (de-spreading) will therefore recover the user data, which in this case is a binary “1”. In the non-synchronized case, the locally generated codes is time offset with respect to the received codes. De-spreading, multiplying, will not result in a binary “1”, but rather an ambiguous levels shown in the diagram. The output of the despreading process is integrated over the chip time interval. The output of the integration is compared to a threshold level to determine the +1 or -1 state of the users data bit. By inspection one can see the value of the integration between the 2 cases above are very different and the uncorrelated interferers will produce a similar result.
Direct Sequence Spread Spectrum

A typical block diagram of a Direct Sequence Spread Spectrum transmitter. The user's source data bits usually in the form of narrowband binary data is multiplied by a higher rate binary Pseudo Random Sequence bits. The combined bit stream is then used to modulate an RF carrier. The code signal consists of a sequence of code bits or “chips” that are either inverted or non-inverted. The chip rate of the code signal must be higher than the bit rate of the information signal in order to obtain the desired spreading bandwidth of the signal.
Direct Sequence Spread Spectrum

The transmitted Direct Sequence Spread Spectrum signal is recovered in the receiver using coherent demodulation, as shown in the slide above. The locally generated PRS code sequence is used to de-spread the spread signal. In the de-spreading process, the receiver must not only know the code sequence used to spread the user data, but the PRS codes on the received signal and the locally generated PRS code must also be time synchronized. Synchronization, also known as tracking, is required throughout the whole transmit-receiving process for correct data recovery. The Code Synchronization block shown in the block diagram above is responsible for this process. After de-spreading, the signal will be demodulated to recover back the original user data.
**Frequency Hopping Spread Spectrum**

- Carrier frequency of the modulated information signal is not constant, it changes (hops) periodically
- The hopping pattern is determined by a spreading code signal.

In Frequency Hopping Spread Spectrum technique, the signal is transmitted over a seemingly random series of frequencies, changing (hopping) from one frequency to another at fixed interval (periodically). The sequence of frequencies (channels) used is dictated by a spreading code signal. Both the transmitter and receiver must use the same frequency hopping spreading code sequence to tune and track the channels in synchronization.

The slide above also illustrates the differences between Frequency Hopping and Direct Sequence frequency usage. In a Frequency Hopping system, the transmitter is transmitting data in a narrow frequency band during the time period that the carrier dwells in the frequency band. In the Direct Sequence system the data is transmitting over the same time period but the signal power is spread over the whole frequency band. This means that power transmitted by a Direct Sequence system within the frequency band will be much lower than that of a Frequency Hopping system. However, the Direct Sequence system will transmits in that frequency band during all time periods while the Frequency Hopping system only transmits data in that frequency band during a single time period. If we compare the average, both systems will transmit at around the same power in the frequency band.
Frequency Hopping Spread Spectrum

A typical block diagram of a Frequency Hopping transmitter is shown in this slide. The source information is baseband modulated on a carrier, usually using Frequency Shift Keying (FSK) modulation technique. The code generator is used to control a fast frequency synthesizer. The frequency synthesizer is responsible for up-converting the modulated signal to the required transmission frequency. The transmission frequency is not constant, it changes/hops periodically based on the hoping rate. The frequency hopping pattern is determined by the PRS code generator.
Frequency Hopping Spread Spectrum

The de-spreading process for a Frequency Hopping spread Spectrum signal can be explained using the block diagram in this slide. The code generator block in the receiver is used to locally generated a code sequence (hopping pattern), which will control the frequency of the local oscillator synthesizer. The output of the frequency synthesizer is then used to down-convert the received signal to the baseband modulated carrier. The synchronized tracking block in the receiver ensures that the hopping of the local oscillator tracks the hopping pattern of the received carrier in order to achieve correct de-spreading of the signal.
Orthogonal Frequency Division Multiplexing (OFDM)

Is **Orthogonal Frequency Division Multiplexing (OFDM)** new?

It has been around for a while! Application using OFDM includes:

- Digital audio
- Digital video broadcasting
- ADSL
- LMDS

And now in Wireless LAN: IEEE802.11a/g and HIPERLAN2

**Orthogonal Frequency Division Multiplexing (OFDM)**

The theoretical work on OFDM was done in the 1930’s at Bell Labs. But OFDM could not become a cost effective approach until the invention of the Fast Fourier Transform in 1965 and the availability of very fast low cost Digital Signal Processors. It has become very popular because of its very high bandwidth efficiency. By its nature it provides both time and frequency diversity. There were many applications that used OFDM before it was adopted for use in Wireless LAN. These include Digital audio, digital video broadcasting, ADSL (Asynchronous Digital Subscriber Loop, high speed internet access via phone lines) and LMDS (Local Multi-point Distribution System).
What Is OFDM?

• OFDM is a multi-carrier modulation technique
• Unlike other modulation technique the carriers have substantial overlap
• Each single high-frequency carrier used, in OFDM transmits multiple high data rates signals concurrently using Sub-carriers
• The Sub-carriers are orthogonal with each other and do not interfere with each other.
• The Sub-carriers are narrow and only experience flat fading

What is OFDM?
Orthogonal Frequency Division Multiplexing (OFDM) is a multiple-carrier modulation technique. Unlike conventional frequency division modulation techniques which uses multiple high frequency carriers that do not overlap, OFDM transmit multiple high data rates signals concurrently on sub-carriers with substantial overlap. These sub-carriers are orthogonal with each other and do not interfere with each other. The sub-carriers are very closely spaced and only experience flat fading. Each sub-carrier needs only single I-Q error correction vector.
OFDM – Basic Concepts

- **Orthogonal Frequency Division Multiplexing**

- **Multi-carrier signaling format**
  - Each carrier = low rate
  - Composite signal = high rate

Orthogonal Frequency Division Multiplexing basically splits a high data rate stream into a number of lower rate data streams which are transmitted over a number of sub-carriers. The IEEE802.11a OFDM structure is summarized on the slide above. IEEE802.11a uses 52 carriers in which 48 are used for data and the remaining 4 are used as pilot. Each sub-carrier is separated by a frequency of 312.5KHz. The bandwidth for IEEE802.11a is 18MHz and the highest data rate of 54Mbps is achieved using 64QAM modulation scheme. As mentioned in the overview slide earlier, IEEE802.11a is being deployed in the 5-6GHz band.
Signal’s Spectrum Has a Sin(x)/x Shape

This drawing shows the real reason for the OFDM spectral characteristics. For a single carrier, we can model the transmitted pulse as a sinusoid multiplied by a RECT function. In the frequency domain, this is simply a sin(x)/x shape convolved with an impulse at the carrier frequency.

The sin(x)/x spectrum has nulls at adjacent carrier frequencies provided the sinusoid is on frequency. The RECT function can have the wrong width if the ADC/DAC sample rates are even a little off in either the transmitter or receiver. The phase noise, again in either the transmitter or the receiver can cause intersymbol interference.

The OFDM signal is comprised of 52 sub-carriers. The sub-carriers at the outer frequency edges are the ones that contribute the most to the sidelobe structure shown in the spectral mask plot.
OFDM: Orthogonal Carriers

In Frequency Division Multiplexing (FDM) systems, the channel spacing is typically greater than the symbol rate to avoid overlapped spectrums. In OFDM the carriers are orthogonal and overlap without interfering with one another. The idea is similar to that of Nyquist filtered SCM signals. The symbols in a single-carrier system overlap in the time domain, but don’t interfere with one another because of the symbol (T) spacing of the zero crossings. For OFDM, the carriers have spectral null at all other carrier frequencies.
Orthogonal Frequency Division Multiplexing

Orthogonal Frequency Division Multiplexing

The “O” in OFDM stands for orthogonal. In Frequency Division Multiplexing systems, the channel spacing is typically greater than the symbol rate, to avoid overlapping the spectrums. In OFDM the carriers are orthogonal and overlap without interfering with one another. The idea is similar to that of Nyquist filtered SCM (single-carrier system) signals. The symbols in a single-carrier system overlap in the time domain, but don’t interfere with one another because of the symbol (T) spacing of the zero crossings. For OFDM, the carriers have spectral null at all other carrier frequencies.

Non-linear distortion and phase noise are the two largest contributing factors to a loss of orthogonality, creating inter-carrier interference. Poor frequency estimation in the receiver is another.
Why OFDM? – Advantages of for OFDM

Advantages of OFDM:

- More robust against multipath propagation effects
- Less sensitive to timing errors
- Higher spectral efficiency
- Very high bandwidth efficiency
- Hardware implementation simplified.

Why OFDM? – Motivation for OFDM

Multi-path and corrections are greatly simplified. Timing and synchronization are more easily implemented. Very high spectral efficiency more Bits/sec/ Hz BW. Orthogonal Sub-Carriers can be very closely spaced without interfering with each other. Minimum parts count to implement the modem, RAM, DSP, IF, RF, and RF Power Amplifier. Receiver reuses most of the components, DSP, RF, and IF.
Wireless LAN Architecture

The layer that sits directly on top of the Physical Layer in the protocol stack is the Data Link Layer. The Data Link Layer provides a reliable and efficient communication protocol between each individual connected users communicating over a medium. The Data Link Layer functions include providing services to the Network layer, error correction and signal detection capability, framing of Physical Layer bits and lastly flow control within a communication medium. Flow control insures slow receivers are able to follow. There are two sub-layers within the Data Link Layer: (1) Medium Access Control (MAC) layer and (2) Logical Link Control (LLC) Layer. The roles of these two sub-layers will be explain in the next few slides.
Data Link Layer
- Medium Access Control (MAC) Layer

• MAC protocol handles regulating the usage of the medium

• The channel access mechanism is the core of the MAC protocol

• Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is the channel access mechanism used by most Wireless LANs system in the ISM bands.

Data Link Layer – Medium Access Control (MAC) Layer

Medium Access Control (MAC) protocol layer is responsible for regulating the usage of the Transmission medium via a channel access mechanism. Being a sub-layer of the Data Link protocol, MAC enable multiple appliances to share a common transmission medium. The channel access mechanism is the core of the MAC protocol. Its functions is to share out the main resource between the radio channel, nodes. The channel access mechanism allocates medium resources to each node. The channel access mechanism tells the station node when to transmit data and when to receive data. One example of a common channel access mechanism is the Time Division Multiple Access (TDMA), which is used in cellular network such as the GSM system. In Wireless LANs system, the common channel access mechanism is the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) technique. CSMA/CA is fundamentally a different approach to controlling channel access. CSMA/CA ensures that all users have to “listen” before they “talk” or “content” (wait its turn). The advantages of CSMA/CA includes it’s compatibility with network protocols such as TCP/IP. CSMA/CA is well adapted to the variable conditions of normal network data traffic and handles interference very well.
Carrier Sense Multiple Access/Collision Avoidance

CSMA/CA is derived from CSMA/CD (Carrier Sense Multiple Access/ Collision Detection), which is the core of Ethernet control. In collision detection, the transceiver is capable of listening while transmitting and therefore can prevent collisions. CSMA/CA can’t directly detect collisions like in CSMA/CD because even if a transceiver could listen on the channel while transmitting, the strength of its own transmissions would mask all other signals on the air. When using other than hardwired medium some other mechanism to prevent multiple nodes trying to use the medium at the same time is required. Collision avoidance is the technique used and its operation can be explained with the aid of the flowchart shown above.

When a user decide to send some data, it will start by listening on the medium (carrier sense), and if it is found that the medium is idle, it will send the first packet in the transmit queue. If the medium is busy, then the user will defers its transmission and continues to monitor the medium until the current transmission is complete. During the data transmission, the user will listen on the channel to see if there is any collision, if there is, then the user will wait for a random amount of time. This process is called contention. When the random delay is done (contention timer expires) and and the medium is idle, then the user will send the data packets. Basically, the user using the shortest random delay wins and transmit its packet. The other users will wait for the next contention to end at the end of the current packet transmission. This is because contention is a random number and it is done for every packets. Each user is given an equal chance to access the medium.

More details on CSMA/CA based on IEE802.11 standard will be covered later.
Carrier Sense Multiple Access/Collision Avoidance

CSMA/CA uses additional techniques to improve performance.

- **Acknowledge/Retransmission**
- **Fragmentation**
- **Request To Send/Clear To Send (RTS/CTS)**
- **Reservation and service slots**

**Carrier Sense Multiple Access/Collision Avoidance**

The MAC protocols uses additional techniques to improve the performance. These techniques include:

**Acknowledge/Retransmission**: This technique is used to detect lost or corrupted packets due to over the air transmission. Once a user node has successfully received a packet, it will send an acknowledge message to the transmitter. If after sending a packet, the transmitter does not receive an acknowledgment, the packet is assumed lost. The transmitter will then retransmit the packet after contending again for the medium. In LAN protocols, this is the LLC layer responsibility.

**Fragmentation**: The principle of fragmentation is to send a large data packet in smaller segments over the medium. When there is an error, only the corrupted segment needs to be retransmitted. If the medium is noisy, a small packet has a higher probability to get through without errors, so the user increases its chance of a successful transmission in bad conditions. The price to pay here is the increase in overhead, because it duplicates packet headers in every fragments.

**Request To Send/Clear To Send (RTS/CTS)**: RTS/CTS is a handshaking technique where a transmitter will send a RTS message and wait for a CTS message from the receiver before sending a packet. This technique minimizes the chances of a collision.

**Reservation and service slots**: The concept of this technique is to offer a period of time where users can contend. These time periods are either called the reservation slot or service slot. User nodes can use a simple Aloha protocol in the slots, that is they transmit and if the transmission fails the node will back off a random number of slots before retrying.
Data Link layer – Logical Link Control (LLC) Layer

• Control the exchange of data between two users across a LAN
• Specifies the mechanism for addressing the source and the destination
• Provides three types of services for a Network layer Protocol
  • Unacknowledged connectionless service
  • Connection-oriented service
  • Acknowledge connectionless service

Data Link Layer – Logical Link Control (LLC) Layer
The Logical Link Control (LLC) layer for LANs handles the transmission of a link-level Protocol Data Unit (PDU) between two stations across a LAN using a MAC controlled link. It provides the addressing and data link control. The LLC layer will receive user data from higher layer protocol and then appends a control header, thus creating an LLC protocol Data Unit (PDU). The LLC PDU is then handed down to the MAC layer, which appends control information at the start and end of the packet, forming a MAC frame. The LLC addressing mechanism and data link control is independent of the topology, transmission medium and medium access control technique chosen.

The LLC provides three types of services for a Network Layer protocol:

Unacknowledged connectionless service: No establishment of data link connection between stations. A datagram-style service that does not include any error-control or flow-control mechanisms. LLC PDUs are sent and received without any acknowledgement of delivery. Individual multicast and broadcast addressing are supported by this service.

Connection-oriented service: This service provides a logical connection between two stations exchanging data. Error-control and Flow-control are included in this service. It does not support multicast and broadcast modes.

Acknowledge connectionless service: Like the unacknowledged connectionless service, this service does not involve the establishment of a logical connection between stations. The difference is that acknowledge connectionless service provides acknowledgement upon successful data delivery. Error-control and Flow-control are supported by this service.
Standardization of Wireless LAN

What are the advantages of having a common standard for Wireless LAN and what are the standards that are available in Wireless LAN? These questions will be answered in this section.
Why Do We Need a Common Standard for Wireless LAN?

The Advantages of Having Common Standards

- Promote Interoperability
- Better migration path to future systems
- Speed up time-to-market
- Increase price competition

Why do we need a standard for Wireless LAN?

In the past, many organizations implement wireless networks in their premises using their own proprietary design. Proprietary wireless networks not only create interoperability issues but are also less flexible in terms of meeting future needs. Just imagine yourself not being able to access the network to get some critical data while you are at your client’s site. The slide here shows a list of advantages in developing a common standard for Wireless LAN implementation.

The key advantage of having a common standard is interoperability. Different vendor’s devices will be able to interoperate with the chosen wireless network type. Take for example, if you buy a Intel’s IEEE802.11b PCMCIA Wireless LAN card and a HP’s PDA with 802.11b feature, you can rest assured that both will be able to work within an 802.11 wireless network without any issues.

Technology is constantly evolving, a 11Mbps wireless network today will soon be replace by a much higher speed network due to the application demand. By having a common standard, it will certainly ensure better and easier migration from existing Wireless LANs system to a higher performance Wireless networking system. One example will be the migration path from the IEEE802.11b standard to the IEEE802.11g standard.

The use of standards helps to speed up product development and reduce time to market. The standard defines many of the implementation specifications so the developer does not need to start at the “beginning”. Standards shorten development time and thus speed up time-to-market.

Standard compliance promotes interoperability and thus users can purchase products from any vendors without worrying that they don’t interoperate. Standards reduce risk by minimizing dependence on a single vendor for products. Smaller companies can now develop wireless LANs products complying to a standard and you can bet that when smaller player comes into the market, price competition will certainly increase.
**Different Types of Standards in Wireless LANs:**

There are three main forums for the standardization of wireless broadband communication systems. They are (1) Institute for Electrical and Electronic Engineers (IEEE) 802.11, (2) European Telecommunication Standards Institute Broadband radio Access Networks (ETSI BRAN), and (3) Multimedia Mobile Access Communications (MMAC) in Japan. IEEE802.11 is the first Wireless LAN standard operating in the Industrial, Scientific and Medical (ISM) band. The standard specifies the MAC and Physical layer. Three options are available for the physical layer as mentioned before, the DSSS, FHSS and Infra red. IEEE802.11b uses complementary code keying modulation technique that pushes the data rate to 11Mbps. Both IEEE802.11a and IEEE802.11g targets a range of data rates from 6Mbps to 54Mbps using Orthogonal Frequency Division Multiplexing (OFDM). The different is that IEEE802.11a operates in the 5GHz Unlicensed National Information Infrastructure (U-NII) band while IEEE802.11g is in the 2GHz ISM (Industrial, Scientific and Medical) band. The reason why there is a shift of the 54Mbps Wireless LAN standard back to the 2.4GHz ISM band is largely due to the challenges face when developing Integrated circuit or modules in the 5GHz range. The ETSI standards group in Europe supports High Performance local Area Network type 1 and 2 (HIPERLAN/1 and 2). The type 1 standard is not getting much attention now as no products has yet been manufactured using this standard. Focus is being put on the HIPERLAN/2 standard, which is the ETSI version of the IEEE802.11a standard. A summary of all these standards is shown on the next slide.

How will the market shake out? The largest deployment of Wireless LAN is IEEE 802.11 and 11b. Modems using 802.11a have been on the market for more than a year.
Summary of Wireless LANs Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Modulation</th>
<th>Data rates</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE802.11</td>
<td>2-GFSK or 4-GFSK FHSS</td>
<td>1 or 2 Mbps</td>
<td>Multiple PHY including Infra red</td>
</tr>
<tr>
<td></td>
<td>BPSK or QPSK DSSS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE802.11b</td>
<td>CCK</td>
<td>5.5 or 11 Mbps</td>
<td>Corporate favorite</td>
</tr>
<tr>
<td>IEEE802.11g</td>
<td>64 OFDM + BPSK, QPSK, 16QAM, 64QAM, CCK</td>
<td>6, 9, 12, 18, 24, 36, 48, 54 Mbps</td>
<td>In development, 48 and 54 Mbps will need new RF design</td>
</tr>
<tr>
<td>IEEE802.11a</td>
<td>64 OFDM + BPSK, QPSK, 16QAM, 64QAM</td>
<td>6, 9, 12, 18, 24, 36, 48, 54 Mbps</td>
<td>ETSI TGj/IEEE working on coexistence strategies</td>
</tr>
<tr>
<td>HIPERLAN 1</td>
<td>GMSK, FSK</td>
<td>23.5 Mbps or 1.5 Mbps</td>
<td>Europe only, no product, non-existence now</td>
</tr>
<tr>
<td>HIPER LAN 2</td>
<td>64 OFDM + BPSK, QPSK, 16QAM, 64QAM</td>
<td>6, 9, 12, 18, 24, 36, 48, 54 Mbps</td>
<td>ETSI TGj/IEEE working on coexistence strategies</td>
</tr>
</tbody>
</table>

Summary of Wireless LANs Standards

A summary of the modulation techniques, the data rates and some comments associated with each Wireless LAN standard is shown in this slide.

In this course, the IEEE802.11b and 802.11a standards will be covered in greater details. One point to note for the IEEE802.11g standard modulation scheme used is dependent on the chip set selected. The standard allows using ether complementary code keying or Orthogonal Frequency Division Multiplexing. The CCK approach uses a QPSK constellation at the transmitter output. The complementary codes are a set of nearly orthogonal complex sequences.

The modulation technique used at present depends on the chip set vender, i.e. Intersil uses CCK modulation whereas Aetheros uses OFDM as the modulation scheme.
IEEE802.11 Wireless LAN Standard

We have so far discussed the Wireless LAN technology in general, covering from its topologies, physical layer as well as the MAC layer. We shall now take a step forward and understand the technology pertaining to the IEEE802.11 standard. This section will be focus on IEEE802.11 and IEEE802.11b standards. IEEE802.11a standard will be cover in the later section.
IEEE 802 LAN and MAN Standards Committee

- Formed in Feb, 1980
- Major working group to develop, maintain and promote the use of IEEE and equivalent IEC/ISO standards
- IEEE802 list of standards:
  - 802.1 (Internet)
  - 802.2 (LLC)
  - 802.3 (Ethernet)
  - 802.4 (Token Bus)
  - 802.6 (Distributed Queue Dual Bus)
  - 802.5 (Token Ring)
  - 802.9 (Isochronous Ethernet)
  - 802.11 (Wireless)

IEEE 802 Wireless LAN Standards Committee

The 802 Local and Metropolitan Area Network Standards Committee was formed in February 1980 with the objective of implementing, maintaining and promoting the use of IEEE and equivalent IEC/ISO standards for LAN and MAN applications. The committee is responsible for producing a series of standards known as IEEE802.x. These standards fall within the Physical and Data Link layer of the OSI reference model (see next slide). Some of the standards include 802.1 for internet, 802.2 for Logical Link Control, 802.3 for Ethernet, 802.4 for Token Bus, 802.5 for Token Ring, 802.6 for Distributed Queue Dual Bus, 802.9 for Isochronous Ethernet and of course 802.11 for Wireless LAN. The scope of this course focuses on the IEEE802.11 standards.
IEEE802 Protocol layers Vs OSI Model

Here is a comparison of the evergreen OSI Reference Model and the IEEE802 protocol stack. From the lowest layer, the IEEE802 protocol Physical layer corresponds to the OSI Physical layer. The Physical layer specifies the transmission medium, modulation and access technique as well as the topology. The IEEE802 protocol breaks up the Data Link layer into two sub-layers; Medium Access Control (MAC) and Logical Link Control (LLC). The functions of these two sub-layers are already being discussed in the earlier section. The LLC user addresses are referred to as LLC Service Access Point (LSAP).
IEEE802.11 WLAN verses IEEE802.3 Ethernet

Wire-line vs Wireless

✦ Both uses the same higher layer protocol (from LLC layer upwards)
✦ IEEE802.11: uses CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)
✦ IEEE802.3: uses CSMA/CD (Carrier Sense Multiple Access/Collision Detection)
✦ IEEE802.11: destination address is not equal to destination location
✦ IEEE802.3: destination address is equal to physical location
✦ IEEE802.11: wireless is more exposed to environment effects
✦ IEEE802.11: user can move from one location to another (mobility)
✦ IEEE802.11: stations are not always connected (power management)
✦ IEEE802.11: subjected to “hidden node problem”

IEEE802.11 Vs IEEE802.3

Wireless LAN serve as an extension, and/or as an alternative to the wired LAN. Let us do a side-by-side comparison between the IEEE802.11 Wireless LAN and the IEEE802.3 Ethernet Wired LAN standard.

The key common characteristic between the two standards is that both uses the same higher layer protocol implementation, i.e from LLC (Logical Link Control) layer. Although both the standards uses Carrier Sense Multiple Access technique (listen before talk) as the channel access mechanism in the MAC layer implementation, there is a difference in how collisions are prevented. Being hardwired IEEE802.3 can uses a collision detection function to prevent collision between two transmission. Where IEEE802.11 does not include a collision function, but rather it avoids the probability of collisions between transmissions by using a random back-off of time. If a station is ready to transmit some data and senses a busy medium the station waits for the set back off time. This is known as collision avoidance (CA) technique.

In IEEE802.11, the destination address is not equivalent to the physical local. The destination address in IEEE802.11 is a message destination and not a fixed location. In IEEE802.3, the destination address given is equivalent to a physical location. IEEE802.11, being wireless is more exposed to environment effects such as multipath fading, attenuation etc. The IEEE802.11 standard allows the user to move from one location to another while staying connected. Although this is a great advantage, the IEEE802.11 implementation will have a higher complexity in terms of roaming between access points and IP networks. Since many mobile wireless devices are battery operated, some form of power management is used to increase battery standby time. The devices are made to go into a “sleep” mode for a time interval defined by the access point. IEEE802.11 devices have, additional issues not present in a wired LAN systems. One key problem is the “hidden node problem” where a source station transmits data to a destination station without knowing that there is another “hidden” station transmitting data to the same destination station. Medium Access Control in all stations “listens” for other stations transmissions and a “hidden station’s signal” is not detectable. This causes an unnecessary collision to occur. IEEE802.11 uses Request To Send/Clear To Send (RTS/CTS) technique to mitigate the “hidden node problem”.

© Agilent Technologies, Inc. 2004
Wireless LAN Network

Before we discuss the details on each of the topology in the IEEE802.11 Wireless LAN architecture, an overview of the architecture will be of benefit. The Extended Service Set (ESS) is made up of a series of Basic Service Sets (BSS) connected together by means of a Distribution System (DS). Each BSS in its simplest form consists of two or more Stations (STA) being link up be an Access Point (AP). The main function of an Access Point is to form an interface between the wireless and wired LAN. All communications between Stations or between a Station and a wired network client will go through the Access Point. There is another type of topology where the Stations communicate directly with each other without going through an Access Point. This type of topology is termed the Independent Basic Service Set (IBSS).
IEEE802.11 Architecture Terminology

• **Station**: Any device that contains a MAC and Physical Layer that conforms to IEEE802.11 standards

• **Access Point**: Any entity that has station functionality and act as a bridge that connects a wireless client device to the wired network

In IEEE802.11, any device that contains a MAC and Physical layer conforming to its standard is termed a Station (STA). The bridge between any wireless client device and the wired network is called the Access Point. An Access Point has station functionality but is not mobile. It forms part of the wired network infrastructure. Access Point is analogous to a basestation used in a cellular phone network. There are two types of Access Points: (1) Dedicated Hardware Access Point (HAP) and (2) Software Access Points which runs on a computer equipped with a wireless network interface card.
Wireless LAN Topologies – Basic Service Set (BSS)

The simplest form of topology in a Wireless LAN network is the Basic Service Set (BSS). A BSS is simply a collection of stations that communicate with one another. There can be two types of BSS within a Wireless LAN network. The first type is known as the Infrastructure BSS (If-BSS) where an access point (AP) is used to facilitate the exchange of data within the BSS. The second type is simply a topology that involves stations communication with one another directly without an AP. This is known as the Independent BSS (Id-BSS) topology.
**Wireless LAN Topologies – Infrastructure Basic Service Set (If-BSS)**

If-BSS is made up of two or more Stations establishing communication using an Access Point as the bridge to the wired network.

**Wireless LAN Topologies - Basic Service Set (BSS)**

An Infrastructure Basic Service Set (If-BSS) contains an Access Point (AP) and a set of arbitrary stations. The function of the Access Point (AP) is to provide a bridge between the wireless LAN and the wired LAN. One of main advantage of having an AP in the BSS is that it allows contention-free modes of operation. An AP being better equipped than a station will be capable of buffering data for various stations within an If-BSS and then deliver the data to the correct station at a convenient time. With this technique, the stations can actually operate in some form of power saving mode (sleep mode). The stations can “fall asleep” for most of the time and then “wake up” to receive buffered data every once in a while. The benefit of this scheme is that battery life can be prolong.
**Wireless LAN Topologies – Independent Basic Service Set (Id-BSS) Network**

An Independent Basic Service Set (Id-BSS) network, or what is commonly known as an ad-hoc network or peer-to-peer network consists of a number of stations (computers) each equipped with a wireless LAN interface card. Each station can communicate directly with all of the other wireless enabled computers. No access point or relay function is required in an ad-hoc network. The set-up for an ad-hoc network is simple and is formed only on a temporary basis. One example where a Id-BSS network can be used is during a business meeting in a conference room, where a group of employees, each with a laptop or a palmtop can be connected to one another to share information and resources. Although, this may be the most straightforward way of connecting between two friendly stations, interoperability between stations and devices due to different vendors designs may be a limitation to this topology.
Ad-Hoc Vs Infrastructure Networking Modes

Basically, the IEEE802.11 define two networking modes; (1) Ad-Hoc Networking mode and (2) Infrastructure Networking mode. The diagrams above show the architecture between the two networking modes.

The Ad–Hoc Networking mode (described in previous slide) is used for peer-to-peer mutual communication between stations without an access point. It does not support access to wired networks.

Networking mode that involves communication between stations through an access point (BSS or ESS) is refer to as an Infrastructure Networking mode. Infrastructure Networking mode allows access to the wired networks via an access point. Direct communication between two stations are not allowed in an Infrastructure Networking mode.
**Wireless LAN Topologies - Distributed System (DS)**

The distributed system basically forms the backbone of the Wireless LAN system. It can be implemented either using wired or wireless connection but typically, the distribution system is an Ethernet wired network. The distribution system is used to interconnect a set of Basic Service Sets (BSSs) so as to create an Extended Service Set (ESS). The IEEE802.11 standard does not provide the definition for the implementation of the distribution system. This means that the system designer has the freedom to decide what distribution system is to be used if multiple access points are necessary to extend the range of the complete wireless LAN system.
Wireless LAN Topologies - Extended Service Set (ESS)

Why ESS?
To extend the coverage of an independent BSS

What is ESS?
Made up of more than one BSS network

Wireless LAN Topologies - Extended Service Set (ESS)
In order to extend the range of coverage of an independent BSS, the IEEE802.11 defines an Extended Service Set (ESS) LAN, as shown in the slide above. The ESS is made up more than one BSS network which will satisfy the requirements of large coverage networks of arbitrary size and complexity. The ESS will appear as a single BSS to the LLC layer at any station associated with any one of the BSSs.
The IEEE802.11 Medium Access Control (MAC) Layer provides many services and features to help make the data transmission more reliable. We shall now take a look at the architecture and operation of the Medium Access Control (MAC) Layer.
IEEE802.11 MAC Architecture

The **Distributed Coordination Function** is a mandatory function of the MAC architecture. DCF is the primary access protocol for automatic sharing of the wireless medium among stations and access points. IEEE 802.11 uses a carrier-sense multiple access / collision avoidance protocol to share the medium. DCF uses a variable delay to hold off stations to avoid having stations transmissions colliding. If the channel is under heavy use the wait interval can be very long. Another optional priority based coordination function is provided to handle time critical data transfers.

The optional priority based **Point Coordination Function** provides for contention free data frame transmissions of time critical data. The **Request To Send/Clear To Send Medium Access Control** can be turned off to increase channel capacity under higher traffic loads. The optional Point Coordination Function reduces channel overhead. But there is a higher risk of collisions from hidden stations with this protocol.
Distributed Coordination Function (DCF)

*Fundamental Access Method (Mandatory!)
*Directly on top of the Physical layer
*Based on Carrier Sense Medium Access/collision Avoidance
*Supports contention services
*Operates solely in the ad hoc network
*Operates either solely or coexists with Point Coordinate Function in an infrastructure network

Distributed Coordination Function (DCF)
The Distributed Coordination Function (DCF) is the fundamental access method used to support asynchronous data transfer on a best effort basis. It is a mandatory coordination function scheme that sits directly on top of the physical layer. DCF uses the Carrier-Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol for sharing the wireless medium. (More of CSMA/CA will be explained later.) By using the CSMA/CA, the DCF supports contention services, meaning that each station with an MAC Service Data Unit (MSDU) queued for transmission must contend for access to the channel. Once it is transmitted, the same station must re-contend for access to the channel for all its subsequent frames. This scheme promotes fair access to the channels for all stations. In an ad-hoc network (If-BSS), DCF operates solely since it does not have an AP to provide PCF scheme whereas in an infrastructure network, DCF can either operates solely or it can coexists with the optional PCF for more time-critical application.
Hidden Node Problem in Wireless LAN

Consider 3 stations STA 1, STA 2 and STA 3

- STA 1 and STA2 can communicate
- STA 3 can communicate with STA 2, but not STA 1 because of (a) obstacles or (b) signal attenuation
- While STA 1 is transmitting to STA 2, STA 3 can incorrectly sense that the channel is idle
- STA 3 will interfere at STA 2 and wipe out the packet from STA 1 if it starts transmitting

Hidden Node Problem in Wireless LAN

There is a likely scenario in a DCF mode Wireless LAN system where two stations start transmitting to the same designated station because one of the transmitting station is totally unaware that the other station has used up the channel. This problem is commonly called the “hidden node problem”. The slide above illustrates a simple example of a hidden node problem.

Let us consider 3 stations (STA 1, STA 2 and STA 3) within a BSS. STA 1 and STA2 can communicate with one another without any issue but STA 3 can only communicate with STA2 but not STA 1. This can be due to some obstacles in-between STA 1 and STA 3 or it can be due to large path loss between them that causes drastic signal attenuation. Because of the fact that STA 3 cannot “hear’ STA 1, there is a likely chance that STA 3 will not be aware of any transmission that is going on between STA 1 and STA 2. STA 3 can incorrectly sense that the channel is idle and thus start its own transmission of data to STA 2. This will cause interference at STA 2 and may even wipe out the packet transmitted from STA 1.
How to solve hidden node problem?

Using Request To Send (RTS) & Clear To Send (CTS)

**RTS:** Source will announce its transmission and this will cause the source’s neighborhood to stop all transmission.

**CTS:** Destination receives the RTS and gives permission to the source to send the data. This will cause the destination’s neighborhood to stop all transmission.

IEEE802.11b defines an optional DCF protocol using RTS-CTS control frames to solve the hidden node problem.

How to solve hidden node problem?

The hidden node problem described in the previous slide can be solve by using a form of handshaking technique. This technique uses the Request-to-Send (RTS) and Clear-to-Send (CTS) signal. The RTS signal is used by the source station to announce its transmission. All the other stations within the coverage area of the source station will detect this signal and thus be informed to stop all transmission. The destination station upon receiving the RTS signal will then give permission to the source station to start sending the data by sending the CTS signal. Similarly, all other stations within the destination station’s coverage area will detect the CTS signal and thus stop all their transmission to prevent collision.

IEEE802.11b defines an optional DCF protocol using RTS and CTS control frames to solve the hidden node problem.
Example: How RTS-CTS works to solve hidden node problem

1. Ready STA 1 sends an RTS to STA 2
2. STA 3 that is close to STA 1 detects an RTS and remains silent for the upcoming STA 1’s data transmission.
3. When STA 2 receives the RTS, it sends back an CTS
4. STA 4 that is close to STA 2 detects the CTS and will remain silent for the upcoming STA 1’s data transmission

Example: How RTS-CTS works to solve hidden node problem

Here is an example to further illustrate how the Ready-to-Send (RTS) / Clear-to-Send (CTS) control frames can help to solve hidden node problem.

Station 1 (STA 1) is ready to send some data to Station 2 (STA 2). It sends a RTS signal to STA 2 to request for this operation. Station 3 (STA 3) that is within the coverage area of STA 1 will detect the RTS signal as well and thus it will remain silent for the upcoming STA 1’s data transmission. When STA 2 receives the RTS signal from STA 1, it gives permission to STA 1 by sending the CTS control frame. This also has an effect of preventing stations that is close to STA 2 from transmitting unnecessarily. In this case, STA 4 that is close to STA 2 will remain silent for the upcoming STA 1’s data transmission because the CTS control frame has indicated that there is already a transmission going on (channel is busy).
## RTS and CTS Controls Frame Format

### RTS Frame (20 octets)

<table>
<thead>
<tr>
<th>Octets:</th>
<th>2</th>
<th>2</th>
<th>6</th>
<th>6</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Frame control</td>
<td>Duration ID</td>
<td>Dest. Address</td>
<td>Source Address</td>
<td>CRC</td>
</tr>
</tbody>
</table>

### CTS Frame (14 octets)

<table>
<thead>
<tr>
<th>Octets:</th>
<th>2</th>
<th>2</th>
<th>6</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Frame control</td>
<td>Duration ID</td>
<td>Dest. Address</td>
<td>CRC</td>
</tr>
</tbody>
</table>

### RTS and CTS Control Frames Format

The RTS duration ID part asks for a time slot in Microsec needed by the sending station to send the data frame, plus CTS frame, 1 ACK frame, and 3 Short Interframe Space intervals (SIFS). The station will process the request and generate a Network Allocation Vector and schedule a CTS (Clear To Send). When the station receives a CTS with its address it will set up to send the number of data frames specified by the CTS Duration ID.
Distributed Coordination Function (DCF) with handshaking procedure (RTS/CTS)

- Uses RTS and CTS control frames to solve hidden node problem in wireless LAN system
- All other neighboring stations within the radio range will only attempt a transmit after a given time
- The given time is termed the Network Allocation Vector (NAV)
- NAV is the amount of time that must elapse before the current transmission session is complete.
- Only after NAV has elapsed can the channel be sampled again for idle status.

**Infrastructure Networking Mode**

Station A  
Station B  
AP

Distributed Coordination Function (DCF) with handshaking procedure (RTS/CTS) handles the hidden station collision problem with time slot allocations. Let us look at an example case. Assume stations A and B can communicate with the AP but not with each other. So an RTS sent by station A is not detected by station B but is detected by the AP. The AP sends a CTS that both stations A and B detect. Station B will wait the time specified in the CTS Duration ID before attempting a medium access and Station A will send the data frame. The Duration ID Field in the RTS frame generates a Network Allocation Vector and the CTS Duration ID field is set to a time length in Microsec that is slightly longer to allow for the frame, 1 CTS, 1 ACK frame plus 3 short interframe space intervals. Only the station addressed will send and all others are quiet during this wait time.
Point Coordination Function (PCF)

• PCF is an optional capability, & must coexist with Distributed Coordination Function
• Provides contention-oriented and contention-free packet transfer
• Uses a Point Coordinator (PC) to perform polling.
• The Access Point acts as a Point Coordinator
• Stations that are capable of operating in the contention-free period (CFP) are known as CF-Pollable stations
• The main applications is on time-bounded services (such as voice, video)
IEEE802.11b Contention-Free Polling Technique

• Access Point (AP) maintains a polling list (CF-Poll list) within the Basic Service Set (BSS)

• CF-Poll list all the Contention-Free Pollable stations.

• During polling, AP issues CF-Poll frames during the Contention Free Period (CFP) in ascending order of Association ID (AID) value within the CF-Poll list

IEEE802.11b Contention-Free Polling Technique

Contention-Free Polling is part of the Point Control Function for optional priority based contention free transfer of time critical frames such as voice and/or video. In contention-free polling technique, the Access Point (AP) maintains a polling list (CF-Poll list) within the Basic Service Set (BSS). The CF-Poll list is a logical construct that contains all the contention-free pollable stations and the list is invisible to all but the Medium Access Control (MAC) in the Access Point. The Access Point (AP) issues CF-Poll frames during the Contention Free Period (CFP) in ascending order of Association ID (AID) value within the CF-Poll list. Stations have to indicate their CF-Pollability within the Capability Information field of their Association and Re-association (see slide 114-115) Request frames while joining a Basic Service Set (BSS). If the station’s CF-Pollability status change, then it must perform a re-association and indicate its status change. In IEEE802.11, the Access Point (AP) always considers piggybacking CF-Poll frames along with the data frames as well as the acknowledgment frames sent so as to improve its efficiency.
**Contention-Free Polling Timing Structure**

Transmission Timing is made up of a Contention-Free Period (CFP) and a Contention Period (CP)

- CFP always start with a beacon frame from the AP that helps to provide synchronization and timing
- During CFP, only the station that is polled by the AP can send data

**Timing Structure of a CFP when it is overlaid with a pure DCF system**

In IEEE802.11, the transmission timing is divided into a Contention-Free Period (CFP) and a Contention Period (CP). The CFP always start with a beacon frame sent by the Access Point (AP). The beacon frame is used to provide synchronization and timing between the Access Point (AP) and the stations (more on beacon frames on slide 106). During the CFP, only the station that is being polled by the Access Point (AP) will be allowed to send data. The length of the CFP and CP is not fixed, they can be adjusted by the Access Point (AP) according to the traffic demand. During the CFP, the value of the Duration ID field (see slide 94 on frame format) is set to 32,768 (meaning bit 15 is “1” and all other bits are “0”) in all the frames transmitted. This is to allow a station that did not receive the beginning of the CFP to be aware that a CFP is ongoing and to prevent it from interfering.
IEEE802.11 Medium Access Control Framing

- IEEE802.11 defines & supports 3 types of frames

- **Management Frame**: Used for timing and synchronization
  Used for association/disassociation with the Access Point (AP)
  Used for authentication/de-authentication

- **Control Frame**: Used for channel reservation
  Used for acknowledgement of data reception

- **Data Frame**: Used for data information transmission

---

IEEE802.11b MAC Framing

The IEEE802.11b defines and supports 3 types of frames:

**Management Frame** is used to help established initial communications between stations and access points. It provides services such as timing and synchronization, association and disassociation as well as authentication and de-authentication.

**Control Frame** is used to provide a more reliable data frames delivery. Control frames in IEEE802.11 includes Request-to-Send (RTS), Clear-to-Send (CTS), Acknowledgement (ACK), Power-Save Poll (PS Poll) and contention-Free End (CF End). These frames are essential in channel reservation mode that is typically use to prevent collision.

**Data Frame** is basically used for data information (e.g. MAC Services Data Units, MSDUs) transmission. Data frames can also carry specific information, supervisory frames, or unnumbered frames from the LLC layer.
IEEE802.11 Medium Access Control Frame Format

Management Frame Format

Octets: 2 2 6 6 6 2 0-2312 4

<table>
<thead>
<tr>
<th>Frame control</th>
<th>Duration ID</th>
<th>Dest. Address</th>
<th>Source Address</th>
<th>BSSID Address</th>
<th>Sequence Control</th>
<th>Frame Body</th>
<th>CRC</th>
</tr>
</thead>
</table>

Control Frame Format

Octets: 2 2 6 4

<table>
<thead>
<tr>
<th>Frame control</th>
<th>Duration ID</th>
<th>Dest. Address</th>
<th>CRC</th>
</tr>
</thead>
</table>

Data Frame Format

Octets: 2 2 6 6 6 2 6 0-2312 4

<table>
<thead>
<tr>
<th>Frame control</th>
<th>Duration ID</th>
<th>Dest. Address</th>
<th>Source Address</th>
<th>BSSID Address</th>
<th>Sequence Control</th>
<th>Tx/Rx Address</th>
<th>Frame Body</th>
<th>CRC</th>
</tr>
</thead>
</table>

IEEE802.11b Medium Access Control Frame Format: The slide above shows the frame format for the management, control and data frames. Each MAC frame, whether it is management, control, data type, is made up of specific bit fields, along with a header and trailer.

Frame Control: Frame Control is a 16-bit (2 Octets) field that carries the information that the MAC layer needs to interpret all of the subsequent fields of the MAC header. The sub-fields are the Protocol version, Frame Type and Subtype, To Distributed System, From Distributed System, More fragments, Retry, Power management, More data, Wired Equivalent Privacy (WEP), and Order.

Duration ID: Duration ID is also a 16-bit (2 Octets) field that alternately carries duration information for NAV computation or a short ID, called Association ID (AID). AID is used by a mobile station to retrieve frames that are buffered for it at the Access Point (AP).

Address: There are 4 types of address fields in the MAC frame format:

Dest. Address - Address of the final destination to which the frame is sent. Either an individual or group address.

Source Address - Address of the MAC that originated the frame. This is always an individual address.

BSSID Address - The Basic Service Set Identifier (BSSID) provides a unique address for a particular BSS in the network. In an If-BSS, the BSSID provides the address of the Access Point. In an Id-BSS, the address is for the station that starts the BSS.

Tx/Rx Address - The Transmitter (Tx) address is the address of the MAC that transmitted the frame onto the wireless medium. The Receiver (Rx) address is the address of the MAC to which the frame is sent over the wireless medium. Rx address can be either an individual or group address.

Sequence Control - Contains 2 sub-fields: fragment number and a 12-bit sequence number. Used to help the receiver eliminate duplicated received frames.

Frame Body - Carries the information specific to the particular data or management frames. When a MAC frame body is carrying payload for a data frame, the frame is called a MAC Service Data Unit (MSDU). If the payload is for a management frame then it is called a MAC Management Protocol Data Unit (MMPDU).

CRC - Contains the Cyclic Redundancy Check result. CCITT CRC-32 polynomial is used on the MAC header and frame body.
IEEE802.11 Access Timing Interval

The standard interval spacing defined by IEEE802.11 is termed Interframe Space (IFS):

- Short IFS (SIFS) – Shortest IFS, providing highest priority access
- PCF IFS (PIFS) – Interval used during PCF operation
- DCF IFS (DIFS) – Interval used during DCF operation, lower priority than PIFS
- Extended IFS (EIFS) – Used by DCF-based stations as a waiting period when a reception error occurs

IEEE802.11b Access Timing Interval

The IEEE802.11 specification defines a standard interval spacing that will determine the amount of delay that a station can access the medium as well as provide various levels of priority. This standard is termed the Interframe Space (IFS). There are basically four types of Interframe Spaces (IFS):

**Short IFS (SIFS):** This is the shortest of the interframe spaces. It provides the highest priority level so that some frames can access the medium before others via a smaller delay interval. Example of frames that uses SIFS are RTS, CTS and ACK.

**PCF IFS (PIFS):** This is the interframe space used by stations that is operating under the Point Coordination Function (PCF). PIFS provides a higher priority over frames sent by the Distributed Coordination Function (DCF). Stations can therefore transmit contention-free traffic if they sense the medium is idle.

**DCF IFS (DIFS):** This is used by all stations operating under Distributed Coordination Function (DCF). This spacing interval is used during the transmission of data frames and management frames and it makes the transmission of these frames lower priority than the PCF transmissions.

**Extended IFS (EIFS):** This is used by DCF-based stations as a waiting period when a reception error (incorrect CRC) occurs. This interval provides sufficient time for the receiving station to send an ACK frame.
### IEEE802.11 Access Timing Interval (cont’)

<table>
<thead>
<tr>
<th>Time Interval Type</th>
<th>IEEE802.11b</th>
<th>IEEE802.11a</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLOT</td>
<td>20us</td>
<td>9us</td>
</tr>
<tr>
<td>SIFS (Short Interframe Space)</td>
<td>10us</td>
<td>16us</td>
</tr>
<tr>
<td>PIFS = SIFS + SLOT</td>
<td>30us</td>
<td>25us</td>
</tr>
<tr>
<td>DIFS = SIFS + 2 SLOTS (DCF Interframe Space)</td>
<td>50us</td>
<td>34us</td>
</tr>
<tr>
<td>Contention Window Min</td>
<td>32 SLOTS</td>
<td>15 SLOTS</td>
</tr>
<tr>
<td>EIFS (Extended Interframe Space)</td>
<td>Variable</td>
<td>Variable</td>
</tr>
</tbody>
</table>

**IEEE802.11b Access Timing Interval (con’t)**

The table on this slide shows the timing standard for IEEE802.11b. The standard defines one slot as 20usec and SIFS as 10usec. PIFS is simply the addition of one SIFS to one slot (10usec + 20usec = 30usec). DIFS is longer than PIFS by a slot, i.e., a timing of 50usec. Contention Window (CW) defines the timing window where stations can contend for the channel. Contention Window timing will determine the back-off time during the contention period.
IEEE802.11 Access Priority

- Different Interframe Space provides various levels of access priority in IEEE802.11

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>Time Interval</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short IFS: ACK, RTS, CTS, second or subsequent MAC Service Data Units of a fragment bursts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PIFS: Time bounced data packet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIFS: Time insensitive data packet</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IEEE802.11b Access Priority

The different Interframe Space (IFS) provides various levels of access priority. The slide here shows a comparison of the different IFS in terms of priority level and time interval. SIFS, having the shortest time interval will provide the highest level of priority. Control frames such as ACK, RTS, CTS will use the SIFS and all second or subsequent MAC Service data Units (MSDUs) of a fragment bursts will also use the SIFS for transmissions. PIFS having a higher access priority level than the DIFS will be useful in time bounded application where DIFS is used in application where time is not a critical issue.
IEEE802.11 Carrier Sense Multiple Access/Collision Avoidance

Let us now discuss how the IEEE802.11 channel access mechanism works together with the Interframe Space (IFS). Before any data transmission can occur, the source station must first sense that the channel is idle for a period longer than DIFS. Once the channel is sensed to be idle for longer than DIFS time unit, it will then start transmitting the data packets. Upon successfully receiving the data packets, the destination station will respond with an ACK frame after SIFS time unit. All other neighboring stations detecting the data will then adjust the NAV (Data + SIFS + ACK) based on the information in the duration ID field. These stations will defer its transmission for the time period of NAV plus DIFS (assuming in a DCF-based operation). After deferring its transmission for a time period of NAV plus DIFS, these stations will go into the contention window period where different stations will have different back-off period to prevent collision during contention.
IEEE802.11 Collision Avoidance Scheme

IEEE802.11b Collision Avoidance Scheme uses a backoff mechanism:

- Stations that have data ready for transmission will compute a random backoff time after the end of the defer access (NAV + DIFS)
- The station decrements its backoff timer during periods where the channel is sensed idle, and freezes its timer when the channel is sensed busy
- The station will transmit the data packet when the backoff timer reaches a value of zero

**The probability of collisions between data packets are minimized because it is very unlikely that two stations uses the same backoff time.**

IEEE802.11b Collision Avoidance Scheme

From the previous slide, we know that the stations will go through a certain backoff time after the end of the defer access (NAV + DIFS). The backoff time is computed based on the Contention Window Minimum value in the specification (more on backoff time on slide 104). The station will decrements its backoff timer during period where the channel is sensed idle. When the channel is sensed busy, the station will freeze its backoff timer. When the backoff timer reaches zero, the station will start to transmit the data packets. This technique is termed the Collision Avoidance scheme. The reason why it can help to avoid collision is because it is very unlikely that the two stations will use the same backoff time, therefore the probability of collision between data packets is very low.
IEEE802.11 CSMA/CA Flowchart

The flow-chart above summarizes the Carrier Sense Multiple Access with Collision Avoidance scheme (CSMA/CA).
Backoff Time Selection in IEEE802.11

0 time slots < Backoff Time < CW-1 time slots

Where CW is termed the contention window

- CW is set to the minimum value (CW_min) for the first transmission
- To reduce the probability of collision, the value of CW is doubled after each unsuccessful transmission attempt. This is repeated until the maximum CW (CW_max) is reached
- IEEE802.11b specifies CW_min to be 32 and CW_max to be 256

Backoff Time Selection in IEEE802.11b

Let us now take a look on how IEEE802.11 defines the backoff time. The backoff time is uniformly chosen to be between 0 to CW-1 time slots, where CW is the contention window. For the first transmission, CW is set to the minimum value (CW_min = 32), meaning that stations can have any value of backoff between 0 to 31 (32 –1 = 31). The backoff procedure is dictated by a binary exponential backoff algorithm, where for each unsuccessful transmission attempt, the value of CW is doubled. This process will be repeated until the maximum CW (CW_max) is reached. IEEE802.11b specifies the CW_min to be 32 and the value of CW_max to be 256.
IEEE802.11b CSMA/CA – Channel Reservation

Issue:

• When a collision occurs, the source CANNOT detect its own transmission or other stations
• Channel continues to transmit its entire data packet.
• If the packet is large, a lot of channel capacity will be wasted (low efficiency)

Solution:

• Use RTS and CTS to reserve the channel before transmitting a large packet
• This technique is know as Channel Reservation

IEEE802.11b CSMA/CA – Channel Reservation

Not mentioned in earlier discussions on Ready-to-Send/Clear-to-Send (RTS/CTS) control frames is that a station can help to improve the efficiency of the Wireless LAN system. The use of the RTS/CTS to reserve the channel before transmitting a large packet is called the channel reservation technique. Channel Reservation scheme helps to prevent wasting channel capacity when a collision occurs. This is because during a collision, the source station cannot detect its own or another stations transmission and thus continues to transmit its entire data packet. If the data packet is large, a lot of channel capacity will be wasted, resulting in poor efficiency. To improve the channel efficiency, the Request-to-Send (RTS) and Clear-to-Send (CTS) is used to reserve the channel before transmitting a large packet.
How Channel Reservation Works?

When we discuss how the different Interframe Space (IFS) is used in the CSMA/CA channel access technique earlier, there is no mention on the use of RTS and CTS to improve channel efficiency. Here is a diagram that shows how channel reservation works. All stations receive the RTS and generates a Network Allocation Vector from the Duration ID field. All stations except the receiver are waiting or Deferring Access for the time set in their NAV (Data + 3 SIFS + CTS + ACK). The NAV value must decrements down to 0 before it can access the medium. To minimize the possibility of all stations trying to access the medium at the same time, and colliding a random back off period is set in all stations.
Recapped of MAC Layer Operation

Before we proceed to look at the MAC layer services defined in IEEE802.11, let us recapped what we have discuss so far on the MAC layer operation. The IEE802.11 standard defines three coordination functions, one is mandatory and the other two are optional. The Coordination functions basically help to avoid collision between between stations. The mandatory coordination function is termed Distributed Coordination Function (DCF). This is based on Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA). DCF provides contention function (stations must content for the use of the channel). This gives fair access to all the stations within the Basic Service Set (BSS). The other two optional coordination functions are DCF with handshaking and Point Coordination Function (PCF). DCF with handshaking uses Request-to-send (RTS) and Clear-to-Send (CTS) to help solve hidden node problem in Wireless LAN. If the developer wants to provide contention-free operation to support services which are time-critical, then they must implement Point Coordination Function. IEEE802.11 defines several access interval timing called Interframe Space (IFS) to provide delay in-between transmitted frames. Depending on the type of IFS (e.g SIFS, DIFS, PIFS) used, different stations will have different levels of priority for accessing the channel. With the combination of CSMA/CA, IFS and RTS/CTS, the MAC layer will provide a more reliable communication between stations in the network.
IEEE802.11 MAC Layer Services

- Synchronization
- Authentication
- Security and Privacy
- Association/Re-association
- Data Transfer
- Power Management

IEEE802.11b MAC Layer Services

All Access Points and stations in 802.11 wireless LAN implement the MAC layer Services. These services support peer to peer Logical Link Control (LLC) entities to exchange MAC service data units (MSDU’s) between MAC service Access points (SAP’s). The MSDU’s carry the LLC-based frames that facilitate functions of the Logical Link Control (LLC) layer. MAC services are the overall mechanism by which the medium is shared via the MSDU’s. The Services include:

Synchronization
Authentication
Security and Privacy
Association/Re-association
Data Transfer
Power Management
How IEEE802.11 stations joins a Network?

• Once a station is turned on, it performs a Scanning process to see if there is any station (Id-BSS) or an AP (If-BSS) to join.

• Two types of Scanning processes:
  • Passive Scanning
  • Active Scanning

• After a successful scan, the station is ready to join in the network – requires the station’s MAC and Physical parameters to be synchronized with the desired network

How IEEE802.11 stations join in a network?

For a IEEE802.11 station to join in a network, it must first find either stations within an Id-BSS or an Access Point (AP) within an If-BSS. Scanning is the process where the station try to find another station or an Access Point. There are two types of scanning processes. The first type is know as Passive Scanning. In passive scanning, the stations only listen for IEEE802.11 traffic and will not transmit. The station under passive scanning will move to a channel and then listen for beacon and probe response frames. This process is repeated by the station scanning different channels until it finds lock with a Basic Service Set. The advantage of passive scanning is that it helps to conserve power but it tends to be slower compare to active scanning. Active scanning, the faster of the two technique requires the station to transmit and obtain responses from other IEEE802.11 stations and Access points. The scanning station will move to a channel and then transmit a probe request frame. If there is a BSS on the channel that matches the Service Set Identifier (SSID) in the probe request frame then the station (if in an Id-BSS) or the Access point (if in an If-BSS) that sent the latest beacon frame within that particular BSS will responds by sending a probe response frame to the scanning station.

After a successful scan is achieved, the station is now ready to join in the network. This requires the station’s MAC and Physical parameters to be synchronized with the desired network. Let us now take a look at how synchronization can be achieve in the Wireless LAN network.
MAC Layer Services - Synchronization

• Stations within the BSS must achieve synchronization with the AP for reliable communications.

• Beacon frames sent out periodically by the AP provides synchronization.

• For independent BSS case, the beacon frame is sent by the station that starts the BSS.

• The beacon frames contain information about the Physical Layer being used and the AP’s clock value. Stations will use the information to update and lock its clock to the AP or Starting Station in a BSS.

MAC Layer Services – Synchronization

For a reliable communication, all the stations within a Basic Service Set (BSS) must have their clock synchronized, meaning that the stations’ clocks must be running in step. In IEEE802.11, synchronization is accomplished by using the beacon frame. Beacon frame is being periodically sent out by the Access Point in an If-BSS or by the station that starts the BSS in an Id-BSS. The beacon frames contain information about the Physical Layer and the Access Point’s clock value. To enable all the stations’ clock to work in unison, a Timer Synchronization Function (TSF) is used to provide a common time base. The Timer Synchronization Function (TSF) maintains a 64-bit timer running at 1MHz. This is periodically updated by the information from the beacon frame. In power management sleep mode (see slide 120 on Power Management), stations need to get synchronized so that they will know when to wake up to receive beacon frames.
Relationship Between Station State and Services

Wireless LAN is an open Broadcast medium so some form of authentication is needed to provide appropriate levels of security. The 802.11 standard describes 2 types of authentication: default is Open System Authentication and optionally Shared Authentication.

A station that enters a BSS requests authentication and have it granted before it can be associated with BSS.

The slide above shows the relationship between the station state and services. What type of IEEE802.11 frames is being send will depend on what is the state existing between a source and a destination. Class 1 frames include control frame such as RTS, CTS, ACK, Contention-free (CF) frames, management frames such as beacon, probe request, authentication, Announcement Traffic Indication Message (ATIM) and data frames. Class 2 frames include management frames such as Association request, Reassociation request and Disassociation frames. Class 3 frames include data frames, management frames, deauthentication, control frames and power-save poll frames.
MAC Layer Services - Authentication

- Authentication is a process for proving client’s identity.
- Prevents unauthorized Wireless LAN users from joining the network.
- Takes place prior to a client station associating with an AP.
- IEEE802.11 defined two types of Authentication process:
  - Open System Authentication
  - Shared Key Authentication

MAC Layer Services – Authentication

Once a station has achieved a successful scan and synchronization, it can then proceed with the authentication and association process to complete its connection to the network. Authentication is a process of providing client’s identity. This is required to prevent unauthorized Wireless LAN users from joining the network. Authentication takes place prior to a client station associating (see slide 114 for Association) with an AP. There are two types of authentication algorithms defined in IEEE802.11 standard. The first type of algorithm is the Open System Authentication. In the Open System Authentication, there is actually no verification of the identity of the stations. More discussion on the Open System Authentication on the next slide. The second type of authentication algorithm is the Shared Key Authentication. This is implemented using a shared Wired-Equivalent Privacy (WEP) Key (more of Shared Key Authentication on slide 110).
Authentication – Open System Authentication

- No verification of the identity of stations! (not really an authentication algorithm)

- The process is as follow:
  - Requesting Station will assert its identity to the receiving station
  - Receiving station will respond with a successful result for the authentication

- Used by BSS that do not implement Wired Equivalent Privacy (WEP) algorithm

- All Wireless LAN should be setup for Shared Key Authentication! But do not!

Authentication – Open System Authentication

Open System Authentication is the default authentication service in IEEE802.11. In Open System Authentication, there is no verification of the identity of stations, this means that it should only be used in applications that do not require positive validation of the station’s identity. For stronger authentication, the Shared Key Authentication should be used. In Open System Authentication, the requesting station will assert its identity to the receiving station, stating its desire to associate with another station or Access Point (AP). The receiving station or Access Point will then respond with a successful result for the authentication. Every wireless LAN should set up a shared key authentication at a minimum to prevent unauthorized access to their network. This step is often neglected and leaves your LAN open for hackers to look through your files. In fact there are hackers that will put chalked symbols on sidewalks and buildings to indicate where fellow hackers can get free access to the internet via your Access point! All that is needed is 802.11a/b modem card plugged into a Laptop!
Authentication – Shared Key Authentication

- Provides a much higher degree of security than the open system authentication process
- Stations must implement WEP (Wired Equivalent Privacy)
- The process is as follow:

  **Step 1**
  Station A → Station B
  Authentication Frame

  **Step 2**
  Station A ← Station B
  Challenge Text (from WEP Services)

  **Step 3**
  Station A → Station B
  Encrypted Challenge Text using a shared key

  **Step 4**
  Station A ← Station B
  Positive Authentication (if decrypted challenge text matches original text) and vice versa

Authentication – Shared Key Authentication

Shared Key Authentication is an optional authentication technique in IEEE802.11. It provides a much higher level of security as compare to the Open System Authentication described previously. In order for stations to use Shared Key Authentication, they must implement Wired Equivalent Privacy (WEP). The two stations going through the Shared Key Authentication process must have a copy of a shared Wired Equivalent Privacy (WEP) key.

The process of the Shared Key Authentication is described as follow:

Step 1 - Station A, requesting to join in a network will first send an Authentication frame to station B.

Step 2 – Station B then reply with an authentication frame that contains a challenge text (128 octets) that is being generated from the WEP services.

Step 3 – Station A, after receiving the challenge text will encrypt it with a shared key and then send it back to Station B.

Step 4 – Upon receiving the encrypted challenge text, Station B will proceed to decrypt the value of the challenge text using the same shared key. It then compare the decrypted text to the original challenge text. If the comparison is positive (both texts matches), Station B will reply with a positive authentication. If the comparison fails (mismatch), Station B will proceed to send a negative authentication to Station A, and no communication will be established between these two stations.
MAC Layer Services – Security and Privacy

The default configurations of the IEEE802.11 system

- “open” – Data is transferred in the “clear”

Any IEEE802.11 device will be able to eavesdrop on traffic that is within range.

Security in IEEE802.11 is accomplished by an optional feature using Wired Equivalent Privacy (WEP) algorithm.

The Wireless LAN system has an open broadcast nature, which makes it somehow insecure. In IEEE802.11, the default configuration is “open”, this means that data is transferred in the “clear”. Any IEEE802.11 device will be able to eavesdrop on traffic that is within range. In order to prevent eavesdropping, the developers have to implement some form of security and privacy to their system. IEEE802.11 standard defines an optional feature to provide such security and privacy. This optional feature uses Wired Equivalent Privacy (WEP) algorithm. As discussed earlier, WEP generates shared encryption keys that both the source and destination stations can use to avoid disclosure to eavesdroppers. IEEE802.11 stations can use WEP alone without authentication services, but to provide a higher level of security, the developers should implement both WEP and authentication together in their system. Many reports have shown that there is an increase in eavesdropping cases on the Wireless LAN network and almost all these cases have happened in networks that do not implement any WEP or authentication.
Wired Equivalent Privacy (WEP)

- WEP provides security to the transferred data using a known method of encryption called RC4
- RC4 employs a secret shared key between the AP and the mobile stations
- Only stations with the exact shared key will be able to decipher the data
- WEP does not protect the Physical header
  - other stations on the network can listen to the control data needed to manage the network

Wired Equivalent Privacy

Wired Equivalent Privacy provides security to the transferred data using a known method of encryption called RC4. RC4 was developed at RSA Data Securities, Inc. (RSADSI). WEP encryption is sometimes known as symmetric encryption simply because RC4 is a symmetric stream cipher. It is symmetric because the same key and algorithm are being use for both encryption and decryption. Only stations that share the same key can correctly decrypt the encrypted frames. RC4 allows the key length to be variable, up to 256 bytes. IEEE802.11 standard states that the key use will be a 40-bit key. Although the standard defines the use of RC4 algorithm and the key in WEP but the way the key is being distributed or negotiated is not being stated in the standard. This means that individual developers will have to design these difficult section on their part.

One important point to take note about WEP is that it does not provide protection to the Physical header. Other stations on the network can listen to the control data needed to manage the network.
Wired Equivalent Privacy Mechanism

The operation of the Wired Equivalent Privacy (WEP) Mechanism can be explained as follow:

1. The original plain text (frame body) is first fed into the Integrity Algorithm block. The Integrity Algorithm block generates a 4-octet Integrity Check Value (ICV). The Integrity Check value (ICV) will be send together with the data such that the destination will perform a check on it to prevent any unauthorized data modification.

2. A shared key will be pass through a pseudo-random number generator. This will result in a shared key sequence, which will have the same length as the plain text plus ICV. The advantage of having the pseudo-random number generator block is to allow simpler key distribution because now only the shared key must be made available, not the variable length key sequence.

3. The next process is the encryption process where the shared key sequence will go through a bitwise exclusive-or (XOR) operation with the plain text plus ICV. The result is an encrypted text which can only be decrypt using the same key. The destination station will decrypt the encrypted text using the shared key that generates the same key sequence used initially to encrypt the frame. The destination station also calculates an Integrity Check Value (ICV) and check to see if it matches the one received. If it mismatch, a failure indication will be send to the MAC management and the station will not proceed to pass the MAC Service Data Unit (MSDU) to the LLC.
MAC Layer Services - Association

• Association is a process of connecting a station to an AP within a BSS

• It is through association that the network knows the current location of the station in the Extended Services Set (ESS) and allows the station to request services.

• Association can only be achieved after a successful authentication

• During association, an association request is sent from the station to the AP

• AP will then decide based on the information in the association request whether to grant the association to the station.

MAC Layer Services – Association

The first step to provide mobility to a station within a Basic Service Set (BSS) is the Association service. Association is a process of connecting a station to an AP within a Basic Service Set (BSS). The association service maps a station to the Distributed System (DS) via an Access Point (AP). It is through association that the network knows the current location of the station in the Extended Services Set (ESS) and thus allows the station to request for services. Stations must first go through a successful authentication before it can achieve association. Station requesting for association will first send an association request to the Access Point (AP). The association request includes several key information such as its data rates, its contention-free capabilities, any WEP supported, high rate Physical options it supports, length of time in “sleep” mode. The Access Point will then based on these information whether it wants to grant the association to the station. Again, the decision criteria for association is not being define in the IEEE802.11 standard.
MAC Layer Services – Re-association

• Since stations are mobile, and can move from one BSS to another – stations can lose contact with AP!

• Re-association is therefore required to allow stations to continue exchanging data frames.

• During re-association, a re-association request is sent by the station to the AP

• Re-association request includes all the information in the original association request, plus the address of the last AP with which the station was associated.

• The station’s previous association will be terminated, once the AP grants the re-association.

MAC Layer Services – Re-association

Once the station gets associated with the Access point, it gains it mobility and is now able to roam around within the Basic Service Set (BSS). If the station starts to move from one Basic Service Set to another, the station can now lose its association status with the Access Point (AP) and thus lose its contact with the Access Point (AP). This is what we normally call disassociation. In order to allow the station to continue exchanging data frame with another station or Access Point (AP), the station must being a new association. This is done by the station sending a re-association request to the Access Point (AP). The re-association request includes all the information in the original association request, plus the address of the last AP with which the station was associated. The last AP’s address allows the AP receiving the re-association request to retrieve any frames at the old Access point (AP) and deliver them to the mobile station. The station’s previous association will be terminated, once the AP grants the re-association.
Re-association – Roaming

As discussed on the previous slide, re-association allows mobile to move from one Basic Service Set to another. Although the capability to roam within an Extended Services Set (ESS) seems to be an attractive feature, the IEEE802.11 standard does not provide specifications for it. This means that vendors or developers will have to implement their own proprietary roaming protocol. Fortunately, several companies (led by Lucent) decided to form a special interest group to collaborate and define a common roaming protocol. This protocol is known as the Inter-Access Point Protocol (IAPP). IAPP basically uses the User Datagram Protocol (UDP) and the Internet Protocol (IP) as a basis for communication.
MAC Layer Services – Data Transfer

- Stations use Carrier Sense Multiple Access /Collision Avoidance technique as medium access scheme.
- Data must be delivered reliability under:
  - Noisy and unreliable medium
  - Must handle hidden node situation
- MAC layer provides the following techniques to ensure reliability in data transfer service:
  - Acknowledgement
  - RTS/CTS frames
  - Fragmentation

MAC Layer Services – Data Transfer

The Medium Access Control (MAC) layer is responsible for transferring data between the Physical and the Logical Link Control (LLC) layer. As covered in the earlier section, the MAC layer uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) technique for regulating the usage of the medium for data transfer. It is important that the MAC layer can reliably transfer the data under non-idea conditions such as a noisy and unreliable medium. It must also transfer the data reliably under hidden node situation. There are three key techniques defined in IEEE802.11 to ensure that this is achieved. The three techniques are the Acknowledgement technique where the destination station will send a reply when it has successfully received the data frame, Request-to-Send/Clear-to-Send control frames technique to solve hidden node problem and lastly Fragmentation technique. As the first two techniques has already been discussed earlier, let us now take a look at the Fragmentation technique and how it can help to ensure a more reliable data transfer over the medium.
Frame Fragmentation

Longer frame is more error prone than a shorter frame in a noisy and interference ridden environment.

Solutions:
- Break the longer frame into smaller fragments
- Frames larger than threshold (dot11FragmentationThreshold set between 256 - 2048 Bytes) are fragmented prior to initial transmission.
- Frames will be fragmented by a size no longer than the value of the dot11FragmentationThreshold MIB (Management Information Base) attribute
- By default, no fragmentation is being performed

Frame Fragmentation

The IEEE802.11 Wireless LAN is subjected to noise and many interferences in the environment. The IEEE802.11b being deployed in the 2.4GHz Industrial, Scientific and Medical (ISM) band have to overcome many competing transmission from other radio standards, such as Bluetooth. Competing IEEE802.11 stations as well as overlapping Basic Service Sets can also poise a problem to the station transmitting data frame. It is understood that a longer frame will be more prone to error than a shorter frame in a noisy and interference ridden environment, therefore if we can minimize the transmission of long frames, we will be able to reduce the frame error rate. The process of breaking up a longer frame into many shorter ones is called Frame Fragmentation. In IEEE802.11, any frames larger than a certain threshold (specified by dot11FragmentationThreshold in the IEEE802.11 standard) will be fragmented prior to initial transmission. The threshold range is user set and has a range of 256 to 2048 Bytes. For noisy and interference prone or in heavy data traffic environments, set the threshold to lower values. It is more efficient to set the number to higher values in normal environments. Frames are fragmented by a size no longer than the value of the dot11FragmentationThreshold Management Information Base (MIB) attribute.
Frame Fragmentation Process

In the previous slide, we have mentioned that if the length of the MSDU to be transmitted is greater than the dot11FragmentationThreshold parameter stored in the management information base (MIB), the MSDU is fragmented. Each fragmented frame has a MAC header, FCS, and a fragment number to indicate position order in the MSDU. Each fragment is sent independently and requires a separate Acknowledgement (ACK) from the receiving station. The receiving station will combine the fragments in the same order based on the fragment number. Although frame fragmentation helps to improve frame error rate, it does however increases the MAC overhead due to a greater number of ACK frames being sent and also the MAC header and CRC being incurred on every fragmented frames.
MAC Layer Services – Power Management

IEEE802.11 supports 2 power modes

• Active Mode and Power-Save Mode

• **Active Mode:**
  - Stations are powered to transmit and receive

• **Power-Save Mode:**
  - Reduces power consumption by turning off the transmitter and receiver ("sleep")
  - "Sleep" interval is defined by the base station
  - Power-Save mode is different in an independent BSS and an infrastructure BSS

MAC Layer Services – Power Management
Since Wireless LAN mobile stations are usually portable and operates on batteries, it is important to make them power efficient so that the batteries life span will be prolong. IEEE802.11 supports two power modes: Active mode and Power-Save Mode. In active mode, stations are powered to transmit and receive continuously. In order to help prolong batteries stand-by time, IEEE802.11 defines another power mode called Power-Save Mode. Power-save mode enables stations to go into “sleep” mode (turn off transmitter and receiver) so as to conserve power without losing information. The “sleep” interval is defined by the base station. IEEE802.11 power-save mode is different in an Independent BSS (Id-BSS) and in an Infrastructure BSS (If-BSS). Let us now take a look at the power-save mode operation in these two types of BSSs.
Power Management – Independent BSS

• A station in an independent BSS will enter the power-save mode when it has successfully completes a data frame handshake with another station.

• Since there is no Access Point, the station will “wake-up” to every beacon transmission

• After the beacon was received, the station will stay awake for a period of time defined by ad hoc traffic indication message window (ATIM)

Power Management – Independent BSS

Power management in an Independent Basic Service Set (Id-BSS) is managed by the individual mobile stations. For a station in an Id-BSS to enter the power-save mode, it must successfully completes a data frame handshake with another station. Since in an Id-BSS, there is no Access Point (AP) to determine when is the time for the station to wake-up to listen to the beacon, the stations will basically wake-up to every beacon transmission. After the beacon was received, the station will stay awake for a period of time defined by Ad hoc Traffic Indication Message (ATIM) window. It is only during this window that other stations requesting to send frames to it will indicate its request. The request is via an Ad hoc Traffic Indicator Message (ATIM) frame and the power-save mode station will then have to acknowledge the frame (handshaking) and remain awake until the end of the next ATIM window. Power-save stations that do not receive any ATIM frame during the ATIM window will go back to sleep after the ATIM window and will only wake up at the next beacon.
Power Management – Infrastructure BSS

- A station enters the power-save mode in an Infrastructure BSS by setting the power-save bit in the frame control sent to the AP.
- The station will enter the power-save mode at the end of the traffic flow.
- Stations will not “wake-up” to every beacon but rather it will “wake-up” at times determined by the AP.

Unlike the Independent Basic Service Set (Id-BSS), the Infrastructure Basic Service Set (If-BSS) has an Access Point, which will manage the power-save mode operation. A station will enter the power-save mode in an Infrastructure BSS (If-BSS) by setting the power-save bit in the frame control that is being sent to the Access Point (AP). The station will enter the power-save mode at the end of the traffic flow. Power-save mode in If-BSS is capable of saving more power as compare to the power-save mode in Id-BSS. This is because the stations in If-BSS do not need to wake-up to every beacon but rather it will wake-up at times determined by the Access Point (AP).
IEEE802.11 Physical Layer

In this section, the following topics on IEEE802.11 Physical Layer will be covered:

(1) Frequency allocation of IEEE802.11b
(2) IEEE802.11 Physical Layer Architecture
(3) Transmit and Receiver Procedure
(4) Antenna Diversity
(5) Modulation Schemes in IEEE802.11 and IEEE802.11b
Frequency Allocation for IEEE802.11b

- Direct Sequence spread spectrum in the 2.4GHz ISM Band
- Occupies 83.5MHz of Bandwidth
- Unlicensed Band – promotes interoperability but crowded with interference!

*Per FCC 00-312, CFR 47 part 15 amended to allow 1W divided by BW in MHz (e.g. 5 MHz = 200mW)

IEEE802.11b is allowed in the unlicensed Industrial, Scientific and Medical (ISM) band. Although IEEE802.11 specifies FHSS, DSSS and Infrared as the three possible technologies of implementing the physical layer, IEEE802.11b uses the DSSS as the spread spectrum technique. The ISM band is a global band occupying a total of 83.5MHz from 2.4 GHz to 2.4835GHz. All countries in the world allocate the same frequency band but its maximum power specification is different in different parts of the world. For example, the maximum radiated peak power is 100mW except in Japan where it is only 10mW/MHz. FCC specifies the maximum radiated peak power in USA as 1W per BW (in MHz).
### DSSS Channels Allocation in ISM Band

<table>
<thead>
<tr>
<th>Freq (GHz)</th>
<th>Ch No.</th>
<th>USA and Canada</th>
<th>Europe</th>
<th>Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.412</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.417</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.422</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.427</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.432</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.437</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.442</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.447</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.452</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.457</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.462</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.467</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.472</td>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.484</td>
<td>14</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### DSSS Channels Allocation Around The World

Different parts of the world have a specific frequency band for DSSS operation. This is dependent on the regulatory authorities in the particular country. As we have mentioned, in U.S. and Canada, there are a total of 11 channels (from 2.412GHz to 2.462GHz) allocated for DSSS operation. In Europe, a wider channel selection is provided, ranging 2.412GHz to 2.472GHz (13 channels). Japan uses the full 14 channels where Spain and France uses a smaller band for DSSS operation.
2.4GHz ISM Band is in heavy use

As is shown in the Spectrogram above the 2.4 GHz ISM band presents many challenges in terms of interference. The interference from multiple μwave ovens reveals that they operate at different frequencies and they swing over a wide frequency ranges. The 802.11a &b devices must handle this environment. The cost will be in terms reduced network performance due to data unit errors and retransmissions.
Wireless LAN Standard in the 5GHz Band

The diagram on this slide illustrates the 5GHz frequency band being deploy for Wireless LAN standards in Europe, Japan and USA.
Physical Layer Architecture

The IEEE802.11b Physical Layer architecture is made up of three entities and/or layers for each station. They are the Physical Layer Management Entity (PLME), Physical Layer Convergence Procedure (PLCP) sublayer and Physical Medium Dependent (PMD) sublayer.

The PLME is responsible for the management functions for the Physical layers by working in conjunction with the MAC layer management.

The PLCP sublayer simplifies the interface between the MAC services and the Physical Layer services. The communication between the MAC layer and the Physical layer is performed via primitives through the Physical layer Service Access Point (PHY SAP). PLCP sublayer is responsible for setting up MAC protocol data units (MPDUs) for transmission as well as delivering incoming frames from the wireless medium to the MAC layer. The PLCP appends fields to the MPDU that contain information needed by the Physical layer. This composite frame is known as PLCP Protocol Data Unit (PPDU). Synchronization between two stations must be achieved if the receiving station is to correctly receive each incoming frame.

The PMD sublayer provides the transmission interface between two station communicating via the wireless medium. The PMD interfaces directly with the wireless medium. It is responsible for modulating and demodulating the frame transmissions.
Physical Layer Carrier Sense Operation

- PMD check if medium is busy or idle
- **Clear Channel Assessment (CCA)** – PLCP sends a PHY-CCA.ind (status field) to the MAC layer to indicate the status of the medium.
- If medium is busy, PLCP will read in the PLCP preamble and header of the incoming frame

Physical Layer Carrier Sense Operation

The PMD (Physical Medium Dependent) in the physical layer will check if the medium is busy or idle. The operation that determines whether the medium is busy or idle is termed the Clear Channel Assessment (CCA) operation. The next slide will explain the 3 different modes of CCA. The PLCP (Physical Layer Convergence Procedure) will send a PHY-CCA.ind primitive to the MAC layer to indicate the status of the medium after the CCA operation. The status field in the PHY-CCA.ind primitive will indicate if the medium is busy or idle. If the medium is busy, the PLCP will read in the PLCP preamble and header of the frame. This is to achieve synchronization of the receiver to the data rate of the signal.
Clear Channel Assessment (CCA)

IEEE802.11b specifies 3 modes of operation for CCA:

Mode 1 Energy above threshold:
RF Power Level Energy Detection threshold, ED, threshold is ≥ –80dBm for transmission power greater than 100mW, ≥ -76dBm for transmission power between 50 to 100mW, and ≥ –70dBm for transmission power lower than 50mW.

Mode 2 Carrier Sense only:
The medium busy if DSSS valid signal detected by PMD, independence of energy, determined by detection valid PLCP header. The medium busy until end of frame.

Mode 3 Carrier Sense with energy above threshold:
A combination of Mode 1 & 2. The medium considered busy if the PMD detects valid DSSS signal that exceeds the ED threshold.

Clear Channel Assessment (CCA)
IEEE802.11 specifies 3 modes of operation for the CCA. All receivers implemented must employ at least one of the modes. The 3 modes are as follow:

Mode 1 Energy above threshold: The PMD measures the energy on the medium (RF Power Level) to check if it is above a given threshold. Is there a signal present? The medium will be considered busy if the energy is above the threshold (Energy Detection threshold, ED). ED threshold is –80dBm for transmission power greater than 100mW, -76dBm for transmission power between 50 and 100mW, and –70dBm for transmission power lower than 50mW.

Mode 2 Carrier Sense only: The medium will be considered busy if a valid DSSS signal is detected by the PMD, with independence of its energy. This is determined by the detection of a valid PLCP header. The medium will be considered busy until the end of the frame as indicated in the PLCP LENGTH field, even if reception is lost.

Mode 3 Carrier Sense with energy above threshold: This mode is a combination of Mode 1 and Mode 2. The medium will be considered busy if the PMD detects a valid DSSS signal that exceeds the ED threshold.
IEEE802.11b DSSS Physical Layer Convergence Procedure Sublayer

DSSS Physical Layer Convergence Procedure Sublayer

The 802.11 specification refers to the DSSS (Direct Sequence Spread Spectrum) PLCP (Physical Layer Convergence Procedure) above as a PLCP protocol data unit (PPDU). The Preamble enables the receiver to synchronize to the incoming signal properly before actual content of the frame arrives. The header field provides information about the rest of the frame, and the PSDU (Physical Layer Convergence Procedure Service Data Unit) is the MPDU (MAC Medium Access Control, Protocol Data Units) the station is sending.

**Sync:** Consists of alternating 0s and 1s. The receiver will synchronize with the received signal upon detecting the Sync field (RF Power).

**Start Frame Delimiter (SFD):** Always contains the pattern 11100110000000.

**Signal:** Identifies the type of modulation that the receiver must use to demodulate the signal. The values are 00001010 for 1Mbps DSSS, 00010100 for 2 Mbps DSSS, 00110111 for 5.5 Mbps, and 01101110 for 11 Mbps.

**Service:** 000000X0 = IEEE802.11 and Bit 2=1/0 indicates whether the transmitter frequency and the symbol clocks are derived from the same oscillator.

**Length:** unsigned 16-bit integer indicating the number of microseconds to transmit the MPDU. Receiver will use this field to determine end of frame.

**Frame Check Sequence:** 16-bit CRC (Cyclic Redundancy Check) error detection algorithm. Note: MAC layer will check for errors in the FCS field. Physical layer does not determine whether errors are present within the PSDU.
Antenna Diversity Concept

Physical layer receive operation uses antenna diversity

Why Antenna Diversity?

To combat signal degradation due to multipath fading, path loss, rain, heat etc.

Antenna Diversity Concept

One of the key physical layer receive operations is **Antenna Diversity**. Why do we need diversity? Antenna Diversity helps to improve the system performance over under fading channel conditions by switching between multiple antennas. Antenna diversity is used to combat signal degradation due to multipath fading, path loss, rain, heat etc.
Antenna Diversity Concept

What is Antenna Diversity?

• Radio receiver has two or more antennas

• The antennas (a few cm apart) can receive very different signal quality

• Receiver can either use Selection or Maximum Ratio Combining techniques

• Avoids most multipath fading conditions

Antenna Diversity Concept

Antenna diversity works on the principle of using multiple antennas at the receiver. The antennae are usually placed a few cm apart and they can receive very different signal quality. There are two common antenna diversity techniques used in the receiver. They are the Selection Diversity and the Maximal Ratio Combining (MRC) techniques. The selection diversity technique is the simpler one among the two common techniques. The receiver basically chooses the antenna based on the largest Signal-to-Noise ratio (SNR) in each symbol interval. Selection diversity technique does not require additional RF receiver chain, meaning that the multiple antennas will share a single RF receiver chain. All the selection diversity implementation requires is a measurement of the power from each antenna and a switch. The simplicity of this technique has made IEEE802.11b Wireless LAN systems employ selection diversity at both the mobile station and access point. In the maximal ratio combining (MRC) technique, the different signals at the multiple receive antennas are combined linearly so as to maximize the instantaneous SNR. Based on optimization theory, the coefficients that will achieve the maximum SNR are calculated and applied.
IEEE802.11b Direct Sequence Spread Spectrum at 1 MBit/Sec

To create a Direct Sequence Spread Spectrum signal, a lower rate data stream is multiplied by a higher rate bit sequence signal. For 1 MBit/sec, the 1 MHz Differential Binary Phase Shift Keyed signal is multiplied (XORing) by an 11 MHz BPSK signal. Although not generally true of DSSS signals, for this particular signal we can say that the input bits determine the phase rotation of the spreading code. We can also say that we have a (Differential) Binary Phase Shift Keyed data signal spread by a BPSK spreading sequence, producing a BPSK constellation.

In spread-spectrum communications, the signal bandwidth is increased (in this case by a factor of 11) without increasing the data rate. Why take the increased bandwidth hit? For increased immunity to interference from signals from microwave ovens, cordless phones, multipath and co-channel signals.

While any spreading sequence could be used, sequences are usually chosen for their spectral properties, and for low cross correlation with other spreading sequences and interfering signals. For 1 and 2 MBit/sec 802.11b, an 11 chip Barker sequence is used. The autocorrelation function for the Barker sequence is 1, -1 or 0 at all offsets except zero, where it’s 11. This makes for a more uniform spectrum, and the receivers have an easier time pulling the signal out of the background clutter.

The sum of the Barker sequence states is +1 or -1 and there are several unique sequences that can be used. Only the receiver using the same Barker sequence will be able to demodulate the signal. All other Spreading codes will appear to be “noise” to the receiver.
IEEE802.11b Direct Sequence Spread Spectrum at 2 MBit/Sec

To double the bit rate from 1 MBit/sec to 2 MBit/sec, the bits are taken two at a time. Instead of 2 phase states of either 0 or 180 degrees there are four phase rotations used: 0, 90, 180 and 270 degrees. The symbol rate remains at 1 MSym/sec with 2 bits per symbol. We can say that there are 2 Binary Phase Shift Keyed signals that are orthogonal to each other, 90° apart that produce a QPSK signal.

Here, each symbol state is spread by an 11 chip sequence at 11 Mbits per sec. At 2 MBit/sec, the input bits are taken two at a time, with four possible output symbols. Each symbol is spread by an 11 chip code. To illustrate, the end of the last chip leaves us in the upper right constellation point. The next dibit transmitted is a “01”. The rotation is + 90° and the next starting point is the upper left constellation point, +I, -Q. The Barker Sequence for this dibit pulls the carrier along the left side of the constellation between ±Q. The final point in the sequence lands us on the –I, -Q constellation point, lower left. The next dibit is a “11” and rotates to the next constellation starting point 180° from –I, -Q. This puts us back to our starting point at I, Q and the Barker sequence pulls the carrier between ±I along the horizontal at +Q.
How to achieve 11MBit/Sec in IEEE802.11b?

At 1 MBit/sec we used an 11 chip Barker sequence with two phase rotations to produce one symbol with two phase states. At 2 MBit/sec we used the same sequence with four phase rotations states and a set vector length to produce one symbol with four phase states. If we were to continue with this approach we would need 2048 states (2^{11} vector magnitude and phase states) rotations of an 11 symbols long to achieve the needed bit sequence for 11 MBit/sec. One can see that the states are very closely spaced in the 256 QAM (2^8 states) constellation and there is little margin for error. Obviously a different approach is needed.

While it would be possible to use a some form of QAM constellation instead of PSK this would have the undesirable side effect of increasing the peak-to-average ratio of the signal, making amplification more difficult and costly. But of even more importance is that

The approach taken, which retains a QPSK constellation at the transmitter output, is called CCK, or complementary code keying. The complementary codes are a set of nearly orthogonal complex sequences.
Complementary Code Keying (CCK) Modulation in IEEE802.11b

Form of Spread Spectrum Modulation

Extends 802.11 data rates to include 5.5 MBit/sec and 11 MBit/sec

There are three rates to keep track of:

- **Chip Rate**: 11 MHz always
- **Bit Rates**:
  - 1 MBit/sec DBPSK 11 chip Barker sequence
  - 2 MBit/sec DQPSK 11 chip Barker sequence
  - 5.5 MBit/sec QPSK, 4 8-chip CCK spreading
  - 11 MBit/sec DQPSK, 64 8-chip CCK spreading
- **Symbol Rates**: 1 MHz (11/11) and 1.375 MHz (11/8)

At all rates, the signal looks like an 11 MHz BPSK or QPSK waveform

CCK (complementary code keying) Modulation in IEEE802.11b

802.11b adds 5.5 and 11 Mbit/sec data rates to the 802.11 standard. In a rather odd twist, the progression of technology in the 802.11 standard is 802.11 to 802.11b to 802.11b., and eventually to 802.11G. Many find the fact that 802.11b is slower than 802.11a confusing.

802.11b is designed for use in the 2.4 GHz “microwave oven” band. The technology behind 802.11b is direct sequence spread spectrum (DSSS). With spread spectrum technology, the chip rate can remain constant while the data rate changes to match conditions. The bit rate is varied by changing both the spreading factor and/or the modulation format. For example, the 1MBit/sec rate has a spreading factor of 11 with a simple BPSK modulation. To double the bit rate to 2 Mbit/sec, Quadrature Phase Shift Keying is used instead of BPSK.

CCK (complementary code keying) uses I/Q modulation with a spreading code 8 chips long at a chipping rate of 11 million chips per second. Each symbol transmitted is represented by a particular CCK spreading code. Each Chip of the spreading code is complex.
IEEE802.11b Spread Spectrum Concepts – 5.5 and 11 MBit/Sec

To achieve 5.5 and 11 MBit/sec rates, the spreading length is first reduced from 11 to 8. This increases the symbol rate from 1 Msym/sec to 1.375 Msym/sec. To achieve 5.5 MBit/sec bit rates with 1.375 MHz symbol rates we need to transmit 5.5/1.375 or 4 bits/symbol. For 11 MBit/sec we obviously need 8 bits/symbol.

The approach taken for 802.11b, which keeps the QPSK spread spectrum signal and still provides the required number of bits/symbol uses all but two of the bits to select from a set of spreading sequences and the remaining two bits to rotate the sequence.

One important difference between the sets of spreading sequences used here, and the single Barker code sequence used for the 1 and 2 Mbit/sec rates is that these sequences are complex. In other words, a Differential Quadrature Phase Shift Keyed signal with QPSK spreading.
Differential Quadrature Phase Shift Keying DQPSK Encoding in IEEE802.11b

<table>
<thead>
<tr>
<th>d0, d1</th>
<th>Even Symbols</th>
<th>Odd Symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>0</td>
<td>π</td>
</tr>
<tr>
<td>01</td>
<td>π/2</td>
<td>3π/2</td>
</tr>
<tr>
<td>11</td>
<td>π</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>3π/2</td>
<td>π/2</td>
</tr>
</tbody>
</table>

DQPSK Encoding Table for 5.5 and 11Mbps Data Rates

DQPSK Encoding in IEEE802.11b

The table above shows the encoded phase for both even and odd symbols. This table applies to both the 5.5 and 11Mbps data rates configuration.
Orthogonal Frequency Division Multiplexing in IEEE802.11a

• IEEE 802.11a Structure:
  • 52 carriers (48 data + 4 pilot)
  • 312.5 kHz spacing
  • 18 MHz bandwidth
  • 54 Mbps composite, max
  • 5-6 GHz frequency range

• IEEE 802.11g: Same as above in the 2.4 GHz ISM Band

Orthogonal Frequency Division Multiplexing in IEEE802.11a

This section of the training covers the concept behind Orthogonal Frequency Division Multiplexing (OFDM) in IEEE802.11a. The advantages of OFDM will be highlighted to show the reasons behind the usage of OFDM in IEEE802.11a.
Creating an OFDM Symbol - One Carrier Example

The constellation shows the Symbol State magnitude and phase of a sub-carrier.

Each FFT bin corresponds to a single sub-carrier.

Inverse Fast Fourier Transform

Creating an OFDM Symbol – One Carrier Example

If you know a little about Fast Fourier Transforms, the concepts behind OFDM will be more easily understood. In this example we are going to create an OFDM signal with only one sub-carrier. The magnitude and phase of the carrier are determined from the symbol to be transmitted, as shown in the constellation diagram. The complex number representing the symbol is loaded into an FFT buffer, and an inverse-FFT calculated. This produces a set of time-domain samples. These samples are then transmitted.

In 802.11a, the IFFT size is 64 complex frequency bins. Of the 64 bins, 52 of the Frequency bins are loaded with data and pilots. The IFFT computes 64 time samples, and all 64 time samples are transmitted. The sinewave with the correct magnitude and phase represents 1 symbol for 1 sub-carrier.
Creating OFDM Signal – One IFFT per Symbol Period

Continuing with the single carrier OFDM example, while the first symbol set is being transmitted, the next symbol set is loaded into the FFT buffer. Notice that the resulting symbol set burst, when joined with the first burst, results in a discontinuity in the set of continuous time samples. This is normal and will result in spectral splatter. The spectral splatter can be attenuated somewhat by windowing the data, as described in the 802.11a standard.
Creating OFDM Signal – Multiple Carrier Example

This diagram shows how a multi-carrier OFDM signal is generated, and how easy it is to have many different modulation formats. In the limit, every carrier could be different! As more carriers are added, the resulting time waveform becomes more complex. This is one of the problems with OFDM. As we’ll show later, the addition of multiple carriers results in a signal with a higher peak-to-average power ratio.
Receiving an OFDM Signal

At the receiver, ignoring channel affects, the time waveform is digitized and then converted back to a symbol using a forward Fast Fourier Transform.
Orthogonality Properties in OFDM

Nulls are *On Bin* if the Tone is *On Bin*

FFT Bin Spacing is 1/T

**802.11a OFDM receiver FFT:**

- FFT Bin spacing = Carrier spacing = 312.5 kHz
- Sample rate = bin spacing x # bin = 20 MSa (64 bins, complex)
- Capture time = 1 / bin spacing = 3.2 µs

Orthogonality Properties in OFDM

Each FFT bin in reality is a spectral line representing a sinewave convolved with a SinX/X function. The SinX/X results from the Fourier transform of the Rectangular Time window. The rectangular time window is also referred to as the Boxcar window. When the sine wave is exactly periodic in the window the zeros in the sinX/X will fall on the adjacent frequency bins. Thus the energy in 1 sub-carrier will not interfere with adjacent frequency bin values. The sub-carriers are said to be orthogonal.
Inter-carrier Interference in OFDM

Frequency Errors and Phase Noise Cause Leakage

This diagram shows how critical receiver frequency tracking is. If the receiver and transmitter are offset in frequency, then the nulls around each carrier won’t land on the adjacent FFT bins. In FFT terminology this is called leakage. For OFDM, the result is inter-carrier interference.
Multipath in an Office Environment

Multipath is a real problem in office and warehouse environments. The problem of delay spread causes the effective signal arrival time to vary across the channel bandwidth. Another issue is “dead zones” where the signal strength drops to very low undetectable levels due to destructive interference. Where two signals arrive at the same location and are 180° out of phase and cancel each other out.
**IEEE802.11a OFDM Has to Deal With Multi-Path**

*Problem:* Multipath Different signal paths cause arrival times for each sub-carrier to be different. When the transmitted symbol time period = receiver capture time, even a little delay spread causes problems.

Multipath effectively means that a signal's arrival time at the receiver varies across the channel bandwidth. The variation across the channel is called the delay spread. When the delay spread time is a significant portion of the symbol time demodulation problems occur. This is true for most digital radio modulation schemes but especially true for OFDM.
How IEEE802.11a OFDM Deals With MultiPath?

Solution: extend the symbol interval time.....

How IEEE802.11a OFDM deals with multipath?
The delay spread issue is handled in OFDM by “Padding” the time record length.
IEEE802.11a Guard Interval – Combats Inter Symbol Interference

A Guard Interval is inserted before Transmission

\[
T_g = 0.8\mu s \\
T_u = 3.2\mu s
\]

The guard interval is often referred to as a “cyclic extension”.

IEEE802.11a Guard Interval – Combat ISI

In the earlier example we ignored the effects of the channel and spliced the two pulses from subsequent symbols together. This won’t work in practice because the channel will still introduce ISI between bursts. To combat this problem, the bursts is modified by a technique know as cyclic extension. In this process, the last 1/4 of the bursts is copied and attached to the beginning of the burst. Due to the periodic nature of the FFT, the junction at the start of the original burst will always be continuous. However, the signal will still suffer from discontinuities at the junctions between adjacent symbol bursts.
How Guard Intervals Combat Multipath – Two Paths/Transmitters Example

This drawing illustrates how the addition of a guard interval helps with ISI. Shown are two copies of the same signal. Each copy took a different path so they will arrive at the receiver at slightly different times. They will be combined in the receiver’s antenna into a single signal. In the time interval denoted by the yellow box marked Tu, the signal will only interfere with itself. This amounts to a scaling and angular rotation of the symbol, nothing more.

In the guard interval region(Tg), it’s easy to see that the resulting signal will have contributions from both symbols -- ISI. The guard interval is ignored in the receiver, so the ISI does not degrade receiver performance.

Obviously the guard interval needs to be larger than the delay spread, but not so long that throughput suffers. In the 802.11a standard, the guard interval is fixed.

Delay spread is not limited to positive delays. In non line-of-site conditions, the shortest path may not be the strongest. The implications on OFDM receivers is that the FFT may not be perfectly aligned with the useful part of the burst (as it’s often called). Instead the receiver will shift the FFT location to the left using part of the guard interval instead of the end of the useful part. In some OFDM standards, a cyclic post-fix is explicitly added. This shifting does not appear to be allowed in the modulation accuracy test, so linear distortion which introduces ISI within the useful part of the burst will increase Error Vector Magnitude.
IEEE802.11a OFDM Signals

Generation of OFDM signals tends to require high performance DSP engines with fast parallel floating point math.

The computational steps include:

- error correction codes added and interleaving the input bit stream, and then mapping the resultant bits, “n” at a time, onto the transmit constellation. (Depending on the desired bit rate, the bits could be mapped one at a time onto a BPSK constellation, or up to 6 bits at a time onto a 64QAM constellation).

- in this example, the four bits “1011” correspond to a 16QAM constellation location, with I-Q coordinates of +0.29 +j0.85. This complex number is then loaded into the next bin in an array of 52 complex values. The process is repeated until 288 (6 bits X 48 bins) bits have been converted, and the entire array filled. (Four of the bins are “pilots”, and get their values from a slightly different source – described later).

- an inverse FFT is then performed on this complex array (to make the math easier, 0+j0 values are appended to either end of the array, so that it’s total length is 64).
IEEE802.11a Spectrums and Limits

The time waveform from the previous slide is up-converted to 5 GHz and amplified for transmission. At the center of the Spectrum is sub-carrier 0 which is not used. The pilot sub-carriers at ± 7 and ± 21 provide time synchronization and initial frequency response compensation.
IEEE802.11a OFDM Frame Format

The IEEE802.11a frame format is very different from the IEEE802.11b frame format because of its OFDM nature. Let us now take a look at the structure of the frame and see how synchronization and equalization are achieved using the frame. IEEE802.11a carrier assignment will also be discussed in this section.
Structure of IEEE802.11a OFDM Frame

The OFDM burst is actually divided into four distinct regions. The first is the Short training sequence. This is followed by a Long training sequence and finally by the Signal and Data symbols. From an RF standpoint the Signal Symbol and the rest of the OFDM symbols are similar.
Structure of IEEE802.11a OFDM Frame

In the Short Training Sequence only every 4th sub-carrier is modulated with an equal amplitude and phase signal. The receiver detects the sub-carriers and does: Gain adjustments, course channel gain and phase estimation and corrections, clock synchronization.
Structure of IEEE802.11a OFDM Frame

The channel Estimation burst is again 8 µSec long and all sub-carriers are transmitting with a signal with the same amplitude and phase. The receiver computes an error correction vector for each sub-carrier. The sub-carrier error vectors when multiplied by measured channel estimation vectors will rotate and gain up each sub-carrier so that the error in the estimation vectors is 0. These correction vectors will be used to correct the data vectors transmitted in the remainder of the burst.
Synchronization and Equalization in IEEE802.11a

IEEE802.11A uses

- Training symbols at the beginning of the burst transmission for synchronization (channel estimation sequence).
- Pilot carriers (-21, -7, +7, +21) for equalization. Always BPSK. The Common Phase Error of the pilots is used to track out close-in phase noise.
Structure of IEEE802.11a OFDM Frame

The 4 μSec Signal segment of the OFDM frame notifies the demodulator how the data is encoded in the Data segments that follow immediately after it. The modulation used in the Signal Segment is Binary Phase Shift Keying. The Agilent 89600A Vector Signal Analyzer will read and report these parameters in its Error Summary Table as shown above.
Structure of IEEE802.11a OFDM Frame

The remaining portion of the frame are the data segments. Each data segment is 4 usec in length. The modulation format and coding rate varies depending on the data rate to be achieved. The table shown above summarizes the different modulation format, coding rate and bits/symbol for each data rate in IEEE802.11a. The maximum number of symbols allowed in each frame is 4096.
IEEE802.11a – OFDM Physical Layer Convergence Procedure (PLCP frame) Format

The 802.11a specification for the Physical layer Convergence Procedure (PLCP) shown above. The Preamble enables the receiver to acquire the incoming OFDM signal properly and synchronize the demodulator.

The OFDM burst actually has four distinct regions. The first is the Short training sequence. This is followed by a Long training sequence and finally by the Signal and Data symbols. From an RF standpoint the Signal Symbol and the rest of the OFDM symbols are similar.

**PLCP Preamble:** Consists of 12 symbols. Ten of them are short for establishing AGC (Automatic Gain Control) and frequency estimate of the carrier signal. The receiver uses the long symbols for fine-tuning. It takes 16 microseconds to “train” the receiver after first receiving the frame.

**Rate:** 8 different rates are available in 802.11a. For example: 1101 in this field means 6Mbps is used and 0011 is for 54 Mbps.

**Reserved:** This field is set to 0.

**Length:** Identifies the number of octets in the frame.

**Parity:** This field is one bit based on positive or even parity, based on the first 17 bits of the frame.

**Tail:** Must be set to all zeros.

**Service:** 16 Bits. The first 7 Bits are zeros and are used to synchronize the descrambler in the receiver. The remaining 9 bits are reserved for future use and are set to all zeros.

**PSDU:** PLCP Service data unit is the payload from the MAC layer being sent.

**Tail:** Six Bit and all zeros appended to the symbol to bring the convolutional encoder to zero state.

**Pad Bit:** Fill-ins to make the Data Field a multiple of the number of coded bits in an OFDM symbol, which is 48, 96, 192, or 288.
**IEEE802.11a – OFDM Physical Medium Dependent (PMD) Sublayer**

<table>
<thead>
<tr>
<th>Data rate (Mbps)</th>
<th>Modulation</th>
<th>Coding rate (R)</th>
<th>Coded bits per subcarrier ($N_{BPSC}$)</th>
<th>Coded bits per OFDM symbol ($N_{CBPS}$)</th>
<th>Data bits per OFDM symbol ($N_{DBPS}$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>BPSK</td>
<td>1/2</td>
<td>1</td>
<td>48</td>
<td>24</td>
</tr>
<tr>
<td>9</td>
<td>BPSK</td>
<td>3/4</td>
<td>1</td>
<td>48</td>
<td>36</td>
</tr>
<tr>
<td>12</td>
<td>QPSK</td>
<td>1/2</td>
<td>2</td>
<td>96</td>
<td>48</td>
</tr>
<tr>
<td>18</td>
<td>QPSK</td>
<td>3/4</td>
<td>2</td>
<td>96</td>
<td>72</td>
</tr>
<tr>
<td>24</td>
<td>16-QAM</td>
<td>1/2</td>
<td>4</td>
<td>192</td>
<td>96</td>
</tr>
<tr>
<td>36</td>
<td>16-QAM</td>
<td>3/4</td>
<td>4</td>
<td>192</td>
<td>144</td>
</tr>
<tr>
<td>48</td>
<td>64-QAM</td>
<td>2/3</td>
<td>6</td>
<td>288</td>
<td>192</td>
</tr>
<tr>
<td>54</td>
<td>64-QAM</td>
<td>3/4</td>
<td>6</td>
<td>288</td>
<td>216</td>
</tr>
</tbody>
</table>

**IEEE802.11a – OFDM Physical Medium Dependent (PMD) Sublayer**

In 802.11a, the data sub-carriers can be modulated using BPSK, QPSK, 16QAM and 64QAM. In some standards you’ll find all of these transmitted at the same time! In 802.11a, only two modulation formats are used simultaneously -- BPSK is one that is always used plus one of the previously mentioned formats.
IEEE802.11a Carrier Assignments

It is useful to consider OFDM from a 2-dimensional point of view. Here we can see the short sequence, which uses every fourth carrier, followed by the long sequence and finally the data carriers. In 802.11a four of the 52 carriers in the data portion of the burst are pilots (only one is shown here). The data carriers change in power level on a symbol-by-symbol basis when 16 or 64 QAM is used.
Conclusions and Summary

The global internet explosion and the rapid growth for mobile data communication needs are the key drivers behind wireless networking.

Wireless LAN has immense amount of potential because of its mobility, simplicity, scalability and low cost of ownership.

IEEE802.11b standard is the most established wireless LAN standard to date. It provides variable data rates up to 11Mbps using CCK modulation.

IEEE802.11a standard, operating in the 5GHz band provides variable data rates up to 54Mbps using OFDM as the multiplexing technique.
Related Agilent Training Courses

★ Using a Vector Signal Analyzer to Make 802.11 Measurements 2 days at your Site Measuring and Evaluation of Your 802.11 Device

Order Number R1362A-250 Productivity Assistance.


Course Part Number H7215B* - 235


★ Spectrum Analysis Measurements. Theory and Fundamental of Spectrum Analysis with Demonstrations using the E440x Economy Spectrum Analyzer an applies to 856x and 859x Spectrum Analyzers.

Course Number H7216B* - 169

* All courses at customers provided location.
References for Additional Information

• RF Testing of Wireless LAN Products, *Application Note 1380-1, Agilent Technologies*

• IEEE802.11 Standard Part 11: Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications, 1999


• Wireless LANs Implementing High Performance IEEE802.11 Networks, *Jim Geier, SAMS*

• OFDM For Wireless Multimedia Communications, *Richard Van Nee and Ramjee Prasad, Artech House Publishers*

• OFDM Wireless LANs: A Theoretical and Practical Guide, *Juha Heiskala and John Terry, SAMS*