Wireless Local Area Networks and the 802.11 Standard

March 31, 2001

Plamen Nedeltchev, PhD

Edited by Felicia Brych

Table of Contents[1]

Introduction 3
Upper Layer Protocols of OSI 3
WLAN Architecture 4
  WLAN topologies 4
  WLAN Components 5
IEEE 802.11, 802.11b and 802.11a Physical Layer 5
  802.11 Physical Layer 5
  802.11b – The Next Step 7
  Sub-layers in the PHY layer 8
  The last step – 802.11a 9
IEEE 802.11, 802.11b and 802.11a MAC Layer 10
  802.11 MAC Layer Services 10
  Collision Sense Multiple Access with Collision Detection 11
  Collision Sense Multiple Access with Collision Avoidance 12
  The “Hidden Station” challenge 13
  MAC Level Acknowledgements 15
  Extended Backoff Algorithm 16
  Frame Types 16
  MAC Frame Formats 16
  MAC Layer for 802.11a 17
802.11 Security 17
Roaming Approach, Association and Mobility 19
Power Management 20
Known Issues and Development Directions 20
  Wireless Device Interoperability in 802.11 21
  Safety 21
Conclusion 21
Glossary 23
References 24

Introduction

Support for wireless local area networks (WLANs) in corporate offices and employee's homes is becoming a necessary activity for networking professionals, requiring new knowledge and training. The purpose of the article is to provide readers with a basic understanding of the 802.11 techniques, concepts, architecture and principles of operations. The standard was designed as a transmission system between devices by using radio frequency (RF) waves rather than cable infrastructure, and it provides mobile, cost-effective solutions, significantly reducing the network installation cost per user. Architecturally, WLANs usually act as a final link between end user equipment and the wired structure of corporate computers, servers and routers.

The standard not only defines the specifications, but also includes a wide range of services including:

- support of asynchronous and time-bounded (time-critical) delivery services;
- continuity of service within extended areas via a Distributed System, such as Ethernet;
- accommodation of transmission rates;
- support of most market applications;
- multicast (including broadcast) services;
- network management services; and,
- registration and authentication services.

The target environment of the standard includes:

- inside buildings such as offices, convention centers, airport gates and lounges, hospitals, plants and residences; and
- outdoor areas, such as parking lots, campuses, building complexes, and outdoor plants.

In 1997, the IEEE released 802.11 as the first internationally sanctioned standard for wireless LANs, defining 1 and 2 Mbps speeds. In September 1999, they ratified the 802.11b "High Rate" amendment to the standard, which added two higher speeds (5.5 and 11 Mbps) to 802.11[1]. The basic architecture, features and services of 802.11b are defined by the original 802.11 standard, with changes made only to the physical layer. These changes result in higher data rates and more robust connectivity.

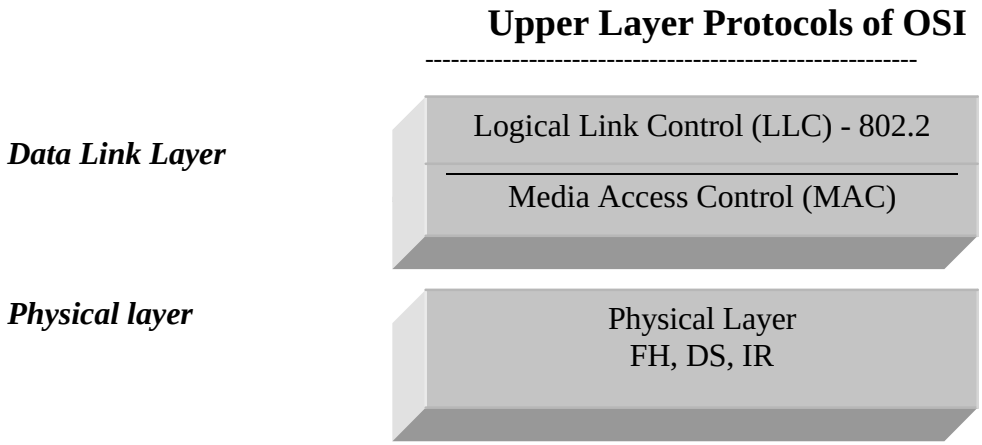


Figure 1. 802.11 standard focuses on the bottom two levels of the ISO model: PHY and MAC

WLAN Architecture

WLAN topologies

IEEE 802.11 supports three basic topologies for WLANs: the Independent Basic Service Set (IBSS), the Basic Service Set (BSS), and the Extended Service Set (ESS). All three configurations are supported by the MAC layer implementation.

The 802.11 standard defines two modes: *ad hoc/IBSS* and *infrastructure* mode. Logically, an *ad-hoc* configuration is analogous to a peer-to-peer office network in which no single node is required to function as a server. IBSS WLANs include a number of nodes or wireless stations that communicate directly with one another on an ad-hoc, peer-to-peer basis, building a full-mesh or partial-mesh topology. Generally, *ad-hoc* implementations cover a limited area and aren't connected to any larger network.

Using *infrastructure* mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). Since most corporate WLANs require access to the wired LAN for services (file servers, printers, Internet links), they will operate in infrastructure mode and rely on an Access Point (AP) that acts as the logical server for a single WLAN cell or channel. Communications between two nodes, A and B, actually flow from node A to the AP and then from the AP to node B. The AP is necessary to perform a bridging function and connect multiple WLAN cells or channels, and to connect WLAN cells to a wired enterprise LAN.
An *Extended Service Set (ESS)* is a set of two or more BSSs forming a single subnetwork. *ESS* configurations consist of multiple BSS cells that can be linked by either wired or wireless backbones. IEEE 802.11 supports ESS configurations in which multiple cells use the same channel, and use different channels to boost aggregate throughput.

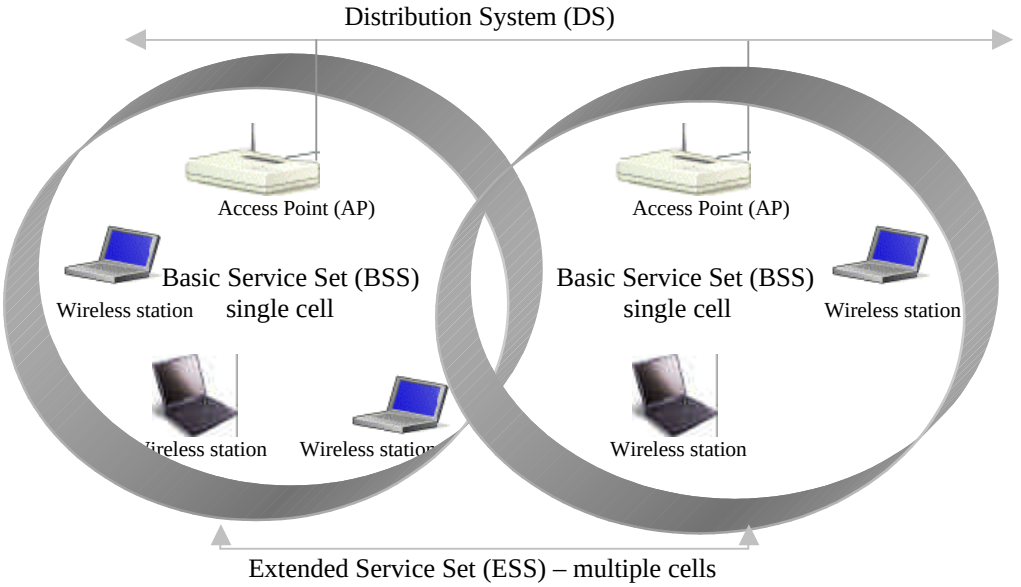


Figure 2. IEEE 802.11 BSS and ESS topologies

WLAN Components

802.11 defines two pieces of equipment, a wireless *station*, which is usually a PC equipped with a wireless network interface card (NIC), and an *access point (AP)*, which acts as a bridge between the wireless and wired networks. An access point usually consists of a radio, a wired network interface (e.g., 802.3), and bridging software conforming to the 802.11d bridging standard. The access point acts as the base station for the wireless network, aggregating access for multiple wireless stations onto the wired network. Wireless end stations can be 802.11 PC Card, PCI, or ISA NICs, or embedded solutions in non-PC clients (such as an 802.11-based telephone handset).

An 802.11 WLAN is based on a cellular architecture. Each cell (BSS) is connected to the base station or AP. All APs are connected to a Distribution System (DS) which is similar to a backbone, usually Ethernet or wireless. All mentioned components appear as an 802 system for the upper layers of OSI and are known as the ESS.

The 802.11 standard does not constrain the composition of the distribution system; therefore, it may be 802 compliant or non-standard. If data frames need transmission to and from a non-IEEE 802.11 LAN, then these frames, as defined by the 802.11 standard, enter and exit through a logical point called a *Portal*. The portal provides logical integration between existing wired LANs and 802.11 LANs. When the distribution system is constructed with 802-type components, such as 802.3 (Ethernet) or 802.5 (Token Ring), then the portal and the access point are the same, acting as a *translation bridge.*

The 802.11 standard defines the distribution system as an element that interconnects BSSs within the ESS via access points. The distribution system supports the 802.11 mobility types by providing logical services necessary to handle address-to-destination mapping and seamless integration of multiple BSSs. An access point is an addressable station, providing an interface to the distribution system for stations located within various BSSs. The independent BSS and ESS networks are transparent to the LLC Layer. http://wwwin.cisco.com/cct/data/itm/wan/sdlc/wtsdllca.htm.

IEEE 802.11, 802.11b and 802.11a Physical Layer

802.11 Physical Layer

At the Physical (PHY) layer, IEEE 802.11 defines three physical techniques for wireless local area networks: diffused infrared (IR), frequency hopping spread spectrum (FH or FHSS) and direct sequence spread spectrum (DS or DSSS). While the infrared technique operates at the baseband, the other two radio-based techniques operate at the 2.4 GHz band. They can be used for operating wireless LAN devices without the need for end-user licenses. In order for wireless devices to be interoperable, they have to conform to the same PHY standard. All three techniques specify support for 1 Mbps and 2 Mbps data rates.

Photonic Wireless Transmission - Diffused Infrared (IR). The only implementation of these types of LANs use infra-red light transmission. Photonic wireless LANs use the 850 to 950 Nm band of infra-red light with a peak power of 2 Watts. The physical layer supports 1 and 2 Mbps data rates. Although

photonic wireless systems potentially offer higher transmission rates than RF based systems, they also have some distinct limitations.

- First, infra-red light like visible light, is restricted to *line of sight* operations. However, the use of diffuse propagation can reduce this restriction by allowing the beam to bounce off passive reflective surfaces.
- Second, the power output (2 Watts) is so low to reduce damage to the human eye, that transmissions are limited to about 25 metres.
- Finally, sensors (receivers) need to be laid out accurately, otherwise the signal may not be picked up.

Photonic-based wireless LANs are inherently secure and are immune (as are optical fiber networks) from electromagnetic radiation which can interfere with cable and RF based systems.

Diffused Infrared (IR). IR communications are described as both indirect and non-line-of sight. The diffused infrared signal, which is emitted from the transmitter, fills an enclosed area like light and does not require line-of-sight transmission. You can point the infrared adapters at the ceiling or at an angle, and the signal will bounce off your walls and ceiling. Changing the location of the receiver does not disrupt the signal. Many diffused infrared products also offer roaming capabilities, which enables you to connect several access points to the network, then connect your mobile computer to any of these access points or move between them without losing your network connection. Usually IR provides a radius of 25 to 35 feet and a speed of 1 to 2 Mbps.

Spread Spectrum (RF) Transmissions. Spread Spectrum (SS) RF systems are true wireless LANs which use radio frequency (RF wireless) transmission as the physical layer medium. Two major sub-systems exist: Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). DSSS is primarily an inter-building technology, while FHSS is primarily an intra-building technology. The actual technique of spread spectrum transmission was developed by the military in an attempt to reduce jamming and eavesdropping. SS transmission takes a digital signal and expands or *spreads* it so as to make it appear more like random background noise rather than a data signal transmission. Coding takes place either by using frequency shift keying (FSK) or phase shift keying (PSK). Both methods increase the size of the data signal as well as the bandwidth. Although the signal appears *louder* (more bandwidth) and easier to detect, the signal is unintelligible and appears as background noise unless the receiver is tuned to the correct parameters.

Frequency Hopping Spread Spectrum Technology (FHSS). Frequency Hopping Spread Spectrum (FHSS) is analogous to FM radio transmission as the data signal is superimposed on, or carried by, a narrow band carrier that can change frequency. The IEEE 802.11 standard provides 22 *hop patterns* or frequency shifts to choose from in the 2.4GHz ISM band. Each channel is 1MHz and the signal must shift frequency or *hop* at a fixed hop rate (U.S. minimum is 2.5 hops/sec). This technology modulates a radio signal by shifting it from frequency to frequency at near-random intervals. This modulation protects the signal from interference that concentrates around one frequency. To decode the signal, the receiver must know the rate and the sequence of the frequency shifts, thereby providing added security and encryption.

FHSS products can send signals as quickly as 1.2 to 2 Mbps and as far as 620 miles. Increasing the bandwidth (up to 24 Mbps) can be achieved by installing multiple access points on the network. In FS, the 2.4 GHz band is divided into 75 one-MHz sub-channels. In order to minimize the probability that two senders are going to use the same sub-channel simultaneously, frequency-hopping is used to provide

a different hopping pattern for every data exchange. The sender and receiver agree on a hopping pattern, and data is sent over a sequence of sub-channels according to the pattern. FCC regulations require bandwidth up to 1 MHz for every sub-channel which forces the FHSS technique to spread the patterns across the entire 2.4 GHz, resulting in more hops and a high amount of overhead.

Direct Sequence Spread Spectrum (DSSS). Spread spectrum was first developed by the military as a secure wireless technology. It modulates (changes) a radio signal pseudo-randomly so it is difficult to decode. This modulation provides some security, however, because the signal can be sent great distances, you do risk interception. To provide complete security, most spread spectrum products include encryption.

DSSS works by taking a data stream of zeros and ones and modulating it with a second pattern, the *chipping sequence*. The sequence is also known as the Barker code which is an 11-bit sequence (10110111000). The chipping or spreading code is used to generate a redundant bit pattern to be transmitted, and the resulting signal appears as wide band noise to the unintended receiver. One of the advantages of using spreading codes is even if one or more of the bits in the chip are lost during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. The ratio between the data and width of spreading code is called *processing gain.* It is 16 times the width of the spreading code and increases the number of possible patterns to 2^{16} (64k), reducing the chance of cracking the transmission.

The DS signaling technique divides the 2.4 GHz band into 14 twenty-two MHz channels, of which 11 adjacent channels overlap partially and the remaining three do not overlap. Data is sent across one of these 22 MHz channels without hopping to other channels, causing noise on the given channel. To reduce the number of re-transmissions and noise, chipping is used to convert each bit of user data into a series of redundant bit patterns called "chips." The inherent redundancy of each chip, combined with spreading the signal across the 22 MHz channel, provides the error checking and correction functionality to recover the data.

Spread spectrum products are often interoperable because many are based on the IEEE 802.11 standard for wireless networks. DSSS is primarily an inter-building technology, while FHSS, is primarily an intra-building technology. DSSS products can be fast and far reaching.

802.11b – The Next Step

All previously mentioned coding techniques for 802.11 provide a speed of 1 to 2 Mbps, lower than the wide spread IEEE 802.3 standard speed of 10 Mbps. The only technique (with regards to FCC rules) capable of providing higher speed is DSSS which was selected as a standard physical layer technique, supporting 1 to 2 Mbps and two new speeds of 5.5 and 11 Mbps.

The original 802.11 DSSS standard specifies the 11-bit chipping, or *Barker sequence,* to encode all data sent over the air. Each 11-chip sequence represents a single data bit (1 or 0), and is converted to a waveform, called a *symbol,* that can be sent over the air. These symbols are transmitted at a 1 MSps (1 million symbols per second), using a sophisticated technique called *Binary Phase Shift Keying (BPSK) (see http://www.physics.udel.edu/wwwusers/watson/student_projects/scen167/thosguys/psk.html).* In the case of 2 Mbps, a more sophisticated implementation called *Quadrature Phase Shift Keying (QPSK)* is

used (see http://www.ee.byu.edu/ee/class/ee444/simulink/oqpsk/oqpsk.html). It doubles the data rate available in BPSK, via improved efficiency in the use of the radio bandwidth.

To increase the data rate in the 802.11b standard, in 1998, Lucent Technologies and Harris Semiconductor proposed to IEEE a standard called CCK (Complementary Code Keying). Rather than the two 11-bit Barker code, CCK uses a set of 64 eight-bit unique code words, thus up to 6 bits can be represented by any code word (instead of the 1 bit represented by a Barker symbol). As a set, these code words have unique mathematical properties that allow them to be correctly distinguished from one another by a receiver, even in the presence of substantial noise and multi-path interference (e.g., interference caused by receiving multiple radio reflections within a building).

The 5.5 Mbps rate uses CCK to encode 4 bits per carrier, while the 11 Mbps rate encodes 8 bits per carrier. Both speeds use QPSK as the modulation technique and signal at 1.375 MSps. QPSK uses four rotations (0, 90, 180 and 270 degrees) to encode 2 bits of information in the same space as BPSK encodes 1. The trade-off is that you must increase power or decrease range to maintain signal quality. Due to the fact the FCC regulates output power of portable radios to 1 watt EIRP (equivalent isotropically radiated power), range is the only remaining factor that can change. Thus, for 802.11 devices, as you move away from the radio, the radio adapts and uses a less complex (and slower) encoding mechanism to send data, resulting in the higher data rates. Table 1 identifies the differences.

Data Rate	Code Length	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11 (Barker Sequence)	BPSK	1 MSps	1
2 Mbps	11 (Barker Sequence)	QPSK	1 MSps	2
5.5 Mbps	8 (CCK)	QPSK	1.375 MSps	4
11 Mbps	8 (CCK)	QPSK	1.375 MSps	8

Table 1. 802.11b Data Rate Specifications

Sub-layers in the PHY layer

The PHY layer is divided into two sub-layers, called the PLCP (Physical Layer Convergence Protocol) sub-layer and the PMD (Physical Medium Dependent) sub-layer. The PMD is responsible for the encoding. The PLCP presents a common interface for higher-level drivers to write to, and it provides carrier sense and CCA (Clear Channel Assessment), which is the signal the MAC (Media Access Control) layer needs to determine whether the medium is currently in use.

PLCP preamble		PLCP header				Payload
Synchronization	SFD	Signal	Service	Length	HEC	(variable)

Figure 3. IEEE 802.11b DSSS PHY frame format

PLCP Preamble. The PLCP consists of a 144-bit preamble that is used for synchronization to determine radio gain and to establish CCA. This is PHY dependent, and includes:

- **Synch**: A 128-bit sequence of alternating zeros and ones, which is used by the PHY circuitry to select the appropriate antenna (if diversity is used), and to reach steady-state frequency offset correction and synchronization with the received packet timing.
- **SFD**: A Start Frame delimiter which consists of the 16-bit binary pattern 1111001110100000, which is used to define frame timing and mark the start of every frame and is called the SFD (Start Frame Delimiter)..

PLCP Header. The header consist of 48 bits, it is always transmitted at 1 Mbps and contains logical information used by the PHY Layer to decode the frame. It consists of:

- **Signal:** 8 bits which contains only the rate information, encoded in 0.5 Mbps increments from 1 Mbit/s to 4.5 Mbit/s;
- **Service:** 8 bits reserved;
- **Length:** 16 bits and represents the number of bytes contained in the packet (useful for the PHY to correctly detect the end of packet);
- **Header Error Check Field:** 16 Bit CRC of the 48 bit header.

The PLCP introduces 24 bytes of overhead into each wireless Ethernet. Because the 192-bit header payload is transmitted at 1 Mbps, 802.11b reduces the efficiency on the PHY layer by 15%.

The last step – 802.11a

As we have mentioned earlier 802.11b pick for a coding technique is based on DSSS, a technology, developed by the military as a secure wireless technology. This technology works by modulating (changing) a radio signal pseudo-randomly so that it is difficult to decode. This modulation provides some security; however, because the signal can be sent great distances, you do risk interception. To provide complete security, most spread spectrum products include encryption. Spread spectrum products are often interoperable because many are based on the proposed IEEE 802.11 standard for wireless networks. Direct sequence spread spectrum is primarily an inter-building technology, while frequency hopping spread spectrum, on the other hand, is primarily an intra-building technology.

Unlike 802.11b, 802.11a was designed to operate in the more recently allocated 5-GHz UNII (Unlicensed National Information Infrastructure) band. Unlike ISM band, which offers about 83 MHz in the 2.4 GHz spectrum, IEEE 802.11a utilizes almost four times that of the ISM band, because UNII band offers 300 MHz of relatively free of interference spectrum. And unlike 802.11b, the 802.11a standard is using a **frequency division multiplexing** technique, which is expected to be more efficient in inter-building environments. As previously mentioned, the FCC has allocated 300 MHz of spectrum for UNII in the 5-GHz block, 200 MHz of which is at 5,150 MHz to 5,350 MHz, with the other 100 MHz at 5,725 MHz to 5,825 MHz. The first advantage of the 802.11a before 802.11b is that the standard operates in 5.4 GHz spectrum, which gives it the performance advantage of the high frequencies. But frequency, radiated power and distance together are in an inverse relationship, so moving up to the 5-GHz spectrum from 2.4 GHz leads to shorter distances and/or requirements for more power. That is why the 802.11a Standard increases the EIRP to the maximum 50 mW. The 5.4 GHz, spectrum is split into three working "domains" and every domain has restrictions for maximum power.

The second advantage lies on the coding technique, 802.11a is using. The 802.11a uses an encoding scheme, called COFDM or OFDM (coded orthogonal frequency division multiplexing) http://www.cclinf.polito.it/~s83797/cofdm.htm. Each sub-channel in the COFDM implementation is about 300 KHz wide. COFDM works by breaking one high-speed data carrier into several lower-speed sub-carriers, which are then transmitted in parallel. Each high-speed carrier is 20 MHz wide and is broken up into 52 sub-channels, each approximately 300 KHz wide. COFDM uses 48 of these sub-channels for data, while the remaining four are used for error correction. COFDM delivers higher data rates and a high degree of signal recovery, thanks to its encoding scheme and error correction. Each sub-channel in the COFDM implementation is about 300 KHz wide. To encode 125 Kbps, well-known BPSK is used, yielding a 6,000-Kbps, or 6 Mbps, data rate. Using QPSK, it is possible to encode up to 250 Kbps per channel, which combined achieves 12-Mbps data rate. And by using 16-level quadrature amplitude modulation encoding 4 bits per hertz, and achieving data rate of 24 Mbps, the Standard defines basic speeds of 6,12 and 24 Mbps, which every 802.11a-compliant products must support. Data rates of 54 Mbps are achieved by using 64QAM (64-level quadrature amplitude modulation), which yields 8 bits/10 bits per cycle, and a total of up to 1.125 Mbps per 300-KHz channel. With 48 channels, this results in a 54-Mbps data rate. On February 15, 2001 Cisco Systems completed its acquisition of Radiata Incorporated, a company, supporting the standard speeds and 36Mbps, 48Mbps and 54 Mbps as well. The maximum theoretical data rate of COFDM is considered 108 Mbps.

IEEE 802.11, 802.11b and 802.11a MAC Layer

802.11 MAC Layer Services

The MAC layer provides various services to manage authentication, de-authentication, privacy and data transfer.

Authentication. The authentication service is the process of proving client identity which takes place prior to a wireless client associating with an AP. By default, IEEE 802.11 devices operate in an Open System, where essentially any wireless client can associate with an AP without checking credentials. True authentication is possible with the use of the 802.11 option known as *Wired Equivalent Privacy* or WEP, where a shared key is configured into the AP and its wireless clients. Only those devices with a valid shared key will be allowed to be associated to the AP.

De-authentication. The de-authentication function is performed by the base station. It is a process of denying client credentials, based on incorrect authentication settings, or applied IP or MAC filters.

Association. The association service enables the establishment of wireless links between wireless clients and APs in infrastructure networks.

Disassociation. The service which cancels the wireless links between wireless clients and APs in infrastructure networks.

Re-association. The re-association service occurs in addition to association when a wireless client moves from one BSS to another. Two adjoining BSSs form an ESS if they are defined by a common ESSID, providing a wireless client with the capability to roam from one area to another. Although re-

association is specified in 802.11, the mechanism that allows AP-to-AP coordination to handle roaming is not specified.

Privacy. By default, data is transferred in the clear allowing any 802.11-compliant device to potentially eavesdrop on similar PHY 802.11 traffic within range. The WEP option encrypts data before it is sent wirelessly, using a 40-bit encryption algorithm known as RC4. The same shared key used in authentication is used to encrypt or decrypt the data, allowing only wireless clients with the exact shared key to correctly decipher the data.

Data transfer. The primary service of MAC layer is to provide frame exchange between MAC layers. Wireless clients use a Collision Sense Multiple Access with Collision Avoidance (CSMA/CA) algorithm as the media access scheme.

Distribution. The distribution function is performed by DS and it is used in special cases in frame transmission between APs.

Integration. This is a function performed by the *portal*, where essentially the portal is design to provide logical integration between existing wired LANs and 802.11 LANs.

Power management. IEEE 802.11 defines two power modes: an *active* mode, where a wireless client is powered to transmit and receive; and, a power save mode, where a client is not able to transmit or receive, consuming less power. Actual power consumption is not defined and is dependent upon the implementation.

Collision Sense Multiple Access with Collision Detection

The classic (CSMA/CD) method is a very effective mechanism in a wired environment, enabling speeds of 10 (T-base), 100 (Fast-Ethernet), or 1000 (Gigabit-Ethernet). However, this mechanism immanently allows conflicts (collisions) and supports exponential backoff mechanism, reducing the throughput in a very competitive environment with a high number of active users. Collision levels of 30-40 %, even less, could cause a very significant degradation of the overall performance of the active users [2], [3 see http://eman.cisco.com/NETWORKING/tech_ref/access_capacity_planning.pdf**].** On the other hand, the backoff algorithm could defer the transition of the data for up to 367 ms in the 10Mbps networks. Therefore, the CSMA/CD mechanism creates an opportunistic discipline to access the common media and makes the response time a predictable value for at least a "not worst than" scenario.

Creating a mechanism to prevent the potential conflicts in the shared medium has always been a challenge for Network Designers. A set of different proposals and drafts are available, initially for the wired and lately for wireless environments, based on so-called collision avoidance techniques. The basic idea is to negotiate the data exchange before the collision happens [4], or to force the non-active users to defer their translation for a period of time. The first approach provides additional mechanisms for reducing the collision-based delays, allowing collision on the negotiating stage and providing collision-free data transfer thereafter. The second approach is based on handshaking procedures, timeslots or polling techniques. Both approaches deal with early and late collisions, as well as adjacent and far-end active stations. However, unlike wired networks, CSMA/CD cannot be implemented for WLANs for two obvious reasons. First, in CSMA/CD, one of the basic suggestions is all stations hear each other, unlike WLAN, where this cannot be guaranteed. There is a "hidden station" effect where the

station hears the AP, but does not hear all other members of the cell. Secondly, it is not possible to both transmit and receive on the same channel using radio transceivers, unless we use a full duplex radio which could increase the price significantly.

Collision Sense Multiple Access with Collision Avoidance

Collision avoidance mechanisms are related more to deterministic type of networks, making the response time predictable. They are a "hybrid" media access technique. The system is stable at overload conditions (*See Figure 3)* and supports traffic burst characteristics [1] (see *Figure 4).* The trade-off for collision avoidance mechanism's more predictable response time is the speed, where 1, 2, 5 and 11 Mpbs are typical due to strong timing restrictions and the frame header overhead. However, the frame header provides the necessary frame formats to support the access mechanism.

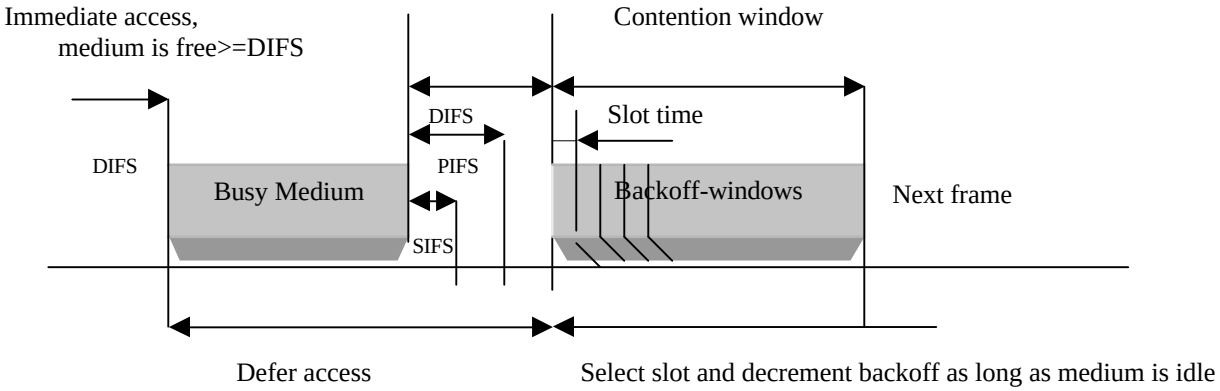


Figure 3: 802.11 Collision avoidance mechanism.

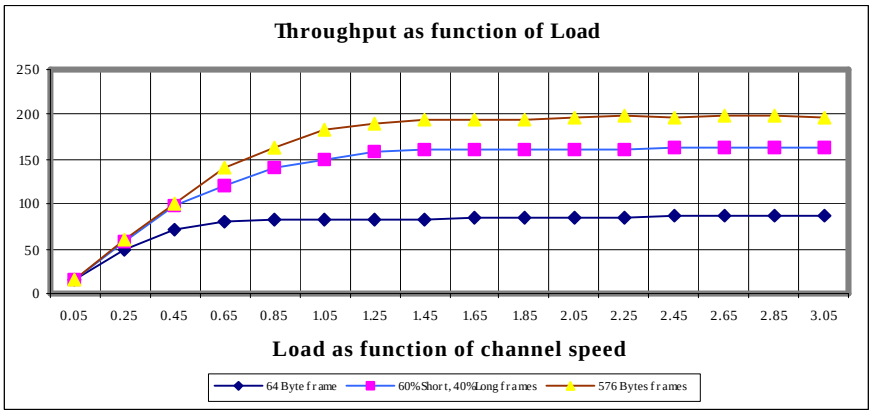


Figure 4. Throughput efficiency in IEEE 802.11.

At the MAC layer, the 802.11 standard for CSMA/CA defines two different access methods: the Distributed Coordination Function (DCF) and the Optional Point Coordination Function (PCF).

Optional Point Coordination Function (PCF). Point Coordination Function is used to implement time-critical services, like voice or video transmission. PCF is optional and it is a provision in 802.11 to ensure contention free service. In PCF, a single AP controls access to the media and a point coordinator resides in the AP. If a BSS is set up with PCF enabled, time is spliced between the system being in PCF

mode and in DCF mode, which is a classical time-sharing technique with a central coordinator. During the periods when the system is in PCF mode, the access point will poll each station for data, and after a given time move on to the next station, providing a guaranteed maximum latency. Due to this approach, the PCF is provides lower transfer delay, essentially excluding the possible collision control. No station is allowed to transmit unless it is polled, and stations receive data from the access point only when they are polled. By using this higher priority access, the AP issues polling requests to the stations for data transmission.

A limitation of PCF is it is not particularly scalable due to the fact a single AP needs to have control of media access and must poll all stations which can be ineffective in large networks. The PCF is especially utilized for asynchronous data, voice and mixed applications (voice, data, video) and allows contention and contention free mechanisms to co-exist, by alternating the *Contention Free Contention Free* and *Contention Contention* operation under PCF control. The Network Allocation Vector (NAV) is used to prevent *Contention* traffic until the last PCF transfer resets the function using "Reset NAV" in the last (CF_End) frame from the AP.

Distributed Coordination Function (DCF). Distributed Coordination Function in 802.11 is based on a CSMA/CA mechanism. DCF works by a station willing to transmit data, senses the medium first. If the medium is busy, then the station defers its transmission to a later time, but if the medium is free for a specified time (called Distributed Inter Frame Space (DIFS)), the station transmits. The receiving station then checks the CRC of the received packet and sends an acknowledgement (ACK) packet. This receipt indicates to the transmitting station that there were no collisions detected. If the sender does not receive ACK, then it re-transmits the last fragment.

In this class of opportunistic protocols, the central question is "how to deal with possible collisions"? In 802.3, the transmitting station recognizes the collision and goes to re-transmission phase based on an *exponential random backoff* algorithm.

The "Hidden Station" challenge

The "hidden station" affect is a typical WLAN situation, where the stations don't hear each other, but they hear AP.

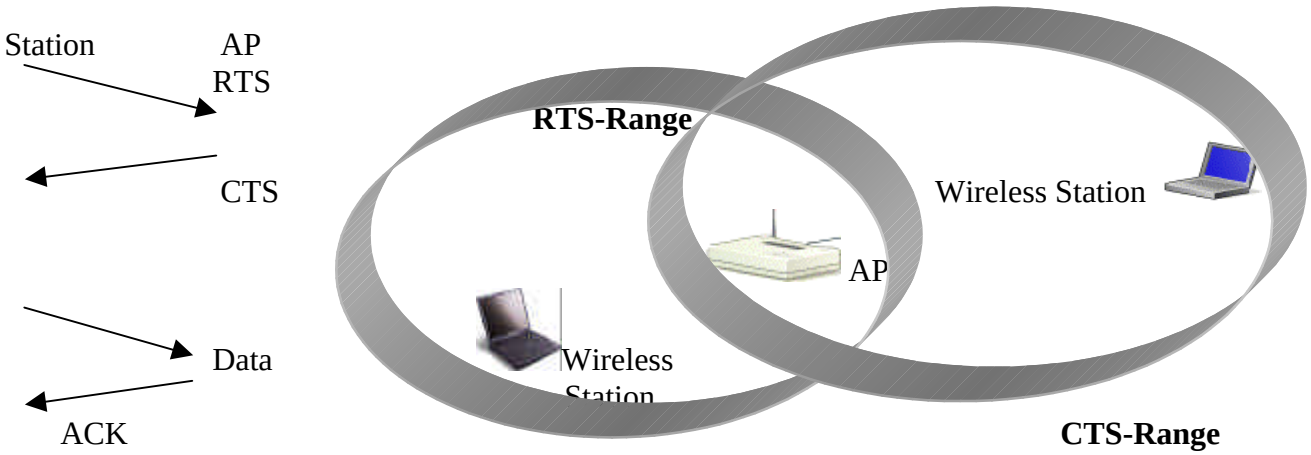


Figure 5. Hidden Station challenge

The effect of the hidden station could cause a collision at any stage of the transmit-receive process. To reduce the probability of two stations colliding, the standard defines a Virtual Carrier Sense mechanism.

Virtual Carrier Sense. A station waiting to transmit a packet will first transmit a short control packet called Request To Send (RTS) which includes the source, destination and the duration of the following transaction (the packet and the respective ACK). If the medium is free, the destination station responds with a response control packet called Clear To Send (CTS) which includes the same duration information. All stations receiving either RTS and/or CTS, set their Virtual Carrier Sense indicator (called NAV, for Network Allocation Vector), for the given duration and use this information together with the Physical Carrier Sense when sensing the medium. The mechanism reduces the probability of a collision on the receiver area by a station that is "hidden" from the transmitter to the short duration of the RTS transmission because the station hears the CTS and "reserves" the medium as busy until the end of the transmission.

The duration information on the RTS also protects the transmitter area from collision during the ACK potentially caused from stations that are out of range of the acknowledgment station. Due the short frames of RTS and CTS, the method also reduces the overhead of collisions. If the packet is significantly bigger than the RTS, the packets can be transmitted without the RTS/CTS transaction. The station controls the process by *RTS Threshold* setting**.** The transmitting node or **A** (see *Figure 5),* sends an RTS request to the AP requesting to reserve a fixed amount of time necessary to transmit a frame of given length. When the medium is available, the AP broadcasts a CTS message that all stations can hear and **B** has the requested amount of air time.

RTS Threshold feature increases available bandwidth by eliminating RTS/CTS traffic from the air, thus reducing the cost. By setting *RTS length threshold* to a maximum value, the transmitter will effectively never use RTS and the option is virtually switched off. One example is shown in *Figure 6.* If the hidden station is a non-issue, the threshold can be switched off. If a user decides to switch it on by setting some threshold, there is always a trade off between introducing more overhead and reducing retransmission of messages due to the hidden node problem. The situation in which the RTS/CTS is very helpful is the outdoor point-to-multi-point environment in which the hidden node problem can be a larger problem.
The following diagram shows how the RTS/CTS mechanism works for **A** as a transmitter (or T.Station), **B** as a receiver (or R.Station) and the NAV settings for their neighbors.

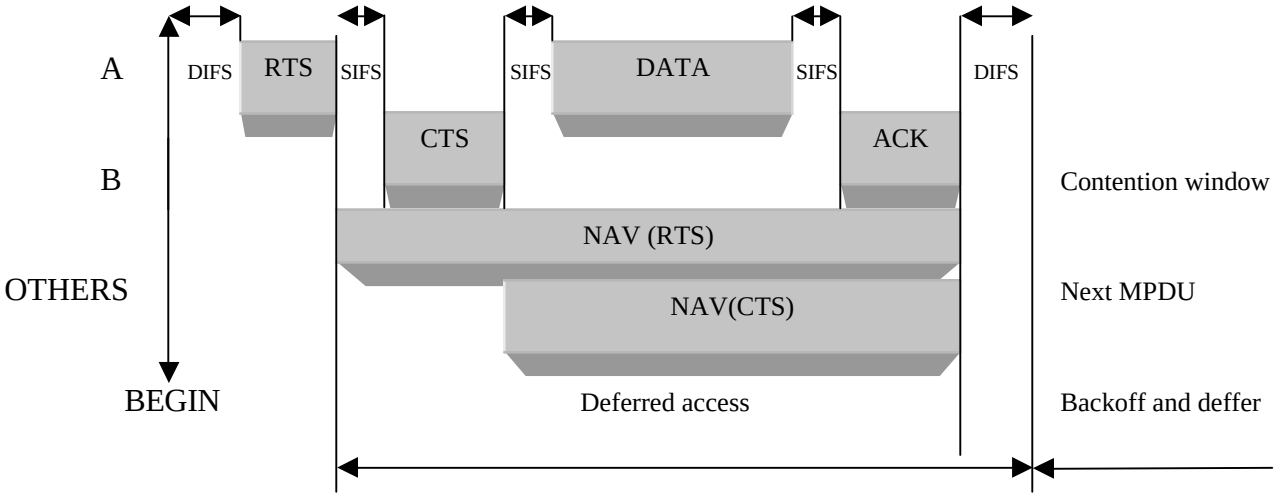


Figure 5. The NAV state is combined with the physical carrier sense to indicate the busy medium.

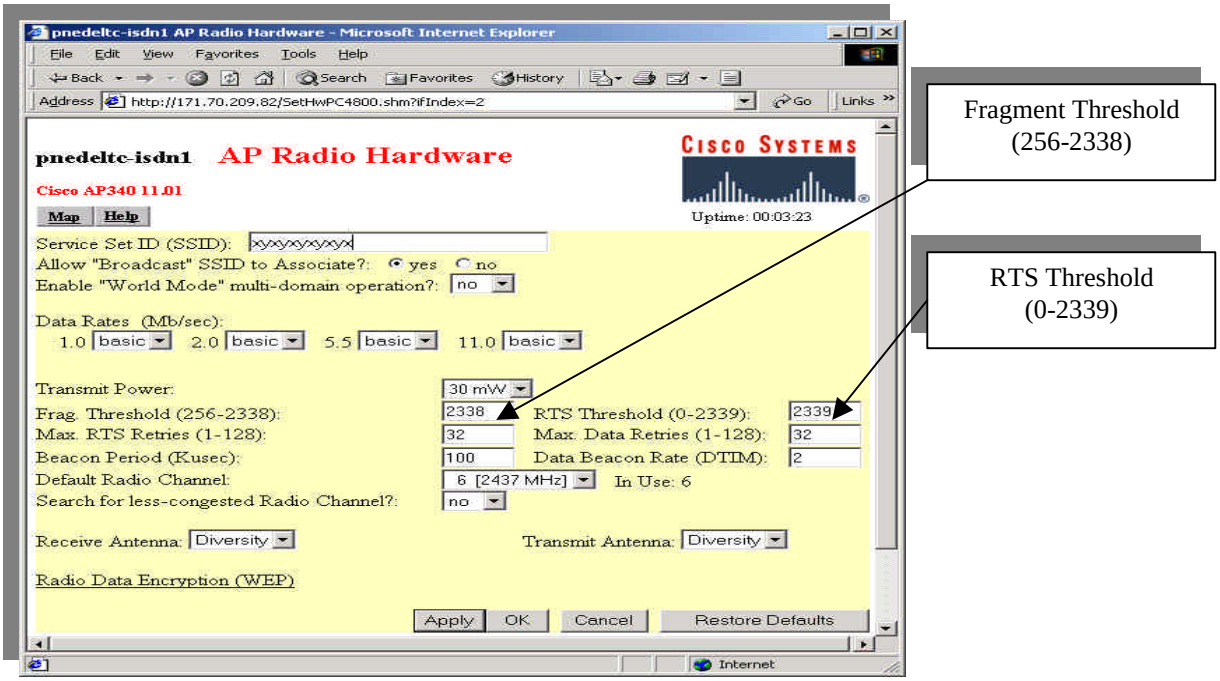


Figure 6. RTS Threshold settings on Cisco AP340, ver. 11.01

MAC Level Acknowledgements

The typical Ethernet packets are several hundred bytes long, with the longest Ethernet packet up to 1518 bytes. It is better to use smaller packets in a wireless LAN environment and the following reasons explain why this is true.

1. Due to the higher Bit Error Rate of a radio link, the probability of a packet getting corrupted increases with the packet size.
2. In the case of packet corruption, the smaller the packet, the less overhead to retransmit.
3. On a FHSS, the medium is interrupted periodically (for 20 ms) for hopping, so the smaller the packet, the smaller the chance the transmission will be postponed.

However, it does not make sense to introduce a protocol dealing only with small packets, so a simple fragmentation/reassembly mechanism is added to the MAC layer. The mechanism is a simple Send-and-Wait algorithm, where the transmitting station is not allowed to transmit a new fragment until one of the following happens: it receives an ACK for the send fragment, or it decides that the fragment was retransmitted too many times and drops the whole frame. The standard does allow the station to transmit to a different address between retransmissions of a given segment. This is useful when the AP has several outstanding packets to different destinations and one of them does not respond.

The standard defines 4 types of inter frame spaces to provide different priorities:

1. Short Inter Frame Space (SIFS) is used to separate transmissions belonging to the single dialog (Fragment-ACK) and it is the minimum inter frame space. There is, at most, one single station to transmit at any given time, therefore giving it priority over all other stations. This value for 802.11 PHY is fixed to 28 ms, time enough for the transmitting station to be able to switch back to receive mode and be capable of decoding the incoming packet.
2. Point Coordination IFS (PIFS) is used by the Access Point (or Point Coordinator) to gain an access over the medium before any other station. The value is SIFS + Slot Time, i.e. 78 ms.
3. Distributed IFS (DIFS) is the inter frame space used for a station willing to start a new transmission, which is calculated as PIFS plus one slot time, i.e. 128 ms.

4. Extended IFS (EIFS) which is a longer IFS used by a station that has received a packet that could not understand. This is needed to prevent the station from colliding with a future packet, belonging to the current dialog.

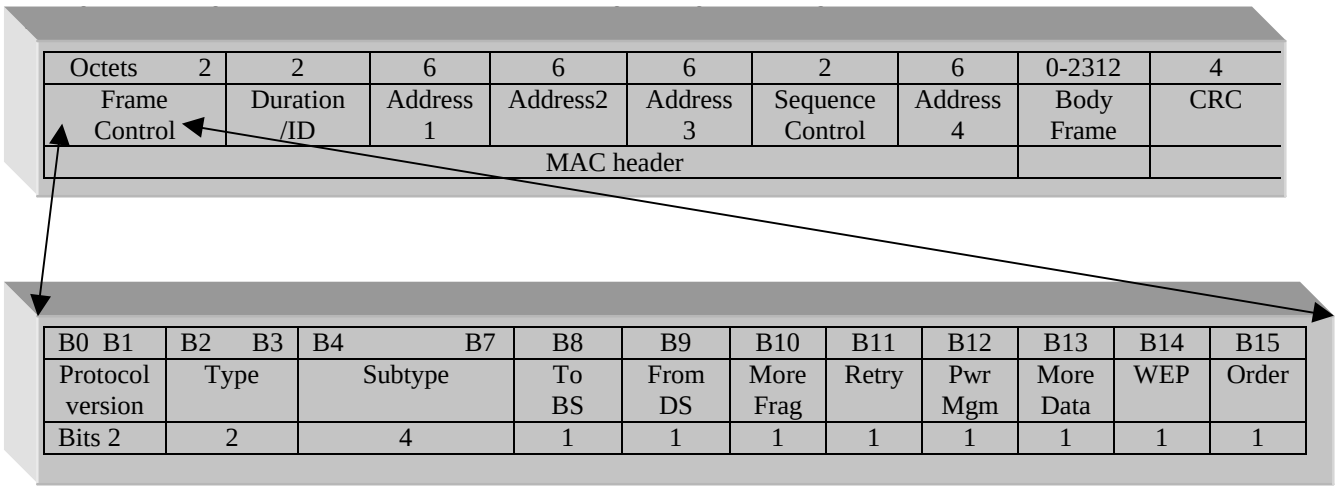
Extended Backoff Algorithm

Backoff is a well-know method used to resolve contention between different stations waiting to access the media [2]. This method requires each station to choose a random number (n) between 0 and a given number (16 for 802.3), and weight this number X *slot times*. The slot time is defined as a way a station will always be capable of determining if another station has accessed the medium at the beginning of the previous slot. It reduces the collision probability by half. Each station listens to the network, and the first station to finish its allocated number of slot times begins the transmission. If any other station hears the first station talk, it stops counting down its back-off timer. When the network is idle again, it resumes the countdown. In addition to the basic back-off algorithm, 802.11 adds a back-off timer that ensures fairness. Each node starts a random back-off timer when waiting for the contention window. This timer ticks down to zero while waiting in the contention window. Each node gets a new random timer when it wants to transmit. This timer isn't reset until the node has transmitted. The 802.11 standard defines an e*xponential backoff algorithm* which must be executed in the following cases: when the station senses the medium before the first transmission of the packet, and the medium is busy; after each retransmission; and, after a successful transmission. The only case when this mechanism is not used, is when the station decides to transmit a new packet and the medium has been free for more than DIFS.

Frame Types

There are three main types of frames used in the MAC layer: data, control and management. Data frames are used for data transmission. Control Frames are used to control access to the medium (e.g. RTS, CTS, and ACK). Management Frames are transmitted the same manner as data frames to exchange management information, but are not forwarded to upper layers (e.g. beacon frames). Each frame type is subdivided into different subtypes according to their specific function.

MAC Frame Formats



Octets 2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration /ID	Address 1	Address2	Address 3	Sequence Control	Address 4	Body Frame	CRC
MAC header								

B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B12	B13	B14	B15
Protocol version	Type	Subtype	To BS	From DS	More Frag	Retry	Pwr Mgm	More Data	WEP	Order
Bits 2	2	4	1	1	1	1	1	1	1	1

Figure 7. MAC sub-layer frame format

MAC Layer for 802.11a

The 802.11a standard uses the same MAC functions as 802.11b, therefore, inheriting the MAC format from 802.11 to 802.11a technology will not have a significant impact on network operations [5 http://www.networkcomputing.com/1201/1201ws1.html]. However, a well-known drawback of 802.11 MAC format is while PHY layer is gaining from increased power and a new coding scheme, MAC format is reducing the effect due to significant overhead, caused by the objective and design to provide a collision-free and efficient environment. Inheriting the 802.11b MAC inefficiency, the 802.11a's expected rates are in the range of 38 Mbps, even for 54 Mbps. Unlike 802.11b, 80211a does not require headers to be transmitted at 1 Mbps, which theoretically could increase the expected throughput efficiency by 15%.

802.11 Security

Wireless LANs transmit signals over much larger areas than those of wired media, such as twisted-pair, coaxial cable, or optical fiber. Therefore, WLANs have a much larger area to protect. There is significant regulatory and standards progress in the area of wireless security conducted by the 802.11 and IEEE 802.10 standards committees who are responsible for developing security mechanisms for all 802 series LANs. As a result of their coordinated work, IEEE 802.11 provides a mechanism for authentication and encryption.

An IEEE 802.11 wireless station will not process data over the wireless network unless its network ID, also called a *Basic Service Set Identification* (SSID), is the same as other stations on the network. Sent in every 802.11 data packet, the network ID is a six-byte code word that distinguishes one WLAN from another. APs check the network ID when each station initiates a connection to the network and if the ID doesn't match the one stored in the access point, then the station cannot establish a connection to the WLAN. Thus, an intruder must obtain the network ID necessary to join the network. With the correct network ID, someone could configure a portable computer with an appropriate radio card and gain access to the WLAN, unless the servers and applications require a username and password.

Another level of security is the 802.11's *Wireless Equivalent Privacy* (WEP) protocol. Most WLAN vendors offer WEP as an option for their standard radio cards and access points. Because wireless is a shared medium, everything transmitted or received over a wireless network can be intercepted. Encryption and authentication are always considered when developing a wireless networking system. The goal of adding these security features is to make wireless traffic as secure as wired traffic. The IEEE 802.11b standard provides a mechanism to do this by encrypting the traffic and authenticating nodes via the WEP protocol. *Cisco WEP* is a hardware based symmetric encryption mechanism that only reduces the overall performance by 2-3%.

A WEP feature called *shared key authentication*, ensures only authorized stations can access the WLAN. Shared key authentication operates as follows (see *Figure 8).*

1. A station requesting 802.11 service sends an authentication frame to another station.
2. When a station receives the initial authentication frame, the station replies with an authentication frame containing 40/128 octets of challenge text.
3. The requesting station copies the challenge text into an authentication frame, encrypts it with a shared key using the WEP service, and sends the frame to the responding station.

4. The receiving station decrypts the challenge text using the same shared key and compares it to the challenge text sent earlier. If they match, the receiving station replies with an authentication acknowledgement. If not, the station sends a negative authentication notice.

Another way to compromise a wireless LAN is to use specialized equipment to capture information bits sent over the air, decode them, and read the contents of email, files, or financial transactions. This doesn't necessarily require the network ID because the monitoring equipment doesn't need to establish a connection to the wireless LAN. The equipment passively listens to the transmissions as they propagate through the air. However, this action does require the proper monitoring equipment to correctly demodulate the received spread spectrum signal.

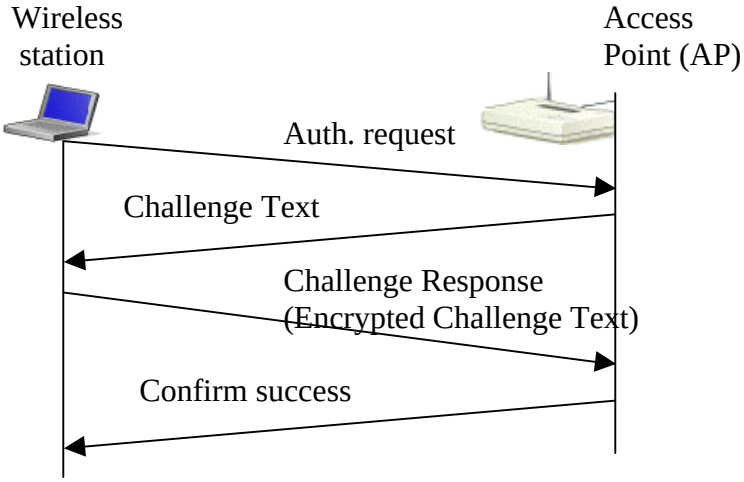


Figure 8. Shared key authentication

This security problem also exists with wired Ethernet networks but to a lesser degree. Current flow through the wires emits electromagnetic waves that can be received with sensitive listening equipment known as a sniffer. This method usually requires the intruder to be within the physical boundaries of the company.

To avoid this problem on the wireless LAN, use WEP to encrypt transmissions between stations to avoid disclosure to eavesdroppers. WEP uses the RC4 encryption engine and a 40-bit key. Stations can also utilize WEP without authentication services but the security recommendation is to implement both WEP and authentication to minimize vulnerability to packet snooping.

Whenever encryption and authentication are implemented in any system, three things must be considered: the customer's need to privacy, easy of use and government regulations.
The RC4 WEP protocol, used in 802.11b is an attempt to balance all the above-mentioned considerations. The RC4 encryption algorithm is a symmetric stream cipher that supports a variable length key. The WEP 40-bit encryption built into 802.11b WLANs should be sufficient for most applications, however, the weak part of this mechanism is the static key mechanism used by the WEP.

The Cisco WLAN security solution allows open, shared key and network-EAP authentication types, and 40 or 128 bits key size [6 http://wwwin.cisco.com/cmc/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm] and [7]. WLAN security needs to be integrated into an overall network security strategy. In particular, a user may implement network layer encryption such as IPSec across both wired and wireless portions of

the network, eliminating the need to have 802.11 security in place. Another alternative for customers is to choose to have critical applications encrypt their own data, thereby ensuring all network data such as IP and MAC addresses are encrypted along with the data payload.

Other access control techniques are available in addition to the 802.11 WEP authentication technique. Some vendors provide a table of MAC addresses in an *Access Control List* to be included in the access point, restricting access to clients whose MAC addresses are on the list. Clients can then be explicitly included (or excluded) at will.

Due to different factors, including government regulations, WEP is designed for moderate, but not strong security. There are known [8 http://www.niksula.cs.hut.fi/~mkomu/docs/wirelesslansec.html] and unknown [9 http://www.commweb.com/article/COM20010206S0001] issues with WEP. The official position of the 802.11 Security Group is "WEP is not intended to be a complete security solution, but, just as with physical security in the wired LAN case, should be supplemented with additional security mechanisms such as access control, end-to-end encryption, password protections, authentication, virtual private networks, and firewalls, whenever the value of the data being protected justifies such concern. The IEEE 802.11 working group is currently developing an extension to WEP which will be incorporated in a future version of the standard. Any IEEE 802.11 installation where data privacy is a concern should use WEP". See http://slashdot.org/articles/01/02/15/1745204.shtml.

Roaming Approach, Association and Mobility

The 802.11 MAC layer is responsible for how a client associates with an access point. The standard includes mechanisms to allow a client to roam among multiple APs that can be operating on the same or separate channels. Each AP transmits a beacon signal which includes a time stamp for client synchronization, a traffic indication map, an indication of supported data rates, and other parameters. Roaming clients use the beacon to gauge the strength of their existing connection to an AP. If the connection is considered weak, the roaming station can attempt to associate itself with a new AP. The roaming station first performs a scanning function to locate a new AP on the same or different channel. If the station decides that link to its current AP is poor, the station uses a scanning function to find another AP or uses information from previous scans.

The specific actions which occur as a user roams from one AP to another is as follows.

1. The station sends a re-association request to a new AP.
2. If the re-association response is successful, then station has roamed to the new AP otherwise, the station scans for another AP.
3. If AP accepts a re-association request, the AP indicates re-association to the Distribution System, the DS information is updated, and the old AP is notified through the DS.

Re-association usually occurs because the wireless station has physically moved away from the original access point, causing the signal to weaken. In other cases, re-association occurs due to a change in radio characteristics in the building, or due simply to high network traffic on the original access point. High network traffic causes re-association which also performs a "load balancing" function. This process of dynamically associating and re-associating with APs allows a customer to set up WLANs with very broad coverage by creating a series of overlapping 802.11b cells throughout a building or across a campus.

Power Management

Most LAN NICs are available in PCMCIA Type II format, thus portable and mobile handheld computing equipment can be connected to the corporate network via a wireless connection. Although the problem in most cases, is these devices must rely on batteries to power the electronics. In addition to controlling media access, the 802.11 HR MAC supports power conservation to extend the battery life of portable devices. This technique enable wireless NICs to switch to lower-power standby modes periodically when not transmitting, reducing the drain on the battery.

The standard supports two power-utilization modes, called *Continuous Aware Mode* and *Power Save Polling Mode*. The MAC layer implements power management functions by putting the radio to sleep (i.e. lowering the power drain) when no transmission activity occurs for some specific or user-defined time period. Although, a resulting problem is a sleeping station can miss critical data transmissions. 802.11 solves this problem by incorporating buffers to queue messages. The standard calls for sleeping stations to awaken periodically and retrieve any applicable messages. The client radio will wake up periodically in time to receive regular *beacon* signals from the access point. The beacon includes information regarding which stations have traffic waiting for them, and the client can thus awake upon beacon notification and receive its data, returning to sleep afterward.

Known Issues and Development Directions

Roaming Techniques

802.11b defines how a station associates with APs, it does not define how APs track users as they roam about, either at Layer 2 between two APs on the same subnet, or at Layer 3 when the user crosses a router boundary between subnets. The first issue is handled by vendor-specific inter-AP protocols (IAPP), which vary in performance http://www.ieee802.org/11/. If the protocol is not efficient, there is a chance of packets being lost as the user roams from access point to access point. It is expected the WECA and the IEEE will create standards in this area.

An incomplete but useful alternative to the Layer 3 roaming problem is to implement the *Dynamic Host Configuration Protocol* (DHCP) across the network. DHCP allows any users who shut down or suspend their portable computer before crossing to a new network to automatically obtain a new IP address upon resuming or turning on their notebook. DHCP (RFC 1531) enables hosts on a network to boot up and send a DHCP (BOOTP) request to a broadcast address in order to gain an IP address for its use.

Cisco's IOS provides an innovative *local-area mobility* (LAM). LAM is a mechanism intended to be a solution for mobility needs within an enterprise environment where DHCP is not available, or the hosts don't have the new software implemented. LAM technology enables statically addressed hosts/PCs to move from their local subnet to another location within an enterprise network while maintaining transparent connectivity without any software changes on the host; upgrading the concept of "transparent bridging" to "transparent routing" [10 http://wwwin.cisco.com/cmc/cc/pd/iosw/ioft/lam/tech/lamso_wp.htm].

The second issue is related to the Layer 3 roaming mechanisms. The most popular of these is Mobile IP, which is currently known as RFC 2002 in the Internet Engineering Task Force (IETF). As Mobile IP is

not finalized, Cisco's Mobile IP concept which supports RFC 2002, 2003 and 2006 offers the most complex solution in environments where a wireless technology is being utilized [12 http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.htm#xtocid224992]. This includes cellular environments as well as wireless LAN situations that may require roaming. Mobile IP works by having an access point assigned as the "home agent" for each user. Once a wireless station leaves the home area and enters a new area, the new access point queries the station for its home agent. Once it has been located, the packet forwarding is established automatically between the two access points to ensure the user's IP address is preserved and the user can transparently exchange data.

Wireless Device Interoperability in 802.11

Standardization and interoperability among devices utilizing the same PHY is the intent of the IEEE 802.11 specification. At the physical level, the three modulation schemes are incompatible with each other, so an infrared wireless client will not synchronize to a DSSS AP. However, even among devices with the same PHY, a few key ingredients are necessary to achieve multi-vendor interoperability but are absent from the current ratified standard. Examples of these limitations are as follows:

1. The standard does not specify the handoff mechanism to allow clients to roam from one AP to another.
2. The standard does not state how an AP addresses data framing between the wired and the wireless media.
3. There is no conformance test suite specified to verify that a device is compliant with the IEEE 802.11 specification. Vendor claims for compliance to the 802.11 standard should be ratified by a neutral third party.

Safety

All WLANs must meet stringent government and industry standards for safety. Yet, there are concerns raised across a number of wireless technology industries, regarding the health risks of wireless use. To date, scientific studies have been unable to attribute adverse health effects to WLAN transmissions. The output power of WLAN is already limited by FCC regulations to under 100 mW (2 and 30 mW in Cisco's Aironet 340/350 Series product), much less than that of a mobile phone. It is expected that any health effects related to radio transmissions would be correlated to power and physical proximity to the transmitter.

Conclusion

The history of CSMA and CSMA/CD demonstrate the designers are always able to overcome the speed restrictions, creating more sophisticated and faster PHY techniques. While the limited throughput has been the most critical issue for WLANs, a very competitive 22 Mbps is expected soon. Moving from the most popular 900 MHz band, typical for early WLAN applications, to the unlicensed 2.4 GHz, is just a step to the 5.7 GHz band. The IEEE's specification 802.11a for equipment operating at 5-GHz supports up to a 54-Mbps rate, and soon we will witness the breakthrough of the 100 MBps barrier. Integrating the wireless ports and interfaces in Cisco's LAN switches and low-end and even middle-

range routers, suitable for SOHO and ROBO environment, is a logical next step for providing a cost effective and robust solution to meet the needs of high growth mobile enterprises.

Glossary

AP-access point
BPSK - Binary Phase Shift Keying
BSS - Basic Service Set
CCK-Complementary Code Keying
COFDM or OFDM (coded orthogonal frequency division multiplexing)
CRC - cyclic redundancy check
CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD - Carrier Sense Multiple Access with Collision Detection
CTS - Clear to Send
DCF - Distribution Coordination Function
DHCP - Dynamic Host Configuration Protocol
DS - distribution system
DSSS - direct sequence spread spectrum
ESS - Extended Service Set
FCC - Federal Communications Commission (USA)
FHSS - Frequency Hopping Spread Spectrum
IBSS - Independent Basic Service Set
IEEE - Institute of Electrical and Electronics Engineers
IETF - Internet Engineering Task Force
IP - Internet Protocol
IPSec - Internet Protocol security
ISM - Industry, Scientific, and Medical
ISO - International Organization for Standardization
LLC - Logical Link Control
MAC - Media Access Control
MIB - management information base
NIC - network interface card
NOS - network operating system
PCF - Point Coordination Function
PCI - Peripheral Component Interconnect
QPSK - Quadrature Phase Shift Keying
RC4 - Ron's Code or Rivest's Cipher
RTS - Request to Send
SNMP - Simple Network Management Protocol
TCP/IP - Transmission Control Protocol/Internet Protocol
WECA - Wireless Ethernet Compatibility Alliance
WEP - Wired Equivalent Privacy
WLAN - wireless local area network
WLANA - Wireless LAN Alliance

References

[1] Hayes Vic, Tutorial on 802.11 to 802, http://grouper.ieee.org/groups/802/11/Tutorial/MAC.pdf

[2] J. Blommers, “Practical Planning for Network Growth”, Prentice Hall PTR&HP, 1996

[3] P. Nedeltchev, Network Capacity planning in SOHO, Global RA Conference, San Jose, April’00 http://eman.cisco.com/NETWORKING/tech_ref/access_capacity_planning.pdf16

[4] P. Nedeltchev, Throughput efficiency of Network Adapter with Collision Avoidance as a M/G/1 model, 40th anniversary of VNVAU, Shumen, Bulgaria,1988.

[5] J. Conover, “80211a: Making Space for Speed”, Network Computing, January 8, 2001. http://www.networkcomputing.com/1201/1201ws1.html

[6] Wireless LAN Security, http://wwwin.cisco.com/cmc/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

[7] M. Andrade, Security for Next Generation, Wireless LANs ver.1.1. http://wwwin.cisco.com/cmc/cc/pd/witc/ao340ap/prodlit/wlanw_in.htm#xtocid191020

[8] http://www.niksula.cs.hut.fi/~mkomu/docs/wirelesslansec.html

[9] http://www.commweb.com/article/COM20010206S0001

[10] http://wwwin.cisco.com/cmc/cc/pd/iosw/ioft/lam/tech/lamso_wp.htm

[11] http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t1/mobileip.htm#xtocid224992