NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

WIRELESS LOCAL AREA NETWORKS

Graduation Project
COM- 400

Submitted By: Rajaie Ibrahim (20011763)

Supervisor: Asst. Prof. Dr. Firudin muradov

Nicosia-2005

ACKNOWLEDGEMENTS

Firstly I would like to present my special appreciation to my supervisor *Asst. Prof. Dr Firudin Muradov*, His trust in my work and me and his priceless awareness for the project has made me do my work with full interest. His friendly behavior with me and his words of encouragement kept me doing my project.

Secondly I offer special thanks to my family, who encouraged me in every field of life and try to help whenever I needed. They enhanced my confidence in myself to make me able to face every difficulty easily. I am also grateful to my mother whose prayers have helped me o keep safe from every dark region of life and my father whose words for me had made this day comes true. And because of them I am able to complete my work

I would also like to pay my special thanks to my all friends who helped me and encouraged me for doing my work. Their reluctance and friendly environment for me has helped me allot. I want to thank them as they contributed their time and provided very helpful suggestions to me.

ABSTRACT

Today, wireless local area networks (WLAN's) are being constructed in many different locations and locales. The reason for assembling such networks is typically to provide network and Internet access within the building where one is installed.

However, there are many uses for WLAN's that go beyond single-location connectivity. For instance, many airports now offer areas that have wireless network connectivity as well as places such as conference rooms. This type of sparse placement of WLAN's has proven demand, but the fact that the locations of these wireless "hot spots" are usually far from each other results in zero connectivity outside the designated areas. This paper describes a system that was simulated in the network simulator, NS that allows for billing to take place between opted-in WLAN operators in order to allow for these "hot spots" to extend out of corporate areas and into regions covered by access points owned by the general public. This system allows for connection sharing between wireless access points and average users that are outside of the range of wireless connectivity of their local network so that these users can still gain access to the Internet by hopping through these "outer" access points based on a previously-agreed-upon pricing scheme.

TABLE OF CONTENTS

INTRODUCTION

A wireless local area network (WLAN) is two or more computers joined together using radio frequency (RF) transmissions. This differs from a wired LAN, which uses cabling to link together computers in a room, building, or site to form a network.

Although WLANs can be independent they are more typically an extension to a conventional wired network. They can allow users to access and share data, applications, internet access or other network resources in the same way as wired networks.

Wireless LANs are typically used with wireless enabled mobile devices such as notebook computers, PDAs and Tablet PCs. This allows users to take advantage of the flexibility, convenience and portability that WLANs can provide.

Wireless Data Networks can be easily considered as the ultimate limit to data communications, if flexibility, mobility and ease of relocation are considered as the most important parameters of a network. Wireless LANs (WLANs) are just the wireless counterparts of those traditional low-ranges, high bit rate and shared medium communication networks termed as Local Area Networks by the IEEE and HIPERLAN.

The first chapter is all about explaining what are wireless (LANs) technologies. It is an introduction chapter in which wireless (LANs) is described in details.

The second chapter is all about giving details of what are the types of wireless (LANs).

The third chapter presents the 802.11 Standard and WLAN Architecture and I have explained how 802.11 Standard works in details.

The last fourth chapter is about the network security and gives an overview of the security functions specified in two wireless LAN standard, namely in the IEEE 802.11 and the HIPERLAN. There is also some discussion about the threats and vulnerabilities

in wireless networks compared to wired networks. And last but not least the protocols and mechanisms needed in the secure wireless LAN are described.

CHAPTER ONE

1. INTRODUCTION TO WIRELESS (LANs)

1.1Overview

A wireless local area network (LAN) is a flexible data communications system implemented as an extension to or as an alternative for, a wired LAN. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Thus, wireless LANs combine data connectivity with user mobility.

Wireless LANs have gained strong popularity in a number of vertical markets, including health-care, retail, manufacturing, warehousing, and academia. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Today wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers.

There are two types of WLANs, infrastructure WLANs and independent WLANs. Infrastructure WLANs, where the wireless network is linked to a wired network, is more commonly deployed today. In an infrastructure WLAN, the wireless network is connected to a wired network such as Ethernet, via access points, which possesses both Ethernet links and antennas to send signals. These signals span microcells, or circular coverage areas (depending on walls and other physical obstructions), in which devices can communicate with the access points, and through these, with the wired network (*see picture below*). In a wireless LAN, devices can move within and between coverage areas without experiencing disruption in connectivity as long as they stay within range of an access point or extension point (similar to an access point) at all times

1.2 How Wireless LANs Work:

Wireless LANs use electromagnetic airwaves (radio or infrared) to communicate information from one point to another without relying on any physical connection. Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver. By superimposing the transmitted data onto the radio carrier, data can be accurately extracted at the receiving end. This is generally referred to as modulation of the carrier by the information being transmitted. Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier.

Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver tunes in one radio frequency while rejecting all other frequencies.

In a typical wireless LAN configuration, a transmitter/receiver (transceiver) device, called an access point, connects to the wired network from a fixed location using standard cabling. At a minimum, the access point receives, buffers, and transmits data between the wireless LAN and the wired network infrastructure. A single access point can support a small group of users and can function within a range of less than one hundred to several hundred feet.

End users access the wireless LAN through wireless-LAN adapters, which are implemented as PC cards in notebook or palmtop computers, as cards in desktop computers, or integrated within hand-held computers. Wireless LAN adapters provide an interface between the client network operating system (NOS) and the airwaves via an antenna. The nature of the wireless connection is transparent to the NOS.

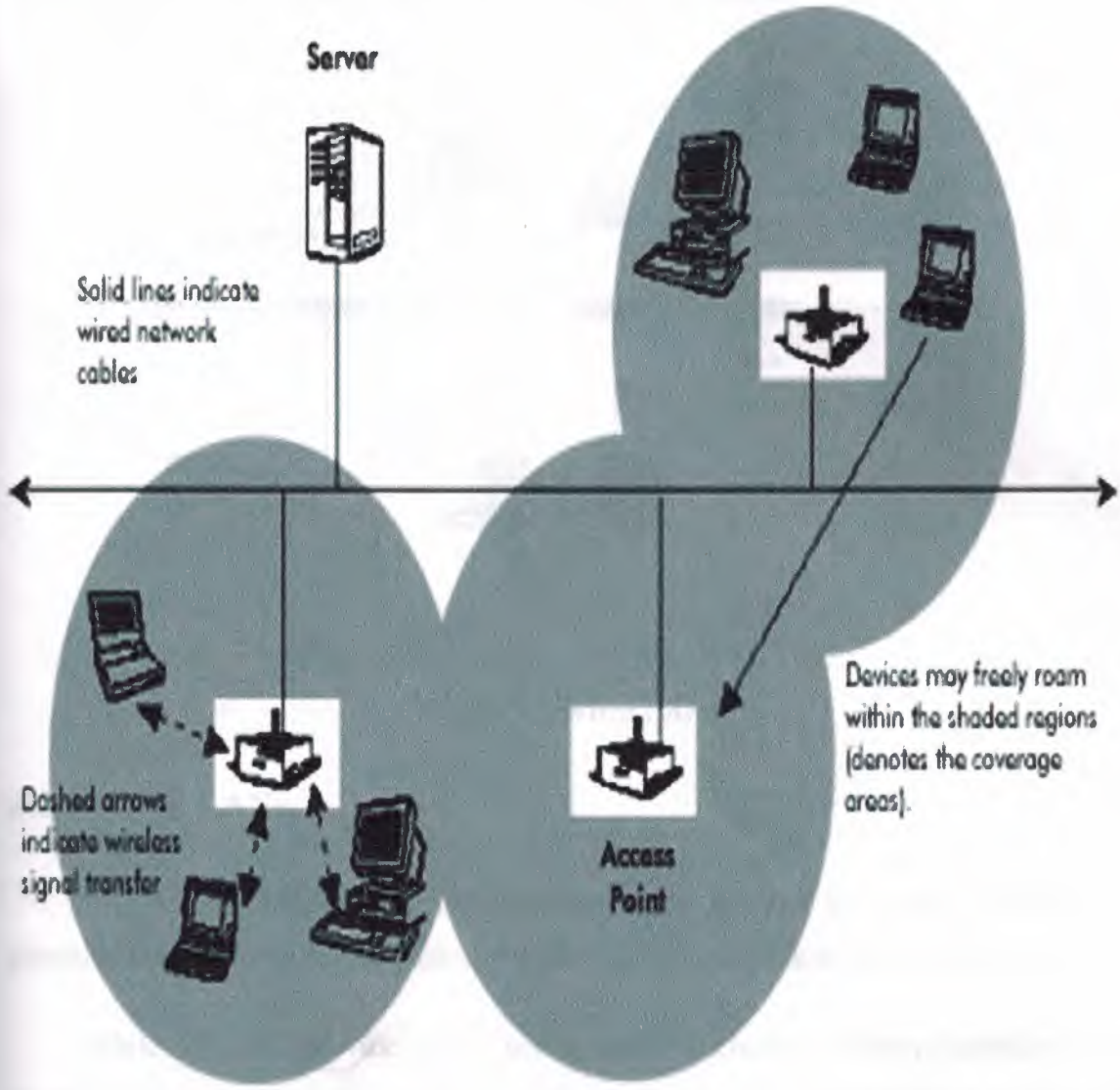


Figure 1.1 Wireless LAN Layout

In an (infrastructure) wireless LAN, devices communicate wirelessly with access points, which are connected to the wired network. Devices can maintain network connectivity while roaming in the shaded region.

This model can be compared to those of wired LANs where devices connect via cables to hubs, or common wiring points, and from these to a central server. However, in wired networks, each hub has a finite number of jacks, and thus, can only connect a

preset number of devices. Wire line networks are also confined by the existence of fixed cables, which limit connection to specified locations (seethe next picture).

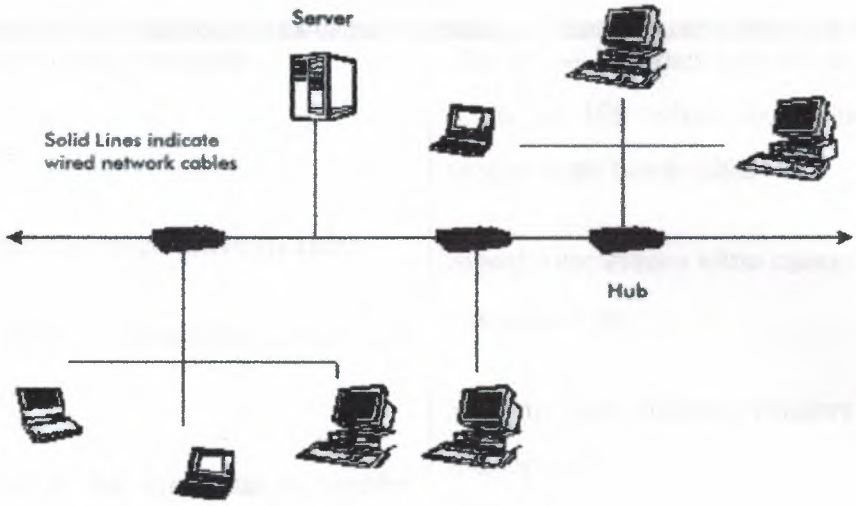


Figure 1.2 Wired LANs

1.2.1 Wired LANs

In a wired LAN, devices are connected to the network via cables. Devices are generally anchored to a set location depending on the placement of the network lines.

While WLANs provide some key benefits, including security, mobility, and scalability, they are currently much slower than wired LANs. For example, a wired LAN using 10BaseT Ethernet ranges from 10 – 100 Mbps. Other pros and cons of wireless LANs (in comparison with wired LANs) are listed in the table below:

Wireless LAN Pros and Cons

Pros	Cons
Easier to deploy and configure	Slower — Ethernet speeds range from 10 mbps to 100 mbps; corporate networks require high bandwidths
More secure	Signal interference often causes disruptions in connection
Ultimately more cost-effective (scalable)	Systems from different vendors may not be interoperable
Facilitates office relocation Easier to maintain	Costly installation
Makes available real-time data in broader range of coverage areas	

1.3 Wireless LAN Glossary's

a. access point: a device that connects the wireless network to the wired network. As a transceiver, it sports an antenna to send and receive signals from the various devices, providing coverage areas in which devices can roam freely.

b. extension point: a device that acts like an access point and connects the wireless network. Unlike access points, extension points do not connect the wireless network to the wire line but rather extend coverage areas between and beyond access points.

c. infrastructure network: the more common form of a wireless LAN. Infrastructure networks are comprised of WLANs connected to wired LANs and contain access points to channel network traffic.

d. Independent network: a peer-to-peer network containing devices (with network adapters) connected to one another, independent of a managing server or other form of administration.

e. LAN adapter: generally a PC card in the portable device with an integrated antenna to receive signals from the access point/extension point. Can also be integrated into handhelds.

f. Microcell: a coverage area in which devices can roam freely with a wireless connection. Microcells are generally circular (depending on the existence of interfering objects such as walls) and overlap to enable seamless connection as a user wanders through the wireless network. spread spectrum-a radio frequency technology most commonly used in WLANs. Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) are two examples of the spread-spectrum technique.transceiver-a device, such as a LAN adapter, used to receive signals sent by the transmitter.transmitter-a device that sends signals to the transceiver (typically an access point or an extension point in WLANs).

1.4 Wireless LANs Advantages

The widespread reliance on networking in business and the rapid growth of the Internet and online services are strong testimonies to the benefits of shared data and shared resources. With wireless LANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. Wireless LANs offer the following productivity, convenience, and cost advantages over traditional wired networks:

Mobility: Wireless LAN systems can provide LAN users with access to real-time information anywhere at work and in the home.

Installation Speed and Simplicity: Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.

Installation Flexibility: Wireless technology allows the network to go where wire cannot go.

Reduced Cost-of-Ownership: While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation

expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.

Scalability: Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area.

1.5 How Wireless LANs Are Used in the Real World

Wireless LANs frequently augment rather than replace wired LAN networks—often providing the final few meters of connectivity between a wired network and the mobile user. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

Doctors and nurses in hospitals are more productive because hand-held or notebook computers with wireless LAN capability deliver patient information instantly.

Consulting or accounting audit teams or small workgroups increase productivity with quick network setup.

Students holding class on campus greens can access the Internet to consult the catalog of the Library of Congress or class notes.

Network managers in dynamic environments minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

Training sites at corporations and students at universities use wireless connectivity to access information, information exchanges, and learning.

Trade show and branch office workers minimize setup requirements by installing pre-configured wireless LANs needing no local MIS support.

Warehouse workers use wireless LANs to exchange information with central databases, thereby increasing productivity.

Senior executives in meetings make quicker decisions because they have real-time information at their fingertips.

1.6 Wireless LAN Technology's

Manufacturers of wireless LANs have a range of technologies to choose from when designing a wireless LAN solution. Each technology comes with its own set of advantages and limitations.

1.6.1 Narrowband Technology

A narrowband radio system transmits and receives user information on a specific radio frequency. Narrowband radio keeps the radio signal frequency as narrow as possible just to pass the information. Undesirable crosstalk between communications channels is avoided by carefully coordinating different users on different channel frequencies.

A private telephone line is much like a radio frequency. When each home in a neighborhood has its own private telephone line, people in one home cannot listen to calls made to other homes. In a radio system, privacy and noninterference are accomplished by the use of separate radio frequencies. The radio receiver filters out all radio signals except the ones on its designated frequency.

From a customer standpoint, one drawback of narrowband technology is that the end-user must obtain an FCC license for each site where it is employed.

1.6.2 Spread Spectrum Technology

Most wireless LAN systems use spread-spectrum technology, a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. Spread-spectrum is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the tradeoff produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. There are two types of spread spectrum radio: frequency hopping and direct sequence.

1.6.3 Frequency-Hopping Spread Spectrum Technology

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.

1.6.4 Direct-Sequence Spread Spectrum Technology

Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered (and, of course, more bandwidth is required). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low-power wideband noise and is rejected by most narrowband receivers.

1.6.5 Infrared Technology

A third technology, little used in commercial wireless LANs, is infrared. Infrared (IR) systems use very high frequencies, just below visible light in the electromagnetic spectrum, to carry data. Like light, IR cannot penetrate opaque objects; it is either directed (line-of-sight) or diffuse technology. Inexpensive directed systems provide limited range of approximately 3 feet and typically are used for personal area networks. Occasionally directed systems are used in specific wireless LAN applications. High performance directed IR is impractical for mobile users and is therefore used only to implement fixed sub-networks. Diffuse or reflective IR wireless LAN systems do not require line-of-sight, but cells are limited to individual rooms.

1.7 Wireless LAN Configuration

Wireless LANs can be simple or complex. At its most basic, two PCs equipped with wireless adapter cards can set up an independent network whenever they are within range of one another. This is called a peer-to-peer network. On-demand networks, such as in this example, require no administration or preconfiguration. In this case each client would only have access to the resources of the other client and not to a central server.

Figure 1.3: A wireless peer-to-peer network

Installing an access point can extend the range of an ad hoc network, effectively d0oubling the range at which the devices can communicate. Since the access point is connected to the wired network, each client can have access to server resources as well as to other clients. Each access point can accommodate many clients; the specific number

depends on the number and nature of the transmissions involved. Many real-world applications exist where a single access point services from 15-50 client devices.

Figure 1.4: Client and Access Point

Access points have a finite range, on the order of 500 feet indoor and 1000 feet outdoors. In a very large facility such as a warehouse, or on a college campus, it may be necessary to install more than one access point. Access point positioning is accomplished by means of a site survey. The goal is to blanket the coverage area with overlapping coverage cells so that clients can range throughout the area without ever losing network contact. The ability of clients to move seamlessly among a cluster of access points is called *roaming*. Access points hand the client off from one access point to another in a way that is invisible to the client, ensuring unbroken connectivity.

Figure 1.5: Multiple access points and roaming

To solve particular problems of topology, the network designer might choose to use Extension Points to augment the network of access points. Extension Points look and function like access points, but they are not tethered to the wired network as are APs. EPs function just as their name implies: they extend the range of the network by relaying signals from a client to an AP or another EP. EPs can be strung together in order to pass along messaging from an AP to far-flung clients (just as humans in a bucket brigade pass pails of water hand-to-hand from a water source to a fire).

Figure 1.6: Use of an extension point

One last item of wireless LAN equipment to consider is the directional antenna. Let's suppose you had a wireless LAN in your building A and wanted to extend it to a leased building, B, one mile away. One solution might be to install a directional antenna on each building with each antenna targeting the other. The antenna on A is connected to

your wired network via an access point. The antenna on B is similarly connected to an access point in that building, which enables wireless LAN connectivity in that facility.

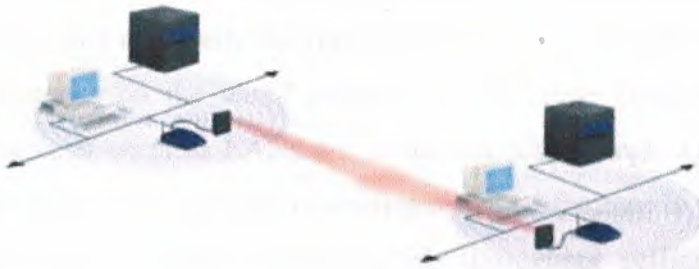


Figure 1.7: The use of directional antennas

1.8 Customer Considerations

While wireless LANs provide installation and configuration flexibility and the freedom inherent in network mobility, customers should be aware of the following factors when considering wireless LAN systems.

1.9 Range and coverage

The distance over which RF waves can communicate is a function of product design (including transmitted power and receiver design) and the propagation path, especially in indoor environments. Interactions with typical building objects, including walls, metal, and even people, can affect how energy propagates, and thus what range and coverage a particular system achieves. Solid objects block infrared signals, which imposes additional limitations. Most wireless LAN systems use RF because radio waves can penetrate most indoor walls and obstacles. The range (or radius of coverage) for typical wireless LAN systems varies from under 100 feet to more than 300 feet. Coverage can be extended, and true freedom of mobility via roaming, provided through microcells.

1.10 Throughput

As with wired LAN systems, actual throughput in wireless LANs is product- and set-up-dependent. Factors that affect throughput include the number of users, propagation factors such as range and multipath, the type of wireless LAN system used, as well as the latency and bottlenecks on the wired portions of the LAN. Data rates for the most widespread commercial wireless LANs are in the 1.6 Mbps range. Users of traditional Ethernet or Token Ring LANs generally experience little difference in performance when using a wireless LAN. Wireless LANs provide throughput sufficient for the most common LAN-based office applications, including electronic mail exchange, access to shared peripherals, Internet access, file transfer, and access to multi-user databases and applications.

As a point of comparison, state-of-the-art V.90 modems transmit and receive at data rates of less than the advertised 56.6 Kbps. In terms of throughput, a wireless LAN operating at 1.6 Mbps is (almost thirty times faster than the state-of-the-art V.90 modem)

1.11 Integrity and Reliability

Wireless data technologies have been proven reliable through more than fifty years of wireless application in both commercial and military systems. While radio interference can cause degradation in throughput, such interference is rare in the home or workplace. Robust designs of proven wireless LAN technology and the limited distance over which signals travel result in connections that are far more robust than cellular phone connections and provide data integrity performance equal to or better than wired networking.

1.12 Compatibility with the Existing Network

Most wireless LANs provide for industry-standard interconnection with wired networks such as Ethernet or Token Ring. Wireless LAN nodes are supported by network operating systems in the same fashion as any other LAN node through the use of the

appropriate drivers. Once installed, the network treats wireless nodes like any other network component.

1.13 Interoperability of Wireless Device

Wireless LAN systems from different vendors may not be interoperable. For three reasons. First, different technologies will not interoperate. A system based on spread spectrum frequency hopping (FHSS) technology will not communicate with another based on spread spectrum direct sequence (DSSS) technology. Second, systems using different frequency bands will not interoperate even if they both employ the same technology. Third, systems from different vendors may not interoperate even if they both employ the same technology and the same frequency band, due to differences in implementation by each vendor.

1.14 Interference and Coexistent

The unlicensed nature of radio-based wireless LANs means that other products that transmit energy in the same frequency spectrum can potentially provide some measure of interference to a wireless LAN system. Microwave ovens are a potential concern, but most wireless LAN manufacturers design their products to account for microwave interference. Another concern is the co-location of multiple wireless LANs. While wireless LANs from some manufacturers interfere with wireless LANs, others coexist without interference.

1.15 Licensing Issues

In the United States, the Federal Communications Commission (FCC) governs radio transmissions, including those employed in wireless LANs. Other nations have corresponding regulatory agencies. Wireless LANs are typically designed to operate in portions of the radio spectrum where the FCC does not require the end-user to purchase a license to use the airwaves. In the U.S. most wireless LANs broadcast over one of the ISM (Instrumentation, Scientific, and Medical) bands. These include 902-928 MHz, 2.4-2.483 GHz, 5.15-5.35 GHz, and 5.725-5.875 GHz. For wireless LANs to be sold in a

particular country, the manufacturer of the wireless LAN must ensure its certification by the appropriate agency in that country.

1.16 Simplicity/Ease of Use

Users need little new information to take advantage of wireless LANs. Because the wireless nature of a wireless LAN is transparent to a user's network operating system, applications work the same as they do on wired LANs. Wireless LAN products incorporate a variety of diagnostic tools to address issues associated with the wireless elements of the system; however, products are designed so that most users rarely need these tools.

Wireless LANs simplify many of the installation and configuration issues that plague network managers. Since only the access points of wireless LANs require cabling, network managers are freed from pulling cables for wireless LAN end users. Lack of cabling also makes moves, adds, and changes trivial operations on wireless LANs. Finally, the portable nature of wireless LANs lets network managers preconfigure and troubleshoot entire networks before installing them at remote locations. Once configured, wireless LANs can be moved from place to place with little or no modification.

1.17 Security

Because wireless technology has roots in military applications, security has long been a design criterion for wireless devices. Security provisions are typically built into wireless LANs, making them more secure than most wired LANs. It is extremely difficult for unintended receivers (eavesdroppers) to listen in on wireless LAN traffic. Complex encryption techniques make it impossible for all but the most sophisticated to gain unauthorized access to network traffic. In general, individual nodes must be security-enabled before they are allowed to participate in network traffic.

1.18 Cost

A wireless LAN implementation includes both infrastructure costs, for the wireless access points, and user costs, for the wireless LAN adapters. Infrastructure costs depend primarily on the number of access points deployed. The number of access points typically depends on the required coverage region and/or the number and type of users to be serviced. The coverage area is proportional to the square of the product range. Wireless LAN adapters are required for standard computer platforms.

The cost of installing and maintaining a wireless LAN generally is lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, a wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it. Second, because wireless LANs simplify moves, adds, and changes, they reduce the indirect costs of user downtime and administrative overhead.

1.19 Scalability

The design of wireless networks can be extremely simple or quite complex. Wireless networks can support large numbers of nodes and/or large physical areas by adding access points to boost or extend coverage.

1.20 Battery Life for Mobile Platforms

Since end-user wireless products are designed to run off the AC or battery power from their host notebook or hand-held computer, wireless products have no direct wire connectivity of their own.

1.21 Safety

The output power of wireless LAN systems is very low, much less than that of a hand-held cellular phone. Since radio waves fade rapidly over distance, very little exposure to RF energy is provided to those in the area of a wireless LAN system. Wireless LANs must meet stringent government and industry regulations for safety. No adverse health affects have ever been attributed to wireless LANs.

1.22 Summary

Flexibility and mobility make wireless LANs both effective extensions and attractive alternatives to wired networks. Wireless LANs provide all the functionality of wired LANs, without the physical constraints of the wire itself. Wireless LAN configurations range from simple peer-to-peer topologies to complex networks offering distributed data connectivity and roaming. Besides offering end-user mobility within a networked environment, wireless LANs enable portable networks, allowing LANs to move with the workers that use them.

CHAPTER TWO

2. TYPES OF WIRELESS LANs

2.1 Overview

It might seem obvious that the key differentiating factor between wireless LANs and wireless WANs is that they operate in a local area, but local operation has many significant and not necessarily obvious consequences. First and foremost, wireless LANs operate at much higher speeds, ranging from 1 Mbps to 20 Mbps compared to wireless WANs, which today range from 4 Kbps to 30 Kbps. Higher speeds are possible because that band of the spectrum is shared by a much smaller number of users. Whereas a cellular base station can serve a radius of over 10 kilometers (six miles), a wireless LAN access point typically serves a maximum radius of about a hundred meters. Due to the shorter distances involved in wireless WANs, radio signals experience less interference and distortion from the environment, thus reducing the amount of error control required. Users are also stationary or moving at walking speeds, while wide area networks support users moving at highway speeds where signals are subject to a form of interference known as Rayleigh fading. Another factor is that smaller distances result in much better signal-to-noise ratios. All these factors in combination allow much higher throughputs.

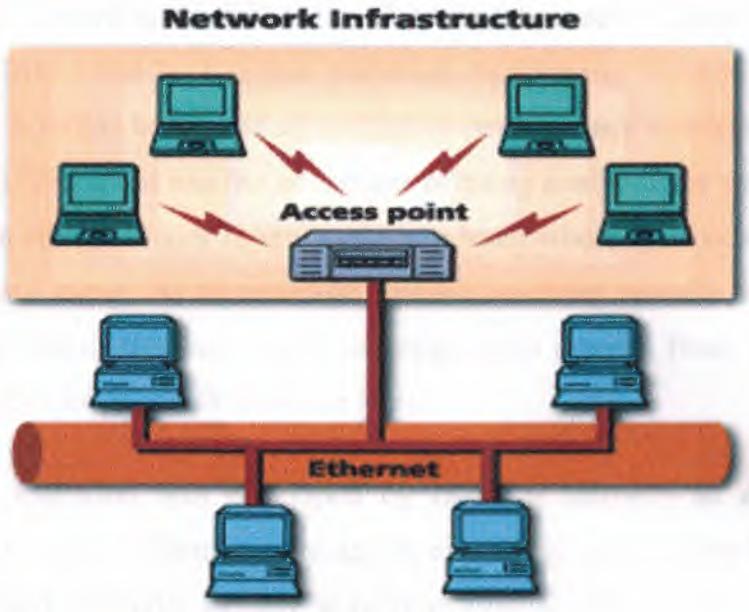
The higher throughput of wireless LANs has the virtue of allowing you to use existing network operating systems and applications (e.g., file and printer sharing, database access) compared to the modem-like applications for wireless WANs. And unlike wireless WANs, which are mostly operated by public carriers with usage fees, you get to buy and operate your own network. This gives you control of the whole network, but leaves you responsible for its proper installation and functioning. Fortunately, wireless LAN technology is well past its infancy and is ready to meld into your organization as a reliable subsystem. And the radio bands used by nearly all wireless LANs let you deploy networks without obtaining a license.

In this section, we delve into the different topologies available: spread spectrum, which is the most common RF technology used today (the two types of spread spectrum include direct sequence and frequency hopping); a low-power, narrowband approach that enables higher speeds; HiperLAN, which is a European standard; and infrared approaches.

2.2 Topologies

The term wireless is actually somewhat misleading, since most wireless LANs interconnect with wired networks. The bulk of the distance between a wireless node and another node may well be over wires or fiber. Nevertheless, it is possible to build a network that is completely wireless. In such an instance, the physical size of the network is determined by the maximum reliable propagation range of the radio signals. Networks such as these are referred to as ad hoc networks, and are well suited for temporary situations such as meetings, conferences and sporting events.

It is more likely that you will install what is called an infrastructure network, where your WLAN connects to an existing wired LAN. In this instance you will need an access point that effectively bridges wireless LAN traffic onto your LAN. This function may be handled by software in a workstation that houses both a wireless card and a wired (e.g., Ethernet) card. But most wireless LAN vendors recommend dedicated hardware called an access point for this function. The access point can also act as a repeater for wireless nodes, effectively doubling the maximum possible distance between nodes.



2.3 Spread Spectrum

Most wireless LANs today use spread spectrum technology, not because spread spectrum is the best radio technology for wireless LANs but more as a result of FCC rules (Federal Code of Regulations 15.247) that allow for unlicensed operation in a number of radio bands, including 902 to 928 MHz, 2.400 to 2.483 GHz and 5.725 to 5.85 GHz. These are the industrial, scientific and medical (ISM) bands where unlicensed users are "secondary users" of the band and must not interfere with licensed primary users. Fortunately such interference has not been an issue because wireless nodes are restricted to 1 watt of power for transmissions and because the nature of spread spectrum is that it appears as noise to all but intended receivers.

Nevertheless, as a user of wireless LAN technology you need to be aware that primary users of the spectrum are not restricted to 1 W of transmission and could potentially interfere with your network. Moreover, companies are finding more an d more use for the ISM bands, including wireless speakers and cordless telephones. The Metricom Ricochet network for instance, uses the 900-MHz ISM band. Will you experience interference problems using spread spectrum? Probably not, but you may want to think twice before using wireless LANs for mission-critical or life-and-death applications.

In today's market, the 900-MHz ISM band best serves consumer products, while the 2.4-GHz band best serves midrange performing wireless LANs (1 to 3 Mbps) and the 5.7-GHz band best serves higher-performance wireless LANs (5 to 10 Mbps). The 2.4-GHz band has the advantage of being available for unlicensed use in some European countries and Japan, and is the band where most new wireless LAN products operate today. As to coverage, spread spectrum usually operates over a typical range of about 100 meters and coverage areas ranging from 5,000 to 25,000 square meters (50,000 to 250,000 square feet).

Spread spectrum was developed by the U.S. military as a robust radio technology that is both difficult to jam and to eavesdrop on. It works by spreading a signal that would normally occupy a certain amount of spectrum over a much broader amount of spectrum. There are two forms of spread spectrum: frequency hopping and direct sequence. Both are allowed by FCC rules.

In frequency hopping, the signal dwells momentarily on one frequency, then hops to another, then another in a pseudorandom sequence that eventually repeats itself. A receiver must hop at exactly the same time to exactly the right frequency to be able to receive the signal. FCC rules require that the band be divided into a certain number of frequencies and that the hopper must use a certain number of these frequencies.

Direct sequence is very different. Each "one" in the binary data is converted to a sequence of predetermined ones and zeroes and each "zero" is converted to the inverted sequence. The binary data in the sequences are referred to as chips, and the ratio of chips to original bits is referred to as the spreading ratio, or gain, of the system. FCC rules require a minimum spreading ratio or gain.

Some wireless LANs are based on frequency hopping, some on direct sequence. Direct sequence allows higher throughputs, although such designs may cost more and use more power. There is almost a holy war about which type of spread spectrum is better, though mobile designs today tend to use frequency

hopping. You should choose your network based on features and price, and not on which spread spectrum technology it uses.

2.4 Low-Power Narrowband

An alternative approach to spread spectrum that some wireless LAN vendors are using is to transmit narrowband signals at low-power levels, a method allowed by FCC CFR 15.249 rules. By transmitting at low-power levels, vendors do not have to use spread spectrum, which gives them the ability operate at higher data rates. RadioLAN's product uses this approach and operates at 10 Mbps in the 5.8-GHz band with 50 milliwatts (mW) of peak transmission power. The price of this higher performance is a reduced transmission range of about 30 meters (100 feet) in an office environment.

2.5 HiperLAN

HiperLAN, an abbreviation for Higher Performance Radio LAN, is a wireless technology standard developed by the European Telecommunications Standards Institute. It boasts very impressive capabilities, including a data rate of about 24 Mbps using a channel width of 23.5 MHz. In Europe, spectrum is available in the 5.15 to 5.3 GHz range, allowing for five separate channels. This type of throughput readily supports multimedia applications. Unfortunately, no commercial products are yet available. But the technology is under consideration for new spectrum in the United States in the 5-GHz band as part of the U.S. Unlicensed National Information Infrastructure band.

2.6 Infrared LANs

An alternative approach to radio-based wireless L ANs is infrared communications. Infrared networking uses electromagnetic radiation with wavelengths of 820 to 890 nanometers, corresponding to a frequency of about 350,000 GHz. The advantages of IR include no need for licenses, no safety issues, huge potential capacity and good control of interference. IR does not penetrate

receivers can be designed either for directional use or for diffuse use, where signals bounce off walls and other objects to reach the receiver. In fact, IR is specified as one of the physical layer options in the new IEEE 802.11 standard.

Though it is a promising technology, there are relatively few IR LAN products available today. But one type of infrared technology that has been broadly deployed is the use of IR for short point-to-point connections following standards specified by the Infrared Data Association.

2.7 Infrared Data Association (IRDA)

The Infrared Data Association is a consortium of vendors that has defined low-cost IR communications characterized by:

- Directional point-to-point communications of up to one meter
- 115-Kbps and 4-Mbps connectivity
- Walk-up ad hoc connectivity for LAN access, printer access, and portable computer to portable computer communications

Many laptops today include IRDA ports, though devices such as LAN access points and printers with IR capability are not yet very common. The IRDA estimates some 60 million IRDA ports in the market.

2.8 Unlicensed PCS

When allocating spectrums for Personal Communications Service, the FCC included some bands for what is called unlicensed PCS: 1910 to 1920 MHz and 2390 to 2400 MHz were reserved for data and 1920 to 1930 MHz for voice. Unfortunately, restrictions on the use of this spectrum have limited its usefulness for wireless data to the extent that no product offerings are yet available

2.9 Wireless Basics

This section introduces some of the concepts involved in wireless LANs which are necessary to understand any discussion about wireless LANs.

There are five guiding principles that determine the way in which wireless communications work:

- **Bandwidth is scarce**

Wireless communication requires radio (or infrared) spectrum, and while the number and type of applications are increasing rapidly the available bandwidth is severely constrained. As bandwidth is scarce it is very expensive in line with the laws of supply and demand (hence the multi-billion sales for third generation (3G) mobile telephony licenses). While the cost of providing bandwidth is falling the price of processing and storage is falling much faster which means that data requirements are currently growing much faster than the rate at which the available bandwidth is growing. The cost of wired access is falling much faster than the cost of wireless bandwidth with the result that the cost gap between wired and wireless communications is currently growing, and is likely to continue to do so.

On the other hand because the cost of processing is falling faster, improved compression and other techniques can be used to help make better use of the available bandwidth.

- **Complete coverage of a campus is hard**

Wireless signals of the type used for wireless LANs decay rapidly (with the square of the distance from the transmitter at best); this means that many access points (LANs) or base stations (mobile telephony) are needed. Also, the higher the frequency the faster signals decay, the more base stations are needed and the greater the cost.

To complicate matters further, the higher the frequency used the greater the bandwidth available, but the faster the signal decays, and these need to be balanced when designing a network.

- **The environment is hostile**

Wire and fibre provide an excellent medium for signals. The air through which wireless signals must travel is a very poor environment due to echoes off obstacles, humidity etc. This means that complex error correction systems are needed which are not only expensive to design and build but also require additional bandwidth to work.

- **Power consumption in mobile devices**

For mobile devices battery power is a problem. The greater the distance being communicated over, the greater the signal power required and hence the size and weight of battery needed to make it work. This places a major constraint on both the signal strength and the processing used to encode and decode signals.

- **Cost**

Increasingly devices are mobile, and if they are to include wireless connections the costs need to be kept very low so as not to inflate the overall cost too much; this means that design and building costs must be low.

One of the design criteria for Bluetooth was that the chipset needed should cost around $5 so as not to inflate the price of devices using Bluetooth.

A variety of different modes of wireless interconnection have been developed. They can roughly be divided into personal area networks (PAN), local area networks (LAN) and wide area networks (WAN). The diagram shows the ways in which the various different types of wireless network may be used together to provide the best performance and mobility. The figure shows a student with a PDA (but it could equally well be a laptop) and a mobile phone. When students are at

college they would use normally use the wireless LAN from their PDA to access the college intranet and the internet, they might also exchange data between a desktop PC that they were using (perhaps for some specialist purpose) and their PDA using Bluetooth rather than using the LAN. This is particularly likely in computer labs where the computers would be on a wired LAN and there may be no wireless LAN available. At home the student might plug their PDA into a network or dock at home, but in the future they may well dock a PDA to a computer using Bluetooth, or if they have a laptop they may have a wireless LAN at home. On the move they can send and receive data via their mobile phone, using Bluetooth to send the data from the PDA to the mobile phone.

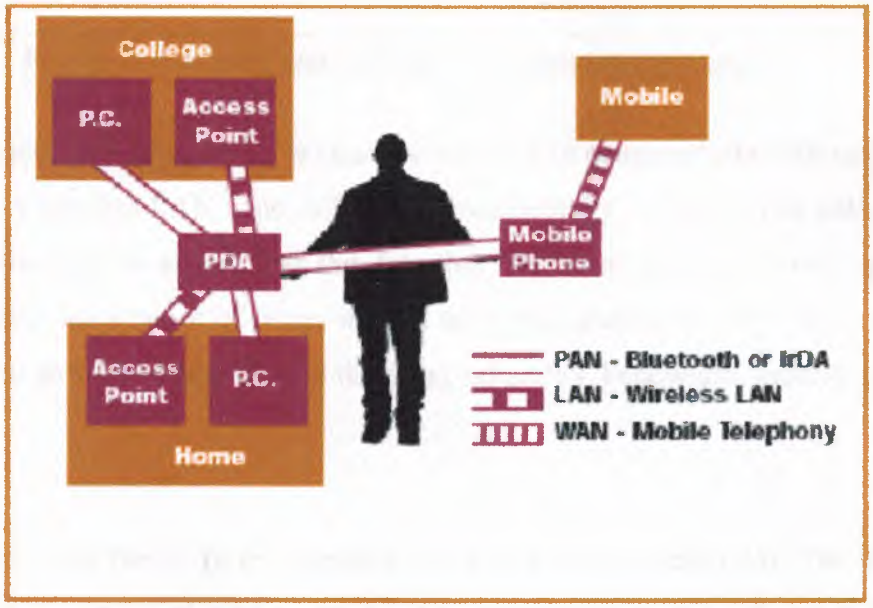


Figure 1. wireless user in differing environments

Figure 2 shows the various types of wireless communication and their data rates and mobility. From this it can be seen that there is a balance to be struck between performance and mobility, and that there will always be a mixed environment as each of the types of communication offers different advantages.While some offer good data rates (measured in Mb/s) others offer better geographic coverage.

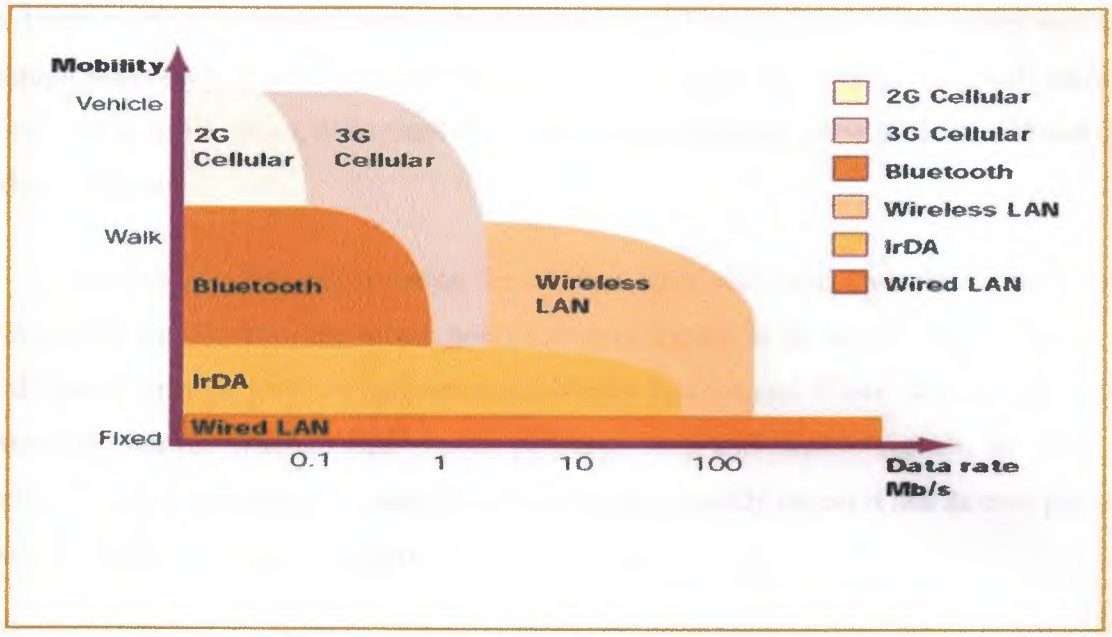


Figure 2. data rates and mobility for communication types

The function of any LAN is to enable computers to communicate with each other. In this respect a wireless LAN is no different. Fundamentally, it needs to be able to send and receive data, and to ensure that the data that has been sent is correctly received. Beyond this there are a range of issues needed to build a usable network. These include addressing (how to know where to send the data), reliability, bandwidth, security etc.

Many of these functions are identical in a wired and wireless LAN. The way that some of the issues are resolved have to be different because air is a less reliable and secure medium than wire (or fibre).

A wireless LAN consists of a number of access points linked to the wired LAN backbone1. The access points provide a wireless service to the users and connect this into the LAN. The access point can communicate with all devices within range that are using the same standards.

The range is determined by the type of technology, the power of the signal and the environment in which it is being used. Typically this is around 10 m for Bluetooth to around 50 m for wireless LAN technologies - though the higher bandwidth technologies

are likely to offer maximum bandwidth for about 15-20 m. Although radio waves will go through walls they do lose some of their power, and hence the distance they will travel. Wires, metal grills, pipes, even shelves of books will all absorb some of the signal and so reduce its range.

Each device that will be using the wireless LAN will need a wireless card which will receive signals from the access point and send signals to the access point. A variety of different types of wireless card are available for laptops and PDAs. It is important to remember that the wireless LAN needs power to send and receive signals, so using a wireless LAN will flatten the computer's battery more quickly unless it has its own power source. Roll on wind up computers.

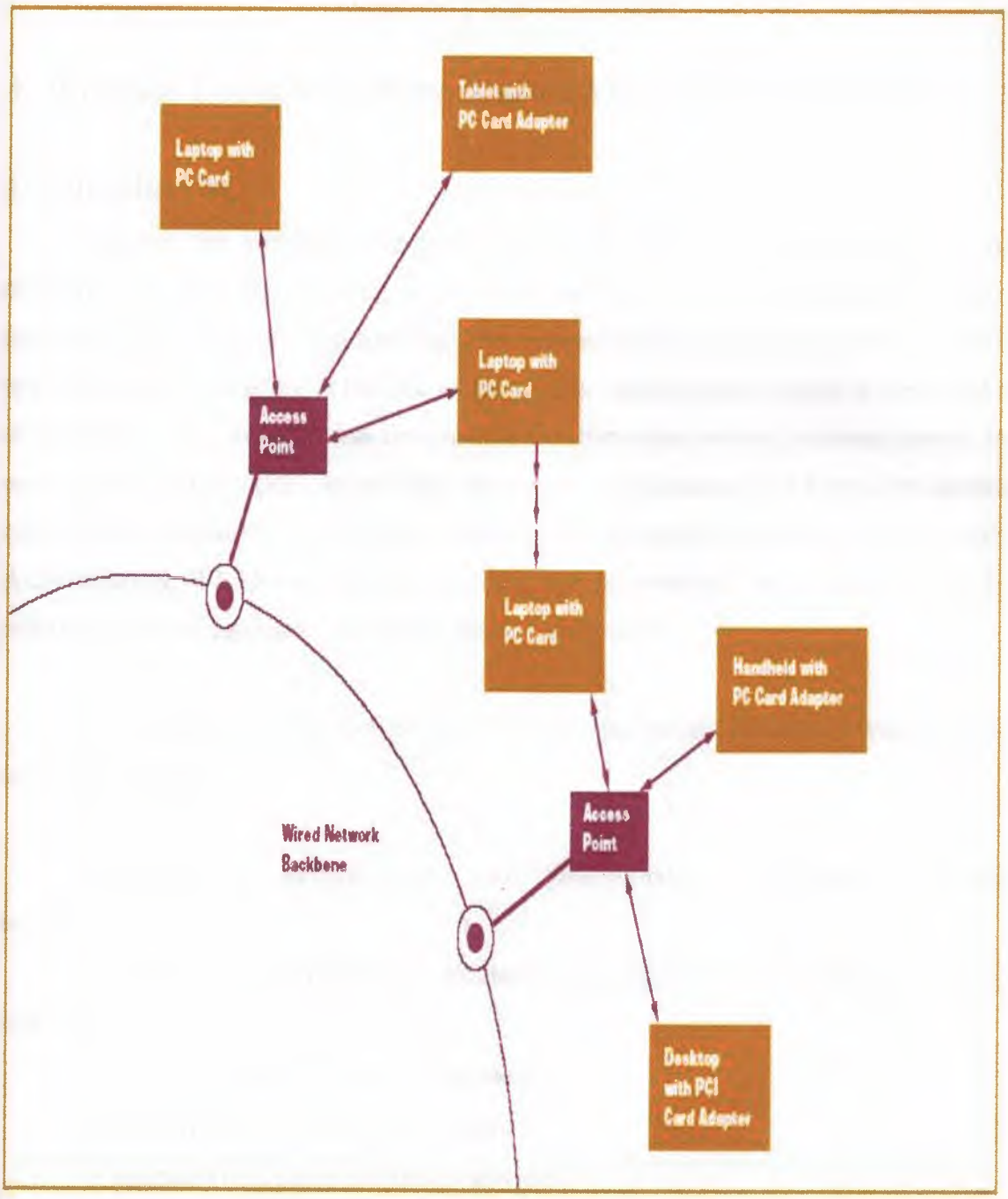


Figure 3. wireless LAN set up

CHAPTER THREE

3. Wireless Local Area Networks and the 802.11 Standard

3.1 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.

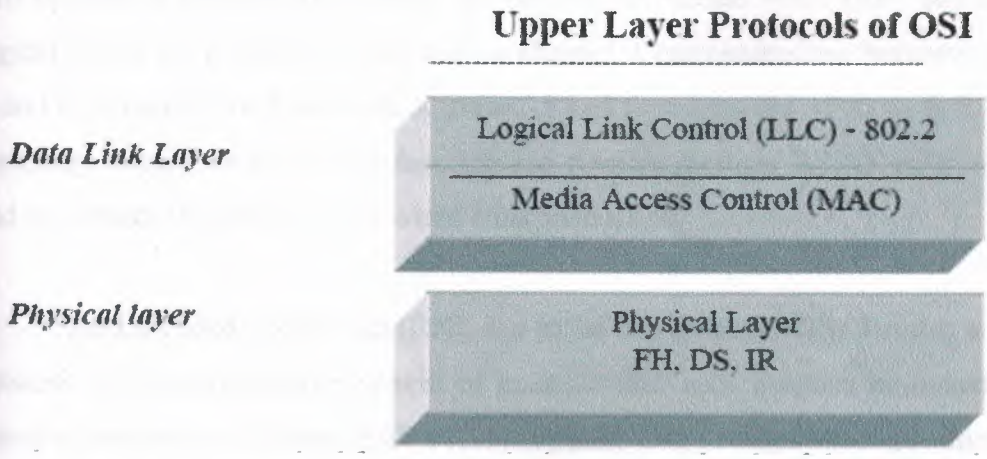


Figure 1. 802.11 standard focuses on the bottom two levels of the ISO model: PHY and MAC

3.2 WLAN Architecture

3.2.1 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 sub network. 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 uses the same channel, and use different channels to boost aggregate throughput.

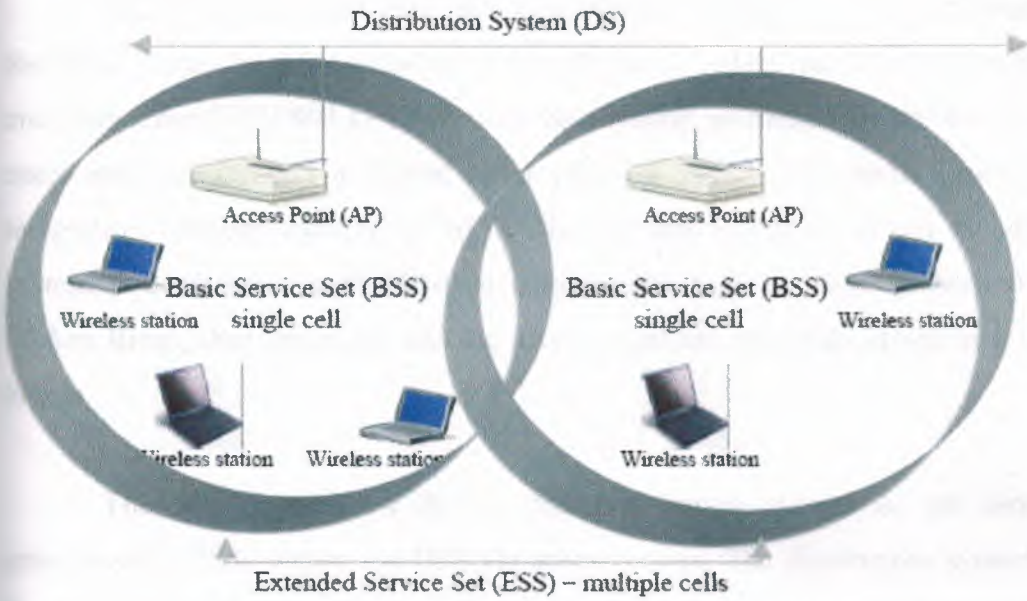


Figure 2. IEEE 802.11 BSS and ESS topologies

3.2.2 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.

3.3 IEEE 802.11, 802.11b and 802.11a Physical Layer

3.3.1 802.11 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 base band, 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 uses infra-red light transmission. Photonic wireless LANs use the 850 to 950 Nm band of infrared 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 meters.
- 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 subsystems 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, and is primarily an intra-building technology. DSSS products can be fast and far reaching.

3.3.2 802.11b – 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) In the case of 2 Mbps, a more sophisticated implementation called Quadrature Phase Shift Keying (QPSK) is 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

3.3.3 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.

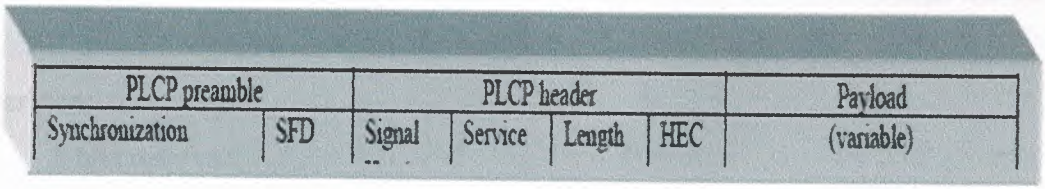


Figure 3. IEEE 802.11b DSSS PHY frame format

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%.

3.3.4 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 signals 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) 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 802.11 acompliant 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.

3.4 IEEE 802.11, 802.11b and 802.11a MAC Layer

3.4.1 802.11 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.

3.4.2 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], 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

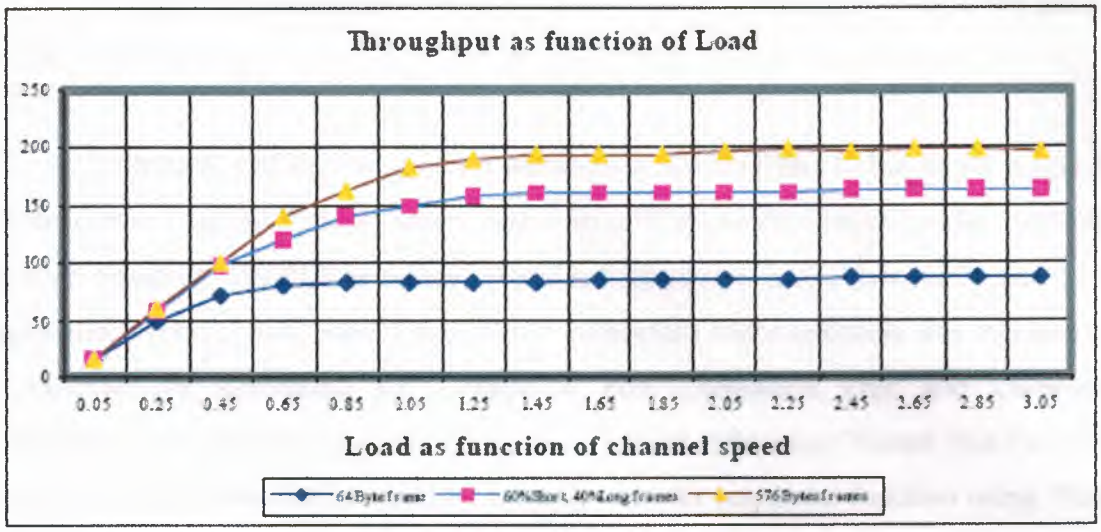


Figure 4. Throughput efficiency in IEEE 802.11.

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 timecritical 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.

3.4.4 The "Hidden Station" challenge

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

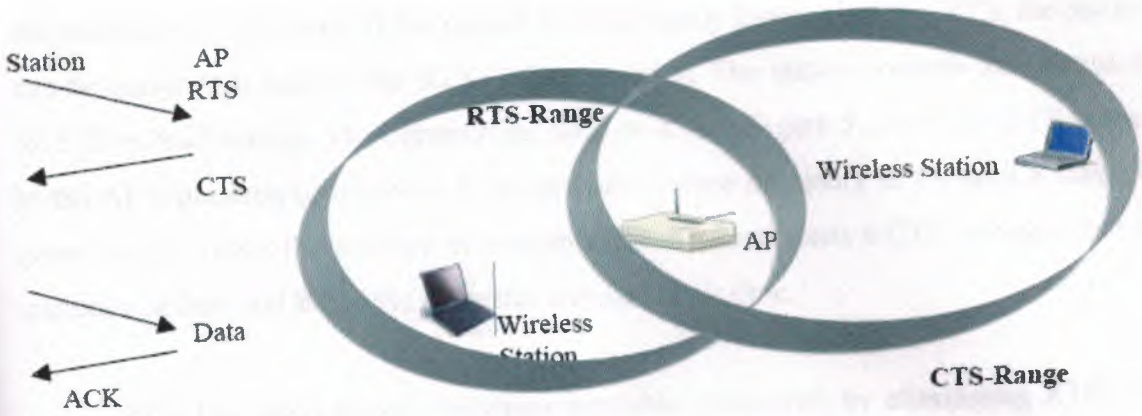


Figure 5. Hidden Station challenge

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

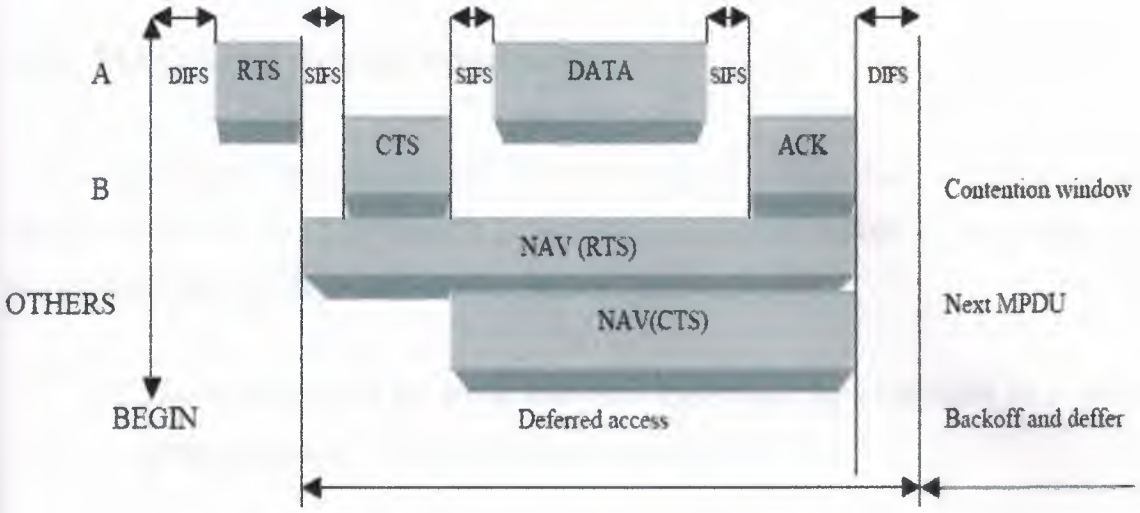


Figure 5. The NAV state is combined with the physical carrier sense to indicate the busy medium.

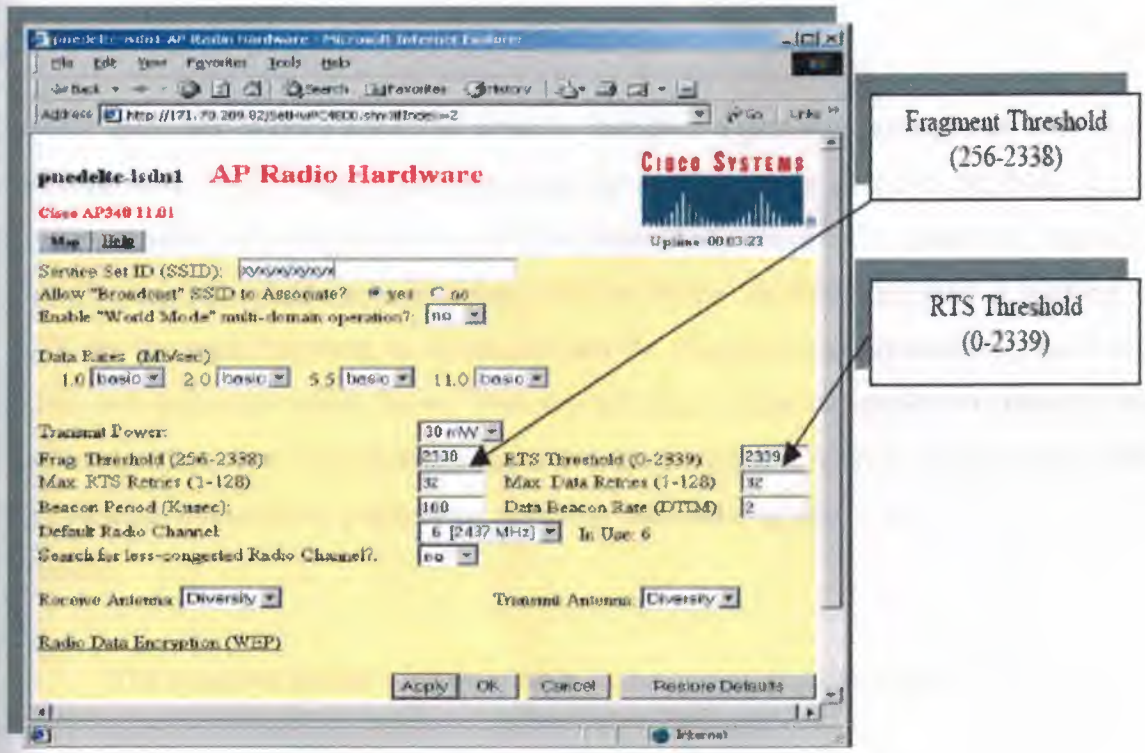


Figure 6. RTS Threshold settings on Cisco AP340, ver. 11.01

3.4.5 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.

3.4.6 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 exponential backoff algorithm which must be executed in the following cases: when the station senses the medium before the

3.4.9 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 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%.

3.5 802.11 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.

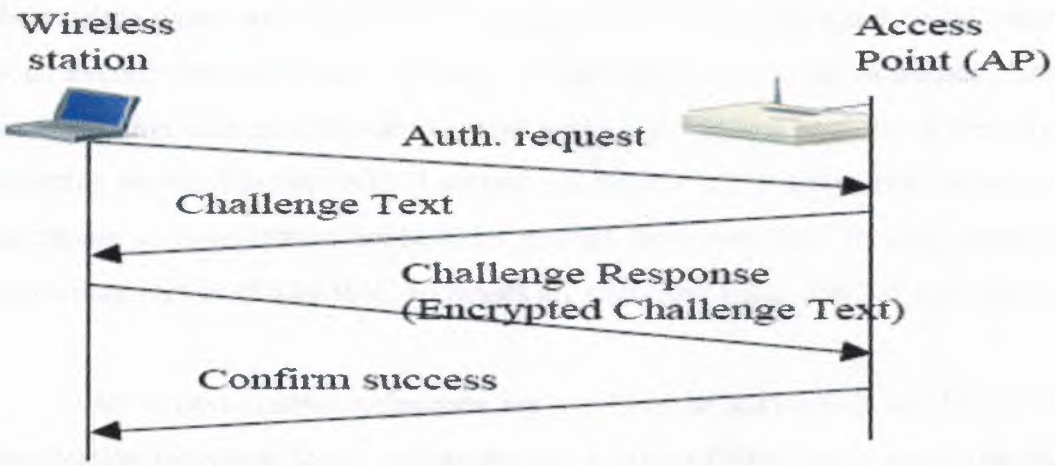


Figure 8. Shared key authentication

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 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 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".

3.6 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.

3.7 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.

3.8 Known Issues and Development Directions

3.8.1 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), 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".

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 .

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.

3.8.2 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.

3.8.3 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.

3.9 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.

3.10 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 Allianc

CHAPTER FOUR

4. Security in Wireless Local Area Networks

4.1 Introduction

Around 1980 was the concept of the wireless LAN introduced and since 1985 have many companies tried to implement variety of wireless LAN applications using spread spectrum, infrared and traditional wide band radio technologies. Now is the real breakthrough of the wideband wireless applications happening; the IEEE 802.11 standard, approved June 1997, gives a solid platform for new applications and the chips supporting IEEE 802.11 are already in the market. The wireless office market revenue was year 1996 $390 million from which $218 million belonged to wireless LANs and it is expected to break a billion dollar in early next millennium.

The commercial wireless LAN applications can be divided in five category:

- LAN extension - indoor wire replacement
- Inter-LAN bridges - outdoor wire replacement
- Campus Area Networks (CAN) - wireless LANs with infrastructure
- Ad-hoc networking - wireless LANs without infrastructure
- Nomadic access - a wireless LAN service

Today's existing applications aims at four category of applications :

- Healthcare industry
- Factory floors
- Banking industry
- Educational institutions

The security issues in the wireless environment are much more stressed than in the wired networks, but there are still products without any security functions and even the IEEE 802.11 specifies the security functions as an optional feature. Anyhow the

network equipment. So there is a real need for developing the security in the wireless networks.

4.2 Abbreviations and Definitions

In this document are following abbreviations (table 1) and definitions (table 2) used.

Table 1: Abbreviations

AP	Access Point
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BSS	Basic Service Set; A set of stations communication wirelessly on the same channel in the same area. (in IEEE 802.11)
CA	Certificate Authority
CAC	Channel Access Control (in HIPERLAN)
CAM	Channel Access Mechanism (in HIPERLAN)
CCITT	Comité Consultatif International Télégraphique et Téléphonique (now ITU-T)
ESS	Extended Service Set; A set of BSSs and wired LANs with Access Points that appear as a single logical BSS. (in IEEE 802.11)
ETSI	European Telecommunications Standards Institute
ETR	ETSI Technical Report
GSM	Global System for Mobile communications
HIPERLAN	HIgh PErformance Radio Local Area Network
HM-entity	HIPERLAN MAC entity
ICV	Integrity Check Vector
IEEE	Institute of Electrical and Electronics Engineers

4.3.1 HIPERLAN

HIPERLAN is ETSI's wireless broadband access standard, which defines the MAC sublayer, the Channel Access Control (CAC) sublayer and the physical layer. The MAC accesses the physical layer through the CAC, which allows easy adaptation for different physical layers. Currently defined physical layers use 5.15 - 5.30 GHz frequency band and support 2 048 Kbps synchronous traffic and up to 25 Mbps asynchronous traffic. HIPERLAN has following properties :

- it provides a service that is compatible with the ISO MAC service definition in ISO/IEC 15 802-1
- its operations are compatible with the ISO MAC bridges specification ISO/IEC 10 038 for interconnection with other LANs
- it may be deployed in pre-arranged or an ad-hoc fashion
- it supports node mobility
- it may have a coverage beyond the radio range limitation of single node
- it supports both asynchronous and time-bounded communication by means of a Channel Access Mechanism (CAM) with priorities providing hierarchical independence of performance
- its nodes may attempt to conserve power in communication by arranging when they need to be active for reception

The HIPERLAN specification defines an encryption-decryption scheme for optional use in the HIPERLAN. In this scheme, all HM-enties of a HIPERLAN shall use a common set of shared keys, referred as the HIPERLAN key-set. Each of these keys has an unique key identifier. Plain text is ciphered by XOR operation with random sequence generated by confidential algorithm, which uses as an input the secret key and initialization vector send in every MPDU. ETSI claims that defined scheme utilizes the level of protection of a wired LAN .

eavesdropping	Capturing the data by an unintended party
end-to-end	From the sending node to the intended receiver
integrity	The message can not be modified or replaced by unintended parties
key management	The policy to distribute and save the private and public keys
plain text	The data to be send before ciphered
pre-arranged	In pre-arranged configuration the wireless LAN has some fixed components, like bases
private key	A sensitive key that must not be compromised
public key	A non-sensitive that can be published
shared key	A secret key common to many users or network nodes
station-to-station	From one node to the next one in the network
transitive trust	An attack exploiting the host-host or network-network trust

4.3 Standards

This section describes two existing wireless network standards concentrating on the security functions they provide. The proprietary solutions (like Lucent Technologies WaveLAN), existing mobile telephone networks (like GSM) and future technologies (like wireless ATM or UMTS) are out of the scope of this paper.

ISO	International Standard Organisation
IV	Initialization Vector
LAN	Local Area Network
MAC	Medium Access Control
MPDU	MAC Protocol Data Unit
PEM	Privacy Enhanced Mail
PHY	Physical layer
PRNG	Pseudo Random Number Generator
bps	bits per second
SKCS	Shared Key Cryptography System
UMTS	Universal Mobile Telecommunications System
WEP	Wired Equivalent Privacy

Table 2: Definitions

ad-hoc	In ad-hoc configuration the wireless LAN has no fixed components
authentication	The identification of the parties
base	Usually fixed base station of the wireless LAN, sometimes referred as Access Point
cipher text	The data after ciphering
confidentiality	Only intended parties can access the data
coverage	The area where the transmission of the node can be heard
denial of service	An attack preventing the system from being used

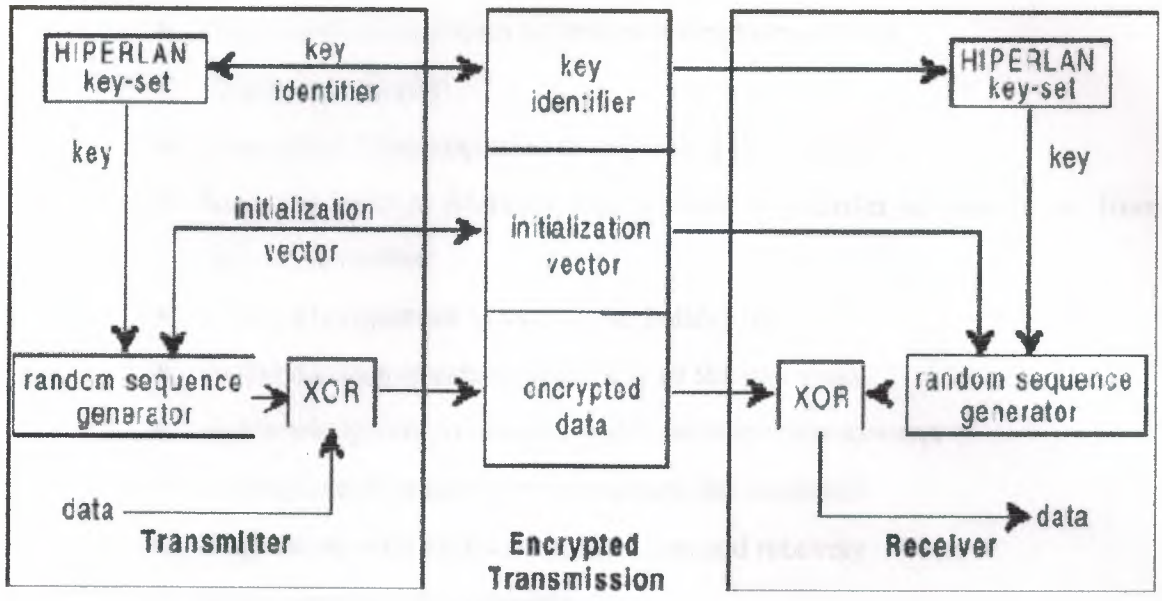


Figure 1: HIPERLAN encryption-decryption scheme

It is impossible to say anything for sure about the protection level that the WEP offers, because the algorithms are not available. But the lack of the independent and public analysis arouses some suspicions about the strength of the algorithms. The HIPERLAN standard does not define any kind of authentication, which sounds very strange for this kind of system. In my humble opinion one should not trust the security level offered by the HIPERLAN specification in any sensitive application, but use some additional mechanism to gain the security requirements sat to the wireless LAN.

4.3.2 IEEE 802.11

The IEEE 802.11 standard defines the physical layers and the MAC sublayers for the wireless LANs. There are three different physical layers: Frequency Hopping Spread Spectrum Radio, Direct Sequence Spread Spectrum Radio and Baseband Infrared. All physical layers can offer 2 Mbps data rate, the radio PHYs uses 2 400 - 2 483.5 MHz frequency band. The MAC layer is common for all three PHY and has the following features:

- Support of Iso-chronous as well as Asynchronous data
- Support of priority
- Association/Disassociation to an AP in a BSS or ESS
- Re-association or Mobility Management to transfer of association from one AP to another
- Power Management to save in the battery time
- Authentication to establish identity of the terminals
- Acknowledgment to ensure reliable wireless transmission
- Timing Synchronization to coordinate the terminals
- Sequencing with duplication detection and recovery
- Fragmentation / Re-assembly

The IEEE 802.11 defines two authentication schemes: Open System Authentication and Shared Key Authentication. The former is actually a null authentication, all mobiles requesting the access are accepted to the network. The later one uses shared key cryptography to authenticate the mobile. When a mobile request authentication, the base sends 128 octet (1024 bits) long random number to the mobile encrypted using shared key. The mobile decrypts the random number using the same shared key than the base and sends that back to the base. If the number that the base receives is correct, the mobile is accepted to the network. All mobiles allowed to connect to the network uses the same shared key, so this authentication method is only able to verify if the particular mobile belongs to the group of the mobiles allowed to connect to the network, but there is no way to distinct the mobiles from each other. There are also no means to authenticate the network by the mobile. The IEEE 802.11 does not define any key management functions.

The IEEE 802.11 defines an optional Wired Equivalent Privacy (WEP) mechanism to implement the confidentiality and integrity of the traffic in the network. WEP is used at the station-to-station level and does not offer any end-to-end security. WEP uses the RC4 PRNG algorithm based on a 40 bit secret key and a 24 bit initialization vector (IV) send with the data. WEP includes an integrity check vector

(ICV) to allow integrity check. One MPDU frame contains the clear text IV and ICV and the cipher text data block, so receiver is always able to decrypt the cipher text block and to check the integrity. The IV can always be new or reused for a limited time. The scheme is illustrated in.

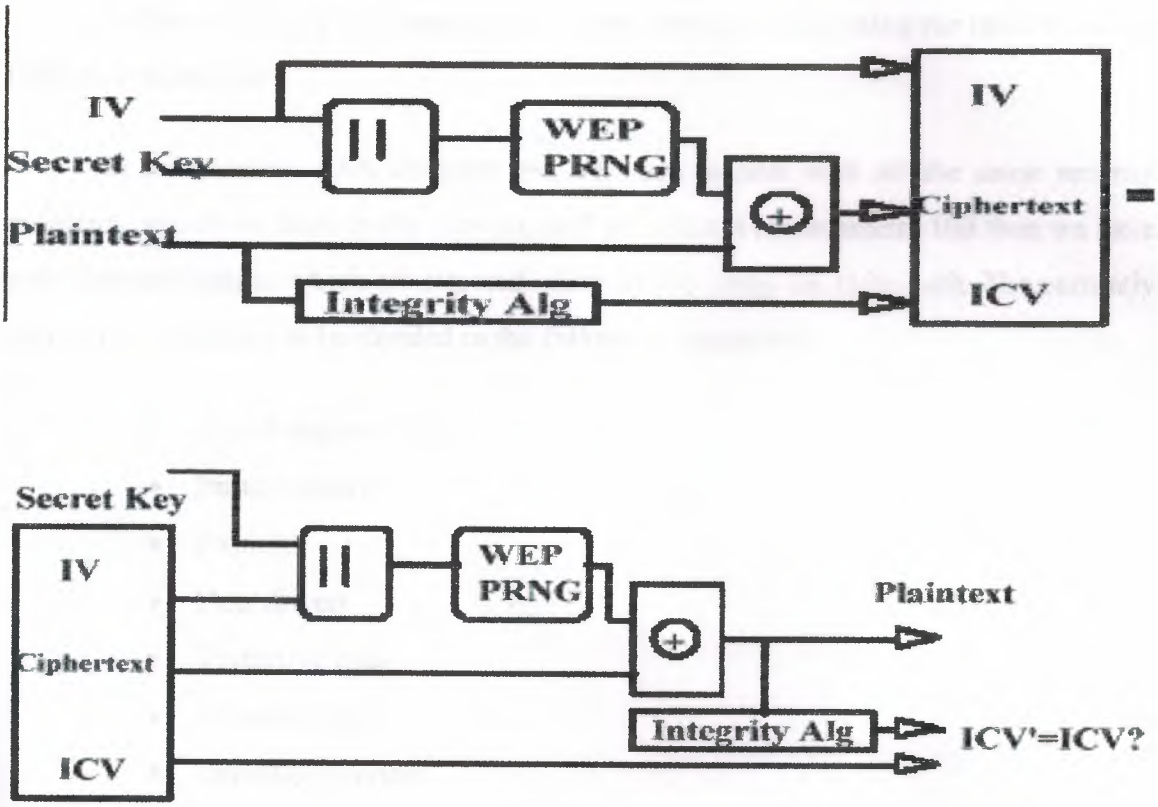


Figure 2: WEP mechanism

The PRNG algorithm used in IEEE 802.11 is RC4 from RSA inc. The actual algorithm is not public, but has been studyed in independent research laboratories under nondisclossure agreements and no weaknesses has not yet been reported, which does not guarantee that these does not exist. Anyway the secret key used is only 40 bits long, which can be solved by brute-force attack in 2 seconds with $100 000 hardware and 0.2 seconds with $1 000 000 hardware according the 1995 figures ; today the hardware prices are significantly lower. And even with some additional strength gained with variable IV the protection level of WEP may not be considered strength enough for the most sensitive

applications. The Shared Key Authentication scheme could be easily fooled using for example the play-back attack. So anyway an additional authentication mechanism is needed.

4.4 Threats and Vulnerabilities Compared to Wired LANs

In this section we will concentrate on the wireless LANs using the radio path as a transmission medium.

In the wireless LAN environment we have to deal with all the same security problems, which we have in the conventional wired LAN environment. But then we have some security issues, which are stressed when we are using the radio path. The currently know active attacks can be divided in the following categories:

- Social engineering
- Impersonation
- Exploits
- Data driven
- Transitive trust
- Infrastructure
- Denial of Service

The four first of these are similar in wired and wireless environment, so these are not discussed in this paper. Despite of the active attacks there exists the passive eavesdropping which is discussed at first.

4.4.1 Eavesdropping

Eavesdropping is very easy in the radio environment, when one sends a message over the radio path, everyone equipped with a suitable transceiver in the range of the transmission can eavesdrop the message. This kind of transceiver equipment, for example standard wireless LAN mobile, maybe with special antenna, are very reasonable priced.

The sender or intended receiver has no means to know if the transmission has been eavesdrop or not, so this kind of eavesdropping is absolutely undetectable.

The frequency band and transceiver power used has a great effect on the range where the transmission can be heard. When we are using 2 or 5 MHz radio band and transceiver power up to 1 W, as in the case of the current wireless LAN standards, the traffic of wireless LAN can be eavesdropped from outside the building which the network is operating if there is no special electromagnetic shielding. So we can not truly trust that our network stays inside our office building.

In the wireless LAN environment the ease of eavesdropping justifies quite costly procedures to guarantee the confidentiality of the network traffic. In all wireless LAN standards this is taken care by some kind of link level ciphering done by MAC-entities, but the safety gained with these algorithms may not be good enough for the most demanding applications.

4.4.2 Transitive Trust

When we have a wireless LAN as a part of our enterprise network, it offers one interface to the attacker, requiring no physical arrangements, to intrude on our network. In wired networks we can always track the wire from our computer to the next network node, but when we are working in the wireless environment there is no such way to find out with whom we are talking to. That makes the efficient authentication mechanisms crucial for the security of the wireless LANs. In all cases the both parties of the transmission should be able to authenticate each others.

The wireless LAN could be used as a launch pad to the transitive trust attack. If the attacker can fool our wireless LAN to trust the mobile he controls, then there is one hostile network node inside all firewalls of our enterprise network and it is very difficult to prevent any hostile actions after that. This kind of attack can be done from outside of our site with standard wireless LAN hardware compatible with our equipment. The only real protection against this kind of attacks is the strong authentication mechanism of the mobiles accessing the wireless LAN. The discovery of the unsuccessful attacks must rely

on the logging of unsuccessful logging attempts, but it might be very hard to find out if there has been a real attack attempt, because in the normal operation there comes unsuccessful logon attempts due the high BER in radio path and from mobiles that belongs to some other wireless LAN.

The other kind of transitive trust attack, special for wireless networks, is fooling the mobile to trust the base controlled by attacker as our base. When mobile is switched on it usually tries first to logon the network with strongest signal and if that fails then the rest ones in the order of the signal power. Now, if attacker has a base with high transmission power, he may be able to fool our mobiles to try first to logon the attackers network. Now there is basically two possibilities: the attacker may let as to logon his network and make it pretend our network and find out the passwords secret keys, etc. or the attacker may just reject our logon attempts but record all the messages during the logon process and find out the secret keys or passwords used in authentication in our network by analyzing these messages. The former case is very difficult to implement without very detailed information about our network services and is probably detected very soon, but the later one requires just standard base hardware, maybe with a special antenna, compatible with our equipment, and is very difficult to detect, because the mobiles do not usually report unsuccessful logon tries to the upper layers and the are a lot of unsuccessful logon attempts even in the normal circumstances. The only protection against these attacks is an efficient authentication mechanism which allows the mobile authenticate the base without any disclosure of the secret keys or passwords it uses to logon our network.

4.4.3 Infrastructure

The Infrastructure attacks are based on some weakness in the system: the software bug, configuration mistake, hardware failure, etc. This kind of situations will certainly occur in wireless LANs, too. But protection against this kind of attacks are almost impossible - You do not know about the bug until something happens. So the only thing to do is to keep the possible damages as small as possible.

4.4.4 Denial of Service

Due the nature of the radio transmission the wireless LANs are very vulnerable against denial of service attacks. If attacker has powerful enough transceiver, he can easily generate such a radio interference that our wireless LAN is unable to communicate using radio path. This kind of attack can be done from outside of our site, for example from a van parked on the street or from an apartment in the next block. Equipment needed to commit this kind of attack can be bought from any electronic store with reasonable price and any short-wave radio enthusiast has the knowledge needed to construct the equipment.

The protection against this kind of attacks is very difficult and expensive. The only total solution is to have our wireless network inside of the faraday cage, but this is applicable only in the very rare cases. But it is easy for authorities to locate the transceiver used to generate interference, so the attacker has limited time before the transceiver is found.

In the other hand the wireless LANs are not so vulnerable than the wired LANs to the other kind of denial of service attacks. For example the fixed LAN node can be isolated from the network by simple cutting the wire, which is not possible in wireless environment. If attacker cuts down the power of the whole site, then all wired networks are usually useless, but the wireless LANs can be used in the ad-hoc configuration with laptops or other battery powered computers.

4.5 Secure Solution

One can easily see that the standards described in chapter 3 does not fulfill the security requirements against the attacks described in chapter 4. This section will present some mechanisms and protocols that makes the wireless LANs safer.

4.5.1 Design Goals

The major requirement for this kind of solution is the seamless integration into existing wired networks. It is very probable that we have plenty of fixed network nodes already installed in our enterprise network, so we should avoid any modifications needs to the existing nodes.

There are different alternatives for securing a connection: end-to-end security at the application level, end-to-end security at the transport layer and link security at the link layer. In current data networks are only few commonly used end-to-end security schemes (like SSL and SSH), so the link security is the only applicable approach, if we want to leave our existing network alone.

Dropping end-to-end mechanisms out rules the user authentication out. We have only station-to-station (or machine-to-machine) authentication left, since those are the entities primry communicating over the wireless link. Machine-to-machine authentication is in fact conceptually correct for a security protocol at the link layer.

Another design goal is the two-way authentication, for the reasons discussed in 4.2 it is vital that both the base and the mobile are able to authenticate each others. Authentication mechanism should enable the identification of the mobiles and allow distinct keys used in different bases and mobiles.

The final goal is to have some flexibility to utilize the future advances in the cryptography. The should also be some interoperability between all versions of the wireless products, even if there exist different regulatory limitations for the use of the cryptography.

4.5.2 Design Overview

The solution discussed here needs several modifications for current wireless LAN products and standards, so the implementation of this solution is not currently feasible. But the aim is more to show the direction to which the evolution should go.

This is a hybrid solution: the authentication is done using public key cryptography and the ciphering of the transmission uses shared key cryptography. Shared keys are created during the authentication and may be changed during the transmission. The actual cryptography algorithms are not defined, because of the rapid development in this area.

4.5.3 Authorization

Table 3. defines nomenlactures used in this chapter.

Table 3: Nomenlactures	
E(X,Y)	encryption of Y under key X
MD(X)	Message Digest of X
Pub_CA	Public Key of Certification Authority
Priv_CA	Private Key of Certification Authority
Pub_Mobile	Public key of Mobile Host
Priv_Mobile	Private Key of Mobile Host
Pub_Base	Public key of Base Station
Priv_Base	Private Key of Base Station
Cert_Mobile	Certificate of Mobile Host
Cert_Base	Certificate of Base Station
Sig(X,Y)	signature of Y with key X where Sig(X,Y) = E(X, MD(Y))
Signed(X,Y)	resulting signed message {Y, Sig(X,Y)}

The authorization mechanism uses certificates formatted according to CCITT X.509 used in X.500 and PEM. A certificate contains the following information: {Serial Number, Validity Period, Machine Name, Machine Public Key, CA name}. Each certificate is signed by CA which might in our case be the enterprise's own CA.

The first message send from the mobile to the base contains following information: {Cert_Mobile, CH1, List of SKCSs}. CH1 is randomly generated number. The List of SKCSs is transmitted to allow negotiation of the used algorithm, the algorithm identifier and the key size are sent in the list.

When the base has received the first message, it will attempt to verify the signature on Cert Mobile. A valid signature proofs the public key in the certificate belongs to a certified mobile host but it is not sure if the certificate actually belongs to the mobile that submitted it. If the certificate is invalid, the base rejects the connection attempt.

Now the base will reply to the mobile by sending the message containing {Cert_Base, E(Pub_Mobile, RN1), Chosen SKCS, Sig(Priv_Base, {E(Pub_Mobile, RN1), Chosen SKCS, CH1, List of SKCSs}}}. Random Number RN1 is saved internally for later use. Chosen SKCS is one from the list sent by mobile and includes the algorithm identifier and the key size, the Chosen SKCS is the most secure from those supported by both the base and the mobile.

The mobile validates Cert Base, if certificate is valid, the Mobile will verify using the public key of the Base the signature off the message. The signature is valid and the base authenticated if the CH1 and the List of SKCSs matches with those sent by mobile to the base. Since the list of SKCSs is included in the signature, the attacker can not send the weakened list of SKCSs by jamming original message and sending his own, and we need not to sign the first message.

Now the mobile sends to the base message containing: {E(Pub_Base, RN2), Sig{Priv_Mobile, {E(Pub_Base, RN2), E(Pub_Mobile, RN1)}}}. The RN2 is a random

number generated by the mobile. The mobile will use the RN1 XOR RN2 as a session key for now on.

The Base verifies the signature of the message using Pub_Mobile obtained from Cert_Mobile in the first message. If the signature is valid, the mobile is authenticated. Next the base will decrypt E(Pub_Base, RN2) with it's own private key. Now the base can form the session key RN1 XOR RN2.

The session key is formed from two parts sent in different messages to gain better protection. Now the compromising of the mobile's private key does not compromise the whole traffic between the base and the mobile. Since the both halves of the session key are random and equal length, knowing either RN1 or RN2 tells nothing about the session key.

If all these steps has succeeded the mutual authentication has been done and the session is established. Figure 3 summarizes the authentication protocol. The correctness of this protocol is proofed in.

This authentication should be done in the MAC layer, before any network access is granted to the mobile. If we give to the mobile IP address before the authentication, it may be used as a launch pad even if it's authentication request is rejected.

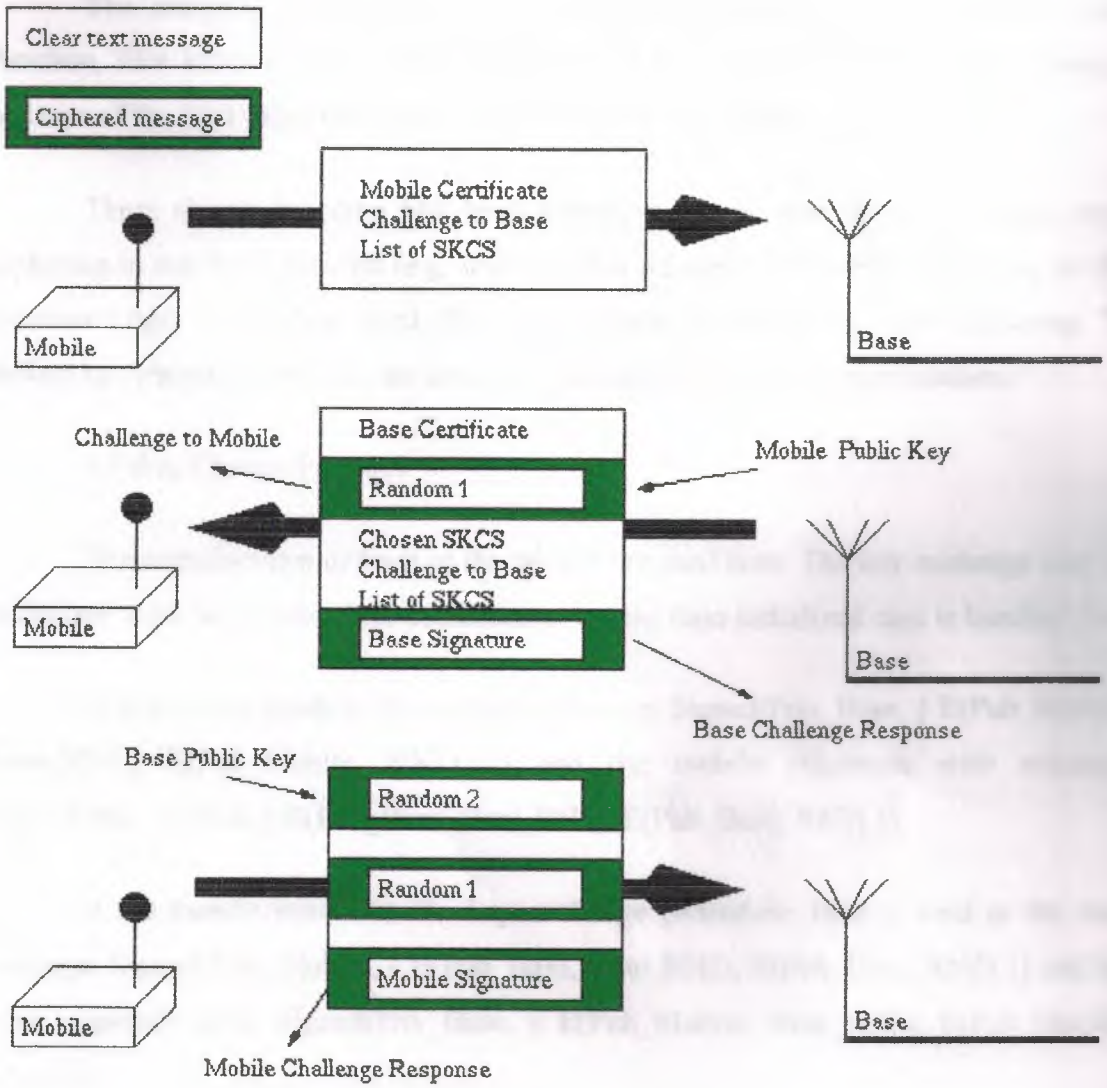


Figure 3: Authentication Protocol

4.5.4 Integrity and Confidentiality

The confidentiality can be archived by using some existing symmetric cryptography algorithm, like IDEA or DES. Once the session key is agreed, using mechanism described in 5.3, available algorithms are strong enough for our purposes. Anyhow the high BER on the radio link may set some limitations for the selected algorithm.

The integrity is archieved by a fingerprint generated by some one-way hash function, like MD5 or SHA. There should be a fingerprint in each MPDU message, because of the high pakect loss rate in the wireless environment.

There should be some link level ciphering in any case. If we are using some ciphering in our fixed network (e.g. IPSEC), then we can select weaker ciphering for the wireless LANs in the link level. But there should in anyway be some ciphering: To defend against traffic analysis we have to cipher also the network layer headers.

5.5 Key Change Protocol

The nomelactures defined in the table 3 are used here. The key exchange may be initialized from both ends of the communication, the base initialized case is handled first.

First the base sends to the mobile a message: Signed(Priv_Base, { E(Pub_Mobile, New_RN1), E(Pub_Mobile, RN1) }) and the mobile responses with message: Signed(Priv_Mobile, { E(Pub_Base, New_RN2), E(Pub_Base, RN2) }).

If the mobile initializes the key exchange procedure, then it send to the base message: Signed(Priv_Mobile, { E(Pub_Base, New_RN2), E(Pub_Base, RN2) }) and the base responses with: Signed(Priv_Base, { E(Pub_Mobile, New_RN1), E(Pub_Mobile, RN1) }).

Again the value new_RN1 XOR new_RN2 is used as the new session key. The values RN1 and RN2 are always the last ones used. In both cases the RN1 always refers to the random number generated by the base and RN2 the random number generated by the mobile. The values of RN1 and RN2 are verified against the internally saved values and if those does not match, the key exchange is ignored. Now the key exchanges can not be played back and we do not need to save any sequence numbers.

4.5.6 Key Management

The key management is one of the stuffest part implement convenient way. One possible procedure using the smart card technology is described below:

1. CA creates the private and public keys inside the smard card by the way that the private key is never readable from the smart card.
2. CA signs the public key with his private key and stored the signed public key to the smart card.
3. The smart card is given to the end user, which may now use the smart card in any wireless LAN mobile.

In order to avoid reading the private key from the smart card the public key cryptography system must be run inside the smart card and the calculation power of the smart cards sets some limitations for the efficiency of this approach. Of course the smart card reader is needed for each mobile used in the wireless LAN. But it is not very wild guess that the smart card technology will become more efficient and cheaper in the near future.

The concept described here is not the only one: it is also possible to use the Wep of Trust scheme for the key management (like in PGP) or the user may generate the key par by himself and then give the public key to the CA for the certificate signing, but the user identification must be somehow done also in this case.

4.5.7 Solution Analysis

The solution described above fulfills are goals stated in 5.1: The authentication mechanism implements the mutual authentication. The negotiation of the symmetric cryptography algorithm gives some flexibility between different versions and allows future enhancements. The concept does not need any modifications to the existing networks.

This solution is designed for maximum security, which may limit the performance of the network. One may consider using faster ciphering for example the insensitive video clips, but a much better (and therefore slower) ciphering for sensitive traffic. There is no end-to-end security offered, that must be taken care in upper layers.

Key management using the smart cards has been found quite functional even in mass products, like GSM. The major challenge is the limited computing power in the smart card, which leads to the longer authentication time. The time used for authentication may become critical if mobile moves from one base station to another and the hand over procedure must be performed. The authentication procedure during hand over could be speed up by using different authentication scheme described in, but this kind of optimization is out of the scope of this paper. The longer computing time leads also to the greater power consuption, which is always one critical aspect in the mobile environment.

This concept does not support multiple CAs and in large networks that may become a problem, anyhow the multiple CA support could be archived with just minor modifications described in. Another problem for this kind of concept is multicast support, this solution has no support for ciphered multicast.

4.6 Conclusions

The current wireless LAN standards offer very unsatisfactory level of security and one could not truly trust them. When using products based on these standards must the security issues been taken care in the upper layers. The authentication mechanism described in 5.3 may be used over IP to perform end-to-end authentication, as described in, but this approach gives a potential launch pad for the attacker.

Some commonly used attacks are more stressed in wireless environment and some additional effort should be used to prevent those. The nature of the radio communication makes it practically impossible to prevent some attacks, like denial of service using radio interference. When the wireless networks are used in strategic applications, like manufacturing or hospitals, the possibility of this kind of attack should be taken into account with a great care.

As showed in chapter 5 the quite secure wireless LAN is possible to implement with current technology. The current hardware could be used with only some modifications in the MAC layer protocols and over that new MAC the current IP may be

used without any problems. Anyway it is not probable that products supporting this level of security comes to the markets soon, mostly due the USA regulations; almost all manufactures are American.

CONCLUSION

Demand for wireless access to LANs is growing due to a rapidly increasing number of mobile devices, such as laptops and PDAs. Users want untethered network access at all times and everywhere. WLAN is a solution that is very attractive to satisfy needs of such users. Due to the fact that data are transmitted through such an open medium, special measures need to be put in place to insure data security and integrity. Current widely deployed 802.11b standard was shown to have significant security flaws in its implementation. Vendors have already put out new solutions to resolve some of the issues with the 802.11standard, but those solutions have been available for only a few months and it is hard to say if they will pass the test of time. Data security in wireless LANs will continue to be an exciting field of research for the scientific community and the wireless industry in general.

REFERNCES

[1] K. Pahlavan, A. Zahedi, P. Krishnamurthy. Evolving Wireless LAN Industry - Products and Standards. Invited paper PIMRC'97, Worcester Polytechnic Institute, 1997

[2] A. Zahedi, P. Krishnamurthy, S. Bagchi, K. Pahlavan. An Update on the Evolution of the Wireless LAN Services. Worcester Polytechnic Institute, 1997

[3] ETS 300 652. High PErformance Radio Local Area Network (HIPERLAN) Type 1; Functional specification. ETSI, 1996

[4] ETS 300 652. High PErformance Radio Local Area Network (HIPERLAN) Type 1; Functional specification - URGENT TECHNICAL CORRECTION. ETSI, 1997

[5] TR 101 054. Rules for the management of the HIPERLAN Standard Encryption Algorithm (HSEA). ETSI, 1997

[6] draft standard IEEE 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE, 1996

[7] CCITT X.509 The Directory - Authentication Framework. CCITT, 1988

[8] T. Raivisto. Applying Cryptography to GSM Short Message Services. Master Thesis, Helsinki University of Technology, Espoo 1997

[9] J. Blommers, "Practical Planning for Network Growth", Prentice Hall PTR&HP, 1996

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

[11] M. Andrade, Security for Next Generation, Wireless LANs ver.