NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

WIRELESS LOCAL AREA NETWORKS

Graduation Project
COM-400

Submitted By: Zaher Aldein mahameed

STUDENT NUMBER: 20011309

SUPERVISOR: DR. MURAT TEZER

NICOSIA-2005

ACKNOWLEDGEMENT

First of all, I feel proud to pay my special regards to my project adviser Dr. Murad Tezer. He never disappointed me in any affair. He delivered me too much information and did his best of efforts to make me able to complete my project. He has Devine place in my heart and I am less than the half without his help. I am really thankful to my teacher.

More over I want to pay special regards to my parents who are enduring these all expenses and supporting me in all events. I am nothing without their prayers. They also encouraged me in crises. I shall never forget their sacrifices for my education so that I can enjoy my successful life as they are expecting. They may get peaceful life in Heaven.

And also I want to thank my uncle who has given me a lot of support. At the end I am again thankful to those all persons who helped me or even encouraged me to complete me, my project. My all efforts to complete this project might be fruitful.

To the best of my knowledge, I want to honor those all persons who have supported me or helped me in my project. I also pay my special thanks to my all friends who have helped me in my project and gave me their precious time to complete my project.

ABSTRACT

Wireless LAN is a group of computers which is connected together by wireless interfacing devices, and this group of computers has a different standards and protocols than other computer networks, which we are going to see in this project.

Wireless LAN helps organizations raise profits, cut costs, and increase efficiency. Wireless devices can be installed as an extension of your Ethernet™ backbone or as a standalone network.

Wireless networks offer many organizations a variety of key competitive advantages. Today's demanding and competitive marketplace environment has become extremely data-intensive.

Wireless LAN technology was specifically developed to move large amounts of data quickly and cost effectively. Wireless LANs have proven to help organizations of all kinds boost productivity, cut costs, and dramatically increase profitability by quickly accessing data.

Wireless technologies have become increasingly popular in our everyday business and personal lives. Personal digital assistants (PDA) allow individuals to access calendars, e-mail, address and phone number lists, and the Internet. Some technologies even offer global positioning system (GPS) capabilities that can pinpoint the location of the device anywhere in the world. Wireless technologies promise to offer even more features and functions in the next few years.

TABLE OF CONTENTS

Acknowledgment	i
Abstract	ii
Table of contents	iii
Introduction	vi
1. Over view of local area net work (LAN)	1
1.1 Introduction	1
1.2 How and why network exist	1
1.3 Goals of computer network	3
1.4 Classification of computer network	3
1.5 Local area network	6
1.6 LANs& WANs comparison	6
1.7 Major components of LANs	8
1.8 Types of local area network	9
1.8.1 Peer-to-Peer	9
1.8.2 Client server	10
1.9 Local area network connectivity devices	10
1.9.1 Repeaters	10
1.9.1.1 Repeaters features	12
1.9.2 Bridges	12
1.9.3 Routers	14
1.9.4 Brouters	16
1.9.5 Hubs	18
1.9.6 Gateways	18
1.10 Local area network(LAN) in the work place and its advantage	19
1.11 Emerging technology, wireless network	20
2.1 Introduction to wireless LAN	22
2.2 Wireless networks	22
2.2.1 Wireless LANs	23
2.2.2 Ad-hok network	23
2.3 What is wireless LAN	24
2.4 How does a wireless work	27
2.4.1 AD-HOK	27
2.4.2 Infrastructure	28
2.5 Benefits of wireless LAN	29
2.6 Where is wireless LAN being used	30
2.7 What is the advantages of wireless LAN	30
2.8 What is the disadvantages of wireless LAN	31
2.9 Wireless LAN benefits	31
2.9.1 Wireless flexibility	33
2.9.2 Remote connectivity	33
2.9.3 Prototyping	34
2.10 Wireless LAN applications	34
2.11 Wireless devices	36
2.11.1 Personal digital assistance	36
2.11.2 Smart phone	36
2.12 Standardization of wireless LAN	37
2.13 Equipment standards for wireless at LAN 2.4 GHz and 5 GHz	37
2.14 Frequency bands available internationally for 5GHz wireless	34

services
2.15 Radio technology 45
2.16 Alternative wireless technology 47
2.16.1 Bluetooth 47
2.16.2 Home RF 50
2.16.3 3G 51
3.1 Introduction to wireless LAN security 53
3.2 Wireless LAN threats and risk mitigation 54
3.3 Emerging wireless LAN technologies 56
3.4 Federal information processing standards 57
3.5 Security of 802.11 of wireless LAN 59
3.5.1 Security features of 802.11 wireless LAN per the standards 59
3.5.1.1Authentication 60
3.5.1.2 Privacy 62
3.5.1.3 Integrity 63
3.5.2 Problems with the IEEE 802.11 standard security 65
3.6 Security problems with WEP 65
3.7 Security requirements and threats 68
3.7.1 Loss of confidentiality 69
3.7.2 Loss of integrity 72
3.7.3 Loss of network availability 72
3.7.4 Other security risks 73
3.8 Risk mitigation 74
3.8.1 Management countermeasure 74
3.8.2 Operational countermeasure 75
3.8.3 Technical countermeasures 77
3.8.3.1 Software solutions 77
3.8.3.1.1 Access point configuration 77
3.8.3.1.2 Software patches and upgrades 79
3.8.3.1.3 Authentication 80
3.8.3.1.4 Personal firewalls 81
3.8.3.1.5 Intrusion detection system (IDS) 81
3.8.3.1.6 Encryption 84
3.8.3.1.7 Security assessment 85
3.8.3.2 Hardware solutions 85
3.8.3.2.1 Smart cards 86
3.8.3.2.2 Virtual private networks 86
3.8.3.2.3 Public key infrastructure (PIK) 90
3.9 Wireless LAN security check list 91
3.10 Security of Bluetooth 92
3.10.1 Security features of Bluetooth 94
3.10.1.1 Authentication 96
3.10.1.2 Confidentiality 98
4 Problems and solution to wireless LAN 100
4.1 Easy access 100
4.2 Rogue access point 100
4.3 Unauthorized use of service 101
4.4 Service and performance constraint 102
4.5 MAC spoofing and session 104
4.6 Traffic analysis and eaves dropping 105

4.7 Higher level attacks 106
4.8 Wireless sniffer 106
4.9 Broadcast monitoring 107
4.10 Arpspoofing and hijacking 107
4.11 Hijacking SSL(source socket layer) and SSH (source shell) connection 107
4.12 Wired equivalent privacy(WEP) 108
4.12.1 Attacks against WEP 108
4.13 What are the solution to minimize Wireless LAN security risk 109
4.13.1 Wireless security risk and architecture design 109
4.13.2 Basic field coverage 109
4.13.3 Threat base station as un rusted 109
4.13.4 Base station and configuration policy 109
4.13.4.1 802.1X security 110
4.13.4.2 MAC addressing filtering 110
4.13.4.3 Base station discovery 110
4.13.4.3.1 Honey pots FAK-AP 111
4.14 Wireless protection 111
4.15 Who is making 802.11 security solution 112
4.15.1 802.11 gateway infrastructure 112

INTRODUCTION

A Network is a group of computers and other devices that connected to each other. The most common types of Networks are LAN, WAN MAN. Wireless local area networks (WLANs) are the same as the traditional LAN but they have a wireless interface. With the introduction of small portable devices such as PDAs (personal digital assistants), the WLAN technology is becoming very popular. WLANs provide high speed data communication in small areas such as a building or an office. It allows users to move around in a confined area while they are still connected to the network. Examples of wireless LAN that are available today are NCR's waveLAN and Motorola's ALTAIR.

For some time, companies and individuals have connected computer with local area networks (LANs). This allowed the ability to access and share data, application and other services not resident on any one computer. The LAN users have at disposal much more information, data and applications then they could otherwise store by themselves.

With the increasing number of portable computers and highly mobile users, the need of wireless Local Area Networks is increasing. Wireless LANs are especially needed in environments that make the use of cable difficult or impractical. The main advantages offered by wireless LANs are portability, low installation costs and quick set up time.

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.

CHAPTER ONE

1. OVERVIEW OF LOCAL AREA NETWORKS (LANs)

1.1 Introduction

A network is a group of computers, printers, and other devices that are connected together with cables. Information travels over the cables, allowing network users to exchange documents & data with each other, print to the same printers, and generally share any hardware or software that is connected to the network. Each computer, printer, or other peripheral device that is connected to the network is called a node. Networks can have tens, thousands, or even millions of nodes. In the simplest terms, a network consists of two or more computers that are connected together to share information.

Principal components of a computer network:

- Computers (processing nodes or hosts)
- Data communication system (transmission media, communication processors, modems, routers, bridges, radio systems, satellites, switches, etc)

1.2 How and Why Network Exists?

The concept of linking a large numbers of users to a single computer via remote terminal is developed at MIT in the late 50s and early 60s. In 1962, Paul Baran develops the idea of distributed, packet-switching networks. The first commercially available WAN of the Advances Research Project Agency APRANET in 1969. Bob Kahn and Vint Cerf develop the basic ideas of the Internet in 1973.

In early 1980s, when desktop computers began to proliferate in the business world, then intent of their designers was to create machines that would operate independently of each other. Desktop computers slowly became powerful when applications like spreadsheets, databases and word processors included. The market for desktop computers exploded, and dozens of hardware and software vendors joined in the fierce competition to exploit the open opportunity for vast profits. The competition spurred intense technological development, which led to increased power on the desktop and lower prices. Businesses soon discovered that information is useful only when it is communicated between human beings. When large information being handled, it was impossible to pass along paper copies of information and ask each user to reenter it into

their computer. Copying files onto floppy disks and passing them around was a little better, but still took too long, and was impractical when individuals were separated by great distances. And you could never know for sure that the copy you received on a floppy disk was the most current version of the information-the other person might have updated it on their computer after the floppy was made.

For all the speed and power of the desktop computing environment, it was sadly lacking in the most important element: communication among members of the business team. The obvious solution was to link the desktop computers together, and link the group to shared central repository of information. To solve this problem, Computer manufactures started to create additional components that users could attach to their desktop computers, which would allow them to share data among themselves and access centrally located sources of information. Unfortunately the early designs for these networks were slow and tended to breakdown at critical moments.

Still, the desktop computers continued to evolve. As it became more powerful, capable of accessing larger and larger amounts of information, communications between desktop computers became more and more reliable, and the idea of a Local Area Network (LAN) became practical reality for businesses. Today, computer networks, with all their promise and power, are more complicated and reliable than stand-alone machines. Figure 1.1 shows the network connectivity in UK.

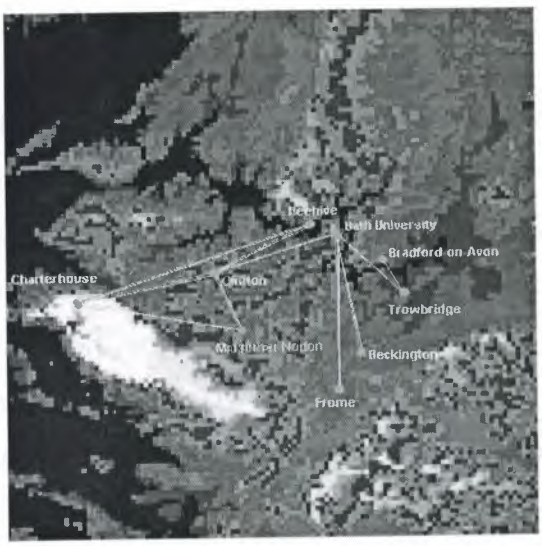


Figure 1.1 Computer Network Connectivity in UK

1.3 Goals of Computer Networks

1. Resource sharing and accessing them independently of their location.
2. Providing a universal environment for transmission of all kinds of information: data, speech, video, etc.
3. Supporting high reliability of accessing resources.
4. Distribution of loads according to the requirements very fast main frames, minis, PCs, etc.

1.4 Classification of Computer Networks

Network Classification Like snowflakes, no two networks are ever alike. So, it helps to classify them by some general characteristics for discussion. A given network can be characterized by its:

- Size: The geographic size of the network
- Security and Access: Who can access the network? How is access controlled?
- Protocol: The rules of communication in use on it (ex. TCP/IP, NetBEUI, AppleTalk, etc.)
- Hardware: The types of physical links and hardware that connect the network Computer experts generally classify computer network into following categories:
- Local Area Network (LAN): A computer network, with in a limited area, is known as local area network (e.g in the same building)
- Wide Area Network (WAN): A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.
- Metropolitan Area Network (MAN): A data network designed for a town or city. In terms of geographic breadth, MANs are larger than local-area networks (LANs), but smaller than wide-area networks (WANs). MANs are

usually characterized by very high-speed connections using fiber optical cable or other digital media.

- Campus Area Network (CAN): The computer network within a limited geographic area is known as campus area network such as campus, military base etc.
- Home Area Network (HAN): A network contained within a user's home that connects a person's digital devices. It connects a person's digital devices, from multiple computers and their peripheral devices to telephones, VCRs, televisions, video games, home security systems, fax machines and other digital devices that are wired into the network.

In figure 1.2 the connecttivity of local area networks to metropolitan area networks and typical use of metropolitan area networks to provide shared access to a wide area network is shown.

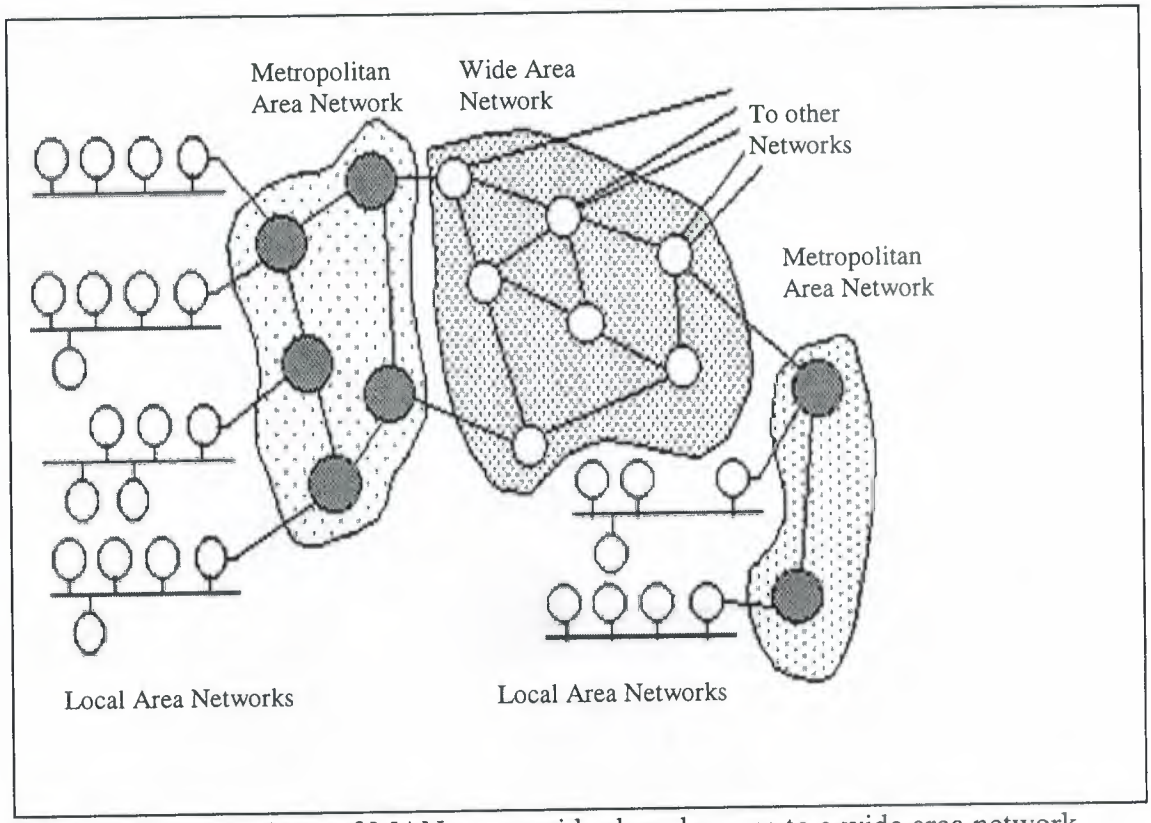


Figure 1.2 A typical use of MANs to provide shared access to a wide area network

Computer networks are used according to specified location and distance. In table 1.1 it is shown that which technology can be applied to the specific location and specific distance.

Table 1.1 Network Techonologies that Fit in Different Communication Spaces

NETWORK TYPE	DEFINITION	DISTANCE RANGE	COMMUNICATION SPACE
LAN	Local Area Network	0.1 to 1 Km	Building, floor, Room
WAN	Wide Area Network	100 to 10000+ Km	Region, Country
MAN	Metropolitan Area Network	10 to 100 Km	City
CAN	Campus Area Network	1 to 10 Km	Campus, Military base, Compnay site
HAN	Home Area Network	0.1 Km	Home

Table 1.1 Network Techonologies that Fit in Different Communication Spaces

In Figure 1.3 a chart is shown which specifies the distances and speeds of different networks.

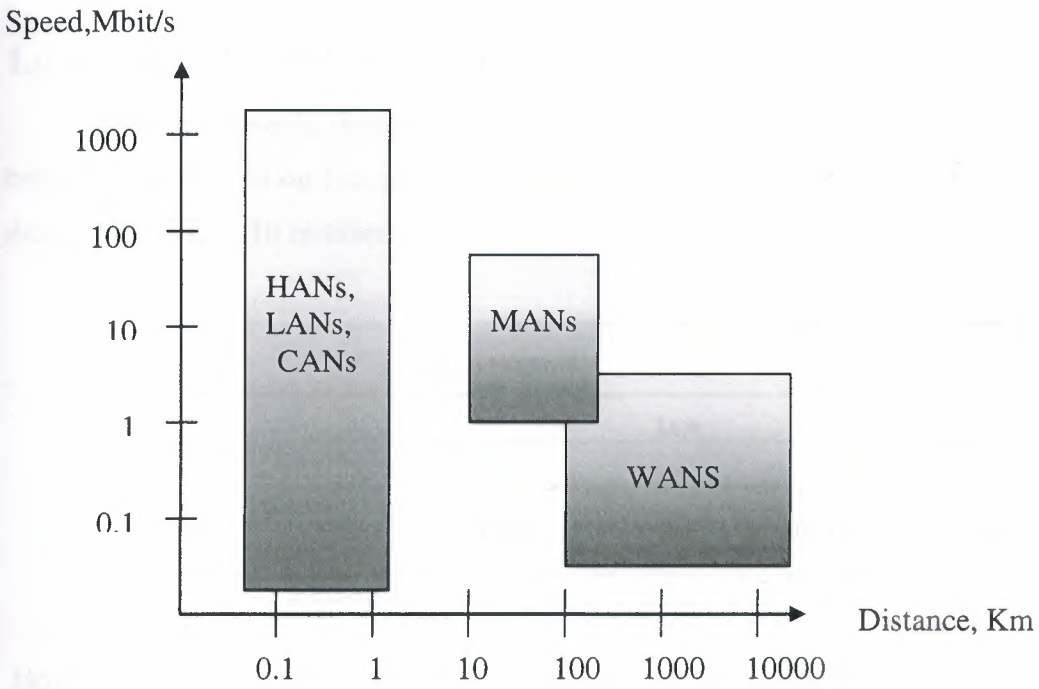


Figure 1.3 Distances and Speeds of the Different Networks

1.5 Local Area Networks

LANs are networks usually confined to a geographic area, such as a single building, office. LANs can be small, linking as few as three computers, but often link hundreds of computers used by thousands of people. The development of standard networking protocols and media has resulted in worldwide proliferation of LANs throughout business organizations. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions. Most LANs are built with relatively inexpensive hardware such as Ethernet cable and network interface cards (although wireless and other options exist). Specialized operating system software is also often used to configure a LAN. For example, some flavors of Microsoft Windows -- including Windows 98 SE, Windows 2000, and Windows ME -- come with a package called Internet Connection Sharing (ICS) that support controlled access to resources on the network.

1.6 LANs & WANs Comparison

LANs are usually faster than WANs, ranging in speed from 230 Kbps up to and beyond 1 Gbps (billion bits per second) as shown in Figure 1.4. They have very small delays of less than 10 milliseconds.

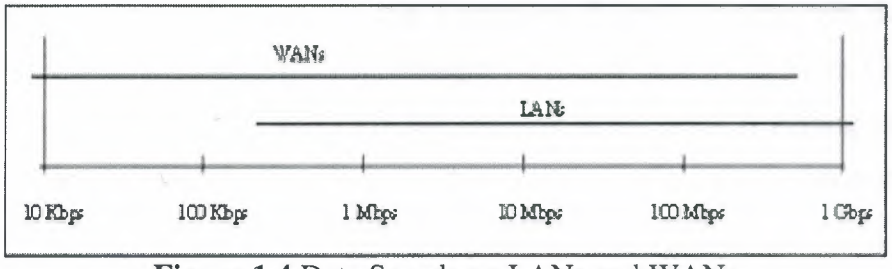


Figure 1.4 Data Speeds on LANs and WANs

How does one computer send information to another? It is actually rather simple.

The figure 1.5 shows and explains a simple network.

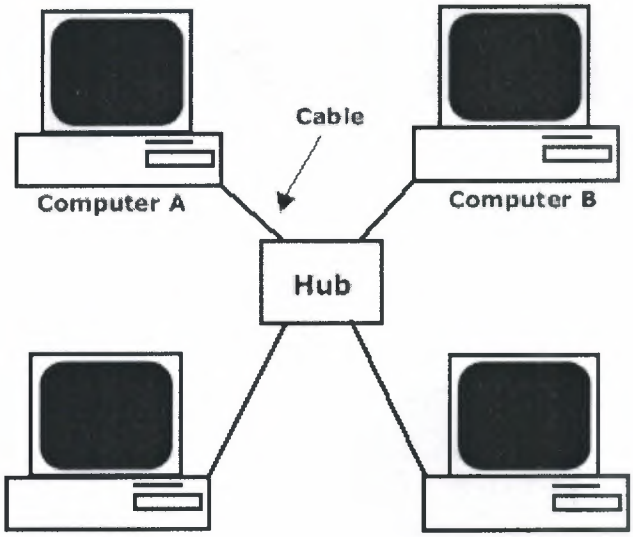


Figure 1.5 Simple Network

1. If Computer A wants to send a file to Computer B, the following would take place: Based on a protocol that both computers use, the NIC in Computer A translates the file (which consists of binary data -- 1's and 0's) into pulses of electricity.
2. The pulses of electricity pass through the cable with a minimum (hopefully) of resistance.
3. The hub takes in the electric pulses and shoots them out to all of the other cables.
4. Computer B's NIC interprets the pulses and decides if the message is for it or not. In this case it is, so, Computer B's NIC translates the pulses back into the 1's and 0's that make up the file.

Sounds easy. However, if anything untoward happens along the way, you have a problem, not a network. So, if Computer A sends the message to the network using NetBEUI, a Microsoft protocol, but Computer B only understands the TCP/IP protocol, it will not understand the message, no matter how many times Computer A sends it. Computer B also won't get the message if the cable is getting interference from the fluorescent lights etc. or if the network card has decided not to turn on today etc.

Figure 1.6 shows small Ethernet local area network.

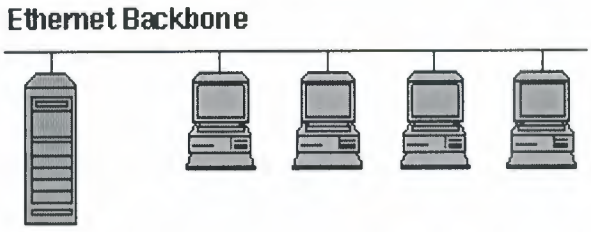


Figure 1.6 Small Ethernet LAN

The figure 1.7 shows briefly the interconnection of two LANs

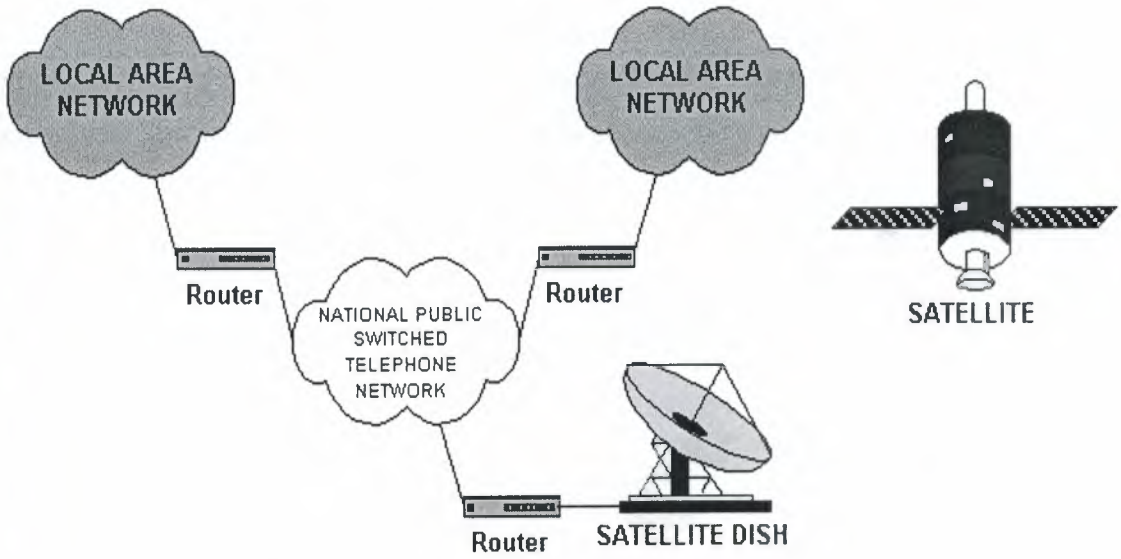


Figure 1.7 Interconnection of two LANs

1.7 Major Components of LANs

- Servers.
- Client / Workstation.
- Media.
- Shared Data.
- Shared Printers and other peripherals.
- Network Interface Card.
- Hubs / Concentrator.
- Repeaters, Bridges, Routers, Brouters, Gateways
- Physical connectors.

- Protocols.
- Network operating system (NOS).

1.8 Types of Local Area Networks

LANs are usually further divided into two major types:

1.8.1 Peer-to-Peer:

A peer-to-peer network doesn't have any dedicated servers or hierarchy among the computers. All of the computers on the network handle security and administration for themselves. The users must make the decisions about who gets access to what.

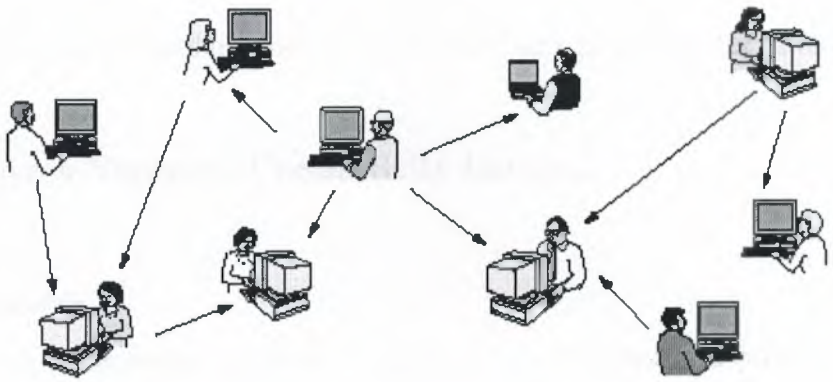


Figure 1-3. peer-to-peer system there are no fixed clients and server

Peer-to-peer communication really hit the big time around 2000 with a service called Napster, which at its peak had over 50 million music fans swapping music, in what was probably the biggest copyright infringement in all of recorded history (Lam and Tan, 2001; and Macedonia, 2000). The idea was fairly simple.

Members registered the music they had on their hard disks in a central database maintained on the Napster server. If a member wanted a song, he checked the database to see who had it and went directly there to get it. By not actually keeping any music on its machines, Napster argued that it was not infringing anyone's copyright. The courts did not agree and shut it down.

However, the next generation of peer-to-peer systems eliminates the central database by having each user maintain his own database locally, as well as providing a list of other nearby people who are members of the system. A new user can then go to any existing member to see what he has and get a list of other members to inspect for

more music and more names. This lookup process can be repeated indefinitely to build up a large local database of what is out there. It is an activity that would get tedious for people but is one at which computers excel.

Legal applications for peer-to-peer communication also exist. For example, fans sharing public domain music or sample tracks that new bands have released for publicity purposes, families sharing photos, movies, and genealogical information, and teenagers playing multi person on-line games. In fact, one of the most popular Internet applications of all, e-mail, is inherently peer-to-peer. This form of communication is expected to grow considerably in the future.

1.8.2 Client-Server:

A client-server network works the same way as a peer-to-peer network except that there is at least one computer that is dedicated as a server. The server stores files for sharing, controls access to the printer, and generally acts as the dictator of the network.

1.9 Local Area Networks Connectivity Devices

1.9.1 Repeaters

Boost signal in order to allow a signal to travel farther and prevent attenuation. Attenuation is the degradation of a signal as it travels farther from its origination. Repeaters do not filter packets and will forward broadcasts. Both segments must use the same access method, meaning that you can't connect a token ring segment to an Ethernet segment. Repeaters will connect different cable types.

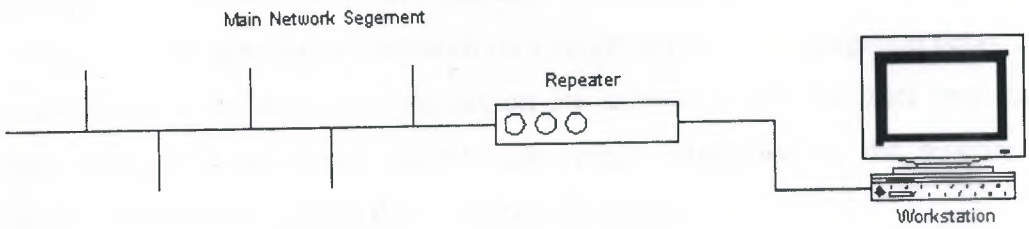


Figure 1.8 Repeater with workstation

- Also repeater extend the network segment by REGENERATING the signal from one segment to the next
- Repeaters regenerate BASEBAND, digital signals
- Don't translate or filter anything
- Is the least expensive alternative
- Work at the Physical layer of OSI
- Both segments being connected must use the same access method e.g. an 802.3 CSMA/CD (Ethernet) LAN segment can't be joined to an 802.5 (Token Ring) LAN segment. Another way of saying this is the Logical Link Protocols must be the same in order to send a signal.
- BUT repeaters CAN move packets from one physical medium to another: for example can take an Ethernet packet from a thinnet coax and pass it on to a fiber-optic segment. Same access method is being used on both segments, just a different medium to deliver the signal
- They send every bit of data on => NO FILTERING, so they can pass a broadcast storm along from on segment to the next and back. So you want to use a repeater when there isn't much traffic on either segment you are connecting.
- There are limits on the number of repeaters which can be used. The repeater counts as a single node in the maximum node count associated with the Ethernet standard [30 for thin coax].
- Repeaters also allow isolation of segments in the event of failures or fault conditions. Disconnecting one side of a repeater effectively isolates the associated segments from the network.
- Using repeaters simply allows you to extend your network distance limitations. It does not give you any more bandwidth or allow you to transmit data faster.
- Why only so many repeaters are allowed on a single network: "propagation delay". In cases where there are multiple repeaters on the same network, the brief time each repeater takes to clean up and amplify the signal, multiplied by the number of repeaters can cause a noticeable delay in network transmissions.
- It should be noted that in the above diagram, the network number assigned to the main network segment and the network number assigned to the other side of the repeater are the same.

- In addition, the traffic generated on one segment is propagated onto the other segment. This causes a rise in the total amount of traffic, so if the network segments are already heavily loaded, it's not a good idea to use a repeater.
- A repeater works at the Physical Layer by simply repeating all.. data from one segment to another.

1.9.1.1 Repeater features

- Increase traffic on segments
- Limitations on the number that can be used
- Propagate errors in the network
- Cannot be administered or controlled via remote access
- No traffic isolation or filtering

1.9.2 Bridges

Functions the same as a repeater, but can also divide a network in order to reduce traffic problems. A bridge can also connect unlike network segments (i.e. token ring and Ethernet). Bridges create routing tables based on the source address. If the bridge can't find the source address it will forward the packets to all segments.

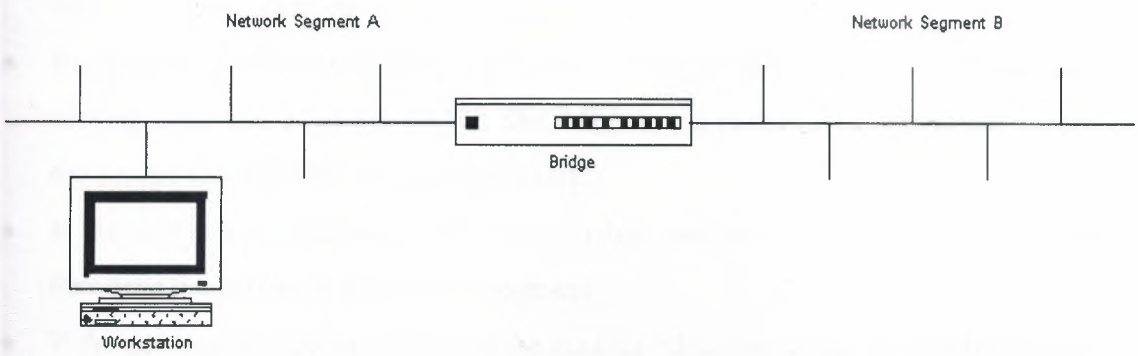


Figure 1.9 Bridge with work station

- Bridge have all the abilities of a repeater
- Bridges can take an overloaded network and split it into two networks, therefore they can divide the network to isolate traffic or problems and reduce the traffic on both segments
- Bridges expand the distance of a segment

- Link UNLIKE PHYSICAL MEDIA such as twisted-pair (10Base T) and coaxial Ethernet (10Base2)
- VERY IMPORTANT: they can link UNLIKE ACCESS CONTROL METHODS, on different segments such as Ethernet and Token Ring and forward packets between them. Exam Cram says this is a Translation Bridge that can do this - not all bridges - but my observation is questions don't necessarily mention the distinction.
- Bridges work at the Data Link Layer of the OSI model => they don't distinguish one protocol from the next and simply pass protocols along the network. (use a bridge to pass NetBEUI, a non-routable protocol, along the network)
- Bridges actually work at the MEDIA ACCESS CONTROL (MAC) sublayer. In fact they are sometimes called Media Access Control layer bridges. Here's how they deal with traffic:
- They listen to all traffic. Each time the bridge is presented with a frame, the source address is stored. The bridge builds up a table which identifies the segment to which the device is located on. This internal table is then used to determine which segment incoming frames should be forwarded to. The size of this table is important, especially if the network has a large number of workstations/servers.
- They check the source and destination address of each PACKET
- They build a routing table based on the SOURCE ADDRESSES. Soon they know which computers are on which segment
- Bridges are intelligent enough to do some routing: If the destination address is on the routing table and is on the SAME SEGMENT, the packet isn't forwarded. Therefore, the bridge can SEGMENT network traffic
- If the destination address is the routing table, and on a remote segment, the bridge forwards the packet to the correct segment
- If the destination address ISN'T on the routing table, the bridge forwards the packet to ALL segments.
- BRIDGES SIMPLY PASS ON BROADCAST MESSAGES, SO they too contribute to broadcast storms and don't help to reduce broadcast traffic
- Remote Bridges
- Two segments are joined by a bridge on each side, each connected to a synchronous modem and a telephone line
- There is a possibility that data might get into a continuous loop between LANs

- The SPANNING TREE ALGORITHM (STA)
  - Senses the existence of more than one route
  - Determines which is the most efficient and
  - Configures the bridge to use that route
  - This route can be altered if it becomes unusable.
  - Transparent bridges (also known as spanning tree, IEEE 802.1 D) make all routing decisions. The bridge is said to be transparent (invisible) to the workstations. The bridge will automatically initialize itself and configure its own routing information after it has been enabled.
  - Comparison of Bridges and Repeaters
  - Bridges
  - Regenerate data at the packet level
  - Accommodate more nodes than repeaters
  - Provide better network performance than repeaters because they segment the network
  - Implementing a Bridge
  - It can be an external, stand-alone piece of equipment
  - Or be installed on a server

1.9.3 Routers

A router is an Intermediate System (IS) which operates at the network layer of the OSI reference model. Routers may be used to connect two or more IP networks, or an IP network to an internet connection. A router consists of a computer with at least two network interface cards supporting the IP protocol. The router receives packets from each interface via a network interface and forwards the received packets to an appropriate output network interface. Received packets have all link layer protocol headers removed, and transmitted packets have a new link protocol header added prior to transmission.

The router uses the information held in the network layer header (i.e. IP header) to decide whether to forward each received packet, and which network interface to use to send the packet. Most packets are forwarded based on the packet's IP destination address, along with routing information held within the router in a routing table. Before a packet is

forwarded, the processor checks the Maximum Transfer Unit (MTU) of the specified interface. Packets larger than the interface's MTU must be fragmented by the router into two or more smaller packets. If a packet is received which has the Don't Fragment (DF) bit set in the packet header, the packet is not fragmented, but instead discarded. In this case, an ICMP error message is returned to the sender (i.e. to the original packet's IP source address) informing it of the interface's MTU size. This forms the basis for Path MTU discovery (PMTU). The routing and filter tables resemble similar tables in link layer bridges and switches. Except, that instead of specifying link hardware addresses (MAC addresses), the router table specify network (IP addresses). The routing table lists known IP destination addresses with the appropriate network interface to be used to reach that destination. A default entry may be specified to be used for all addresses not explicitly defined in the table. A filter table may also be used to ensure that unwanted packets are discarded. The filter may be used to deny access to particular protocols or to prevent unauthorized access from remote computers by discarding packets to specified destination addresses. A router forwards packets from one IP network to another IP network. Like other systems, it determines the IP network from the logical AND of an IP address with the associated subnetwork address mask. One execption to this rule is when a router receives an IP packet to a network broadcast address. In this case, the router discards the packet. Forwarding broadcast packet can lead to severe storms of packets, and if uncontrolled could lead to network overload.

A router introduces delay (latency) as it processes the packets it receives. The total delay observed is the sum of many components including:

- Time taken to process the frame by the data link protocol
- Time taken to select the correct output link (i.e. filtering and routing)
- Queuing delay at the output link (when the link is busy)
- Other activities which consume processor resources (computing routing tables, network management, generation of logging information)

The router queue of packets waiting to be sent also introduces a potential cause of packet loss. Since the router has a finite amount of buffer memory to hold the queue, a router which receives packets at too high a rate may experience a full queue. In this case

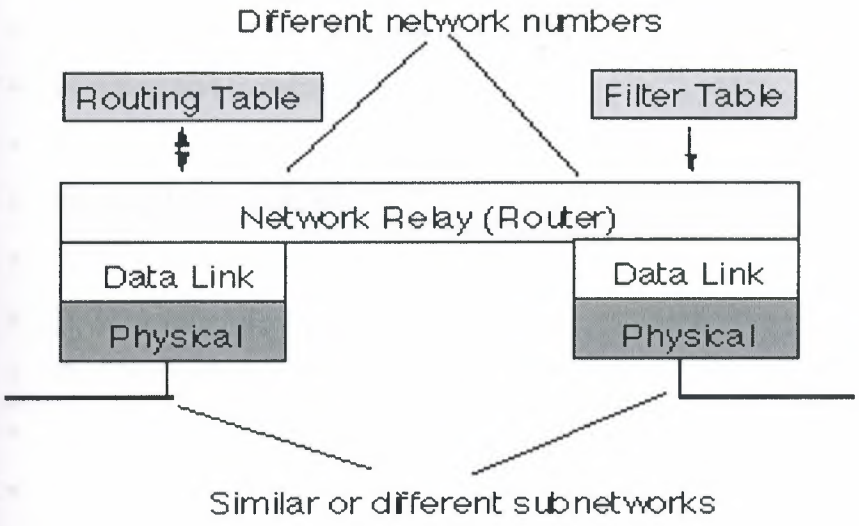


Figure 1.10: Shows Architecture of a Router

The router has no other option than to simply discard excess packets. If required, these may later be retransmitted by a transport protocol. Routers are often used to connect together networks which use different types of links (for instance an HDLC link connecting a WAN to a local Ethernet LAN). The optimum (and maximum) packet lengths (i.e. the Maximum Transfer Unit (MTU) is different for different types of network. A router may therefore use IP to provide segmentation of packets into a suitable size for transmission on a network. Associated protocols perform network error reporting (ICMP), communication between routers (to determine appropriate routes to each destination) and remote monitoring of the router operation (network management).

1.9.4 Brouters

A brouter has the best features of both routers and bridges in that it can be configured to pass the unroutable protocols by imitating a bridge, while not passing broadcast storms by acting as a router for other protocols.

- Determine the best path for sending data and filtering broadcast traffic to the local segment. They DON'T pass on broadcast traffic
- Work at the Network layer of OSI => they can switch and route packets across network segments

- They provide these functions of a bridge
- Filtering and isolating traffic
- Connecting network segments
- Routing table contains
- All known network addresses
- How to connect to other networks
- Possible paths between those routers
- Costs of sending data over those paths
- Not only network addresses but also media access control sublayer addresses for each node
- Routers
- REQUIRE specific addresses: they only understand network numbers which allow them to talk to other routers and local adapter card addresses
- Only pass Packets to the network segment they are destined for.
- Routers don't talk to remote computers, only to other routers
- They can segment large networks into smaller ones
- They act as a safety barrier (firewall) between segments
- They prohibit broadcast storms, because broadcasts and bad data aren't forwarded
- Are slower than most bridges can join dissimilar access methods: a router can route a packet from a TCP/IP Ethernet network to a TCP/IP Token Ring network
- Routers don't look at the destination computer address. They only look at the NETWORK address and they only pass on the data if the network address is known => less traffic
- **Routable protocols:**
    - DECnet, IP, IPX, OSI, XNS, DDP (Apple)
    - Routable protocols have Network layer addressing embedded
- **Non-routable protocols:**
    - LAT, NetBEUI, DLC
    - Non-routable protocols don't have network layer addressing

1.9.5 Hubs

There are many types of hubs:

- Passive hubs are don't require power and are simple splitters or combiners that group workstations into a single segment
- Active hubs require power and include a repeater function and are thus capable of upporting many more connections.
- Intelligent hubs provide
- Packet switching
- Traffic routing

1.9.6 Gateways

Often used as a connection to a mainframe or the internet. Gateways enable communications between different protocols, data types and environments. This is achieved via protocol conversion, whereby the gateway strips the protocol stack off of the packet and adds the appropriate stack for the other side.

- The TRANSLATOR -- allows communications between dissimilar systems or environments
- A gateway is usually a computer running gateway software connecting two different segments. For example an Intel-based PC on one segment can both communicate and share resources with a Macintosh computer or an SNA mainframe. Use gateways when different environments need to communicate. One common use for gateways is to translate between personal computers and mainframes
- GSNW is a gateway to allow Microsoft clients using SMB to connect to a NetWare server using NCP.
- Gateways work at the Application --> Transport layer
- They make communication possible between different architectures and environments
- They perform protocol AND data conversion / translation.
- They takes the data from one environment, strip it, and re-package it in the protocol stack from the destination system
- They repackage and convert data going from one environment to another so that each environment can understand the other environment's data

- Gateway links two systems don't use the same
- Protocols
- Data formatting structure
- Languages
- Architecture
- They are task specific in that they are dedicated to a specific type of conversion: e.g. "Windows NT Server -> SNA Server Gateway"
- Usually one computer is designated as the gateway computer. This adds a lot of traffic to that segment
- **Disadvantages of the gateways**
    - They slow things down because of the work they do
    - They are expensive
    - Difficult to configure
- Remember, gateways can translate
    - Protocols e.g. IPX/SPX --> TCP/IP
    - And data (PC --> Mac)

1.10 Local Area Networks (LAN) in the work place and its advantages

Network allows more efficient management of resources. For example, multiple users can share a single top quality printer, rather than putting lesser quality printers on individual desktops. Also network software licenses can be less costly than separate, stand alone licenses for the same number of users.

Network helps keep information reliable and up-to-date. A well managed, centralized data storage system allows multiple users to access data from different locations, and limit access to data while it is being processed.

Network helps speeds up data sharing. Transferring files across a network is almost always faster than other, non-network means of sharing files.

Networks help business service their clients more effectively. Remote access to centralized data allows employees to service clients in the field, and clients to communicate directly to suppliers.

Speed: Networks provide a very rapid method for sharing and transferring files. Without a network, files are shared by copying them to floppy disks, then carrying or sending the disks from one computer to another. This method of transferring files is very time-consuming.

Security: Files and programs on a network can be designated as "copy inhibit," so that you do not have to worry about illegal copying of programs. Also, passwords can be established for specific directories to restrict access to authorized users.

Centralized Software Management: One of the greatest benefits of installing a local area network is the fact that all of the software can be loaded on one computer (the file server). This eliminates that need to spend time and energy installing updates and tracking files on independent computers throughout the building.

Electronic Mail: The presence of a network provides the hardware necessary to install an e-mail system. E-mail aids in personal and professional communication for all personnel, and it facilitates the dissemination of general information to the entire school staff. Electronic mail on a LAN can enable students to communicate with teachers and peers at their own school. If the LAN is connected to the Internet, people can communicate with others throughout the world. Network allows workgroups to communicate more effectively. Electronic mail and messaging is a staple of most network systems, in addition to scheduling systems, project monitoring, on-line conferencing and groupware, all of which help work teams be more productive.

Workgroup Computing: Workgroup software (such as Microsoft BackOffice) allows many users to work on a document or project concurrently. For example, educators located at various schools within a county could simultaneously contribute their ideas about new curriculum standards to the same document and spreadsheets.

1.11 Emerging Technology, Wireless Networks

Wireless networking refers to hardware and software combinations that enable two or more appliances to share data with each other without direct cable connections. Thus, in its widest sense, wireless networking includes cell and satellite phones, pagers, two-way radios, wireless LANs and modems, and Global Positioning Systems (GPS). Wireless LANs enable client computers and the server to communicate with one another without direct cable connections. Figure 1.8 and 1.9 shows the wireless network.

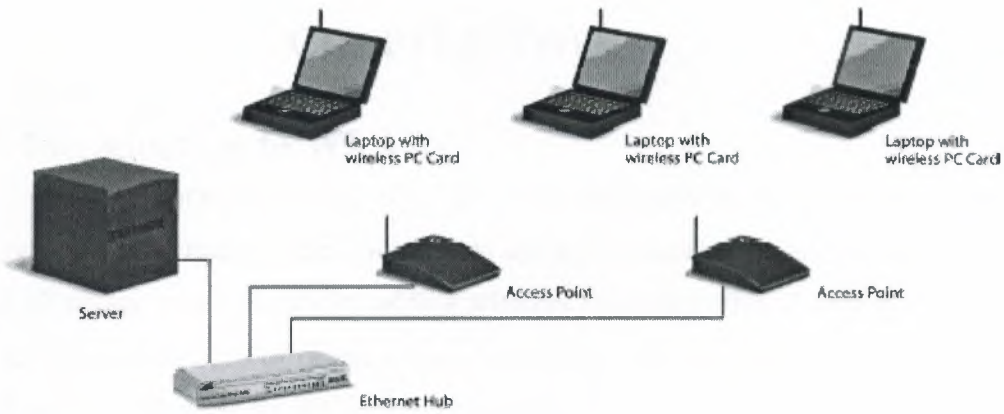


Figure 1.11 Wireless Network

Figure 1.12 Wireless Peer-to-Peer Network

CHAPTER TWO

2.1 Introduction to WLANs

Wireless Local Area Networks (WLANs) have moved quickly to the mainstream and are now found in many homes, businesses and public areas. Organisations have been keen to take advantage of the flexibility adding wireless networks offer. A recent study by the Meta Group found that 30% of organizations have implemented wireless networks and that over 50% will have done so by 2006[1]. The emergence of new security standards has also increased confidence in WLANs. Users are becoming more familiar with the technology and are increasingly expecting wireless access to be available. There is a wide range of products and standards involved in WLAN technology and more continue to emerge. This paper will focus on wireless LAN and the issues surrounding its implementation.

2.2 Wireless Networks

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range: Wireless Wide Area Networks (WWAN), WLANs, and Wireless Personal Area Networks (WPAN). WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), and Mobitex. WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others. WPAN, represents wireless personal area network technologies such as Bluetooth and IR. All of these technologies are "tetherless"—they receive and transmit information using electromagnetic (EM) waves. Wireless technologies use wavelengths ranging from the radio frequency (RF) band up to and above the IR band.2 The frequencies in the RF band cover a significant portion of the EM radiation spectrum, extending from 9 kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of gigahertz (GHz). As the frequency is increased beyond the RF spectrum, EM

energy moves into the IR and then the visible spectrum. (See Appendix A for a list of common wireless frequencies.) This document focuses on WLAN and WPAN technologies.

2.2.1 Wireless LANs

WLANs allow greater flexibility and portability than do traditional wired local area networks (LAN).

Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point device. An access point communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (approximately 100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network device. Access point cells can be linked together to allow users to even "roam" within a building or between buildings.

2.2.2 Ad Hoc Networks

Ad hoc networks such as Bluetooth are networks designed to dynamically connect remote devices such as cell phones, laptops, and PDAs. These networks are termed "ad hoc" because of their shifting network topologies. Whereas WLANs use a fixed network infrastructure, ad hoc networks maintain random network configurations, relying on a master-slave system connected by wireless links to enable devices to communicate. In a Bluetooth network, the master of the piconet controls the changing network topologies of these networks. It also controls the flow of data between devices that are capable of supporting direct links to each other. As devices move about in an unpredictable fashion, these networks must be reconfigured on the fly to handle the dynamic topology. The routing that protocol Bluetooth employs allows the master to establish and maintain these shifting networks.

Figure 2-1 illustrates an example of a Bluetooth-enabled mobile phone connecting to a mobile phone network, synchronizing with a PDA address book, and downloading e-mail on an IEEE 802.11 WLAN.

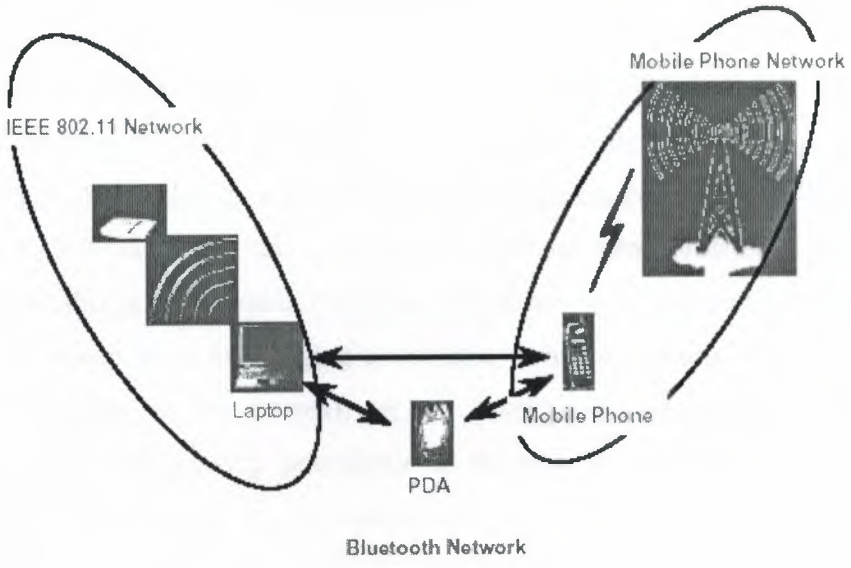


Figure 2-1. Notional Ad Hoc Network

2.3 What is a wireless LAN?

A wireless LAN (WLAN) is a wireless local area network. That is, it is a high bandwidth, two-way data communications network using radio or infrared as the medium of transmission rather than optical fiber or copper cable and operating over a limited geographic area.10 The components of WLANs usually include two types of equipment: a wireless station and an access point, although peer-to-peer networking is sometimes employed. The wireless station is typically a laptop or personal computer (PC) equipped with a wireless network interface card (NIC). Such a card may also be installed in a desktop computer or handheld device, such as a personal digital assistant (PDA), or equipment in a kiosk. The NICs use radio frequencies or infrared beams to enable connections to the WLAN. For public access services, access points can be provided in a number of public places such as airports and coffee shops.

The NIC automatically search through the channels to find WLANs. Once the NIC finds the correct channel, it starts "setting up a connection" with the access point. While WLAN technologies were originally designed to complement the existing fixed-connection

LANs, they can be used to replace wired access or to extend existing wired infrastructure. WLANs are being deployed not only in business but also by end-users as a cost-saving measure or for convenience.

Instead of installing expensive wiring infrastructure, the WLAN user has access to communications by use of a small radio transmitter. Any computer with WLAN can potentially pick up the signal as long as it is within its reach. WLANs are often not completely "wireless" in that supporting the wireless workstations are a number of existing wired broadband backbone networks. The exception to this is peer-to-peer networks, which may be created on ad hoc basis: for example, networks of laptop users exchanging documents during a meeting. The increasing prevalence of WLANs depends, in this context, on the development of existing broadband networks. At the same time, the growing popularity of WLANs is expected to provide an incentive for the construction of networks for shared use. It is now possible to envision a communications world consisting of base stations that connect to the Internet through wired broadband networks, and local connectivity.

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.

Currently, Wireless LAN technology is significantly slower than wired LAN. Wireless LANs have a nominal data transfer rate of between 11 and 54 Megabits per second (Mbps) compared to most wired LANs in schools which operate at 100Mbps. Newly installed wired networks can now operate at up to 1,000Mbps (1Gb).

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.

There are several wireless technologies in existence, but most wireless LANs use wireless Ethernet technologies based on IEEE 802.11 standards (see: Current Standards).

The term Wi-Fi (Wireless Fidelity) is often used to refer to 802.11 wireless networks. It comes from the testing and certification programme run by the Wi-Fi Alliance (see below) to ensure wireless products from different manufacturers comply with standards and are interoperable.

WLANs emerged for business use in the early 1990s. At that time, however, speed limitations, lack of hardware compatibility, insufficient awareness among consumers, etc., slowed diffusion. As a result, most enterprises remained with their existing wired networks instead of moving to WLANs. However, many of these initial problems have been overcome, and now there is significant growth in the WLAN market.

Worldwide, the 802.11 market, including 802.11b and 802.11a, has reportedly increased from revenues of USD 231.4 million in the first quarter of 2001 to USD 380.2 million in the second quarter of 2002.

During 2002, many businesses, which include such chains as McDonald's, Starbucks Coffee, and MOS Burger, have been installing WLANs and creating "hot spots" one after another in certain model outlets for the convenience of their customers.

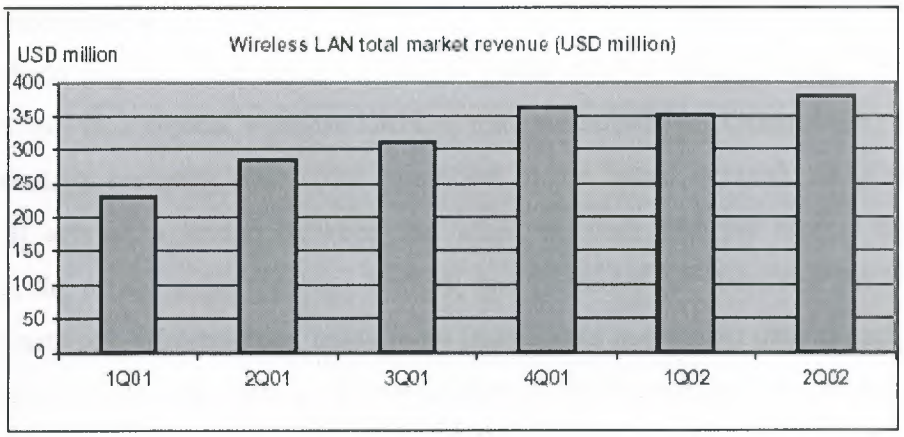


Figure 2.2: Wireless LAN Total Market Revenue Between The First Quarter of 2001 and Second Quarter of 2002

2.4 How does a WLAN work?

To access a wireless network all devices will need to have a wireless network interface card (NIC) either built in, or installed separately. Wireless NICs are available in various forms and with different interfaces to suit different devices e.g. PCMCIA and PCI cards; CF (Compact Flash) and SD (Secure Digital) cards; and USB wireless network adaptors. In all cases the necessary software drivers may also need installing. Increasingly, portable devices are being sold with wireless LAN connectivity as a standard feature. Most new laptop and tablet PC models for example have in-built wireless and this is also now included on many PDAs. Built-in wireless adapter cards have now overtaken external wireless adapter cards in the market. There are two main types of wireless network configuration: ad-hoc mode and infrastructure mode.

2.4.1. Ad-hoc

Networks are the simplest form of wireless network created by two or more wireless enabled computers communicating with each other directly. These types of WLANs are useful for creating small dynamic networks. However, these ad-hoc networks have similar limitations as wired peer to peer networks and are only really suitable for occasional, small networks of a few computers. Ad-hoc networks cannot provide the same security as properly implemented infrastructure mode networks.

2.4.2.Infrastructure

Mode requires one or more access points (APs) through which the network cards communicate. In a typical wireless LAN, a transmitter/receiver (transceiver) device, called an access point, is normally physically connected to the wired network using standard Ethernet cabling. It acts as a bridge between the wired network and the remote computer(s). At a minimum, the access point receives, buffers, and transmits data between the wireless LAN and the wired network infrastructure, using radio frequencies to transmit data to each user.

Access points can have a varying amount of intelligence and functionality built-in. There are two main types of AP. "Thick" APs are fully functional and can handle all processes. "Thin" APs only include radios and antennas and rely on controllers (WLAN switches/appliances) for other functionality including managing APs, security and authentication. There is also a third hybrid category with some limited radio frequency management functionality, but that still need controllers to function fully.

The vast majority of WLANs use fully functional (thick) APs in a decentralised architecture. The APs are usually deployed in stand-alone mode, but in larger networks where the communication between APs poses an unacceptable load, a controller can be used to handle load balancing and roaming. There is a management overhead in configuring and managing each access point, although overlay management tools are available (see Managing WLANs).

Centralised architectures are far less common. In these networks all traffic passes through the controllers (WLAN switches/WLAN Appliances), which handle load balancing and other management functions. The APs deal with RF access and often enforce policies set by the controller. Various manufacturers balance the functionality between controllers and APs differently. Centralized networks are generally considered easier to manage than decentralized networks. They can also allow seamless roaming of users across subnets. However, these tend to be single vendor solutions and the increased cost of centralized equipment is usually only justified in large, complex or multi-site deployments.

2.5 Benefits of wireless LANs

The cost of deploying WLANs is less than wired networks while having most of the capabilities of wired. There are no cabling and associated labour costs and the spectrum used is mostly deregulated. Network access can be set up rapidly permanently or for temporary use (*e.g.* a conference). In addition, WLANs provide opportunities for "third parties" to use the network free of charge. WLANs are also convenient. They provide users with more mobility and flexibility by allowing them to maintain broadband connection when they roam from one area of coverage to another. WLANs can also be a partial solution to the last-mile problem as well as to geographical digital divide in a longer term by providing community networks at a lower cost. WLANs also provide fast transmission speed with most WLANs transmitting at speeds of at least 2 Mbps and with typical maximum speeds of 10 Mbps.

A feature of WLANs that has captured public imagination is that they may be used to provide broadband access in public places and, sometimes at no perceived charge to the user. In some cases such public access results from the ability to use private corporate wireless networks aimed at providing service within a building, but that can be accessed outside of buildings because they are not fully secured. Such "free rides" can also be deliberate as a result of individuals setting up neighbourhood hot spots. The ability to access broadband networks free of charge from public locations has led to the concept of "warchalking"

Box 1. Warchalking

Putting chalk marks on pavements and walls to show the location of wireless networks is becoming popular in some countries such as the United Kingdom and the US. This phenomenon, called "warchalking", derives from the early days of telecommunications networks when hackers would engage in "wardialing", the process of trying to find phone lines being used by computers that were ripe for hacking. Users looking for free Internet access drive or walk in the hope of finding areas where wireless access has "spilled" into the street. In this context, the so-called "wardriving" and "warwalking" phenomena have developed.

Unpaid access to wireless broadband networks has led to some major cable and telephone companies that provide broadband wired connections to complain that customers are violating their service agreements by giving others a "piggyback" using WLANs to extend the reach of wired broadband networks. For example, a spokesman for Time Warner Cable argued that free

riding on WLANs was similar to cable theft.14 From a legal perspective, this issue may become important in the future.

2.6 Where are WLANs being used?

The DfES 'Survey of Information and Communications Technology in Schools 2004' report indicated that, of the secondary schools with a network, 54% had some wireless LAN provision. For primary and special schools this figure was 21%[2].

In business: WLANs are increasingly being installed by business to provide flexible access, or for specific tasks such as stock taking in warehouses.

In the wider community:

Wireless networks can be used for public access to the Internet. Commercially available public access wireless networks are more commonly known as 'hotspots' and there are now thousands of these throughout the UK; located at railway stations, airports, hotels, in certain public libraries, in cafés and eating establishments, and at underground stations in London.

2.7 What are the advantages of a WLAN?

A wireless LAN has some specific advantages over wired LAN:

- Access to the network can be from anywhere in the school within range of an access point, giving users the freedom to use ICT where and when it is needed.
- It is typically easier and quicker to add or move devices on the network (once in place, a wired LAN can be difficult to move and expensive to change.) Increasing the overall network coverage of the wireless LAN can often be achieved by adding further access points.
- Small dynamic ad hoc networks can be created very quickly and relatively easily.
- It is typically easier and quicker to provide connectivity to the network in areas where it is difficult or undesirable to lay cable or drill through walls. Instances might be:
  -where a school is located on more than one site or is made up of several buildings.
  -when implementation is anticipated to be temporary or semi-permanent

-when only one device is required at a remote part of a building or site

-In historic buildings where traditional cabling would be difficult to in stall or inappropriate

- Where wireless enabled laptop computers are used, any classroom in range of an access point can become a 'computer suite', potentially increasing the use of ICT across the curriculum
- While the initial investment required for wireless LAN hardware can be similar to the cost of wired LAN hardware, installation expenses can be significantly lower
- Wireless provides increased flexibility for teachers. A teacher with a wireless enabled laptop can access the wireless network to show students work, share resources, obtain information from the internet from anywhere within range of an AP, without being tied to a wired PC. This flexibility is further enhanced when combined with a wireless projector.
- Portability. They allow computer devices to move around the school with the pupil rather than the pupil going to a specific place to use a device. This allows for outdoor field work and work in non-classroom spaces (library, canteen, gymnasium/sports hall, playground).

2.8 What are the disadvantages of a WLAN

- As the number of devices using the network increases, the data transfer rate to each device will decrease accordingly.
- The current data rates of wireless networks means that high bandwidth activities are better done on wired networks
- As wireless standards change, it may be necessary, or at least desirable, to upgrade to higher specifications of wireless which could mean replacing wireless equipment (wireless NICs, access points etc). Currently, wireless standards are changing more quickly than wired standards.
- Security is more difficult to guarantee.
- Devices will only operate at a limited distance from an access point, with the distance largely determined by the standard used. Obstacles between the access point and the

user, like walls, glass, water, trees and leaves can also determine the distance of operation. Poor signal reception has been experienced around reinforced concrete school buildings; these may require higher numbers of access points which in turn increases overall cost.

- In practice, a wireless LAN on its own is not a complete solution and will still require a wired LAN to be in place to provide a network backbone.
- Data speeds drop as the user moves further away from the access point
- It is easier to make a wired network 'future proof' for future requirements
- As the number of people using wireless devices increases, there is the risk that certain radio frequencies used for wireless will become congested and prone to interference; particularly the 2.4GHz.frequency.

A significant problem arising from the use of WLANs is security. In comparison with wired technology, the nature of radio transmission inevitably includes the possibility of eavesdropping. This issue will be dealt in a separate section of this paper.

As the numbers of systems in operation grow, services operating in close proximity result in service degradation . This is especially true where services are deployed outdoors or in public locations. This problem is particularly severe where spread spectrum technologies are used. IEEE standards 802.11 and 802.11b are frequency hopping spread spectrum modulation (FHSS) and direct sequence spread spectrum (DSSS) modulation respectively in the 2.4 GHz band. Both standards lack interference mitigation measures or any form of operational etiquette. Where services are co-located, degradation of operation is therefore inevitable. Further technical developments, mainly at 5 GHz band, seek to improve the potential for systems to co-exist by employing better modulation schemes (for example OFDM, orthogonal frequency division multiplexing), agreed channel plans, random back off, transmit power control (TPC) and dynamic frequency selections (DFS)

Another difficulty relates to the nature of radio propagation at microwave frequencies. In the frequency bands used for WLANs transmitter power limits are relatively low. WLANs are therefore a short-range networking solution. Users will find communications disrupted once they move out of range. A further difficulty is that there is no agreed international roaming standard. In order for roaming to work, frequency allocations must be unified, standards for operation must

be harmonise, billing systems must be interoperable, and service operators must be sure of the ability of their partners to provide a similar quality of services.15 Even then systems from different vendors may not be inter-operable even if they employ the same technology and the same frequency band due to differences in implementation.

WLANs may also face difficulties in making a business case for investment. Costs to build a nationwide proprietary wireless network in the United States are high (some estimates put this at around USD 1 billion) and the return on investment is at present not sure. Further, the free-riding phenomenon tends to put a damper on profit expectations.
It is likely that free wireless Internet services will continue for a period of time as a grassroots effort.

However, there are potential customers, especially business users, who are willing to pay for a better quality of WLAN services. In many cases, business customers will be willing to pay monthly subscription fees to ensure continuous access as well as certain level of service and security. Widespread adoption of
WLANs in businesses might lay the groundwork for individuals to set up their own WLAN access points. It must always be emphasised, however, that WLANs can never be more than a "best efforts" service where they operate in deregulated radio spectrum.

2.9 Wireless LAN benefits

The key benefits of using Wireless LANs in education include:

2.9.1Wireless Flexibility

The ability to move beyond the traditional computer suite or classroom.
Most schools are not flood-wired, with lots of cabling and power sockets in every room. This usually means that some areas are beyond the reach of a cabled network. As many teaching resources are now on line, either on the school's network or on the Internet, this can create problem

2.9.2 Remote connectivity. The ability to maintain connectivity to central resources while working in a remote location, such as outdoors. Wireless LANs can provide network connectivity in locations where it is difficult or expensive to deploy a cabled network connection.

2.9.3 Prototyping.

Wireless LAN allows the prototyping of small, connected learning environments without high capital costs involved with cabling. These benefits are not offered by cabled networks, but there are also some drawbacks to using wireless technology.

2.10 Wireless LAN application

There are a number of WLAN applications for businesses as well as residential users. Vertical markets such as health care, education, manufacturing, retail, and warehousing were early users of WLAN technology. For example, it has been suggested that WLANs shorten hospital visits because they deliver medical information to physicians and other hospital staff when and where they require it.16 By the same token, workers in warehouses can use a portable computer to verify the inventory by WLAN to see if an item is available. The use of WLANs at school is also gradually percolating in some OECD countries. In the United Kingdom, for example, thousands of schools use both 2.4 GHz and 5 GHz band enabled equipment to distribute broadband services and to provide wire free working in the classroom.

Nowadays, there is also a significant amount of interest in WLAN technologies in the public access markets. WLAN users have Internet access in local access points called "hot spots" such as coffee shops, hotels, train stations and airports. The hot spots allow portable computing devices equipped with wireless cards to connect to the Internet. This type of application is raising interest especially as new portable computing devices, such as PDAs, emerge. Thus, some private companies are developing a system for public WLAN services. For example, Cisco Systems is working with Internet service providers (ISPs) across Europe to equip international airports with wireless broadband technologies in an effort to enable broadband access for business travellers on the move.17 But, although the number of WLAN hot spots is growing rapidly in some OECD countries such as the United States, particularly in urban areas, they are still difficult to find in the most countries and in rural areas.

The SOHO (small office home office) market segment is viewed as particularly important for WLANs with some predictions estimating growth at about 40% between 2003 and 2006.18 In

the arena of Wi-Fi telephony (discussed later) WLAN is expected to work as a means to provide ubiquitous telephone services, which are essential to the SOHO markets. It will be of great convenience that WLANs replace the need to install and pay for traditional Ethernet CAT5 cabling and jacks in the office infrastructure with a simpler as well as cost-effective solution, although not all telephony requires CAT5 cabling. In very recent years, some new types of applications have emerged. For example, Air Canada has been using Wi-Fi networks to find people who are about to miss their flights and to process their tickets as well as give them seat assignments on the flight.19 In the United States, about 150 homes in Houston use WLAN to create wireless billboards in order to replace scribbled notes on kitchen refrigerators which serve as a family bulletin board. There is also a pilot project in which WLANs are used to help cook a meal.20 WLANs also might provide an innovative application in combination with voice over IP technology, particularly in the arena of corporate telephony.21 Traditionally, voice and data networks have been separate. With the emergence of Voice over IP (VoIP) technology it has become possible to transmit telephone conversations over any packet-switched IP networks. As a result, IP telephony using wireless technology, which is called Wi-Fi telephony, has started to develop. IP networks are cost-effective but less secure compared with traditional telephony circuits. An increasing number of enterprises have adopted Wi-Fi telephony, where mobile users are easily identified. They usually have control over the coverage area, bandwidth utilisation as well as required Quality of Service (QoS) implementation. In this way, Wi-Fi users in the enterprise have the same features and accessibility to the corporate telephony system as their wired colleagues.

WLAN applications are also developing in residential areas. Residential IP telephone service can easily be made available if the cost of Wi-Fi telephones is equivalent to PSTN costs. In some countries contractors are now putting equipment for use of WLANs into each new home. For example, Canadian house builders in the towns of Embrun, Russell and Metcalfe are installing a wireless box of Storm Internet, a wireless ISP, in each house because a number of new buyers are not interested in a rural house if it cannot get broadband Internet access.22 With a WLAN, multiple terminals can be connected to a single line, allowing everyone in the family to use the Internet at the same time if they choose.23

Another technology that could be used in WLAN applications is ultra-wide band (UWB). The combination of low power, short range, and high data rate communications makes UWB a good

match for home or office networking. UWB can also be used as a replacement for Bluetooth (described later) to provide wireless connection to peripherals.

2.11 Wireless Devices

A wide range of devices use wireless technologies, with handheld devices being the most prevalent form today. This document discusses the most commonly used wireless handheld devices such as text messaging devices, PDAs, and smart phones.

2.11.1 Personal Digital Assistants

PDAs are data organizers that are small enough to fit into a shirt pocket or a purse. PDAs offer applications such as office productivity, database applications, address books, schedulers, and to-do lists, and they allow users to synchronize data between two PDAs and between a PDA and a personal computer. Newer versions allow users to download their e-mail and to connect to the Internet. Security administrators may also encounter one-way and two-way text-messaging devices. These devices operate on a proprietary networking standard that disseminates e-mail to remote devices by accessing the corporate network. Text-messaging technology is designed to monitor a user's inbox for new e-mail and relay the mail to the user's wireless handheld device via the Internet and wireless network.

2.11.2 Smart Phones

Mobile wireless telephones, or cell phones, are telephones that have shortwave analog or digital transmission capabilities that allow users to establish wireless connections to nearby transmitters. As with WLANs, the transmitter's span of coverage is called a "cell." As the cell phone user moves from one cell to the next, the telephone connection is effectively passed from one local cell transmitter to the next.

Today's cell phone is rapidly evolving to integration with PDAs, thus providing users with increased wireless e-mail andInternet access. Mobile phones with information-processing and data networking capabilities are called "smart phones." This document addresses the risks introduced by the information processing and networking capabilities of smart phones.

2.12 STANDARDIZATION OF WIRELESS LAN

The WLAN industry has emerged as one of the rapidly growing sectors in the telecommunications arena. It has been reported that worldwide sales of WLAN equipment, consisting of network interface cards, access points and bridges, reached USD 450 million in the first quarter of 2002, which is a three percent increase from the end of 2001 and 55% increase from the first quarter of 2001.24 This market development owes much to the introduction of standardization in WLAN products. Standardization has allowed WLANs to inter-operate between vendors. It implies that a variety of WLAN equipment can be used over the same wireless infrastructure. Standardization has also benefited performance and cost. For example, standardization has helped expand product lines and lower costs of components, lowering prices for users. The most important area of standardization is that of standardizing the frequency bands used to provide communications. A de facto worldwide band has developed at 2.4 GHz (2400-2483.5 MHz). This has happened because this band is designated for industrial, scientific and medical (ISM) use. However co-existence with true ISM devices is detrimental to the development of WLAN services and other bands are being sought. The three bands at 5 GHz (Band A-5150-5350 MHz, Band B-5470-5725 MHz and Band C-5725-5875 MHz) are considered to be the best candidates. However, to promote the greatest economic development it will be necessary for all three bands to be allocated to this service on a worldwide basis. WRC 2003 will consider bands A and B, whereas C is not on the agreed agenda.

2.13 Equipment standards for WLANs at 2.4 GHz and 5 GHz

There is a confusing range of different equipment available for operation of WLANs. Across the world the lack of unified frequency bands and operating parameters means that there are wide variations in equipment availability and suitability. The main radio frequency bands used are around 2.4 GHz and 5 GHz. Infrared technology may also be used but has largely been abandoned due to the physical DSTI/ICCP/TISP(2002)10/FINAL 13 constraints that use of infrared places on range and path. Each WLAN technology has its own advantages.
Accordingly, it is very difficult to choose the best technology. The following table briefly summarises themain WLAN standards.

Table2.1: Main WLAN Standards

Standard	Frequency band	Year approved	Comments
IEEE 802.11	2.4 GHz	July 1997	Frequency hopping spread spectrum ~2Mbit/s
IEEE 802.11a	5 GHz	September 1999	OFDM but without dynamic frequency selection (DFS) 20-54 Mbit/s.
IEEE 802.11b	2.4 GHz	September 1999	Direct sequence spread spectrum up to 11 Mbit/s
IEEE 802.11g	2.4 GHz	To be approved	OFDM or Direct sequence spread spectrum up to 54 Mbit/s similar to IEEE 802.11a&b standards but in the 2.4 GHz band
IEEE 802.11h	5 GHz	Awaiting the results of the WRC	International agreement on DFS parameters was reached in January 2003 at the ITU. The WRC in
HIPERLAN 2	5 GHz	Awaiting the results of the WRC	July 2003 will consider mandatory use of DFS in harmonised international frequency allocations for WLAN at 5 GHZ
Bluetooth	2.4 GHz		FHSS bit rate less than 1 Mbit/s
IEEE 802.16	5 GHz (band C)	In development at the moment	Closely associated with the European HIPERMAN standard and intended for fixed wireless access.
HIPERMAN	5 GHz (band C)	In development	

No single standard is likely to emerge in the future to support WLANs. As with all radio technologies, different equipment and protocols suit different applications. Some researchers also mentioned that these specifications would be developed to co-exist with one another rather than to replace each other.

- **802.11b**

When creating a WLAN standard at the 802.11 Working Group established by the IEEE 802 Executive Committee, 802.11b emerged as an extension to 802.11 with data rates of 1 and 2 Mbps in order to satisfy future needs. While 802.11a was also an extension of 802.11, 802.11b has been given great attention by the industry as a standard for WLANs. As mentioned earlier, 802.11b is well known as "Wi-Fi" (wireless fidelity) and this seal will provide users the assurance that products bearing this logo will work together. At the present economic juncture of the ICT industry 802.11b has now become one of the bright spots for the telecommunications as well as PC industries. Indeed, it has been reported that the number of 802.11b users grew from almost zero in early 2001 to more than 15 million at the end of 2001.34

The 802.11b standard uses DSSS and can provide data rates up to 11 Mbps at 2.4 GHz. Sales of network cards for laptop and desktop computers as well as Wi-Fi access points are increasing rapidly. One difficulty of this standard, which uses 2.4 GHz, is that this frequency band is subject to potential interference including other wireless technologies such as Bluetooth, HomeRF,

microwave ovens, cordless phones, and amateur radio.35 It has been suggested that it will eventually be replaced by products that have higher data rates as well as better quality of service and security.

- **802.11a**

The 802.11a standard uses a more modern radio technology, orthogonal frequency division multiplexing (OFDM), to offer data rates up to 54 Mbps in the 5 GHz bands. This technology has several advantages in comparison with currently standardised 802.11b. First, it offers a faster bit rate. It can transmit data up to five times faster than 802.11b. The justification for higher transmission speed lies in the fact that wireless vendors have faced the challenges of supporting increasing numbers of applications that need large bandwidth access, such as streaming video. This feature will have the potential to let wireless access be used for the most demanding applications. OFDM technology does not have the particular vulnerability of spread spectrum techniques to interference from similar systems. 802.11a has been developed in conjunction with the development of HiperLAN2. Both standards intend to make faster and more interference resistant use of the cleaner, more plentiful radio spectrum offered at 5 GHz.

The increase in speed also resulted in a technical challenge caused by "delay spread". Delay spread is caused by the echoing of transmitted radio frequency. Radio signals are always refracted by objects such as walls, floors and furniture so that a baseband processor is required to unravel the divergent received signals. In this context, an innovative technique, OFDM, used in European digital TV and radio transmission, has helped solve this problem.

Secondly, 802.11a has a large capacity. Up to 12 (or 19 in Europe) non-overlapping channels are available in most 5 GHz bands, in contrast to only three channels in the case of 2.4 GHz band. The total bandwidth available in the 5 GHz band, 200 MHz (455 MHz in Europe), is higher than in the 2.4 GHz band, 83.5 MHz. Therefore, 802.11a can support more broadband users simultaneously without conflict.

The higher capacity of this technology will better support densely populated areas. However, despite these advantages, there are some disadvantages, especially in the early stages of use: higher cost, range constraints, and limited product support. In addition, a critical

disadvantage of 802.11a would be the fact that it is not physically compatible with 802.11b. For example, a 2.4 GHz 802.11b access point cannot work directly with a 5 GHz 802.11a network card. Yet, it is possible for the two technologies to communicate. For example, 802.11a users and 802.11b users can be connected to the same LAN and share network resources including broadband Internet access provided that suitable radio equipment for both frequency bands is installed. The principle and essential disadvantage of 802.11a is that it does not include implementation of two vital interference mitigation techniques known as dynamic frequency selection (DFS) and transmit power control (TPC). TPC is a well-known technique whereby when a radio link has been established the equipment lowers the transmit power level to the minimum needed to maintain that link. It has benefits for mobile equipment because it conserves battery power thus increasing operational time between recharging. For the purpose of radio spectrum management, it has huge benefits in cleaning the spectrum. It may be estimated that the number of potential co-existing systems with TPC is of the order of double where it is not deployed. Lack of TPC has huge implications for the economic development of the mass WLAN market since ultimately there is a physical limit to the number of co-existing systems. The aim of good design is to increase that limit to permit greater development. TPC also plays an important role in limiting the cumulative levels of radiation in this band, known as the noise floor. As the noise floor rises at 5 GHz it will tend towards causing interference to satellite and radar systems. When it reaches a certain level it will no longer be possible for these services to co-exist and under the present radio regulations it will be WLANs that will be legally bound to withdraw.

802.11a also lacks DFS and for this reason it is unlikely to be permitted to be used in wide spread deployment in European countries. It is also possible that its operation will be curtailed or restricted in the US as concern grews over its interference potential to radar operation and other services sharing the band. DFS enabled equipment monitors the radio channel for the presence of other users. On detection it backs off, selects another free channel randomly, and moves to it. It continues to monitor throughout. This has the effect of spreading use across all the available channels again maximizing the numbers of co-existing users and protecting other services otherwise prone to interference from the OFDM signal, principally, radar. The specification for DFS has been developed at the ITU and will be an internationally recognized measure.

Lack of TPC and DFS is a fatal flaw in the 802.11a standard and it is very likely that it will be superseded by the 802.11h version, which does include them.

- **802.11g**

The 802.11g standard is defined as a technology for operation at 2.4 GHz which provides higher data rates than 802.11b, up to 54 Mbps, using OFDM. This technology is as fast as 802.11a with more security as well as compatibility with 802.11b. This standard also supports complementary code keying (CCK) modulation and allows packet binary convolutional coding (PBCC) modulation as an option for faster links. Moreover, it has lower costs, thanks to lower-frequency devices that are easier to manufacture, and less path loss than 802.11a.

The disadvantage of 802.11g is operation in the already cluttered 2.4 GHz band. This leads to its lower capacity (fewer available channels) when compared with 802.11a. While the OFDM modulation technology allows higher speeds, the total amount of bandwidth available in the 2.4 GHz frequency remains the same. Unlike 12 channels which are available in the 5 GHz band, 802.11g is still restricted to three channels in the 2.4 GHz band. In this context, some argue that 802.11g is merely a migration path toward the ultimate goal of wireless connectivity at 5 GHz.

- **802.11h**

This standard is supplementary to the media access control (MAC) layer to comply with European regulations for 5 GHz WLANs. European radio regulations for the 5 GHz band require WLAN products to have TPC and DFS.. While some European countries, such as Germany, Ireland, Netherlands and the United Kingdom, are allowing the use of 5 GHz WLANs with TPC and DFS, harmonized use of 5 GHz at a pan-European level may be a slow process. In the US, the FCC is in discussion with military authorities regarding implementation of DFS to protect radar services. It appears likely, therefore, that 802.11h will supersede the current 802.11a MAC layer.

- **HIPERLAN**

Hyper LAN was developed in European countries as a high speed WLAN standard. There are two types of specifications: HiperLAN/1 and HiperLAN/2. Both specifications have been adopted by the European Telecommunications Standards Institute (ETSI). They provide similar features and capabilities to 802.11 standards. HiperLAN/1 was developed as early as 1996 and offers data rates up to 20 Mbps in the 5 GHz range of the radio frequency spectrum. It now, however, appears unlikely that it will be widely adopted since it is based on GMSK modulation (similar to that used for GSM) and in the intervening time technology has moved on. HiperLAN/2 offers data rates up to 54 Mbps in the same radio frequency band.

The PHY layer is the same as that of 802.11a and the two committees co-operated in the development process . Since the lower throughput of the common 802.11a MAC limits its use especially with multimedia applications, Hyper LAN's high bit rate, though it may cost more, may be an effective alternative technology for certain WLAN applications, particularly those involving transmission of video images. Hyper LAN is based on asynchronous transfer (ATM) technology, and can perform better quality of service operation than 802.11 WLAN.

- **MMAC**

In Japan, Multimedia Mobile Access Communications Systems (MMAC) are being developed by the MMAC Promotion Council.37 They intend to transmit data at a high speed with seamless connections to optical fiber networks and include the following sub-systems. Their systems have the following features.

1. High speed wireless access: Wireless access system which can transmit at up to 30 Mbps using the SHF and other band (3-60 GHz), providing high feature video telephone.
2. Ultra high speed wireless LAN: Wireless LAN which can transmit up to 156 Mbps using the millimetre wave radio band (30-300 GHz), providing high quality TV conferences.

3. GHz Band Mobile Access: ATM type wireless access and Ethernet type wireless LAN using 5 GHz band, providing multimedia data transmission at up to 20-25 Mbps for multimedia information.
4. Wireless Home-Link: Wireless home-link which can transmit up to 100 Mbps using the SHF and other band (3-60 GHz), providing multimedia data transmission between PCs and audio visualequipement that transmits multimedia information.

2.14 Frequency bands available internationally for 5 GHz WLAN services

The following table is a summary of the frequency bands that have been made available for 5 GHz WLANs in a number of regions of the world. Bands A and B are on the agenda of WRC 2003, where it is hoped that agreement will be reached on parameters for their use on a worldwide basis for WLANs.

Table2.2: Frequency bands available internationally for 5 GHz WLAN services.

Region	A1) 4900-5000 MHz	A2) 5150-5250 MHz	A3) 5250-5350 MHz	B) 5470-5725 MHz	C) 5725-5875 MHz (ISM)
Australia	Not allowed	SP 1/00 - May 2000 Radiocommunications Class Licence (Low Interference Potential Devices) 2000	SP 1/00 – May 2000 Radiocommunications Class Licence (Low Interference Potential Devices) 2000		SP 1/00 - May 2000 Radiocommunications Class Licence (Low Interference Potential Devices) 2000
Power limit eirp		200 mW indoor use only	200 mW indoor use only		1W
Licensing		Class licence	Class licence		Class licence
Coexistence/ Etiquette		None	None		None

Table2.3: Frequency bands available internationally for 5 GHz.WLAN services.

Region	A1) 4900-5000 MHz	A2) 5150-5250 MHz	A3) 5250-5350 MHz	B) 5470-5725 MHz	C) 5725-5875 MHz (ISM)
USA	Not allowed (*)	U-NII band FCC Part 15 subpart E	U-NII band FCC Part 15 subpart E	Not allowed	U-NII band FCC Part 15 subpart E 5725-5825 MHz
Power limit Power limit eirp		50 mW indoor only 200 mW	250 mW indoor/outdoor 1W		1W indoor/outdoor 4W (FWA) 200 mW (point-to-point with highly directional antennas)
Licensing		Unlicensed	Unlicensed		Unlicensed
Coexistence/ Etiquette		None	None		None
Canada	Not allowed	RSS-210 Issue 3 Par. 6.2.2 (q1)	RSS-210 Issue 3 Par. 6.2.2 (q1)	Not allowed	RSS-210 Issue 3 Par. 6.2.2 (q1) 5725-5825 MHz
Power limit-transmitter Power limit eirp		None stated Indoor use only 200 mW	250 mW 1W		1W 4W (FWA) 200 mW (point-to-point with highly directional antennas)
Licensing		Unlicensed	Unlicensed		Unlicensed
Coexistence/ Etiquette		None	None		None
Europe	Not allowed	ERC Decision (99)23	ERC Decision (99)23 Allowed in specific countries	ERC Decision (99)23 Allowed in specific countries	FWA
Power limit eirp		200 mW Hiperlan indoor use only	200 mW Hiperlan indoor only	1W Hiperlan indoor/outdoor	25 mW
Licensing		Licence exempt	Licence exempt	Licence exempt	Unlicensed
Coexistence/ Etiquette		20 MHz channels assigned DFS & TPC mandatory	20 MHz channels assigned DFS & TPC mandatory	20 MHz channels assigned DFS & TPC mandatory	-
Japan	Ministerial ordinance for radio equipment: Art. 49-21	Ministerial ordinance for radio equipment: Art. 49-20.3	Under study	Not allowed	Not allowed
Power limit eirp	Approximately 200mW (unlicensed)	200 mW indoor use only			
Licensing	Mobile stations: Unlicensed (except eirp exceeds approximately 200mW) Base stations: licensed	Unlicensed			
Coexistence/ Etiquette	20, 10, 5 MHz channels assigned	20 MHz channels assigned			

2.15 Radio technology

Both radio frequency technology and infrared transmission may be used for WLAN implementation. Infrared transmission uses high frequency light waves to transmit data. This technology is cost-effective as well as inexpensive for short-range wireless communications, but it has not been widely accepted because of the limitations of range and its inability to cover an obstructed path. Several radio technologies have been proposed for WLANs.
Since, for economic reasons, most WLANs are based on deregulated and license-free operation often in bands used primarily for other radio services it has been necessary to implement technologies that are interference resistant.

Spread spectrum technology, which is a wideband radio frequency technique, has been a well adopted and successful modulation scheme. The theory of spread spectrum was originally postulated by the Hollywood actress Hedi Lamarr during World War II and was used by the western military until the 1970s to send concealed communications. In this technology, a signal is transmitted using a code that either spreads the signal across the whole available bandwidth or causes it to hop from frequency to frequency in a pre-arranged pattern. The specially designed receiver then removes the unique code preventing illicit eavesdropping. This technology makes the signal difficult to recover without knowing a proprietary spreading code. It also has the benefit of making the system very tolerant of interference from other types of radio system. The spread spectrum modulation system is designed to trade off bandwidth efficiency for reliability and security. While this technology will consume more bandwidth than in the case of narrowband technology, it can coexist with other radio systems without disruption. It is however very vulnerable to interference from other spread spectrum systems since errors can be introduced into the transmitted codes.

The 802.11 standard allows two types of spread spectrum modulation techniques: frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). Both systems are defined for operation in the 2.4 GHz frequency band, typically occupying the 83.5 MHz of bandwidth from 2.400 GHz to 2.483 GHz. With regard to security, they use data encryption methods to prevent unauthorized access as well as user authentication procedures to prevent unauthorized users from gaining access to sensitive data.

The choice between FHSS and DSSS will depend on various factors in relation to users' applications as well as the environment that the system will be operating. FHSS is slightly more resilient in the presence of interference from similar systems, but offers a lower bit rate. DSSS, often referred to as "true spread spectrum", is extremely vulnerable to coding errors.

- **Frequency hopping spread spectrum (FHSS)**

FHSS is a transmission technology which is used where the data signal is modulated with a narrowband carrier signal hopping in a random but predictable sequence from frequency to frequency. The FHSS physical layer has a choice of 22 hop patterns. This technique uses traditional narrowband data transmission with a regular change of the transmission frequency.40 The transmission frequencies are determined by a spreading or hopping code. The FHSS works by transmitting the signal carrier for a short period of time from one band to another.

With FHSS, the signal hops from one frequency to another at a predetermined rate known only to the transmitter as well as receiver. The frequency hopping appear random to anyone who is not aware of the pre-arranged hop pattern. Some countries specify the number of frequencies. In the United States, for example , the FCC regulations require manufactures to use 75 or more frequencies per transmission channel with a maximum dwell time (the time spent at a particular frequency during any single hop) of 400 ms.41 In comparison with DSSS, FHSS is more secure and is used more extensively in military forces. This is because the frequency used in DSSS is fixed and the security provided by the DSSS chipping code is limited.

- **Direct sequence spread spectrum (DSSS)**

This technique broadens the bandwidth needed to transmit a signal by modulating the data stream with a spreading code. With DSSS, a redundant chipping code (bit pattern) is transmitted with each signal burst, and the chipping sequence is known only to the transmitter and receiver. If one or more bits in the pattern are damaged during data transmission, the original data can be recovered on account of the redundancy of the transmission.42 Basically, the longer the chip, the greater the probability that original data can be recovered. DSSS has a better bandwidth and range compared with FHSS, which is currently from 2 Mbps up to 11 Mbps. In addition, DSSS is more resilient to unlike interference than FHSS. As a consequence, DSSS is

more widely implemented in commercial WLAN products. Currently, it is not working well with Bluetooth technology. This is because it is extremely vulnerable to interference from similar systems.

There are also techniques for transmitting large amounts of digital data over a radio wave. One of the most important from the point of view of WLAN would be orthogonal frequency division multiplexing
(OFDM).

- **Orthogonal frequency division multiplexing (OFDM)**

OFDM is designed to minimize the interference, or crosstalk, among channels and symbols comprising data stream. It is significantly less sensitive to inter-symbol interference because a special set of signals is used to build the composite transmitted signal.43 With OFDM, a signal is split into several narrowband channels at different frequencies. It breaks the ceiling of the data bit rate by sending data in a massively parallel fashion. It also slows the symbol rate while packing many bits in each symbol transmission, making the symbol rate substantially slower than the data bit rate. While OFDM has been chosen as the transmission method for the European radio (DAB) and TV (DVB-T) standard, 802.11a, 802.11g and HiperLAN/2 also use OFDM in their physical layers.

2.16 ALTERNATIVE WIRELESS TECHNOLOGIES

2.16.1 Bluetooth

Bluetooth wireless technology has been identified as a potential mass market user of the 2.4 GHz band. Originally developed by Ericsson Mobile Communications in 1994, it was designed to interconnect devices such as cellular phones, laptops, and PDAs with home and business phones as well as computers using short-range connections. Thereby it is touted as a low-cost, low-power, and low-profile technology.

The Bluetooth Special Interest Group (SIG), which comprised companies such as Ericsson, IBM and Toshiba, created the first Bluetooth specification in July 1999. Both 802.11b

and Bluetooth radios share common spectrum in the 2.45 GHz ISM band, but Bluetooth uses FHSS transmission. The target of both radio types are mainly business users. In the ISM band, Bluetooth technology is able to transmit data in a speed of up to 1 Mbps and achieves a throughput of approximately 720 Kbps. While the roles of both technologies are to allow transmission of information between devices by a radio link, there is a clear difference in their roles. It is range of communication, which is used to differentiate between wireless technologies. While WWAN technologies, including cellular phones such as GSM, GPRS, CDMA etc., would be characterized by long range and high power consumption, WLAN technologies are suitable for the usage at medium power and medium range. Wireless Personal Area Network (WPAN) technologies have low power, short range consumption, and Bluetooth is also included in this area. Bluetooth can be used to connect almost any device to any other device within the range available.

Bluetooth has a range of approximately 10 metres compared with WLANs' range of up to 100 meters. Bluetooth is not intended to allow free-roaming users access to wireless networks. This limitation has reduced the popularity of Bluetooth in businesses and homes compared with the 802.11b standard. The following table summarizes three classes of power management that Bluetooth provides.

Table 2.4: Classes of Bluetooth device and power management.

Type of device	Power level	Estimated operating range
Class 3 devices	100 mW	Up to 100 metres
Class 2 devices	2.5 mW	Up to 10 metres
Class 1 devices	1 mW	0.1-10 metres

Bluetooth networks enable a so-called "master-slave relationship" maintained between network devices. Up to eight devices can be networked together in a master-slave relationship called "piconet". In a piconet, one device plays a part of the master of the network with up to seven slaves connected directly to the network, thereby creating a chain of wireless networks.

The master device controls the network, where devices in the piconet operate on the same channel and follow the same frequency hopping sequence.

While Bluetooth permits the establishment of both peer-to-peer networks and networks based on fixed access points, the most popular use would be to interconnect mobile devices that are in the same area. Like WLANs, Bluetooth has a number of benefits for users. For example, Bluetooth can replace cables for a variety of interconnections. It also enables file sharing between available devices. Bluetooth is supported by a variety of devices. Bluetooth may be used with a laptop, handheld device, desktop or any other types of available device. Bluetooth is expected to be utilized in office appliances and home Appliances , in which a variety of applications are created including wireless conference rooms or wireless Internet banking.

There are some disadvantages in the use of Bluetooth. As noted above, its range is apparently much shorter than 802.11b. In this context, some contend that Bluetooth will never pose a serious threat to 802.11 equipment . In addition, costs for Bluetooth chips and other components are still high. With regard to security, Bluetooth did not address security services other than basic services such as ensuring authentication and protection of privacy. Therefore, other means to ensure security would be required to gain the confidence of users. One of the most critical points for the use of Bluetooth is interference with 802.11b. It has been suggested that mutual interference between them will occur if the signals of both systems overlap in both frequency and time. Moreover, both technologies apply packet transmission and time division duplexing, which means that the transmission is intermittent.52 While it is true that they cause interference with each other, it is the nature of radio links to experience interference.53 Technically speaking, both 802.11b and Bluetooth can coexist inasmuch as both devices located near each other do not use the same frequency at the same time. In addition, both technologies have extensive error checking and the ability to retransmit packets in case of occurrence of errors. Therefore, the consequence of interference, if any, is not lost data but decreased throughput. Furthermore, the interference can be limited in itself because of different types of spread spectrum modulation techniques as well as incomplete overlap of the frequency sub-bands used.

It has been reported that 802.11b would degrade to its slowest speed of 1 Mbps at worst cases and Bluetooth could suffer a 22% degradation of its 1 Mbps maximum data rate.55

However, considerable degradation may well be significant for the operation of certain applications and could cause service failure.

In the meantime, some studies show that there is only a partial overlap between Bluetooth and 802.11b, and even with UMTS, and that these technologies are largely complementary from a market perspective.

2.16.2 Home RF

Home RF is a home networking standard developed by Proxim Inc. that combines the 802.11b and Digital Enhanced Cordless Telecommunication (DECT) portable phone standards into a single system.57

While 802.11b was fundamentally designed for the corporate environment, HomeRF was developed to satisfy the needs in home networking applications from the outset. The specification was developed by the Home Radio Frequency Working Group as shared wireless access protocol (SWAP). It allows PCs, cordless telephones and other consumer devices to share and communicate voice as well as data in and around the home without the expense of running new wires.58 Home RF transmits data up to 10 Mbps with a range of up to 50 meters.59 This range might be too short for most business users, but will be suitable for home applications. By the end of 2002, Home RF proponents expect to achieve a data rate of 20 Mbps or faster. Some argue that Home RF may be better as a technology to handle multi-media data than 802.11b.60

Home RF 2.0 uses a frequency hopping technology, which keeps the "data channel" shifting from one frequency to another many times a second. This technology is expected to make it very hard for someone to eavesdrop on the network. Also, Home RF 2.0 has introduced the concept of a "network password" needed to join the network.

Using 2.4 GHz ISM band, Home RF is subject to interference from other devices using the same frequencies such as 802.11b. However, Home RF 2.0 does not interfere with Bluetooth technologies. It has been reported that Home RF offers superior scalability in larger installations thanks to its frequency hopping technology, with support for up to 15 overlapping networks compared with three for WLANs.

2.16.3 3G

In some OECD countries, such as Japan, nationwide 3G wireless networks have already been rolled out. In Japan and Korea, there are reportedly nearly 5 million 3G users respectively.61 The progress of European carriers is relatively slow, but a number of countries have moved from so-called 2G to 2.5G in late 2000 and are developing their 3G infrastructure. The 3G system promises speeds up to 2 Mbps, but it is expensive to deploy the infrastructure.

It has been suggested that 802.11b applications will be a threat for 3G operators. Some point out that deployment of 3G mobile data network might be delayed significantly as carriers look to 802.11-based networks one of the reasons behind these arguments is the fact that Wi-Fi is up to 30 times faster and arguably less expensive in terms of building and maintaining a network than 3G. In addition, WLANs are originally designed not as a system for supporting mobile users but as a simple cable replacement. What is more, unlike 3G, WLAN is the bottom-up technology rolled out by firms with no plans to make a profit in the telecommunications business. For example, firms introducing the Wi-Fi service throughout their stores are doing so to attract customers rather than as a means of entering the broadband business.

However, the Wi-Fi's "threat" to 3G may be somewhat overstated. The biggest drawback facing WLAN providers would be the uncertainty surrounding WLAN service models for public access.63 In addition, some technical issues such as access to radio spectrum, billing, roaming and security can also slow down the commercial development of WLANs.

On the contrary, some contend that Wi-Fi is far from a threat to 3G regardless of its uncertainty in the market. For example, the German regulator RegTP mentioned that these two systems would supplement each other effectively for the benefit of all market players. Some view WLAN and 3G as complementary technologies that will result in more demand for frequencies in the 5 GHz band for new WLAN applications in addition to those in the 2.4 GHz band. Using WLAN frequencies for public applications can be in the interest of UMTS and can lead to success of UMTS. In particular, it has been suggested that 3G is a more consumer-oriented technology whereas WLANs are arguably more focused on enabling those applications that are most demanded by businesses.65 Moreover, WLANs are designed for provision of broadband access in small areas, which is contrary to the mobile networks, which cover wide areas across

the country. In other words, 3G systems will be designed for ubiquitous coverage and true mobile use for vehicles (*i.e.* handing off from one cell to another), whereas Wi-Fi is really designed for short-distance use.

While some companies are developing technology such as mesh networks that they claim will provide coverage to vehicles, the technology is still largely in development and unproven. The main advantage of UMTS is its mobility rather than the transmission rates. Furthermore, seamless roaming capabilities between 802.11b and 3G (UMTS) were demonstrated in September 2002.66 This successful testing will enable mobile users to browse the Internet while roaming between Wi-Fi and 3G with no interruption in the session. Therefore, these two systems, intended for different purposes, can coexist and allow users to access essential broadband applications.

CHAPTER THREE

3.1. Introduction to wireless security

Wireless technologies have become increasingly popular in our everyday business and personal lives. Personal digital assistants (PDA) allow individuals to access calendars, e-mail, address and phone number lists, and the Internet. Some technologies even offer global positioning system (GPS) capabilities that can pinpoint the location of the device anywhere in the world. Wireless technologies promise to offer even more features and functions in the next few years. An increasing number of government agencies, businesses, and home users are using, or considering using, wireless technologies in their environments. Agencies should be aware of the security risks associated with wireless technologies. Agencies need to develop strategies that will mitigate risks as they integrate wireless technologies into their computing environments. This document discusses certain wireless technologies, outlines the associated risks, and offers guidance for mitigating those risks.

Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) and cell phones to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link. A brief overview of wireless networks, devices, standards, and security issues is presented in this section.

3.2. Wireless Security Threats and Risk Mitigation

The NIST handbook An Introduction to Computer Security generically classifies security threats in nine categories ranging from errors and omissions to threats to personal privacy. *6* All of these represent potential threats in wireless networks as well. However, the more immediate concerns for wireless communications are device theft, denial of service, malicious hackers, malicious code, theft of service, and industrial and foreign espionage. Theft is likely to occur with wireless devices because of their portability. Authorized and unauthorized users of the system may commit fraud and theft; however, authorized users are more likely to carry out such acts. Since users of a system may know what resources a system has and the system's security flaws, it is easier for them to commit fraud and theft. Malicious hackers, sometimes called crackers, are individuals who break into a system without authorization, usually for personal gain or to do harm. Malicious hackers are generally individuals from outside of an agency or organization (although users within an agency or organization can be a threat as well). Such hackers may gain access to the wireless network access point by eavesdropping on wireless device communications. Malicious code involves viruses, worms, Trojan horses, logic bombs, or other unwanted software that is designed to damage files or bring down a system. Theft of service occurs when an unauthorized user gains access to the network and consumes network resources. Industrial and foreign espionage involves gathering proprietary data from corporations or intelligence information from governments through eavesdropping. In wireless networks, the espionage threat stems from the relative ease with which eavesdropping can occur on radio transmissions.

Attacks resulting from these threats, if successful, place an agency's systems—and, more importantly, its data—at risk. Ensuring confidentiality, integrity, authenticity, and availability are the prime objectives of all government security policies and practices. NIST Special Publication (SP) 800-26, Security Self- *Assessment Guide for Information* Technology Systems, states that information must be protected from unauthorized, unanticipated, or unintentional modification. Security requirements include the following:

- **Authenticity**: A third party must be able to verify that the content of a message has not been changed in transit.
- **Nonrepudiation**: The origin or the receipt of a specific message must be verifiable by a third party.
- **Accountability**—The actions of an entity must be traceable uniquely to that entity. Network availability is "the property of being accessible and usable upon demand by an authorized entity".

The information technology resource (system or data) must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes Risks in wireless networks are equal to the sum of the risk of operating a wired network (as in operating a network in general) plus the new risks introduced by weaknesses in wireless protocols. To mitigate these risks, agencies need to adopt security measures and practices that help bring their risks to a manageable level. They need, for example, to perform security assessments prior to implementation to determine the specific threats and vulnerabilities that wireless networks will introduce in their environments. In performing the assessment, they should consider existing security policies, known threats and vulnerabilities, legislation and regulations, safety, reliability, system performance, the life-cycle costs of security measures, and technical requirements. Once the risk assessment is complete, the agency can begin planning and implementing the measures that it will put in place to safeguard its systems and lower its security risks to a manageable level. The agency should periodically reassess the policies and measures that it puts in place because computer technologies and malicious threats are continually changing. (For more detailed information on the risk mitigation and safeguard selection process, refer to NIST SP 800-12. To date, the list below includes some of the more salient threats and vulnerabilities of wireless systems:

- All the vulnerabilities that exist in a conventional wired network apply to wireless technologies.

- Malicious entities may gain unauthorized access to an agency's computer or voice (IP telephony) network through wireless connections, potentially bypassing any firewall protections.
- Sensitive information that is not encrypted (or that is encrypted with poor cryptographic techniques) and that is transmitted between two wireless devices may be intercepted and disclosed.
- Denial of service (DoS) attacks may be directed at wireless connections or devices.
- Malicious entities may steal the identity of legitimate users and masquerade as them on internal or external corporate networks.
- Sensitive data may be corrupted during improper synchronization.
- Malicious entities may be able to violate the privacy of legitimate users and be able to track their physical movements.
- Malicious entities may deploy unauthorized equipment (e.g., client devices and access points) to surreptitiously gain access to sensitive information.
- Handheld devices are easily stolen and can reveal sensitive information.
- Data may be extracted without detection from improperly configured devices.
- Viruses or other malicious code may corrupt data on a wireless device and be subsequently introduced to a wired network connection.
- Malicious entities may, through wireless connections, connect to other agencies for the purposes of launching attacks and concealing their activity.
- Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations.
- Malicious entities may use a third party, untrusted wireless network services to gain access to an agency's network resources.
- Internal attacks may be possible via ad hoc transmissions.

As with wired networks, agency officials need to be aware of liability issues for the loss of sensitive information or for any attacks launched from a compromised network.

3.3. Emerging Wireless Technologies

Originally, handheld devices had limited functionality because of size and power requirements. However, the technology is improving, and handheld devices are becoming

more feature-rich and portable. More significantly, the various wireless devices and their respective technologies are merging. The mobile phone, for instance, has increased functionality that now allows it to serve as a PDA as well as a phone.

Smart phones are merging mobile phone and PDA technologies to provide normal voice service and email, text messaging, paging, Web access, and voice recognition. Next-generation mobile phones, already on the market, are quickly incorporating PDA, IR, wireless Internet, e-mail, and global positioning system (GPS) capabilities.

Manufacturers are combining standards as well, with the goal to provide a device capable of delivering multiple services. Other developments that will soon be on the market include global system for mobile communications-based (GSM-based) technologies such as General Packet Radio Service (GPRS), Local Multipoint Distribution Services (LMDS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS). These technologies will provide high data transmission rates and greater networking capabilities. However, each new development will present its own security risks, and government agencies must address these risks to ensure that critical assets remain protected.

3.4. Federal Information Processing Standards

FIPS 140-2 defines a framework and methodology for NIST's current and future cryptographic standards. The standard provides users with the following:

- A specification of security features that are required at each of four security levels
- Flexibility in choosing security requirements
- A guide to ensuring that the cryptographic modules incorporate necessary security features
- The assurance that the modules are compliant with cryptography-based standards.

The Secretary of Commerce has made FIPS 140-2 mandatory and binding for U.S. federal agencies. The standard is specifically applicable when a federal agency determines that cryptography is necessary for protecting sensitive information. The standard is used in

designing and implementing cryptographic modules that federal departments and agencies operate or have operated for them. FIPS 140-2 is applicable if the module is incorporated in a product or application or if it functions as a standalone device. As currently defined, the security of neither 802.11 nor Bluetooth meets the FIPS 140-2 standard.

Federal agencies, industry, and the public rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas.

Cryptographic modules are implemented in these products and systems to provide cryptographic services such as confidentiality, integrity, nonrepudiation, identification, and authentication. Adequate testing and validation of the cryptographic module against established standards is essential for security assurance.

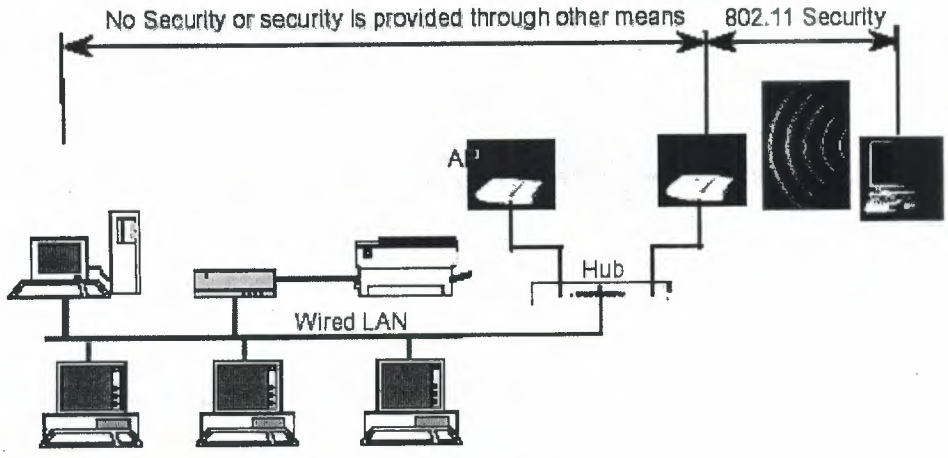
Both federal agencies and the public benefit from the use of tested and validated products. Without adequate testing, weaknesses such as poor design, weak algorithms, or incorrect implementation of the cryptographic module can result in insecure products.

In 1995, NIST, established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to FIPS 140-2, Security Requirements for Cryptographic Modules, and other FIPS cryptography-based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the federal agencies of both countries for the protection of sensitive information. Vendors of cryptographic modules use independent, accredited testing laboratories to test their modules.

NIST's Computer Security Division and CSE jointly serve as the validation authorities for the program, validating the test results. Currently, there are six National Voluntary Laboratory Accreditation Program (NVLAP) accredited laboratories that perform FIPS 140-2 compliance testing.

3.5. Security of 802.11 Wireless LANs

This section discusses the built-in security features of 802.11. It provides an overview of the inherent security features to better illustrate its limitations and provide a motivation for some of the recommendations for enhanced security. The IEEE 802.11 specification identified several services to provide a secure operating environment. The security services are provided largely by the Wired Equivalent Privacy (WEP) protocol to protect link-level data during wireless transmission between clients and access points. WEP does not provide end-to-end security, but only for the wireless portion of theconnection as shown in Figure 3-1.



- **Figure 3.1** Wireless Security of 802.11 in Typical Network

3.5.1. Security Features of 802.11 Wireless LANs per the Standard

The three basic security services defined by IEEE for the WLAN environment are as follows:

- **Authentication**—A primary goal of WEP was to provide a security service to verify the identity of communicating client stations. This provides access control to the network by denying access to client stations that cannot authenticate properly. This service addresses the question, "Are only authorized persons allowed to gain access to my network?"

- **Confidentiality**—Confidentiality, or privacy, was a second goal of WEP. It was developed to provide "privacy achieved by a wired network." The intent was to prevent information compromise from casual eavesdropping (passive attack). This service, in general, addresses the question, "Are only authorized persons allowed to view my data?"
- **Integrity**—Another goal of WEP was a security service developed to ensure that messages are not modified in transit between the wireless clients and the access point in an active attack. This service addresses the question, "Is the data coming into or exiting the network trustworthy—has it been tampered with?" It is important to note that the standard did not address other security services such as audit, authorization, and nonrepudiation. The security services offered by 802.11 are described in greater detail below.

3.5.1.1. Authentication

The IEEE 802.11 specification defines two means to "validate" wireless users attempting to gain access to a wired network: open-system authentication and shared-key authentication. One means, shared-key authentication, is based on cryptography, and the other is not. The open-system authentication technique is not truly authentication; the access point accepts the mobile station without verifying the identity of the station. It should be noted also that the authentication is only one-way: only the mobile station is authenticated. The mobile station must trust that it is communicating to a real AP. A taxonomy of the techniques for 802.11 is depicted in Figure 3-2

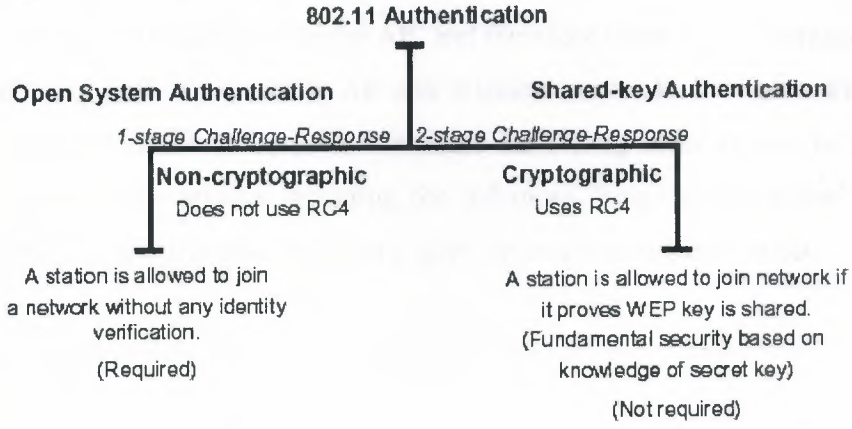


Figure 3.2 Taxonomy of 802.11 Authentication Techniques

With Open System authentication, a client is authenticated if it simply responds with a MAC address during the two-message exchange with an access point. During the exchange, the client is not truly validated but simply responds with the correct fields in the message exchange. Obviously, with out cryptographic validatedation, open-system authentication is highly vulnerable to attack and practically invites unauthorized access. Open-system authentication is the only required form of authentication by the 802.11 specification.

Shared key authentication is a cryptographic technique for authentication. It is a simple "challengeresponse" scheme based on whether a client has knowledge of a shared secret. In this scheme, as depicted conceptually in Figure 3-3, a random challenge is generated by the access point and sent to the wireless client. The client, using a cryptographic key that is shared with the AP, encrypts the challenge (or "nonce," as it is called in security vernacular) and returns the result to the AP. The AP decrypts the result computed by the client and allows access only if the decrypted value is the same as the random challenge transmitted. The algorithm used in the cryptographic computation and for the generation of the 128-bit challenge text is the RC4 stream cipher developed by Ron Rivest of MIT. It should be noted that the authentication method just described is a rudimentary cryptographic technique, and it does not provide mutual authentication. That is, the client does not authenticate the AP, and therefore there is no assurance that a client is communicating with a legitimate AP and wireless network. It is also worth noting that simple unilateral challenge-response schemes have long been known to be weak. They suffer fromnumerous attacks including the infamous "man-in-the-middle" attack. Lastly, the IEEE 802.11 specification does not require shared-key authentication.

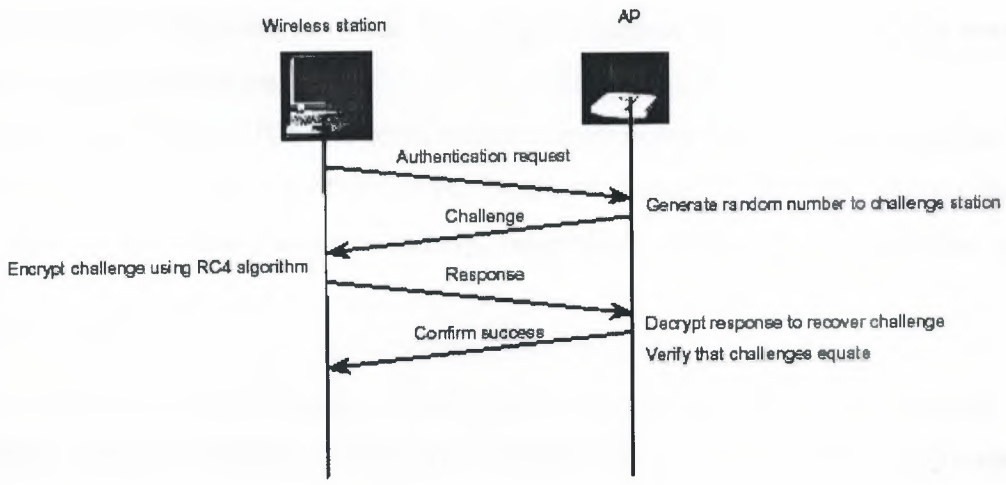


Figure 3.3 Shared-key Authentication Message Flow

3.5.1.2. Privacy

The 802.11 standard supports privacy (confidentiality) through the use of cryptographic techniques for the wireless interface. The WEP cryptographic technique for confidentiality also uses the RC4 symmetric key , stream cipher algorithm to generate a pseudo-random data sequence. This "key stream" is simply added modulo 2 (exclusive-OR-ed) to the data to be transmitted. Through the WEP technique, data can be protected from disclosure during transmission over the wireless link. WEP is applied to all data above the

802.11 WLAN layers to protect traffic such as Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), and Hyper Text Transfer Protocol (HTTP).

As defined in the 802.11 standard, WEP supports only a 40-bit cryptographic keys size for the shared key. However, numerous vendors offer nonstandard extensions of WEP that support key lengths from 40 bits to 104 bits. At least one vendor supports a keysize of 128 bits. The 104-bit WEP key, for instance, with a 24-bit Initialization Vector (IV) becomes a 128-bit RC4 key. In general, all other things being equal, increasing the key size increases the security of a cryptographic technique. However, it is always possible for flawed implementations or flawed designs to prevent long keys from increasing security. Research has shown that key sizes of greater than 80-bits, for robust designs and implementations,

make brute-force cryptanalysis (code breaking) an impossible task. For 80-bit keys, the number of possible keys—a

Key space of more than 1026—exceeds contemporary computing power. In practice, most WLAN deployments rely on 40-bit keys. Moreover, recent attacks have shown that the WEP approach for privacy is, unfortunately, vulnerable to certain attacks regardless of key size .

However, the cryptographic, standards, and vendor WLAN communities have developed enhanced WEP, which is available as a prestandard vendor-specific implementations. The attacks mentioned above are described later in the following sections. The WEP privacy is illustrated conceptually in Figure 3-4.

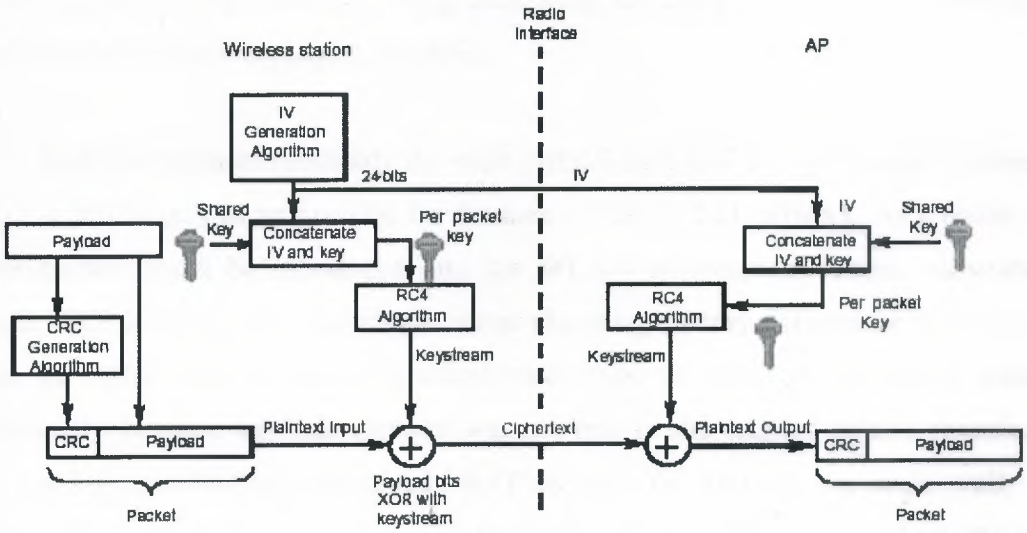


Figure 3.4 WEP Privacy Using RC4 Algorithm

3.5.1.3. Integrity

The IEEE 802.11 specification also outlines a means to provide data integrity for messages transmitted between wireless clients and access points. This security service was designed to reject any messages that had been changed by an active adversary "in the middle." This technique uses a simple encrypted Cyclic Redundancy Check (CRC) approach. As depicted in the diagram above, a CRC-32, or frame check sequence, is computed on each payload prior to transmission. The integrity-sealed packet is then encrypted using the RC4 key stream to provide the cipher-text message. On the receiving

end, decryption is performed and the CRC is recomputed on the message that is received. The CRC computed at the receiving end is compared with the one computed with the original message. If the CRCs do not equal, that is, "received in error," this would indicate an integrity violation (an active message spoofer), and the packet would be discarded. As with the privacy service, unfortunately, the 802.11 integrity is vulnerable to certain attacks regardless of key size. In summary, the fundamental flaw in the WEP integrity scheme is that the simple CRC is not a "cryptographically secure" mechanism such as a hash or message authentication code.

The IEEE 802.11 specification does not, unfortunately, identify any means for key management (life cycle handling of cryptographic keys and related material). Therefore, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the material is left to those deploying WLANs.

Key management (probably the most critical aspect of a cryptographic system) for 802.11 is left largely as an exercise for the users of the 802.11 network. As a result, many vulnerabilities could be introduced into the WLAN environment. These vulnerabilities include WEP keys that are non-unique, never changing, factory-defaults, or weak keys (all zeros, all ones, based on easily guessed passwords, or other similar trivial patterns). Additionally, because key management was not part of the original 802.11 specification, with the key distribution unresolved, WEP-secured WLANs do not scale well. If an enterprise recognizes the need to change keys often and to make them random, the task is formidable in a large WLAN environment. For example, a large campus may have as many as 15,000 APs. Generating, distributing, loading, and managing keys for an environment of this size is a significant challenge. It is has been suggested that the only practical way to distribute keys in a large dynamic environment is to publish it. However, a fundamental tenet of cryptography is that cryptographic keys remain secret. Hence we have a major dichotomy. This dichotomy exists for any technology that neglects to elegantly address the key distribution problem.

3.5.2. Problems with the IEEE 802.11 Standard Security

This section discusses some known vulnerabilities in the standardized security of the 802.11 WLAN standard. As mentioned above, the WEP protocol is used in 802.11-based WLANs. WEP in turn uses a RC4 cryptographic algorithm with a variable length key to protect traffic. Again, the 802.11 standard supports WEP cryptographic keys of 40-bits. However, some vendors have implemented products with keys 104-bit keys and even 128-bit keys. With the addition of the 24-bit IV, the actual key used in the RC4 algorithm is 152 bits for the 128 bits WEP key. It is worthy to note that some vendors generate keys after a keystroke from a user, which, if done properly, using the proper random processes, can result in a strong WEP key. Other vendors, however, have based WEP keys on passwords that are chosen by users;this typically reduces the effective key size.

Several groups of computer security specialists have discovered security problems that let malicious users compromise the security of WLANs. These include passive attacks to decrypt traffic based on statistical analysis, active attacks to inject new traffic from unauthorized mobile stations (i.e., based on known plain text), active attacks to decrypt traffic (i.e., based on tricking the access point), and dictionary-building attacks. The dictionary building attack is possible after analyzing enough traffic on a busy network .

3.6. Security problems with WEP

1. The use of static WEP keys—many users in a wireless network potentially sharing the identical key for long periods of time, is a well-known security vulnerability. This is in part due to the lack of any key management provisions in the WEP protocol. If a computer such as a laptop were to be lost or stolen, the key could become compromised along with all the other computers sharing that key. Moreover, if every station uses the same key, a large amount of traffic may be rapidly available to an eavesdropper for analytic attacks, such as 2 and 3 below.

2. The IV in WEP, as shown in Figure 3-8, is a 24-bit field sent in the clear text portion of a message. This 24-bit string, used to initialize the key stream generated by the RC4 algorithm, is a relatively small field when used for cryptographic purposes. Reuse of the same IV produces identical key streams for the protection of data, and the short IV

guarantees that they will repeat after a relatively short time in a busy network. Moreover, the 802.11 standard does not specify how the IVs are set or changed, and individual wireless NICs from the same vendor may all generate the same IV sequences, or some wireless NICs may possibly use a constant IV. As a result, hackers can record network traffic, determine the key stream, and use it to decrypt the cipher-text.

3. The IV is a part of the RC4 encryption key. The fact that an eavesdropper knows 24-bits of every packet key, combined with a weakness in the RC4 key schedule, leads to a successful analytic attack , that recovers the key, after intercepting and analyzing only a relatively small amount of traffic. This attack is publicly available as an attack script and open source code.

4. WEP provides no cryptographic integrity protection. However, the 802.11 MAC protocol uses a non cryptographic Cyclic Redundancy Check (CRC) to check the integrity of packets, and acknowledge packets with the correct checksum. The combination of non cryptographic checksums with stream ciphers is dangerous and often intr WEP. There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP and noting whether the packet is acknowledged. These kinds of attacks are often subtle, and it is now considered risky to design encryption protocols that do not include cryptographic integrity protection, because of the possibility of interactions with other protocol levels that can give away information about cipher text. oduces vulnerablities, as is the case for WEP.

There is an active attack that permits the attacker to decrypt any packet by systematically modifying the packet and CRC sending it to the AP and noting whether the packet is acknowledged. These kinds of attacks are often subtle, and it is now considered risky to design encryption protocols that do not include cryptographic integrity protection, because of the possibility of interactions with other protocol levels that can give away information about cipher text. Note that only one of the four problems listed above depends on a weakness in the cryptographic algorithm. Therefore, these problems would not be improved by substituting a stronger stream cipher. For example, the third problem listed above is a consequence of a weakness in the implementation of the RC4 stream cipher that is exposed by a poorly designed protocol. Some of the problems associated with WEP and 802.11 WLAN security are summarized in Table 3-1

Table 3.1 Key Problems with Existing 802.11 Wireless LAN Security

Security Issue or Vulnerability	Remarks
1. Security features in vendor products are frequently not enabled.	Security features, albeit poor in some cases, are not enabled when shipped, and users do not enable when installed. Bad security is generally better than no security.
2. IVs are short (or static).	24-bit IVs cause the generated key stream to repeat. Repetition allows easy decryption of data for a moderately sophisticated adversary.
3. Cryptographic keys are short.	40-bit keys are inadequate for any system. It is generally accepted that key sizes should be greater than 80 bits in length. The longer the key, the less likely a comprise is possible from a brute-force attack.
4. Cryptographic keys are shared.	Keys that are shared can compromise a system. As the number of people sharing the key grows, the security risks also grow. A fundamental tenant of cryptography is that the security of a system is largely dependent on the secrecy of the keys.
5. Cryptographic keys cannot be updated automatically and frequently.	Cryptographic keys should be changed often to prevent brute-force attacks.
6. RC4 has a weak key schedule and is inappropriately used in WEP.	The combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 key stream leads to an efficient attack that recovers the key. Most other applications of RC4 do not expose the weaknesses of RC4 because they do not reveal key bits and do not restart the key schedule for every packet. This attack is available to moderately sophisticated adversaries.
7. Packet integrity is poor.	CRC32 and other linear block codes are inadequate for providing cryptographic integrity. Message modification is possible. Linear codes are inadequate for the protection against advertent attacks on data integrity. Cryptographic protection is required to prevent deliberate attacks. Use of noncryptographic protocols often facilitates attacks against the cryptography.
8. No user authentication occurs.	Only the device is authenticated. A device that is stolen can access the network.
9. Authentication is not enabled; only simple SSID identification occurs.	Identity-based systems are highly vulnerable particularly in a wireless system because signals can be more easily intercepted.
10. Device authentication is simple shared-key challenge-response.	One-way challenge-response authentication is subject to "man-in-the-middle" attacks. Mutual authentication is required to provide verification that users and the network are legitimate.
11. The client does not authenticate the AP.	The client needs to authenticate the AP to ensure that it is legitimate and prevent the introduction of rogue APs.

3.7. Security Requirements and Threats

As discussed above, the 802.11 WLAN—or Wi-Fi—industry is burgeoning and currently has significant momentum. All indications suggest that in the coming years numerous organizations will deploy 802.11 WLAN technology. Many organizations—including retail stores, hospitals, airports, and business enterprises—plan to capitalize on the benefits of "going wireless." However, although there has been tremendous growth and success, everything relative to 802.11 WLANs has not been positive.

This subsection will briefly cover the risks to security—i.e., attacks on confidentiality, integrity, and network availability. Figure 3-4 provides a general taxonomy of security attacks to help organizations and users understand some of the attacks against WLANs.

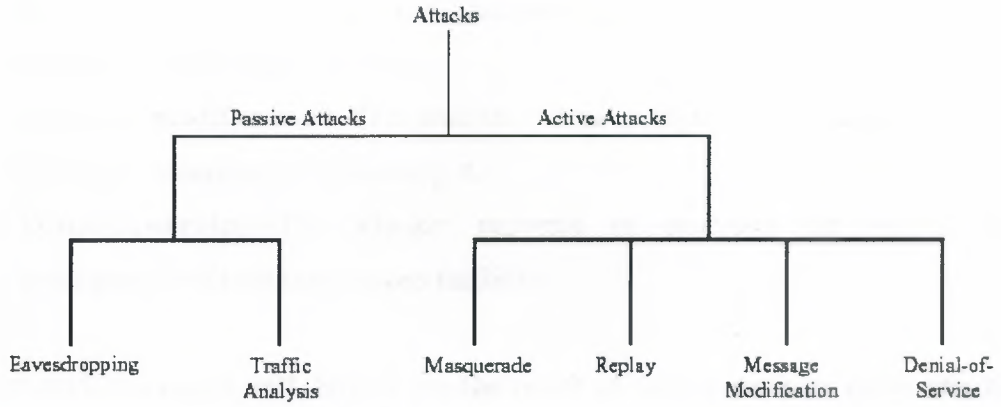


Figure 3.4 Taxonomy of Security Attacks

Network security attacks are typically divided into **passive and active attacks.** These two broad classes are then subdivided into other types of attacks. All are defined below.

1- **Passive Attack**—An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis). These two passive attacks are described below.

- **Eavesdropping** — The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN

between two workstations or tuning into transmissions between a wireless handset and a base station.

- **Traffic analysis**—The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

2- Active Attack—An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below.

- **Masquerading**—The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.
- **Replay**—The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.
- **Message modification**—The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.
- **Denial-of-service**—The attacker prevents or prohibits the normal use or management of communications facilities.

The risks associated with 802.11 are the result of one or more of these attacks. The consequences of these attacks include, but are not limited to, loss of proprietary information, legal and recovery costs, tarnished image, and loss of network service.

3.7.1. Loss of Confidentiality

Confidentiality is the property with which information is not made available or disclosed to unauthorized individuals, entities, or processes. This is, in general, a fundamental security requirement for most organizations. Due to the broadcast and radio nature of wireless technology, confidentiality is a more difficult security requirement to meet in a wireless network. Adversaries do not have to tap into a network cable to access network resources. Moreover, it may not be possible to control the distance over which the

transmission occurs. This makes traditional physical security countermeasures less effective.

Passive eavesdropping of native 802.11 wireless communications may cause significant risk to an organization. An adversary may be able to listen in and obtain sensitive information including proprietary information, network IDs and passwords, and configuration data. This risk is present because the 802.11 signals may travel outside the building perimeter or because there may be an "insider." Because of the extended range of 802.11 broadcasts, adversaries can potentially detect transmission from a parking lot or nearby roads. This kind of attack, performed through the use of a wireless network analyzer tool or sniffer , is particularly easy for two reasons: 1) frequently confidentiality features of WLAN technology are not even enabled, and 2) because of the numerous vulnerabilities in the 802.11 technology security, as discussed above, determined adversaries can compromise the system.

Wireless packet analyzers, such as Air Snort and WEP crack , are tools that are readily available on the Internet today. Air Snort is one of the first tools created to automate the process of analyzing networks. Unfortunately, it is also commonly used for breaking into wireless networks. Air Snort can take advantage of flaws in the key-scheduling algorithm that was provided for implementation of RC4, which forms part of the original WEP standard. To accomplish this, Air Snort requires only a computer running the Linux operating system and a wireless network card. The software passively monitors the WLAN data transmissions and computes the encryption keys after at least 100 MB of network packets have been sniffed. On a highly saturated network, collecting this amount of data may only take three or four hours;
if traffic volume is low, it may take a few days. For example, a busy data access point transmitting 3,000bytes at 11 Mbps will exhaust the 24-bit IV space after approximately 10 hours.16 If after ten hours the attacker recovers two cipher texts that have been using the same key stream, both data integrity and confidentiality may be easily compromised. After the network packets have been received, the fundamental keys may be guessed in less than one second.*17* Once the malicious user knows the WEP key, that person can read any

packet traveling over the WLAN. Such sniffing tools' wide availability, ease of use, and ability to compute keys makes it essential for security administrators to implement secure wireless solutions. Airsnort may not be able to take advantage of the enhanced key-scheduling algorithm of RC4 in a pre-standard implementation.

Another risk to loss of confidentiality through simple eavesdropping is broadcast monitoring. An adversary can monitor traffic, using a laptop in promiscuous mode, when an access point is connected to a hub instead of a switch. Hubs generally broadcast all network traffic to all connected devices, which leaves the traffic vulnerable to unauthorized monitoring. Switches, on the other hand, can be configured to prohibit certain attached devices from intercepting broadcast traffic from other specified devices. For example, if a wireless access point were connected to an Ethernet hub, a wireless device that is monitoring broadcast traffic could intercept data intended for wired and wireless clients. Consequently, agencies should consider using switches instead of hubs for connections to wireless access points.

WLANs risk loss of confidentiality following an active attack as well. Sniffing software as described above can obtain user names and passwords (as well as any other data traversing the network) as they are sent over a wireless connection. An adversary may be able to masquerade as a legitimate user and gain access to the wired network from an AP. Once "on the network," the intruder can scan the network using purchased or publicly and readily available tools. The malicious eavesdropper then uses the user name, password, and IP address information to gain access to network resources and sensitive corporate data.

Lastly, rogue APs pose a security risk. A malicious or irresponsible user could, physically and surreptitiously, insert a rogue AP into a closet, under a conference room table, or any other hidden area within a building. The rogue AP could then be used to allow unauthorized individuals to gain access to the network. As long as its location is in close proximity to the users of the WLAN, and it is configured so as to appear as a legitimate AP to wireless clients, then the rogue AP can successfully convince wireless clients of its

legitimacy and cause them to send traffic through it. The rogue AP can intercept the wireless traffic between an authorized AP and wireless clients. It need only be configured with a stronger signal than the existing AP to intercept the client traffic. A malicious user can also gain access to the wireless network through APs that are configured to allow access without authorization.*19* It is also important to note that rogue access points need not always be deployed by malicious users. In many cases, rogue APs are often deployed by users who want to take advantage of wireless technology without the approval of the IT department. Additionally, since rogue APs are frequently deployed without the knowledge of the security administrator, they are often deployed without proper security configurations.

3.7.2. Loss of Integrity

Data integrity issues in wireless networks are similar to those in wired networks. Because organizations frequently implement wireless and wired communications without adequate cryptographic protection of data, integrity can be difficult to achieve. A hacker, for example, can compromise data integrity by deleting or modifying the data in an e-mail from an account on the wireless system. This can be detrimental to an organization if important e-mail is widely distributed among e-mail recipients. Because the existing security features of the 802.11 standard do not provide for strong message integrity, kinds of active attacks that compromise system integrity are possible. As discussed before, the WEPbased integrity mechanism is simply a linear CRC. Message modification attacks are possible when cryptographic checking mechanisms such as message authentication codes and hashes are not used.

3.7.3. Loss of Network Availability

A denial of network availability involves some form of DoS attack, such as jamming. Jamming occurs when a malicious user deliberately emanates a signal from a wireless device in order to overwhelm legitimate wireless signals. Jamming may also be inadvertently caused by cordless phone or microwave oven emissions. Jamming results in a breakdown in communications because legitimate wireless signals are unable to communicate on the network. Non malicious users can also cause a DoS. A user, for

instance, may unintentionally monopolize a wireless signal by downloading large files, effectively denying other users access to the network. As a result, agency security policies should limit the types and amounts of data that users are able to download on wireless networks.

3.7.4. Other Security Risks

With the prevalence of wireless devices, more users are seeking ways to connect remotely to their own organization's networks. One such method is the use of untrusted, third-party networks. Conference centers, for example, commonly provide wireless networks for users to connect to the Internet and subsequently to their own organizations while at the conference. Airports, hotels, and even some coffee franchises are beginning to deploy 802.11 based publicly accessible wireless networks for their customers, even offering VPN capabilities for added security.

These untrusted public networks introduce three primary risks: 1) because they are public, they are accessible by anyone, even malicious users; 2) they serve as a bridge to a user's own network, thus potentially allowing anyone on the public network to attack or gain access to the bridged network; and 3) they use high-gain antennas to improve reception and increase coverage area, thus allowing malicious users to eavesdrop more readily on their signals.

By connecting to their own networks via an untrusted network, users may create vulnerabilities for their company networks and systems unless their organizations take steps to protect their users and themselves.

Users typically need to access resources that their organizations deem as either public or private. Agencies may want to consider protecting their public resources using an application layer security protocol such as Transport Layer Security (TLS), the Internet Engineering Task Force standardized version of Secure Sockets Layer (SSL). However, in most agencies, this is unnecessary since the information is indeed public already. For private resources, agencies should consider using a VPN unauthorized access to private resources.

Lastly, as with any network, social engineering and dumpster diving are also concerns. An enterprise should consider all aspects of network security when planning to deploy the wireless network.

3.8. Risk Mitigation

Government agencies can mitigate risks to their WLANs by applying countermeasures to address specific threats and vulnerabilities. Management countermeasures combined with operational and technical countermeasures can be effective in reducing the risks associated with WLANs. The following guidelines will not prevent all adversary penetrations, nor will these countermeasures necessarily guarantee a secure wireless networking environment. This section describes risk-mitigating steps for an agency, recognizing that it is impossible to remove all risks. Additionally, it should be clear that there is no "one size fits all solution" when it comes to security. Some agencies may be able or willing to tolerate more risk than others. Also, security comes at a cost: either in money spent on security equipment, in inconvenience and maintenance, or in operating expenses. Some agencies may be willing to accept risk because applying various countermeasures may exceed financial or other constraints.

3.8.1. Management Countermeasures

- Management countermeasures for securing wireless networks begin with a comprehensive security policy. A security policy, and compliance therewith, is the foundation on which other countermeasures, the operational and technical are rationalized and implemented. A WLAN security policy should be able to do the following:
- Identify who may use WLAN technology in an agency
- Identify whether Internet access is required
- Describe who can install access points and other wireless equipment
- Provide limitations on the location of and physical security for access points
- Describe the type of information that may be sent over wireless links
- Describe conditions under which wireless devices are allowed

- Define standard security settings for access points
- Describe limitations on how the wireless device may be used, such as location
- Describe the hardware and software configuration of all wireless devices
- Provide guidelines on reporting losses of wireless devices and security incidents
- Provide guidelines for the protection of wireless clients to minimize/reduce theft
- Provide guidelines on the use of encryption and key management
- Define the frequency and scope of security assessments to include access point discovery.
- Agencies should ensure that all critical personnel are properly trained on the use of wireless technology.
- Network administrators need to be fully aware of the security risks that WLANs and devices pose. They
- Must work to ensure security policy compliance and to know what steps to take in the event of an attack.

Finally, the most important countermeasures are trained and aware users.

3.8.2. Operational Countermeasures

Physical security is the most fundamental step for ensuring that only authorized users have access to wireless computer equipment. Physical security combines such measures as access controls, personnel identification, and external boundary protection. As with facilities housing wired networks, facilities supporting wireless networks need physical access controls. For example, photo identification, card badge readers, or biometric devices can be used to minimize the risk of improper penetration of facilities.

Biometric systems for physical access control include palm scans, hand geometry, iris scans, retina scans, fingerprint, voice pattern, signature dynamics, or facial recognition. External boundary protection can include locking doors and installing video cameras for surveillance around the perimeter of a site to discourage unauthorized access to wireless networking components such as wireless APs. It is important to consider the range of the AP when deciding where to place an AP in a WLAN environment. If the range extends

beyond the physical boundaries of the office building walls, the extension creates a security vulnerability. An individual outside of the building, perhaps "war driving," could eavesdrop on network communications by using a wireless device that picks up the RF emanations.

A similar consideration applies to the implementation of building-to-building bridges. Ideally, the APsshould be placed strategically within a building so that the range does not exceed the physical perimeter of the building and allow unauthorized personnel to eavesdrop near the perimeter. Agencies should use site survey tools (see next paragraph) to measure the range of AP devices, both inside and outside of the building where the wireless network is located. In addition, agencies should use wireless security assessment tools (e.g., vulnerability assessment) and regularly conduct scheduled security audits.

Site survey tools are available to measure and secure AP coverage. The tools, which some vendors include with their products, measure the received signal strength from the APs. These measurements can be used to map out the coverage area. However, security administrators should use caution when interpreting the results because each vendor interprets the received signal strength differently. Some AP vendors also have special features that allow control of power levels and therefore the range of the AP.

This is useful if the required coverage range is not broad because, for example, the building or room in which access to the wireless network is needed happens to be small. Controlling the coverage range for this smaller building or room may help prevent the wireless signals from extending beyond the intended coverage area. Agencies could additionally use directional antennas to control emanations. However, directional antennas do not protect network links; they merely help control coverage range by limiting signal dispersion.

Although mapping the coverage area may yield some advantage relative to security, it should not be seen as an absolute solution. There is always the possibility that an individual might use a high-gain antenna to eavesdrop on the wireless network traffic. It should be recognized that only through the use of strong cryptographic means can a user

gain any assurance against true eavesdropping adversaries. The following paragraphs discuss how cryptography (Internet Protocol Security [IPsec] and VPNs) can be used to thwart many attacks.

3.8.3. Technical Countermeasures

Technical countermeasures involve the use of hardware and software solutions to help secure the wireless environment.*20* Software countermeasures include proper AP configurations (i.e., the operational and security settings on an AP), software patches and upgrades, authentication, intrusion detection systems (IDS), and encryption. Hardware solutions include smart cards, VPNs, public key infrastructure (PKI), and biometrics.*21* It should be noted that hardware solutions, which generally have software components, are listed simply as hardware solutions.

3.8.3.1. Software Solutions

Technical countermeasures involving software include properly configuring access points, regularly updating software, implementing authentication and IDS solutions, performing security audits, and adopting effective encryption. These are described in the paragraphs below.

3.8.3.1.1. Access Point Configuration

Network administrators need to configure APs in accordance with established security policies and requirements. Properly configuring administrative passwords, encryption settings, reset function, automatic network connection function, Ethernet MAC Access Control Lists (ACL), shared keys, and Simple Network Management Protocol (SNMP) agents will help eliminate many of the vulnerabilities inherent in a vendor's software default configuration. Updating default passwords. Each WLAN device comes with its own default settings, some of which inherently contain security vulnerabilities. The

administrator password is a prime example. On some APs, the factory default configuration does not require a password (i.e., the password field is blank).

Unauthorized users can easily gain access to the device if there is no password protection. Administrators should change default settings to reflect the agency's security policy, which should include the requirement for strong (i.e., an alphanumeric and special character string at least eight characters in length) administrative passwords. If the security requirement is sufficiently high, an agency should consider using an automated password generator. An alternative to password authentication is two-factor authentication. One form of two-factor authentication uses a symmetric key algorithm to generate a new code every minute. This code is a one-time use code that is paired with the user's personal identification number (PIN) for authentication. Another example of two-factor authentication is pairing the user's smart card with the user's PIN. This type of authentication requires a hardware device reader for the smart card or an authentication server for the PIN. Several commercial products provide this capability. However, use of an automated password generator or two-factor authentication mechanism may not be worth the investment, depending on the agency's security requirements, number of users, and budget constraints.

Given the need to ensure good password authentication and policies, it is important to note the critical importance of ensuring that the management interface has the proper cryptographic protection to prevent the unauthorized disclosure of the passwords over the management interface. Numerous mechanisms exist that can be exploited to ensure that encrypted access protects those critical "secrets" in transit. Secure Shell (SSH) and SSL are two such mechanisms.

3.8.3.1.2. Software Patches and Upgrades

Vendors generally try to correct known software (and hardware) security vulnerabilities when they have been identified. These corrections come in the form of security patches and upgrades. Network administrators need to regularly check with the vendor to see whether security patches and upgrades are available and apply them as needed. Also, many vendors have "security alert" e-mail lists to advise customers of new security vulnerabilities and attacks. Administrators should sign up for these critical alerts. Lastly, administrators can check with the NIST ICAT25 vulnerability database for a listing of all known vulnerabilities in the software or hardware being implemented. For specific guidance on implementing security patches, see NIST Special Publication 800-40, Applying Security Patches. An example of a software or firmware patch is the RSA Security WEP security enhancement. In November 2001, RSA Security, Inc., developed a technique for the security holes found in WEP.

This enhancement, referred to as "fast packet keying," generates a unique key to encrypt each network packet on the WLAN. The Fast Packet Keying Solution uses a hashing technique that rapidly generates the per packet keys. The IEEE has approved the fast packet keying technology as one fix to the 802.11 protocol.

Vendors have started applying the fix to new wireless products and have developed software patches for many existing products. Agencies should check with their individual vendors to see if patches are available for the products they have already purchased. Another example of a software or firmware patch that will be available as early as late 2002 is WiFi Protected Access (WPA). WPA, which is being promoted by the WiFi Alliance, is an interim security solution that does not require a hardware upgrade in existing 802.11 equipment. WPA is not a perfect solution but is an attempt to quickly and proactively deliver enhanced protection–to address some of the problems with WEP– prior to the full-blown security techniques of IEEE 802.11 TGi. WiFi Protected Access, a subset of the TGi solution, includes two main features:

- **802.1X**

Temporal Key Integrity Protocol (TKIP):The 802.1X port-based access control provides a framework to allow the use of robust upper layer authentication protocols. It also

facilitates the use of session keys–since cryptographic keys should change often. TKIP includes four new algorithms to enhance the security of 802.11. TKIP extends the IV space, allows for per-packet key construction, provides cryptographic integrity, and provides key derivation and distribution. TKIP, through these algorithms, provides protection against various security attacks discussed earlier, including replay attacks and attacks on data integrity. Additionally, it addresses the critical need to change keys. Again, the objective of WPA is to bring a standards-based security solution to the marketplace to replace WEP while giving the IEEE 802.11 Task Group i enough time to complete and finalize the full 802.11i Robust Security Network (RSN), an amendment to the existing wireless LAN standard. RSN, to be available in the 4th quarter of 2003, will also include the Advanced Encryption standard (AES) for confidentiality and integrity. The RSN solution will require hardware replacements.

.

3.8.3.1.3. Authentication

In general, effective authentication solutions are a reliable way of permitting only authorized users to access a network. Authentication solutions include the use of usernames and passwords; smart cards, biometrics, or PKI; or a combination of solutions (e.g., smart cards with PKI).*27* When relying on usernames and passwords for authentication, it is important to have policies specifying minimum password length, required password characters, and password expiration. Smart cards, biometrics, and PKI have their own individual requirements and will be addressed in greater detail later in this document.

All agencies should implement a strong password policy, regardless of the security level of their operations. Strong passwords are simply a fundamental measure in any environment. Agencies should also consider other types of authentication mechanisms (e.g., smart cards with PKI) if their security levels warrant additional authentication. These mechanisms may be integrated into a WLAN solution to enhance the security of the system. However, users should be careful to fully understand the security provided by enhanced authentication. This does not in and of itself solve all problems. For example, a strong password scheme used for accessing parameters on a NIC card does nothing to address the problems with WEPcryptography.

3.8.3.1.4. Personal Firewalls

Resources on public wireless networks have a higher risk of attack since they generally do not have the same degree of protection as internal resources. Personal firewalls offer some protection against certain attacks. Personal firewalls are software-based solutions that reside on a client's machine and are either client-managed or centrally managed. Client-managed versions are best suited to low-end users because individual users are able to configure the firewall themselves and may not follow any specific security guidelines. Centrally managed solutions provide a greater degree of protection because IT departments configure and remotely manage them. Centrally managed solutions allow organizations to modify client firewalls to protect against known vulnerabilities and to maintain a consistent security policy for all remote users. Some of these high-end products also have VPN and audit capabilities. Although personal firewalls offer some measure of protection, they do not protect against advanced forms of attack.

Depending on the security requirement, agencies may still need additional layers of protection. Users that access public wireless networks in airports or conference centers, for example, should use a personal firewall. Personal firewalls also provide additional protection against rogue access points that can be easily installed in public places.

3.8.3.1.5. Intrusion Detection System (IDS)

An intrusion detection system (IDS) is an effective tool for determining whether unauthorized users are attempting to access, have already accessed, or have compromised the network. IDS for WLANs can be host-based, network-based, or hybrid, the hybrid combining features of host- and network-based IDS. A host-based IDS adds a targeted layer of security to particularly vulnerable or essential systems. A hostbased agent is installed on an individual system (for example, a database server) and monitors audit trails

and system logs for suspicious behavior, such as repeated failed login attempts or changes to file permissions. The agent may also employ a checksum at regular intervals to look for changes to system files. In some cases, an agent can halt an attack on a system, although a host agent's primary function is to log and analyze events and send alerts. A network-based IDS monitors the LAN (or a LAN segment) network traffic, packet by packet, in real time (or as near to real time as possible) to determine whether traffic conforms to predetermined attack signatures (activities that match known attack patterns). For example, the Tear Drop DoS attack sends packets that are fragmented in such a way as to crash the target system. The network monitor will recognize packets that conform to this pattern and take action such as killing the network session, sending an e-mail alert to the administrator, or other action specified. Host based systems have an advantage over network-based IDS when encrypted connections. SSL Web sessions or On-VPN connections—are involved. Because the agent resides on the component itself, the host-based system is able to examine the data after it has been decrypted. In contrast, a network-based

IDS is not able to decrypt data; therefore, encrypted network traffic is passed through without investigation. IDS technology on wired networks can have the following limitations if used to protect wireless networks:

- Network-based IDS sensors that have been placed on the wired network behind the wireless access point will not detect attacks directed from one wireless client to another wireless client (i.e., peer to peer) on the same subnet. The wireless access point switches traffic directly between wireless clients.The traffic does not enter the wired network, it is WEP encrypted, and wired-network IDS sensors do not have an opportunity to capture clear-text packets for analysis. As a result, an adversary that successfully connects an unauthorized wireless client to the network can perform discovery and attack against other wireless hosts without detection by the network-based IDS sensor. In this scenario, the data on the other wireless clients is at risk and information gathered from the other clients may be used to form an attack on the wired network.
- IDS sensors on the wired network usually will not detect attempts to "deassociate" (to end an association relationship with) a legitimate client from the wireless network and will not detect the association of an unauthorized wireless client with

the wireless network. Flooding, jamming, and other DoS attacks against wireless devices use physical and data-link layer techniques that are not visible to the IDS sensor at a packet level and generally would not be routed onto the wired network.

- IDS technology for wired networks generally only detects attacks once packets are directed at hosts on the wired network from a compromised wireless client. At that point, the wireless network has already been compromised, and risk to the wired network is imminent. An important goal is to detect and send an alarm on unauthorized wireless activity before it affects the wired network.
- IDS technology on wired networks will not identify the physical location of rogue access points within the building. These rogue access points can act as entry points for unauthorized wireless access from remote locations.
- IDS technology will not detect an authorized wireless device communicating peer-to-peer with an unauthorized wireless device. This scenario can create a bridge into the wired network by allowing an adversary to connect to a wireless device that is operating in "ad hoc" mode. The ad hoc mode allows a wireless device to be used to relay traffic to the network and creates a number of potential attack scenarios. Expansion of a wired network by connecting one or more wireless networks significantly expands the network's security perimeter and introduces risk that may not be addressed by existing intrusion detectiondevices on the wired network. Agencies that want to expand network functionality by adding a wireless capability should examine the existing IDS architecture and consider additional solutions to address the above-mentioned risks. Agencies should consider implementing a wireless IDS solution that provides the following capabilities:
  - Identification of the physical location of wireless devices within the building and surrounding grounds
  - Detection of unauthorized peer-to-peer communications within the wireless network that are not visible to the wired network
  - Analysis of wireless communications and monitoring of the 802.11 RF space and generation of an alarm upon detection of unauthorized configuration changes to wireless devices that violate security policy

- Detection of and alarming for when a rogue access point goes live within the agency's security perimeter
- Detection of flooding and deassociation attempts before they successfully compromise the wireless network
- Provision of centralized monitoring and management features with potential for integration into existing IDS monitoring and reporting software to produce a consolidated view of wireless and wired network security status. Agencies that require high levels of security should consider deploying an IDS because it provides an added layer of security. Agencies that currently employ IDSs should consider the addition of the capabilities above to supplement their existing capabilities. The deployment of IDS obviously comes at a cost and should be considered if financially feasible. In addition to the cost of the system itself, an IDS requires experienced personnel to monitor and react to IDS events and to provide general administration to the IDS database and components. Agencies should also consider using a correlation engine, which receives standard real-time security events from a variety of sensors, such as IDS, firewall, and virus systems. Correlation engines combine in real-time and analyze a wide variety of threats. These threats can include several classes of attacks, such as Distributed Denial of Service (DDoS) attacks.

3.8.3.1.6. Encryption

As mentioned earlier, APs generally have only three encryption settings available: none, 40-bit shared key, and 104-bit setting. The setting of none represents the most serious risk since unencrypted data traversing the network can easily be intercepted, read, and altered. A 40-bit shared key will encrypt the network communications data, but there is still a risk of compromise. The 40-bit encryption has been broken by brute force cryptanalysis using a high-end graphics computer and even low-end computers; consequently, it is of questionable value.*30* In general, 104-bit encryption is more secure than 40-bit encryption because of the significant difference in the size of the cryptographic keyspace. Although this is not true for 802.11 WEP because of poor cryptographic design using IVs, it is

recommended nonetheless as a good practice. Again, users of 802.11 APs and wireless clients should be vigilant about checking with the vendor regarding upgrades to firmware and software as they may overcome some of the WEP problems.

3.8.3.1.7. Security Assessments

Security assessments, or audits, are an essential tool for checking the security posture of a WLAN and for determining corrective action to make sure it remains secure. It is important for agencies to perform regular audits using wireless network analyzers and other tools. An analyzer, again, sometimes called a "sniffer," is an effective tool to conduct security auditing and troubleshoot wireless network issues.

Security administrators or security auditors can use network analyzers, to determine if wireless products are transmitting correctly and on the correct channels. Administrators should periodically check within the office building space (and campus) for rogue APs and against other unauthorized access. Agencies may also consider using an independent third party to conduct the security audits. Independent third-party security consultants are often more up-to-date on security vulnerabilities, better trained on security solutions, and equipped to assess the security of a wireless network. An independent third-party audit, which may include penetration testing, will help an agency ensure that its WLAN is compliant with established security procedures and policies and that the system is up-to-date with the latest software patches and upgrades.*31* For more information on network security.

3.8.3.2. Hardware Solutions

Hardware countermeasures for mitigating WLAN risks include implementing smart cards, VPNs, PKI, biometrics, and other hardware solutions.

3.8.3.2.1. Smart Cards

Smart cards may add another level of protection, although they also add another layer of complexity. Agencies can use smart cards in conjunction with username or password or by themselves. They can use smart cards in two-factor authentication (see above). Agencies can also combine smart cards with biometrics.

In wireless networks, smart cards provide the added feature of authentication. Smart cards are beneficial in environments requiring authentication beyond simple username and password. User certificate and other information are stored on the cards themselves and generally require the user only to remember a PIN number. Smart cards are also portable; consequently users can securely access their networks from various locations. As with an authentication software solution, these tamper-resistant devices may be integrated into a WLAN solution to enhance the security of the system. Again, users should be careful to fully understand the security provided by the smart card solution.

3.8.3.2.2. Virtual Private Networks

VPN technology is a rapidly growing technology that provides secure data transmission across public network infrastructures. VPNs have in recent years allowed corporations to harness the power of the Internet for remote access. Today, VPNs are typically used in three different scenarios: for remote user access, for LAN-to-LAN (site-to-site) connectivity, and for extranets. VPNs employ cryptographic techniques to protect IP information as it passes from one network to the next or from one location to the next. Data that is inside the VPN "tunnel"—the encapsulation of one protocol packet inside another is encrypted and isolated from other network traffic. A VPN for site-to-site connectivity is illustrated in Figure 3-5. In this scenario, traffic communicated from Site A to Site B is protected as it moves across the Internet. Confidentiality, integrity, and other security services are provided as discussed below.

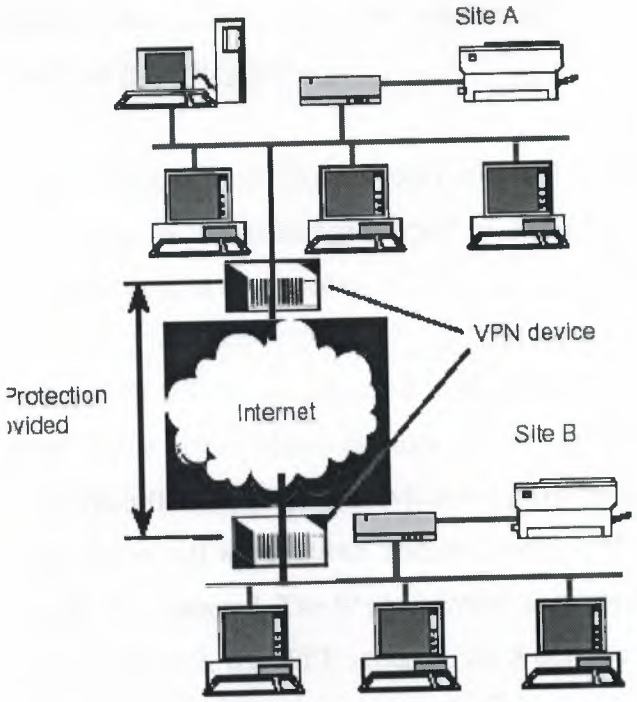


Figure 3-5 Typical Use of VPN for Secure Internet Communications From Site-to-Site

Most VPNs in use today make use of the IPsec protocol suite. IPsec, developed by the Internet Engineering Task Force (IETF), is a framework of open standards for ensuring private communications over IP networks. It provides the following types of robust protection:

- Confidentiality
- Integrity
- Data origin authentication
- Traffic analysis protection.

Connectionless integrity guarantees that a received message has not changed from the original message. Data origin authentication guarantees that the received message was sent by the originator and not by a person masquerading as the originator. Replay protection provides assurance that the same message is not delivered multiple times and that messages are not out of order when delivered. Confidentiality ensures that others cannot read the information in the message. Traffic analysis protection provides assurance that an eavesdropper cannot determine who is communicating or the frequency or volume of communications. The Encapsulating Security Protocol (ESP) header provides privacy and

protects against malicious modification, and the Authentication header (AH) protects against modification without providing privacy.

The Internet Key Exchange (IKE) Protocol allow for secret keys and other protection-related parameters to be exchanged prior to a communication without the intervention of a user.*33* IKEv1 is in the process of being replaced by IKE.

The use of IP sec with WLANs is depicted in Figure 3-11. As shown, the IP sec tunnel is provided from the wireless client through the AP to the VPN device on the enterprise network edge. With IP sec , security services are provided at the network layer of the protocol stack. This means all applications and protocols operating above that layer (i.e., above layer 3) are IP sec protected. The IP sec security services are independent of the security that is occurring at layer 2, the WEP security. As a defense-in-depth strategy, if a VPN is in place, an agency can consider having both IP sec and WEP applied. With a configuration as in Figure 3-6, the VPN encrypts (and otherwise protects) the transmitted data to and from the wired network.

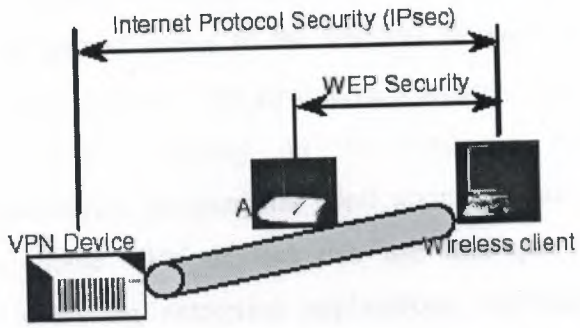


Figure 3-6 VPN Security in Addition to WEP

Figure 3-7 illustrates another example of a wireless network with the "VPN overlay." As shown, with wireless devices with VPNs , clients can connect securely to the enterprise network through a VPN gateway on the enterprise edge. Wireless clients establish IP sec connections to the wireless VPN gateway—in addition to or instead of WEP. Note that the wireless client does not need special hardware; it just needs to be

provided with IP sec/VPN client software. The VPN gateway can use pre shared cryptographic keys or digital (public-key based) certificates for wireless client device authentication.

The reader should recognize that an organization that uses preshared keys for a VPN solution will encounter the same scalability and key distribution problems present in WEP. Additionally, user authentication to the VPN gateway can occur using remote authentication dial-in user service (RADIUS) or one-time passwords (OTP). The VPN gateway may or may not have an integral firewall to restrict traffic to certain locations within the enterprise network. Today, most VPN devices have integrated firewalls that work together to protect both the network from unauthorized access and the user data going over the network.

Integrated VPNs and firewalls save costs and reduce administrative burden. Additionally, the VPN gateway may or may not have the ability to create an audit journal of all activities. An audit trail is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities. A security manager may be able to use an audit trail on the VPN gateway to monitor compliance with security policy and to gain an understanding of whether only authorized persons have gained access to the wireless network. It should be noted that although the VPN approach enhances the air-interface security significantly, this approach does not completely address security on the enterprise network. For example, authentication and authorization to enterprise applications are not always addressed with this security solution. Some VPN devices can use user-specific policies to require authentication before accessing enterprise applications. Agencies may want to seek assistance in developing a comprehensive enterprise security strategy.

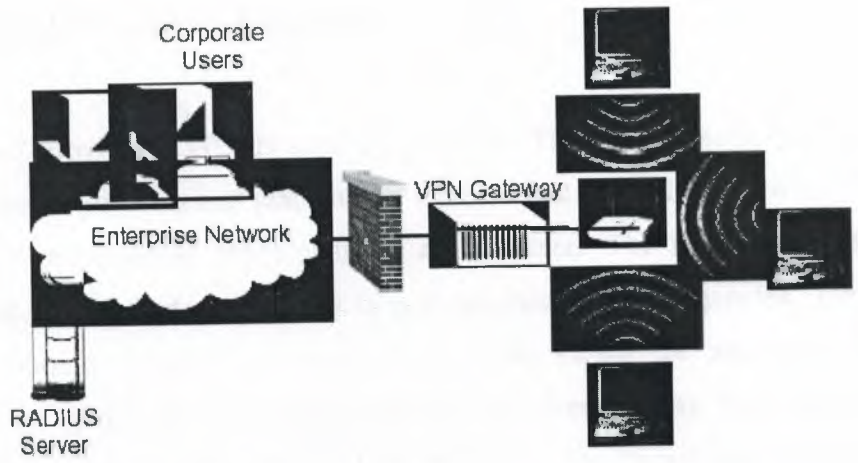


Figure 3.7 Simplified Diagram of VPN WLAN

3.8.3.2.3. Public Key Infrastructure (PKI)

PKI provides the framework and services for the generation, production, distribution, control, and accounting of public key certificates. It provides applications with secure encryption and authentication of network transactions as well as data integrity and nonrepudiation, using public key certificates to do so.

WLANs can integrate PKI for authentication and secure network transactions. Third-party manufacturers, for instance, provide wireless PKI, handsets, and smart cards that integrate with WLANs. Users requiring high levels of security should strongly consider PKI. It provides strong authentication through user certificates, which can be used with application-level security, to sign and encrypt messages. Smart cards provide even greater utility since the certificates are integrated into the card. Smart cards serve both as a token and a secure (tamper-resistant) means for storing cryptographic credentials. Users requiring lower levels of security, on the other hand, need to consider carefully the complexity and cost of implementing and administering a PKI before adopting this solution.

3.9. Wireless LAN Security Checklist

Table 3-2 provides a WLAN security checklist. The table presents guidelines and recommendations for creating and maintaining a secure 802.11 wireless network. For each recommendation or guideline, three columns are provided. The first column, the Best Practice column, if checked, means this is recommended for all agencies. The second column, the "Should Consider" column, if checked, means the recommendation is something that an agency should carefully consider for three reasons. First, implementing the recommendation may provide a higher level of security for the wireless environment by offering some sort of additional protection. Second, the recommendation supports a defense-in-depth strategy. Third, it may have significant performance, operational, or cost impacts. In summary, if the "Should Consider" column is checked, agencies need to carefully consider the option and weigh the costs versus the benefits. The last column, the "Status" column, is intentionally left blank and allows an agency
to use this table as a true checklist. For instance, an individual performing a wireless security audit in an 802.11 environment can quickly check off each recommendation for the agency, asking "Have I done this?"

Table 3-2. Wireless LAN Security Checklist

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
	Management Recommendations			
1.	Develop an agency security policy that addresses the use of wireless technology, including 802.11.	✓		
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.	✓		
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	✓		
4.	Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become available (prior to purchase).	✓		
5.	Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	✓		
6.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	✓		
7.	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	✓		
8.	Complete a site survey to measure and establish the AP coverage for the agency.	✓		
9.	Take a complete inventory of all APs and 802.11 wireless devices.	✓		
10.	Ensure that wireless networks are not used until they comply with the agency's security policy.	✓		
11.	Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.	✓		
12.	Place APs in secured areas to prevent unauthorized physical access and user manipulation.	✓		
	Technical Recommendations			
13.	Empirically test AP range boundaries to determine the precise extent of the wireless coverage.	✓		

3.11. Security of Bluetooth

This section helps the reader to understand the built-in security features of Bluetooth. It provides an overview of the inherent security features to better illustrate its limitations and provide a motivation for some of the recommendations for enhanced security. Security for the Bluetooth radio path is depicted in Figure 3.8

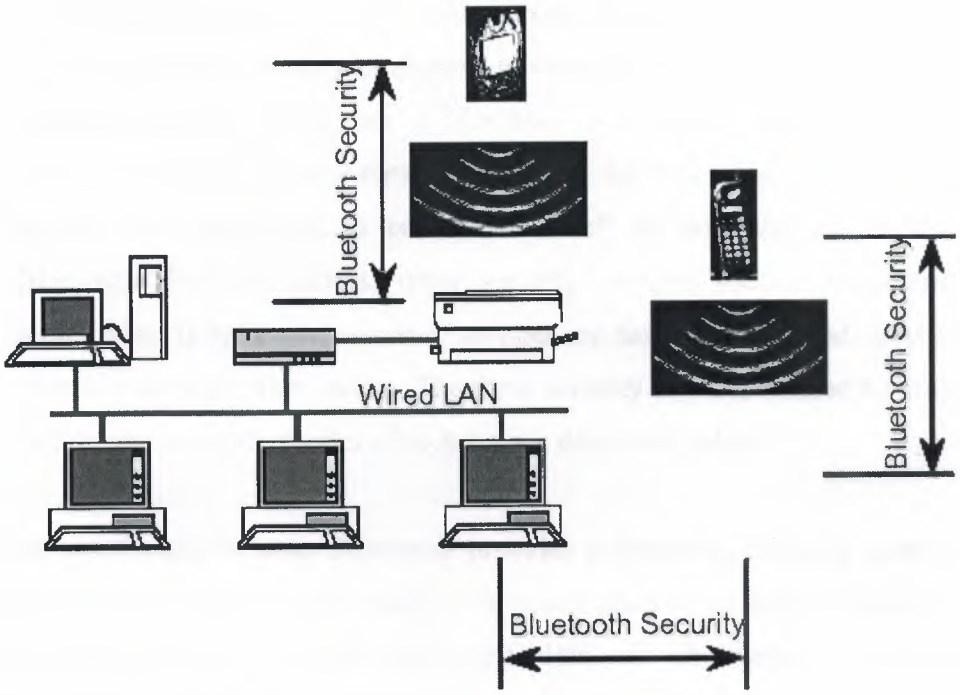


Figure 3.8 Bluetooth Air-Interface Security

Bluetooth Security As shown in the illustration, security for Bluetooth is provided on the various wireless links—on the radio paths only. In other words, link authentication and encryption may be provided, but true end-to-end security is not possible without providing higher layer security solutions on top of Bluetooth. In the example provided, security services are provided between the PDA and the printer, between the cell phone and laptop, and between the laptop and the desktop. Briefly, the three basic security services defined by the Bluetooth specifications are the following:

- **Authentication:** A goal of Bluetooth is the identity verification of communicating devices. This security service addresses the question "Do I know with whom I'm communicating?" This service provides an abort mechanism if a device cannot authenticate properly.
- **Confidentiality**: Confidentiality, or privacy, is another security goal of Bluetooth. The intent is to prevent information compromise caused by

eavesdropping (passive attack). This service, in general, addresses the question "Are only authorized devices allowed to view my data?"

- **Authorization**: A third goal of Bluetooth is a security service developed to allow the control of resources. This service addresses the question "Has this device been authorized to use this service? As with the 802.11 standard, Bluetooth does not address other security services such as audit and Non repudiation. If these other security services are desired or required, they must be provided through other means. The three security services offered by Bluetooth and details about the modes of security are described below.

Also worthwhile to note, Bluetooth provides a frequency-hopping scheme with 1,600 hops/second combined with radio link power control (to limit transmit range). These characteristics provide Bluetooth with some additional, albeit small, protection from eavesdropping and malicious access. The frequency hopping scheme, primarily a technique to avoid interference, makes it slightly more difficult for an adversary to locate the Bluetooth transmission. Using the power control feature appropriately forces any potential adversary to be in relatively close proximity to pose a threat to the Bluetooth network.

3.11.1. Security Features of Bluetooth per the Specifications

Bluetooth has three different modes of security. Each Bluetooth device can operate in one mode only at a particular time. The three modes are the following:

- **Security Mode 1**—Nonsecure mode
- **Security Mode 2**—Service-level enforced security mode
- **Security Mode 3**—Link-level enforced security mode

In Security Mode 1, a device will not initiate any security procedures. In this nonsecure mode, the security functionality (authentication and encryption) is completely bypassed. In effect, the Bluetooth device in Mode 1 is in a "promiscuous" mode that allows other Bluetooth devices to connect to it. This mode is provided for applications for which security is not required, such as exchanging business cards. In Security Mode 2, the service-level security mode, security procedures are initiated after channel establishment at

the Logical Link Control and Adaptation Protocol (L2CAP) level. L2CAP resides in the data link layer and provides connection-oriented and connectionless data services to upper layers. For this security mode, a security manager (as specified in the Bluetooth architecture) controls access to services and to devices. The centralized security manager maintains polices for access control and interfaces with other protocols and device users.

Varying security polices and "trust" levels to restrict access may be defined for applications with different security requirements operating in parallel. Therefore, it is possibleto grant access to some services without providing access to other services. Obviously, in this mode, the notion of authorization—that is the process of deciding if device A is allowed to have access to service X—is introduced. In Security Mode 3, the link-level security mode, a Bluetooth device initiates security procedures before the channel is established. This is a built-in security mechanism, and it is not aware of any application layer security that may exist. This mode supports authentication (unidirectional or mutual) and encryption. These features are based on a secret link key that is shared by a pair of devices. To generate this key, a pairing procedure is used when the two devices communicate for the first time.

The Bluetooth modes are depicted in Figure 3-9

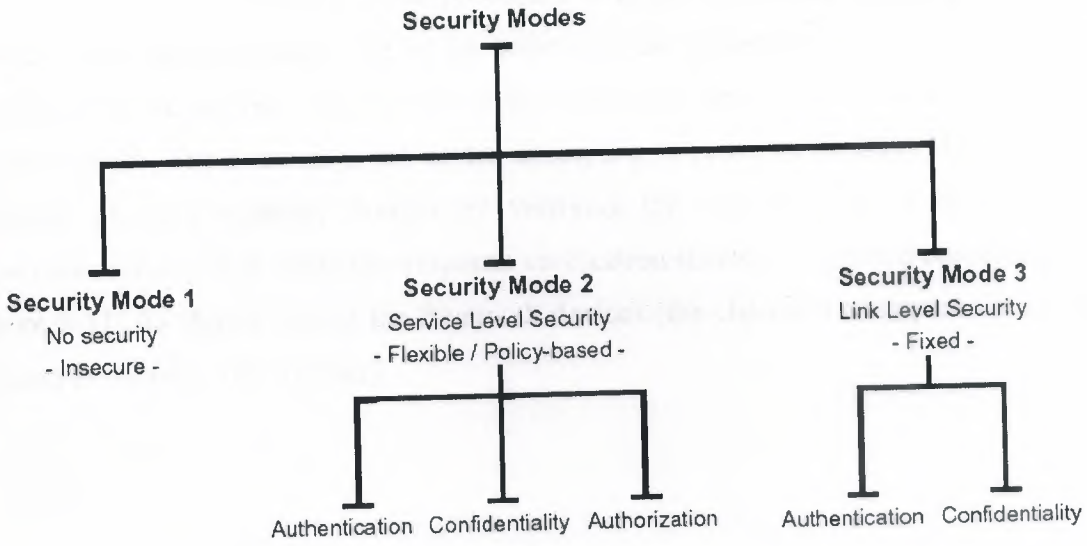


Figure 3.9 Taxonomy of Bluetooth Security Modes

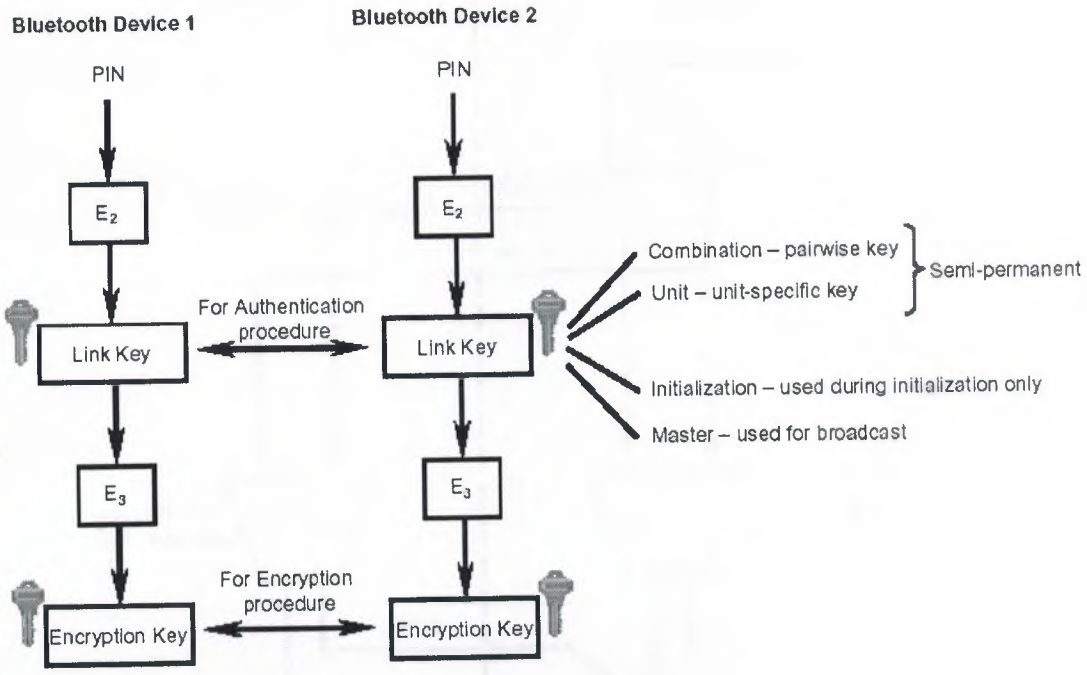


Figure 3.10 Bluetooth Key Generation from PIN

3.10.1.1. Authentication

The Bluetooth authentication procedure is in the form of a "challenge-response" scheme. Two devices interacting in an authentication procedure are referred to as the claimant and the verifier. The verifier is the Bluetooth device validating the identity of another device. The claimant is the device attempting to prove its identity. The challenge-response protocol validates devices by verifying the knowledge of a secret key—a Bluetooth link key. The challenge-response verification scheme is depicted conceptually in Figure 3-11. As shown, one of the Bluetooth devices (the claimant) attempts to reach and connect to the other (the verifier).

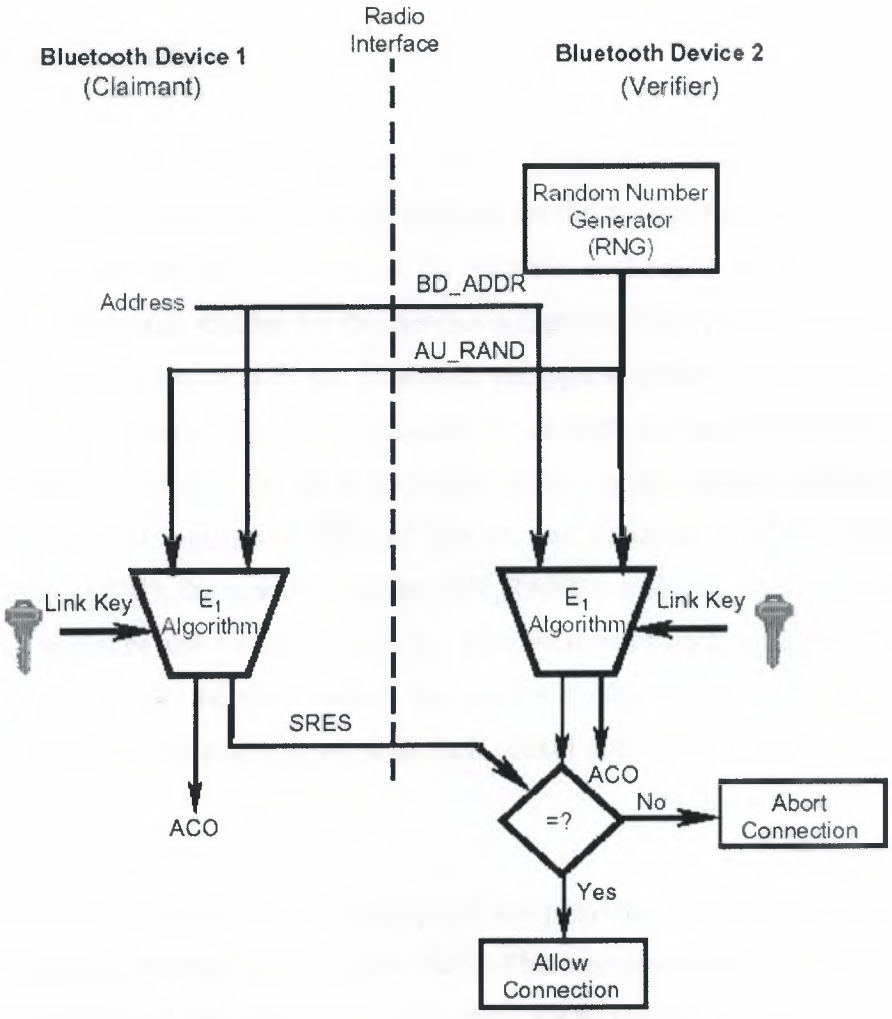


Figure 3.11. Bluetooth Authentication

The steps in the authentication process are the following:

Step 1. The claimant transmits its 48-bit address (BD_ADDR) to the verifier.

Step 2. The verifier transmits a 128-bit random challenge (AU_RAND) to the claimant.

Step 3. The verifier uses the E1 algorithm to compute an authentication response using the address, link key, and random challenge as inputs. The claimant performs the same computation.

Step 4. The claimant returns the computed response, SRES, to the verifier.

Step 5. The verifier compares the SRES from the claimant with the SRES that it computes.

Step 6. If the two 32-bit SRES values are equal, the verifier will continue connection establishment

3.10.1.2. Confidentiality

In addition to the authentication scheme, Bluetooth provides for a confidentiality security service to thwart eavesdropping attempts on the air-interface. Bluetooth encryption is provided to protect the payloads of the packets exchanged between two Bluetooth devices. The encryption scheme for this service is depicted conceptually in Figure 3-12.

As shown in Figure 4-8, the Bluetooth encryption procedure is based on a stream cipher, E0. A key stream output is exclusive-OR-ed with the payload bits and sent to the receiving device. This key stream is produced using a cryptographic algorithm based on linear feedback shift registers (LFSR).*43* The encrypt function takes as inputs the master identity (BD_ADDR), the random number (EN_RAND), a slot number, and an encryption key, which initialize the LFSRs before the transmission of each packet, if encryption is enabled. Since the slot number used in the stream cipher changes with each packet, the ciphering engine is also reinitialized with each packet although the other variables remain static.

As shown in Figure 4-8, the encryption key provided to the encryption algorithm is produced using an internal key generator (KG). This key generator produces stream cipher keys based on the link key, random number (EN_RAND again), and the ACO value. The ACO parameter, a 96-bit authenticated cipher offset, is another output produced during the authentication procedure shown in Figure 3-10. As mentioned above, the link key is the 128-bit secret key that is held in the Bluetooth devices and is not accessible to the user. Moreover, this critical security element is never transmitted outside the Bluetooth device.

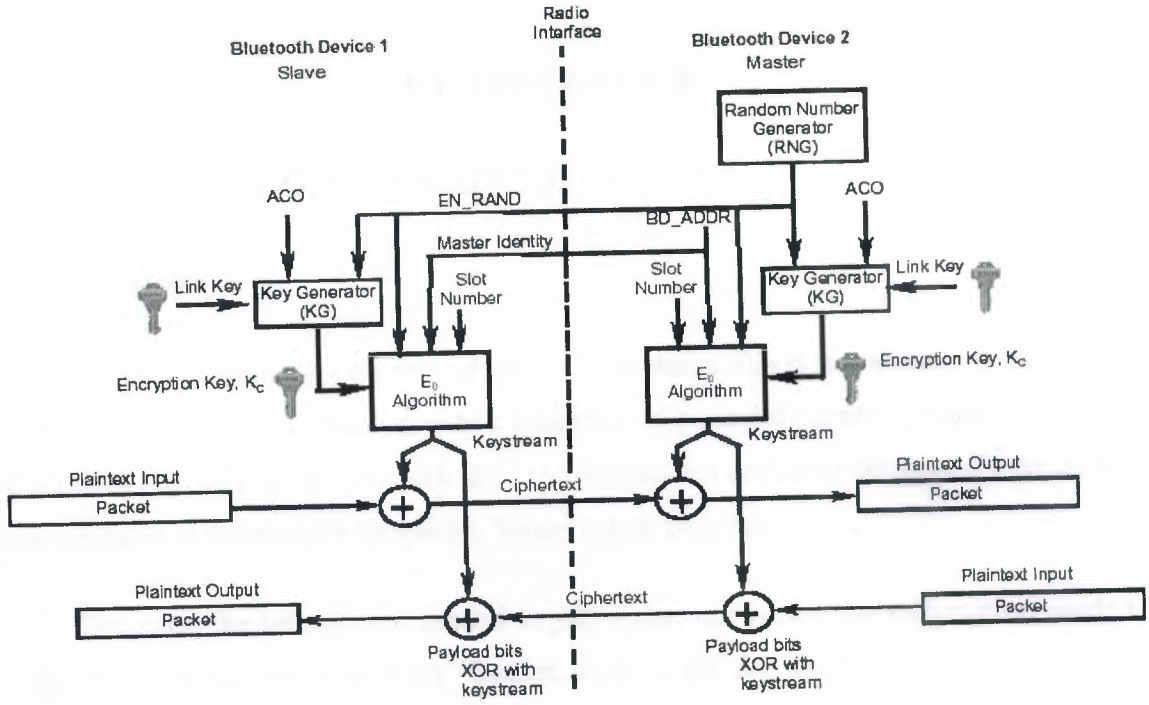


Figure 3.12 Bluetooth Encryption Procedure

The encryption key (KC) is generated from the current link key. The key size may vary from 8 bits to 128 bits and is negotiated. The negotiation process occurs between master devices and slave devices. During negotiation, a master device makes a key size suggestion for the slave. In every application, a "minimum acceptable" key size parameter can be set to prevent a malicious user from driving the key size down to the minimum of 8 bits, making the link totally insecure.

The Bluetooth specification also allows three different encryption modes to support the confidentiality service:

- **Encryption Mode 1**—No encryption is performed on any traffic.
- **Encryption Mode 2**—Broadcast traffic goes unprotected (not encrypted), but individually addressed
- traffic is encrypted according to the individual link keys.
- **Encryption Mode 3**—All traffic is encrypted according to the master link key.

CHAPTER FOUR

4. PROBLEMS AND SOLUTIONS TO WLAN

4.1 Easy Access

Wireless LANs are easy to find. Strictly speaking, this is not a security threat. All wireless networks need to announce their existence so potential clients can link up and use the services provided by the network. 802.11 requires that networks periodically announce their existence to the world with special frames called Beacons.

However, the information needed to join a network is also the information needed to launch an attack on a network. Beacon frames are not processed by any privacy functions, which means that your 802.11 network and its parameters are available for anybody with an 802.11 card. "War drivers" have used high-gain antennas and software to log the appearance of Beacon frames and associate them with a geographic location using GPS.

Short of moving into heavily-shielded office space that does not allow RF signals to escape, there is no solution for this problem. The best you can do is to mitigate the risk by using strong access control and encryption solutions to prevent a wireless network from being used as an easy entry point into the network. Deploy access points outside firewalls, and protect sensitive traffic with VPNs.

4.2. "Rogue" Access Points

Easy access to wireless LANs is coupled with easy deployment. When combined, these two characteristics can cause headaches for network administrators. Any user can run to a nearby computer store, purchase an access point, and connect it to the corporate network without authorization. Many access points are now priced well within the signing authority of even the most junior managers. Departments may also be able to roll out their own wireless LANs without authorization from the powers that be.

"Rogue" access points deployed by end users pose great security risks. End users are not security experts, and may not be aware of the risks posed by wireless LANs. Most existing small deployments mapped by war drivers do not enable the security features on products, and many access points have had only minimal changes made to the default settings. It is hard to believe that end users within a large corporation will do much better

Unfortunately, no good solution exists to this concern. Tools like NetStumbler allow network administrators to wander their building looking for unauthorized access points, but it is expensive to devote time to wandering the building looking for new access points.

Monitoring tools will also pick up other access points in the area, which may be a concern if you are sharing a building or a floor with another organization. Their access points may cover part of your floor space, but their access points do not directly compromise your network and are not cause for alarm. The periodic "walk-through" of your campus is the only way to address the threat of unauthorized deployment. At least network analyzers are moving to a handheld form, so you won't have to carry as much.

4.3. Unauthorized Use of Service

Several war drivers have published results indicating that a clear majority of access points are put in service with only minimal modifications to their default configuration. Nearly all of the access points running with default configurations have not activated WEP (Wired Equivalent Privacy) or have a default key used by all the vendor's products out of the box. Without WEP, network access is usually there for the taking.

Two problems can result from such open access. In addition to bandwidth charges for unauthorized use, legal problems may result. Unauthorized users may not necessarily obey your service provider's terms of service, and it may take only one spammer to cause your ISP to revoke your connectivity.

Whether unauthorized use is a problem depends on the objectives of the service. For corporate users extending wired networks, access to wireless networks must be as tightly

controlled as for the existing wired network. Strong authentication is a must before access is granted to the network.

If you have deployed a VPN to protect the network from wireless clients, it probably has strong authentication capabilities already built-in. Administrators can also choose to use 802.1x to protect the network from unauthorized users at the logical point of attachment. 802.1x also allows administrators to select an authentication method based on Transport Layer Security (TLS), which can be used to ensure that users attach only to authorized access points.

Not all networks, however, need to deploy ironclad user authentication. Theft of service was a major concern for connectivity providers in "hot spots" such as hotels and airports. After all, the business model was to charge for network access, so preventing unauthorized access was a business requirement. In the wake of the spectacular failure of some of the former big-name players like MobileStar, the hot-spot connectivity industry is experimenting with new business models.

Newer players in the market have based the business model on the idea that free wireless network access is an amenity that might draw guests and convention business. In this newer business model, user authentication is necessary only to ensure accountability. Authentication using a Web browser is a perfectly acceptable solution because it allows sessions to be identified and does not require specialized client software or a certain model of 802.11 network interface.

4.4. Service and Performance Constraints

Wireless LANs have limited transmission capacity. Networks based on 802.11b have a bit rate of 11 Mbps, and networks based on the newer 802.11a technology have bit rates up to 54 Mbps. This capacity is shared between all the users associated with an access point. Due to MAC-layer overhead, the actual effective throughput tops out at roughly half of the nominal bit rate. It is not hard to imagine how local area applications might overwhelm such limited capacity, or how an attacker might launch a denial of service attack on the limited resources.

Radio capacity can be overwhelmed in several ways. It can be swamped by traffic coming in from the wired network at a rate greater than the radio channel can handle. If an attacker were to launch a ping flood from a Fast Ethernet segment, it could easily overwhelm the capacity of an access point. Depending on the deployment scenario, it might even be possible to overwhelm several access points by using a broadcast address as the destination of the ping flood.

Attackers could also inject traffic into the radio network without being attached to a wireless access point. The 802.11 MAC is designed to allow multiple networks to share the same space and radio channel. Attackers wishing to take out the wireless network could send their own traffic on the same radio channel, and the target network would accommodate the new traffic as best it could using the CSMA/CA mechanisms in the standard.

Large traffic loads need not be maliciously generated, either, as any network engineer can tell you. Large file transfers or complex client/server systems may transfer large amounts of data over the network to assist users with their jobs. If enough users start pulling vast tracts of data through the same access point, network access may resemble sucking molasses through a straw north of the Arctic Circle in January.

Addressing performance problems starts with monitoring and discovering them. Many access points will report statistics via SNMP, but not with the level of detail required to make sense of end-user performance complaints. Wireless network analyzers can report on the signal quality and network health at a single location, but tools designed for wireless network administrators are only beginning to emerge.

The initial commercial wireless analyzer offerings were straightforward ports of their wired cousins; new products such as AirMagnet's handheld analyzer look like extremely promising additions to the wireless network engineer's toolkit. No enterprise-class wireless network management system has yet emerged. Some performance complaints could be addressed by deploying a traffic shaper at the point at which a wireless LAN connects to your network backbone. While this will not defend against denial of

service attacks, it may help prevent heavy users from monopolizing the radio resources in an area.

4.5. MAC Spoofing and Session Hijacking

802.11 networks do not authenticate frames. Every frame has a source address, but there is no guarantee that the station sending the frame actually put the frame "in the air." Just as on traditional Ethernet networks, there is no protection against forgery of frame source addresses.Attackers can use spoofed frames to redirect traffic and corrupt ARP tables. At a much simpler level, attackers can observe the MAC addresses of stations in use on the network and adopt those addresses for malicious transmissions.

To prevent this class of attacks, user authentication mechanisms are being developed for 802.11 networks. By requiring authentication by potential users, unauthorized users can be kept from accessing the network. (Denial of service attacks will still be possible, though, because nothing can keep attackers from having access to the radio layer.)

The basis for the user authentication mechanism is the 802.1x standard ratified in June 2001. 802.1x can be used to require user authentication before accessing the network, but additional features are necessary to provide all of the key management functionality wireless networks require. The additional features are currently being ironed out by Task Group I for eventual ratification as 802.11i.

Attackers can use spoofed frames in active attacks as well. In addition to hijacking sessions, attackers can exploit the lack of authentication of access points. Access points are identified by their broadcasts of Beacon frames. Any station that claims to be an access point and broadcasts the right service set identifier (SSID, also commonly called a network name) will appear to be part of an authorized network.

Attackers can, however, easily pretend to be an access point because nothing in 802.11 requires an access point to prove it really is an access point. At that point, the attacker could potentially steal credentials and use them to gain access to the network

through a man-in-the-middle (MITM) attack. Fortunately, protocols that support mutual authentication are possible with 802.1x. Using methods based on TLS, access points will need to prove their identity before clients provide authentication credentials, and credentials are protected by strong cryptography for transmission over the air.

Session hijacking will not be completely solved until the 802.11 MAC adopts per-frame authentication. Until that point, if session hijacking is a concern, you must deploy a cryptographic protocol on top of 802.11 to protect against hijacking.

4.6. Traffic Analysis and Eavesdropping

802.11 provides no protection against attacks that passively observe traffic. The main risk is that 802.11 does not provide a way to secure data in transit against eavesdropping. Frame headers are always "in the clear" and are visible to anybody with a wireless network analyzer. Security against eavesdropping was supposed to be provided by the much-maligned Wired Equivalent Privacy specification.

A great deal has been written about the flaws in WEP. It protects only the initial association with the network and user data frames. Management and control frames are not encrypted or authenticated by WEP, leaving an attacker wide latitude to disrupt transmissions with spoofed frames.

Early WEP implementations are vulnerable to cracking by tools such as AirSnort and WEPCrack, but the latest firmware releases from most vendors eliminate all known attacks. The latest products go one step farther and use key management protocols to change the WEP key every 15 minutes. Even the busiest wireless LAN does not generate enough data for known attacks to recover the key in 15 minutes.

Whether you rely on WEP solely, or layer stronger cryptographic solutions on top of it is largely a question of risk management. The latest product releases have no known vulnerabilities. While that is some comfort, the same claim could have been made in July 2001 before release of the current generation of WEP-cracking tools. If your wireless LAN is being used for sensitive data, WEP may very well be insufficient for your needs. Strong

cryptographic solutions like SSH, SSL, and IPSec were designed to transmit data securely over public channels and have proven resistant to attack over many years, and will almost certainly provide a higher level of security.

4.7. Higher Level Attacks

Once an attacker gains access to a wireless network, it can serve as a launch point for attacks on other systems. Many networks have a hard outer shell composed of perimeter security devices that are carefully configured and meticulously monitored. Inside the shell, though, is a soft, vulnerable (and tasty?) center.

Wireless LANs can be deployed quickly if they are directly connected to the vulnerable backbone, but that exposes the network to attack. Depending on the perimeter security in place, it may also expose other networks to attack, and you can bet that you will be quite unpopular if your network is used as a launch pad for attacks on the rest of the world. The solution is straightforward in theory: treat the wireless network as something outside the security perimeter, but with special access to the inside of the network. Although security diligence is time consuming, so is being sued.

4.8. Wireless Sniffer

An attacker can sniff and capture legitimate traffic. Many of the sniffer tools for Ethernet are based on capturing the first part of the connection session, where the data would typically include the username and password. An intruder can masquerade as that user by using this captured information. An intruder who monitors the wireless network can apply this same attack principle on the wireless. One of the big differences between wireless sniffer attacks and wired sniffer attacks is that a wired sniffer attack is achieved by remotely placing a sniffer program on a compromised server and monitor the local network segment. This sniffer based attack can happen from anywhere in the world. Wireless sniffing requires the attacker to typically be within range of the wireless traffic. This is usually around 300 feet range, but wireless equipment keeps strengthening the signal and pushing this range further out.

4.9. Broadcast Monitoring

If a base station is connected to a hub rather than a switch, any network traffic across that hub can be potentially broadcasted out over the wireless network. Because the Ethernet hub broadcasts all data packets to all connected devices including the wireless base station, an attacker can monitor sensitive data going over wireless not even intended for any wireless clients.

4.10. ArpSpoof Monitoring and Hijacking

Normally, in regards to an AP, the network data traffic on the backbone of a subnet would be treated similarly like a network switch, thus traffic not intended for any wireless client would not be sent over the airwaves. This could reduce significantly the amount of sensitive data over the wireless network. An attacker using the arpspoof technique can trick the network into passing sensitive data from the backbone of the subnet and route it through the attacker's wireless client. This provides the attacker both access to sensitive data that normally would not be sent over wireless and an opportunity to hijack TCP sessions.

4.11.Hijacking SSL (Secure Socket Layer) and SSH (Secure Shell) connections.

By using arpspoofing technique, an attacker can hijack simple TCP connections. There are tools that allow for hijacking SSL and SSH connections. Typically, when SSL and SSH connections get hijacked, the only alert to the end-user is a warning that the credentials of the host and certificate have changed and ask if you trust the new ones. Many users simply accept the new credentials, thus allowing an attacker to succeed. A reasonable interim measure to prevent the attack is to have users enable SSH's StrictHostKeyChecking option, and to distribute server key signatures to mobile clients.

4.12.Wired Equivalent Privacy (WEP)

WEP can be typically configured in 3 possible modes:

- No encryption mode
- 40 bit encryption
- 128 bit encryption

WEP, by default out of the box, all base station models analyzed have WEP turned off. 64 bit encryption versus 128 bit encryption provides no added protection against the known flaw in WEP. Most public wireless LAN access points (i.e., airports, hotels, etc) do not enable WEP. Based on statistical analysis in regions like New York, San Francisco, London, Atlanta, most companies do not turn on WEP security on their APs. If the AP does not enable WEP, the wireless clients can not use the WEP encryption.

In some base stations, it is optional whether the encryption is enforced. The WEP encrypted may be turned on, but if it is not enforced, a client without encryption with the proper SSID can still access that base station.

4.12.1 Attacks against WEP

802.11b standard uses encryption called WEP (Wired Equivalent Privacy). It has some known weaknesses in how the encryption is implemented. Using WEP is better than not using it. It at least stops casual sniffers. Today, there are readily available tools for most attackers to crack the WEP keys. Airsnort and others tools take a lot of packets (several million) to get the WEP key, on most networks this takes longer than most people are willing to wait. If the network is very busy, the WEP key can be cracked and obtained within 15 minutes.

The fix for encryption weakness for the standard is not slated to be addressed before 2002. Because of the WEP weakness, wireless sniffing and hijacking techniques can work despite the WEP encrypted turned on. There is the IEEE 802.1X standard which allows network access to be authenticated and keys to be distributed. This allows access to APs to

be authenticated and WEP keys to be distributed and updated. More APs are starting to support this standard.

4.13 What are solutions to minimizing WLAN security risk?

There are many options that organizations can do today to put proper security protection around their wireless strategy and technology.

4.13.1 Wireless Security Policy and Architecture Design

Many organization need to develop a wireless security policy to define what is and what is not allowed with wireless technology. From a holistic view, the wireless network should be designed with the proper architecture to minimize risk.

4.13.2 Basic Field Coverage

Because of wireless leakage, one of the first principals to basic field coverage is to only provide coverage for the areas that you want to have access .By using directional antennas and lowering the transmit power (on commercial class equipment - i.e., Cisco and Lucent), 85% (or higher) of the typical 802.11 signal leakage can be effectively eliminated.

4.13.3 Treat BaseStations as Untrusted

From an network security architecture, the base stations should be evaluated and determined if it should be treated as an untrusted device and need to be quarantined before the wireless clients can gain access to the internal network. The architecture design may include a Wireless DMZ. This WDMZ includes appropriately placing firewalls, VPNs, IDSes, vulnerability assessments, authentication requirements between access point and the Intranet.

4.13.4 Base Station Configuration Policy

The wireless policy may want to define the standard security settings for any 802.11 base station being deployed. It should cover security issues like the Server Set ID, WEP

keys and encryption, and SNMP community words. Turning off broadcast pings on the Access Point makes it invisible to 802.11b analysis tools like NetStumbler.

4.13.4.1 802.1X Security

Windows XP and many hardware vendors are building in 802.1X security standards into their Access Points. This provides a higher level of security than the typical WEP security. The 802.1x standard has a key management protocol built into its specification which provides keys automatically. Keys can also be changed rapidly at set intervals. Check to see if your Access Points support 802.1X.

There have been some security flaws noted by security researches in 802.1X standard. This points out the need for good VPN technology despite this new standard. Here is a document that outlines the issues in 802.1X security:

4.13.4.2 MAC Address Filtering

Some Access Points have the ability to filter only trusted MAC addresses. MAC addresses are suppose to be unique addresses on the network. This feature is usually very difficult to implement in a dynamic environment due to the tedious nature of trying to configure AP for each and every trusted client. The MAC address is transmitted in the clear text, so any intruder can sniff authorized MAC addresses, and with proper tools, configure and masquerade their MAC address as a legitimate MAC address and by-pass this security mechanism. Enabling this security feature can be more effort than the actual security benefit that it provides.

4.13.4.3 Base Station Discovery

- From a wired network search, an organization could identify unknown and rogue base stations by searching for SNMP agents. The rogue base stations are identified as 802.11 devices through SNMP queries for host id.

- Some base stations have a web and telnet interface. By looking at the banner strings of these interfaces, this provides another method of identifying some 802.11 devices.
- An additional means is by using unique TCP/IP attributes like a fingerprint, it can help identify devices as base stations. Most TCP/IP implementations have a unique set of characteristics and many OS fingerprinting technologies use this method for identifying the OS type. This concept can be applied to the base stations.
- From a wireless network search, an organization can identify these rogue base stations by simply setting up a 2.4 GHz sniffer that identifies 802.11 packets in the air. By looking at the packets, you may find the IP addresses to help identify which network they are on. In a densely populated area with many businesses close together, running a sniffer may pick up more the intended organization's traffic, but a close neighboring company.

4.13.4.3.1Honeypots - FakeAP

Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points. Hide in plain sight amongst Fake AP's cacophony of beacon frames. As part of a honeypot or as an instrument of your site security plan, Fake AP confuses Wardrivers, NetStumblers, Script Kiddies, and other undesirables.

4.14 Wireless Client Protection

The wireless clients should be assessed for having the following security technologies:

- firecell (distributed personal firewalls) - lock down who can gain access to the client.
- VPN - adds another layer of encryption and authentication beyond what 802.11 can provide.
- intrusion detection - identify and minimize attacks from intruders, worms, viruses, Trojans and backdoors.
- desktop scanning - identify security misconfigurations on the client.

4.15 Who is making 802.11 Security Solutions?

4.15.1 802.11 Gateway Infrastructure

- BlueSocket: The WG-1000 Wireless Gateway™ offers a single scalable solution to the security, quality of service (QoS) and management issues facing enterprises and service providers that deploy wireless LANs based on the IEEE 802.11b and Bluetooth™ standards.
- EcuTel: Viatores Secure WLAN edition is different from legacy virtual private networks (VPNs) in that it maintains VPN and application sessions uninterrupted with no configuration or re-boot required. Viatores combines two advanced protocols for mobility and security to enable roaming from LANs to WLANs and between WLAN subnets seamlessly and securely. Application sessions and security tunnels are maintained while the user moves from one subnet to another. Roaming users can communicate easily with colleagues, regardless of where they are or how they are connected, because Viatores maintains a single network address. Viatores Secure WLAN edition includes:
    - Industry-strength secure communication well beyond the WEP standard;
    - Seamless roaming from wired to wireless networks and between different wireless networks;
    - Support for two-way, peer-to-peer communication;
    - Data confidentiality and integrity, including key exchanges, digital signatures, and industry-strength encryption;
    - Option to upgrade to secure and seamless roaming from public networks.

CONCLUSION

WLANs allow greater flexibility and portability than do traditional wired local area networks (LAN). Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point device. An access point communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (approximately 100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network device. Access point cells can be linked together to allow users to even "roam" within a building or between buildings.

Wireless LAN is divided into five types, local area network(LAN), wide area network(WAN), metropolitan area network(MAN), campus area net work(CAN) and home area network(HAN). And there are two types of wireless network configuration ad-hoc mode and infrastructure mode

Wireless LAN security is a work in progress. The protocols are evolving to meet the needs of serious users. Until the protocols have proven themselves, the best course of action for network engineers is to assume that the link layer offers no security. Treat wireless stations as you would treat an unknown user asking for access to network resources over an un trusted network.

Polices and resources developed for remote dial-up users may be helpful because of the similarity between a wireless station and a dial-up client. Both are unknown users who must be authenticated before network access is granted, and the use of an un trusted network means that strong encryption (IPSec, SSL, or SSH) should be required. Although this cautious approach requires much more work than simply throwing up some access points, a conservative approach with several layers of defense is the best way to sleep at night. Wireless LAN has some problems like "Rogue" Access Points, MAC spoofing and session hijacking and higher level attaches there fore There are many options that organizations can do today to put proper security protection around their wireless strategy and technology.

REFERENCES

1) Tanebaum Andrew S., Computer Networks, 1996
2) Martin Michael J., Understanding the Network: A Practical Guide to
3) Internetworking, Macmillan Computer publishing, USA, 2000
4) Microsoft, Networking Essentials, Microsoft Corporation, Washington, 1996
5) Draft standard IEEE 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE, 1996
6) Wi-Fi is a registered trademark belonging to the Wi-Fi Alliance, a US-based trade association, and refers to the IEEE 802.11b standard, which is one of the most popular WLAN technologies.
7) See Jason Kane and David C. Yen, "Breaking the Barriers of Connectivity: an Analysis of the Wireless
8) LAN", http://gene.wins.uva.nl/~bcmndeur/6.pdf.
9) WLANA, High-Speed Wireless LAN Options: 802.11a and 802.11g,
10) http://www.wlana.org/pdf/highspeed.pdf.
11) Community network sites: Seattle Wireless (http://www.seattlewireless.net/), NYCwireless (http://www.nycwireless.com/)
13) NetStumbler home page: http://www.netstumbler.com