SIR C R REDDY COLLEGE OF ENGINEERING

Eluru-534007, ELURU Dist, Andhra Pradesh, India

(Approved by AICTE, New Delhi & Permanently affiliated to JNTUK, Kakinada)

Accredited by NBA

Telephone No: 08812-230840, 230565, Fax: 08812-224193

Website: www.sircrrengg.ac.in

WIRELESS NETWORK SECURITY (R204105J)

(Professional Elective-V**)**

Department of Computer Science and Engineering

IV B.Tech I Semester

R20 Regulation

Academic Year: 2024-2025

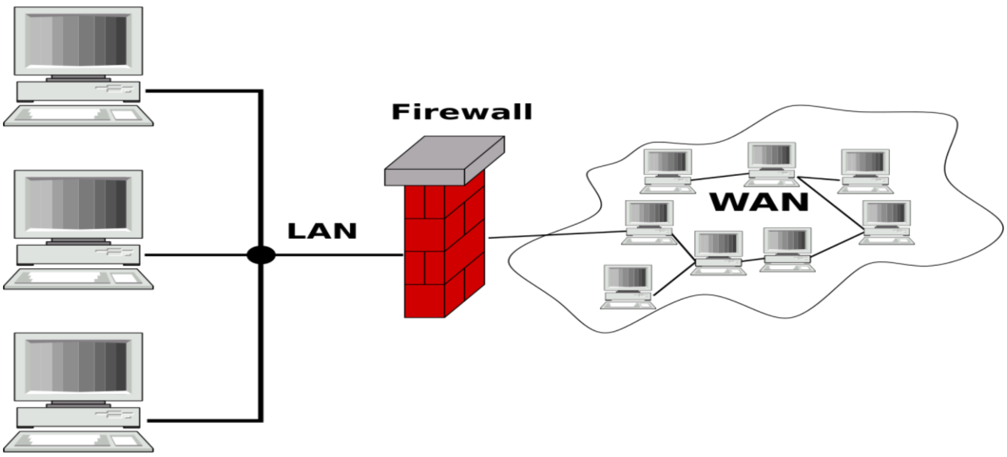
Prepared By: Dr. B. Madhav Rao

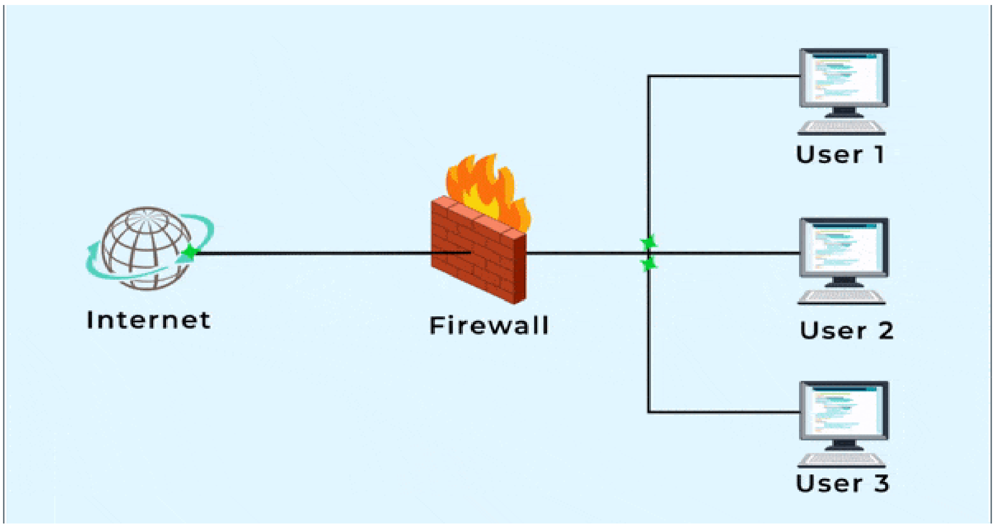
UNIT-I

Introduction to Wireless

Introduction

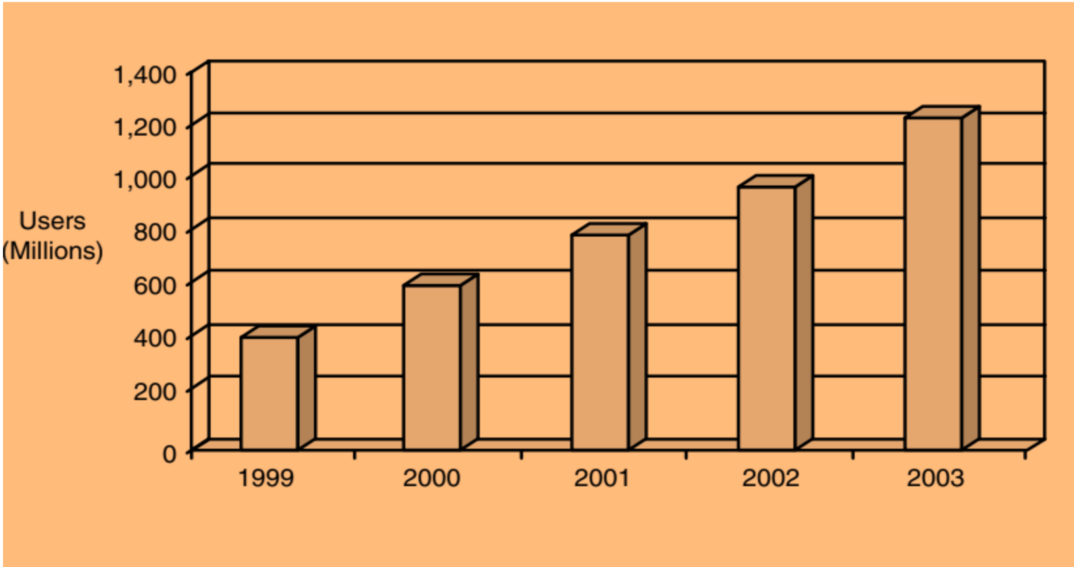
- Network is a group of two or more computers or other electronic devices that are interconnected for the purpose of exchanging data and sharing resources.
- A wireless network is a Computer Network that uses wireless data connections between network nodes.
- There are four main types of wireless networks:
    - WLAN
    - WMAN
    - WWAN
    - WPAN
- Network security is any activity designed to protect the usability and integrity of your network and data.
- Types of Network Security
    - Firewalls
    - Email Security
    - Web Security
    - Wireless Security
- Wireless network security is the process of designing, implementing and ensuring security on a wireless computer network.

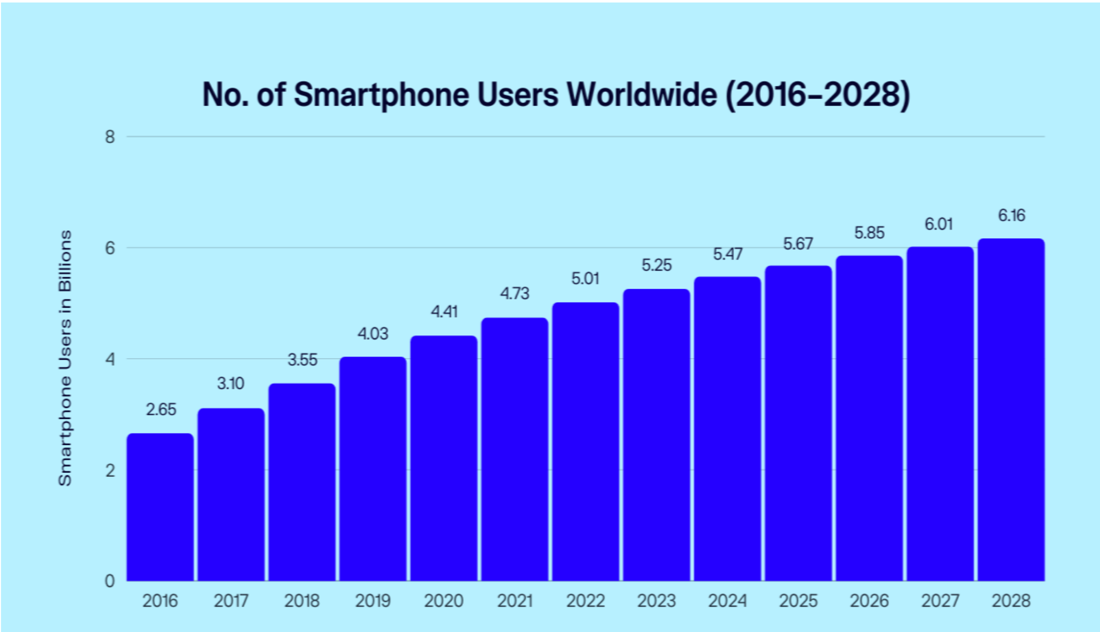




- Guglielmo Marconi transmitted the first wireless radio signal through the Italian hillside in 1894.
- Wireless technologies have transformed how people communicate and receive information.
- Wireless Technology include technologies such as
    - CDMA
    - TDMA
    - GSM
    - 4G
    - WAP
    - GPRS

Worldwide wireless phone users

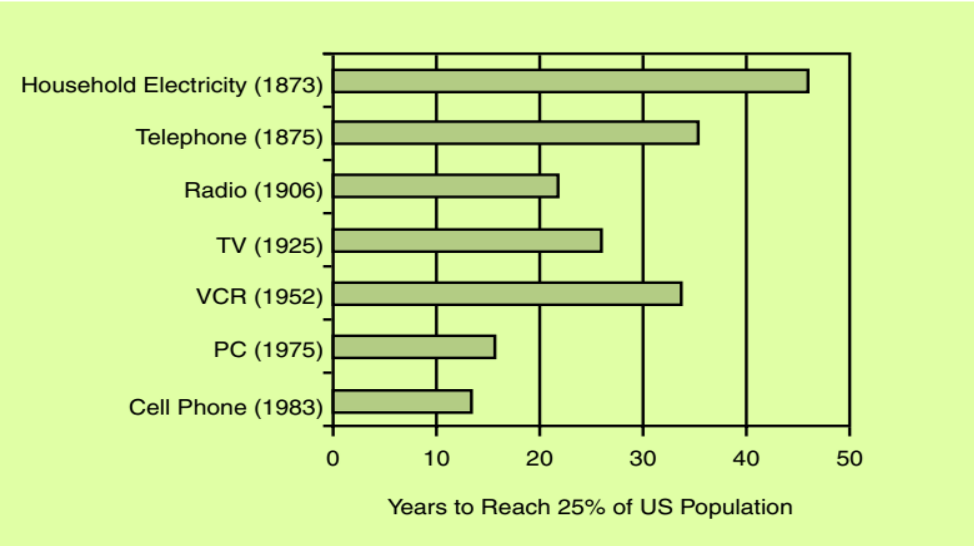




History of Wireless Technologies

- Wireless technology started in the late nineteenth century with the development of Marconi's wireless telegraphy.
- Marconi's technology could only send the dots and dashes of the Morse code.
- It was not capable of sending voice waves.
- Once Marconi's invention demonstrated wireless' potential, individuals and companies raced to develop technology to send voice waves through the air.
- Following Marconi's success, American inventor Reginald Fessenden completed the first true radio broadcast in 1906 and the wireless revolution commenced in earnest.
- By the 1920s, companies such as General Electric (GE), AT&T, and the newly created Radio Corporation of America (RCA) were aggressively creating the first real wireless industry: the AM radio.
- 1930s, as other new technologies such as frequency modulation (FM) radio and television were developed.

Comparative adoption of mass-market technologies



History of Wireless Technologies

- ✓ The 1970s—The First Wireless Networks
- ✓ The 1980s—Wireless Markets Start to Evolve
- ✓ The 1990s—Wireless Networks Mature
- ✓ The Mid-1990s—Other Wireless Networks Emerge
- ✓ The Late 1990s—The Wireless Internet Emerges

The 1970s—The First Wireless Networks

- The first wireless phone systems appeared in the United States in the 1970s.
- Based on technology developed at AT&T's Bell Labs in the late 1940s, these systems were analog, operated in a limited frequency range, and could only handle a low volume of simultaneous calls.
- Initial uses were in law enforcement and public safety.
- The first system of this type to be installed was AT&T's Advanced Mobile Phone Service (AMPS)(1G), which was deployed in Chicago in 1979.

The 1980s—Wireless Markets Start to Evolve

- The Federal Communications Commission (FCC) announced its intention to allocate 40 MHz of spectrum in the major metropolitan markets in the United States.
- This spectrum enabled 666 channels for cellular communication in each major metropolitan market.
- In Europe, the mobile phone market developed quite differently. In the early 1980s, European administrators were developing policies for a European wireless market.

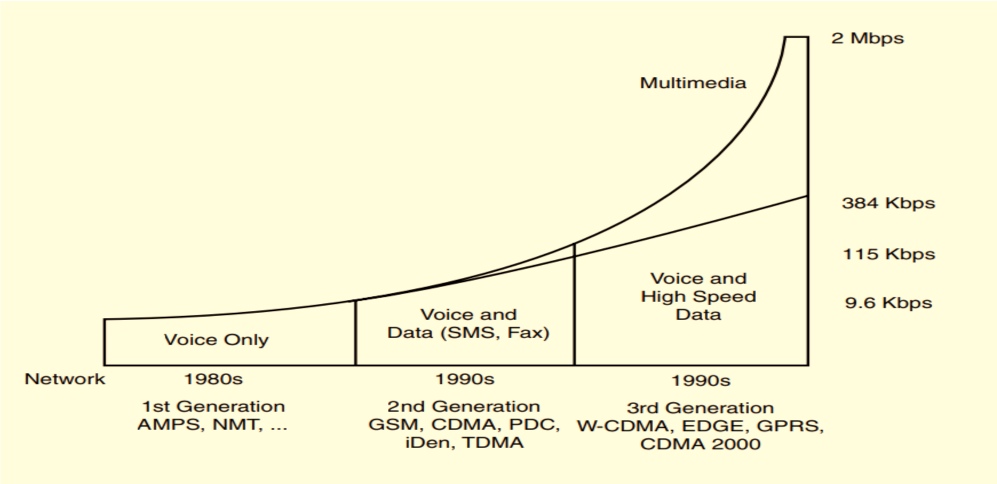
The 1980s—Wireless Markets Start to Evolve

- European telecommunications defined different policies than those of United States
    - State-owned telephone monopolies
    - Geography
    - Mobile population
- In 1982, the Conference of European Posts and Telecommunications Administrations (CEPT) which consisted of the telecommunications administrations of 26 nations.
- The CEPT made two important decisions.
- First, the CEPT decided to create a single European wireless technology standard and established a task force to define that standard.
- Second, the CEPT agreed to allocate wireless spectrum in the 900-MHz band in each country for use with this new wireless network.
- While the CEPT member nations worked on developing the GSM standard, individual nations like the United Kingdom, France, and Germany launched analog-based wireless systems.

The 1990s—Wireless Networks Mature

- During the 1990s, wireless technologies finally burst into the mainstream
- In 1991, the first commercial GSM networks began offering service, starting in Scandinavia.
- Australia became the first operator to offer GSM service outside Europe.
- GSM and the other network standards (TDMA, CDMA, and Personal Digital Communication [PDC]) are known as second-generation (2G) networks.

Networks illustration



Promotions and Discounts in the Polish GSM Market, October 1996 to March 1997

Date	Carrier	Promotion
September 1996	Era and Plus GSM	GSM services launched
October 1996	Plus GSM	601 free minutes with service activation
January 1997	Era GSM	Free Philips phone (valued at $320) with service activation
February 1997	Plus GSM	$100 off activation
February 1997	Era GSM	Phone and service activation for $200
March 1997	Plus GSM	Service activation for only $1

The Mid-1990s—Other Wireless Networks Emerge

- In 1992, the Baby Bells pooled resources to create a new packet-based wireless data network called Cellular Digital Packet Data (CDPD)
- The CDPD networks offered relatively high throughput (up to 19.2 Kbps) and were based on Transmission Control Protocol/Internet Protocol (TCP/IP), making compatibility with the Internet relatively straightforward.
- The wireless LAN standard started in 1990 when the Institute of Electrical and Electronics Engineers (IEEE) started the 802.11 committee to define a wireless LAN standard.

History of Wireless Security

- Ironically, developments in wireless technologies were accompanied by equivalent developments in tools to intercept those wireless signals.
- People flocked to Radio Shack to purchase basic radio scanners. These simple devices were capable of eavesdropping on cellular conversations at will.

Eavesdropping and Jamming

- The relative ease of intercepting transmissions with these devices even led some state governments to consider banning radio scanners and for mobile operators to begin testing encrypted voice and data.
- The eavesdropping fear consisted of two dimensions
- One dimension was that curious citizens could listen in on random conversations.
- The second and more sinister dimension was that government agencies such as the CIA and FBI could intercept conversations at will in the name of law enforcement or national security.
- The wireless networks are susceptible to the following possible breaches
    - Interception of law enforcement data on specialized mobile radio, private radio, or CDPD network.
    - Interception of credit card authorizations over wireless networks.

- Stealing of cellular airtime.
- Interception of e-mail messages on wireless Internet connections.
- Physical breach of security at unmanned base stations or other communications centers.

The Wireless Internet—Wireless Security Moves into the Mainstream

- In the wired Internet, security and privacy issues were important issues.
- Vendors like Netscape and Microsoft supported Secure Sockets Layer/Transport Layer Security.
- SSL/TLS encryption over Hypertext Transfer Protocol (HTTP) in web browsers and web servers.
- The WAP Forum provided an SSL-like alternative called Wireless Transport Layer Security (WTLS).
- The WAP approach required two protocols:
  - WTLS from the wireless handset to the WAP gateway
  - SSL from the WAP gateway to a web server on the Internet.
- During the protocol conversion from WTLS to SSL, data was unencrypted and reencrypted, leaving data temporarily in an unencrypted form.
- This so-called WAP Gap created a level of concern about wireless security that delayed consumer adoption.

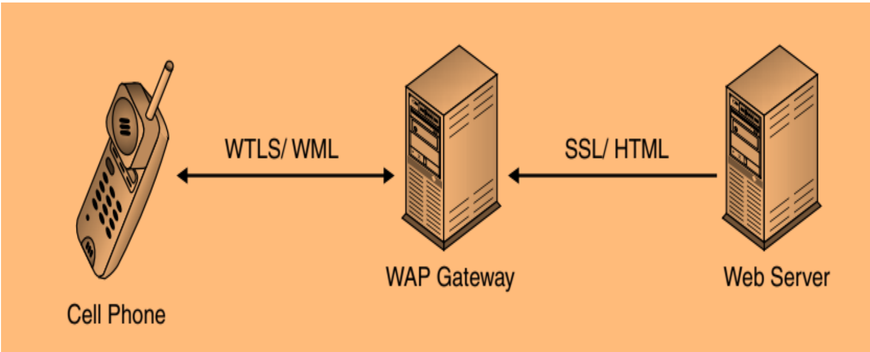


Illustration of WAP

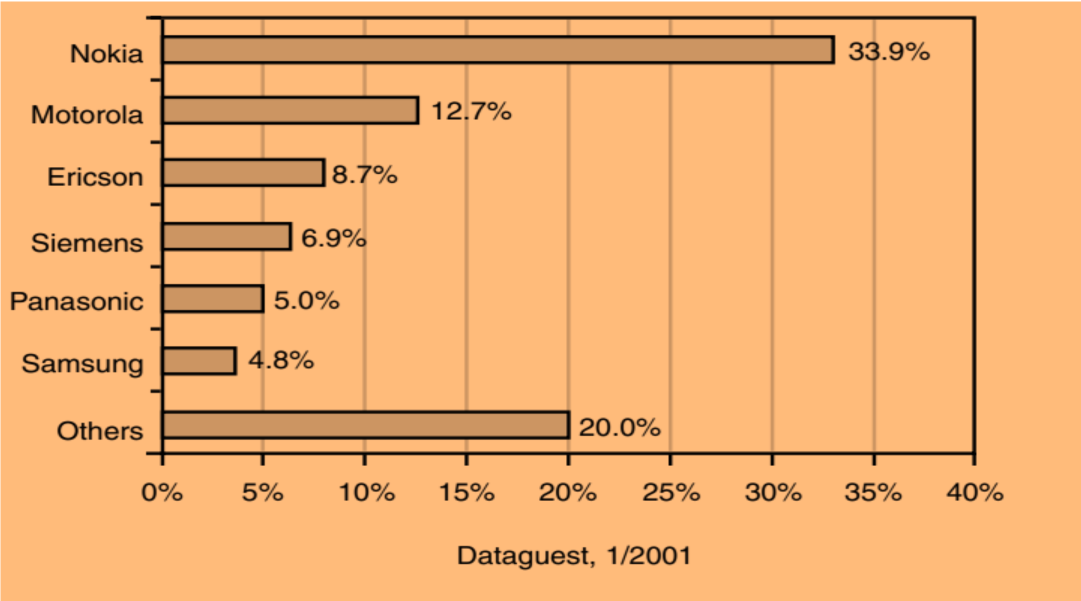
- WTLS was designed specifically because the low-bandwidth and hardware limitations of cellular handsets made implementing wireless SSL technically challenging.
- WAP Forum moved ahead with WTLS to get the wireless Internet off the ground.

Wireless Value Chain

	Wired	Wireless
Device vendors	Dell, Compaq, HP, Toshiba, NEC, IBM, and Apple	Nokia, Motorola, Ericsson, Siemens, Palm, Compaq, and Handspring
Network operators	AOL, AT&T, Prodigy, and Earthlink	Verizon, Vodafone, DoCoMo, and Sprint PCS
Hardware providers	Intel, Cisco, Lucent, Sun, IBM, and EMC	Texas Instruments, Ericsson, Alcatel, Siemens, and Cisco
Content providers	AOL, eBay, Amazon, Yahoo, and MSN	Yahoo, airlines, and Weather.com
Application providers	Microsoft, Oracle, SAP, Lotus, IBM, and BEA Systems	Openwave, iAnywhere, CellPoint, and Jinny

Device Vendors

- This sector is responsible for designing, manufacturing, selling, and marketing myriad wireless devices available to consumers worldwide.
- Voice oriented devices (namely cell phones) compose the vast majority of this category, but there are also wireless data devices from Compaq, Palm, Handspring, and Research in Motion.
- Once the operator purchases the handsets, the handset vendors need to generate demand on the consumer side, usually through advertising promotions highlighting the brand.



Worldwide wireless handset market share, 2000

Network Operators

- The network operators are responsible for building, maintaining, and promoting wireless networks.
- Many network operators (such as Verizon and British Telecom) began as wired operators and used that position to expand into wireless services.
- In the early days of wireless voice, there was little differentiation among network operators.
- Gradually, many markets opened the wireless sector to new entrants, creating more competition.

Operator	Markets Served	Subscribers as of 2001 (in millions)
Vodafone	United Kingdom, Germany, and Japan	96
China Mobile Telecom	China	89
T-Mobil	Germany	42
NTT DoCoMo	Japan	38
Verizon	United States	28
Telefonica	Spain and Latin America	25
Telecom Italia	Italy	22

Major Global Wireless Operators

Hardware Providers

- This sector is always invisible to consumers, but it is a critical supplier to the network operators and handset vendors
- This sector is getting increasing focus because of the migration to faster wireless network.
- These firms provide the hardware for the handset vendors as well as the network switching.

Content Providers

- This sector is responsible for generating and distributing information that can be served up on a wireless device.
- In the wireless world, to a large extent the operators determined what content subscribers could or could not view.
- If content provider X did not have a distribution agreement with network operator Y, network operator Y's subscribers could not view that content.
- Content providers suffer from the same WAP Gap issues facing the network operators.

Application Providers

- This sector is divided into two categories
  - Traditional independent software vendors (ISVs) that have modified existing wired applications for wireless environments.
  - Software vendors that have developed exclusively for wireless environments.
- In 2000, all the major software vendors including Oracle, IBM, Microsoft, and SAP announced plans to make existing applications wireless ready.
- The same year saw the emergence of certain wireless pure-play vendors like Phone.com (now called Open-wave), CellPoint, and Jinny Software.

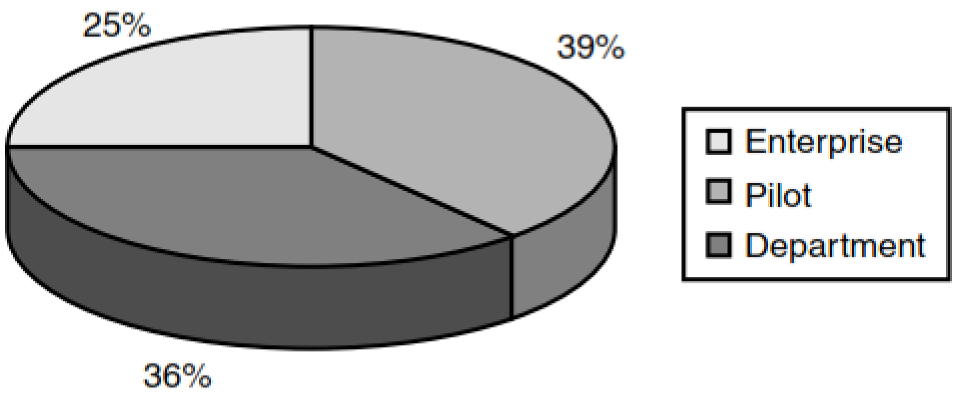
State of the Wireless Industry, 2001

- The overview is split into four geographic regions because the wireless market has evolved quite differently across the globe.

✓ North America
✓ Europe
✓ Japan
✓ Asia

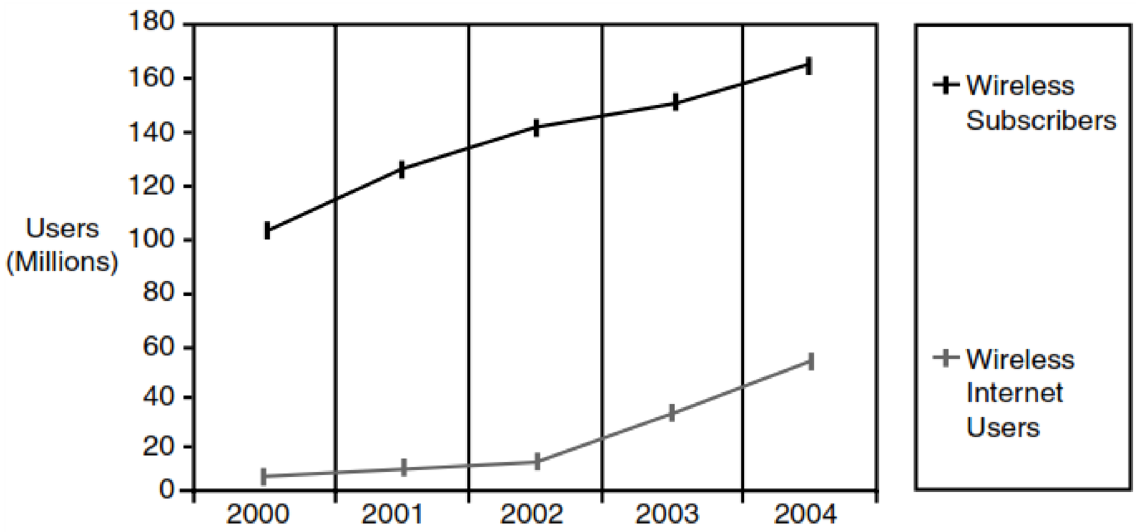
North American Wireless Industry, 2001

- During the early 1990's the NA wireless industry entered a more mature phase. The NA market is divided into 2 segments: Consumer & Enterprise.
- In 2000, enterprises were extremely attracted to wireless data as an important strategic tool that could address three areas.
    - Improved productivity
    - Improved customer service
    - Competitive advantage



InformationWeek survey of enterprise wireless deployments, 2000

Nonetheless, Jupiter Research's analysis shows dramatic growth in U.S. wireless Internet users. By 2005, 33 percent of all wireless subscribers will be using wireless data services.



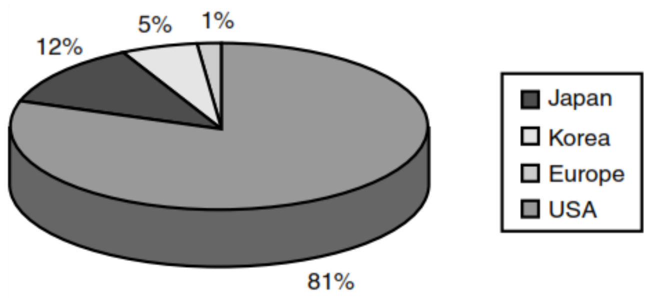
U.S. wireless Internet users, 2000 to 2004

European Wireless Industry, 2001

- European wireless technology have created a very robust and growing wireless market.
- Attitudes toward wireless technologies remained very optimistic in Europe during 2000 and 2001.
- The European wireless market is considerably larger than North America's wireless market. In 2001 European operators enjoyed several benefits over operators in other regions:
  - Stable universal network infrastructure
  - Relatively high cost of wired Internet access
  - Healthy non voice revenue stream
  - Protected incumbent carriers

Japanese Wireless Industry, 2001

- When it comes to wireless technology, Japan is in a class by itself.
- Although Japan chose to adopt their own wireless voice technology in the 1980s (PDC), the Japanese market exploded into the mainstream in the late 1990s.
- DoCoMo (Do is the Japanese word for everywhere) is a subsidiary of Japanese phone monopoly Nippon Telegraph and Telephone (NTT).
- DoCoMo started offering traditional wireless voice in 1992 and quickly became Japan's leading mobile operator with over 35 million subscribers.

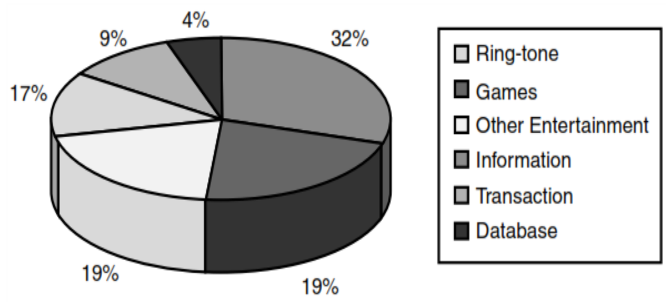


Eurotechnology, 12/00

- In August 1999, DoCoMo launched i-mode, a wireless Internet service.

Advantages

- Service was a packet-switching network, not circuit-based network ("based" meaning that the service was always on).
- It was compatible with existing cellular networks infrastructure - no additional investment was needed.
- Service did not require significant modifications to existing wired web content.



NIT DoCoMo, 12/00

i-mode content by category

Factors

- High cost of fixed Internet access
- Cultural
- Close collaboration with Japanese suppliers
- Dominant incumbent phone monopoly

Asian Wireless Industry, 2001

- Asia’s wireless industry varies from country to country. Macroeconomic conditions are closely linked to the relative state of each individual market.
- In countries with high standards of living like Singapore and Taiwan, wireless usage equals that of many Western European nations (above 50 percent).
- In countries like Indonesia and the Philippines, wireless subscribers are growing rapidly, but the technology is still out of reach financially for a large majority of the respective populations.
- The country that attracts the most attention as a future wireless market is China, 1.2 billion people, wireless vendors are very eager to participate in the Chinese market.
- China is already the second largest wireless market (after the United States, in terms of subscribers), yet only 10 percent of China’s population carries a cell phone.
- China chose GSM and plans to migrate to wideband CDMA (W-CDMA) for its 3G networks.

Metric	Value
Subscribers (as of Dec. 2000)	85,300,000
Cumulative capital investment	$60,000,000
Annual year-2000 cellular service revenue	$16,000,000

Chinese Wireless Market Metrics
(Courtesy of South China Post and Business Weekly)

Wireless Threats

Introduction

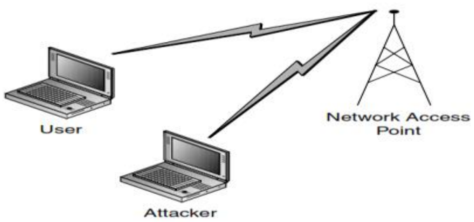
- A threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.
- The threats include computer viruses, data breaches, Injections and Modifications of Data, Denial of Service (DoS) attacks, Man-in-the-Middle (MITM) Attack and other attack vectors.

Uncontrolled Terrain

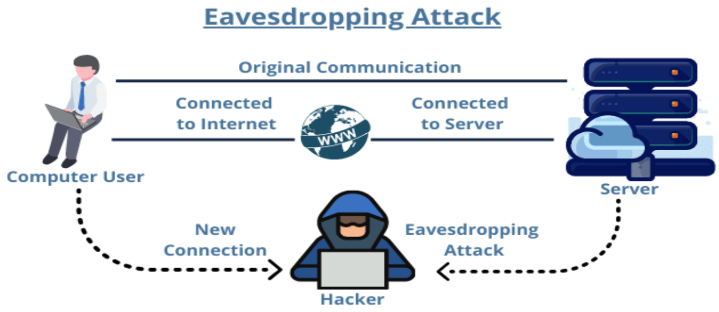
- The major difference between wired and wireless networks is the anonymous, uncontrolled coverage areas between the end points of the network.
- In wide area cellular networks, the wireless medium cannot be controlled at all.
- Current wireless networking technology offers little to control the coverage area.
- The number of attacks that are possible in wireless networks.
- The number of attacks that are not found in traditional wired networks.
- We will review the threats that are unique to wireless environments, the equipment required by the attacker to successfully leverage the threats.
- The problems that occur when roaming from one cell to another, the covert wireless channels, and the cryptographic pitfalls prone to open medium communications.

Eavesdropping

- An eavesdropping attack occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices.
- Eavesdropping, also known as sniffing or snooping, relies on unsecured network communications to access data in transit between devices.
- The most widely known problem with an open, uncontrolled medium like wireless technology is that it is susceptible to anonymous attackers.
- The anonymous attacker can passively intercept radio signals and decode the data being transmitted.
- The equipment used to perform eavesdropping on the network can be as simple as the equipment used to gain access to the network itself.
- This equipment is sometimes given away with mobile phone activation. At the time of this writing, wireless networking cards can be purchased for Under a hundred dollars.
- All wireless devices have the hardware required to send and receive on the wireless network.
- With little or no modification, the devices can be configured to capture all traffic on a particular network channel or frequency.



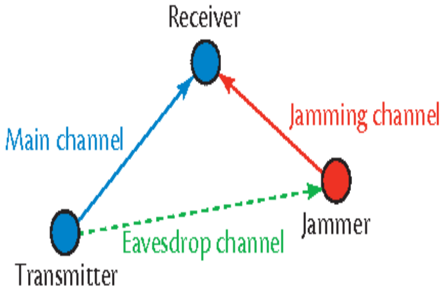
Wireless attacker eavesdropping on wireless communications

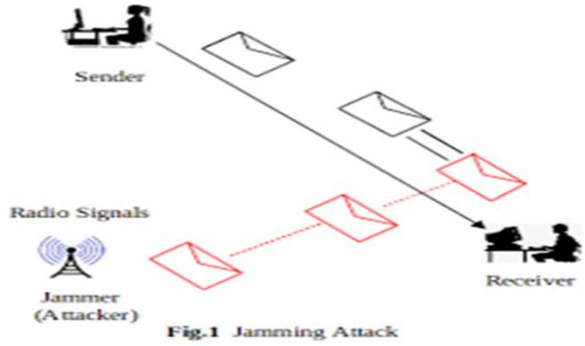


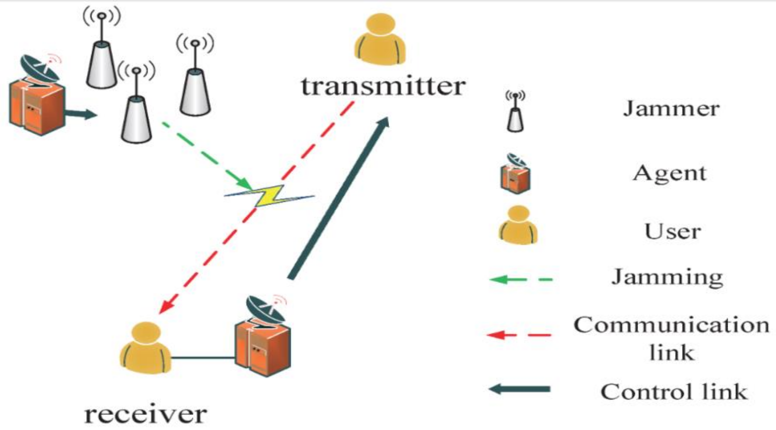
- The attacker must be in proximity to the transmitter in order to receive the transmission.
- These types of attacks are nearly impossible to detect and even harder to prevent.
- The use of antennas and amplifiers enables an attacker to be a considerable distance away from the target during an attack.
- Recent tests of 802.11 wireless networking equipment show that an attacker can be nearly 20 miles away from a target and still receive a signal, thereby eavesdropping on wireless network communications.
- Eavesdropping is used to gather information on the network under attack.
- The primary goals of the attacker are to understand
  - who uses the network
  - what is accessible
  - what the capabilities of the equipment on the network
  - when it is used least and most
  - what the coverage area
- This information is needed to launch an attack on the target network.
- Many commonly used network protocols transmit sensitive data such as username and password information in clear text.
- An attacker may use captured data to gain access to network resources.
- Even if communications are encrypted, an attacker is still presented with the ciphertext, which can be stored and analyzed at a later time.
- Many password encryption algorithms such as Microsoft NTLM can be easily broken.
- Active eavesdropping is possible when an attacker can connect to a wireless network.
- Active eavesdropping on a wireless local area network (LAN) normally involves Address Resolution Protocol (ARP) spoofing.
- This technique was originally designed to sniff a switched network. Essentially, this is a man-in-the-middle attack (MITM) at the data link layer.

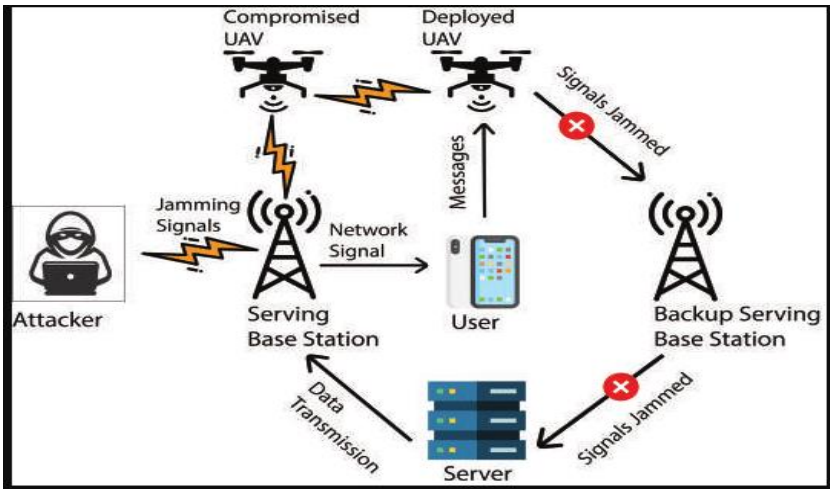
Communications Jamming

- Jamming in the sense of wireless security or wireless networks is defined as disruption of an existing wireless transmission or communication by decreasing the signal-to-noise ratio at receiver side through transmission of interfering wireless signals.
- Jamming occurs when an intentional or unintentional interference overpowers the sender or receiver of a communications link, thereby effectively rendering the communications link useless.



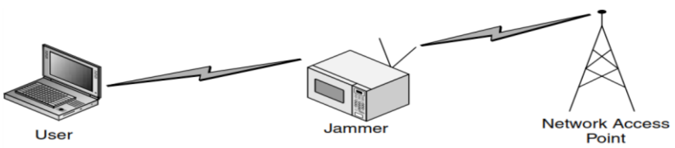






Denial of Service (DoS) Jamming

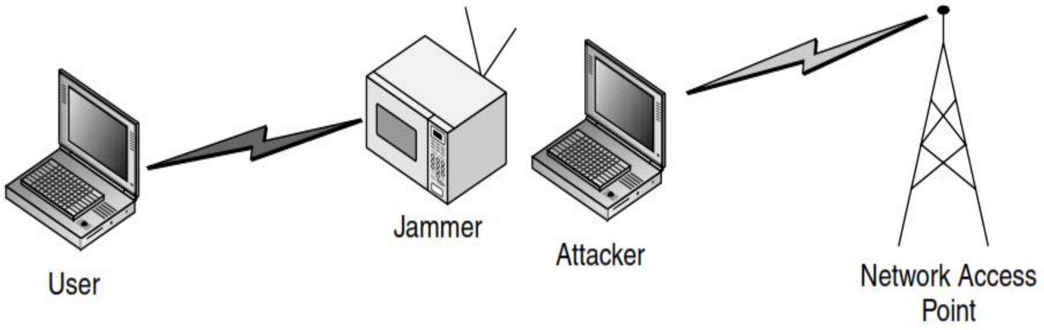
- A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.
- Jamming the entire network can cause a denial of service (DoS) attack.
- The entire area, including both base stations and clients, is flooded with interference so that no stations can communicate with each other.
- This attack shuts down all communications in a given area.



- This type of attack can require a significant amount of power if applied to a broad area.
- DoS attacks on wireless networks may be difficult to prevent and stop.
- Most wireless networking technologies use unlicensed frequencies and are subject to interference from a variety of different electronic devices.

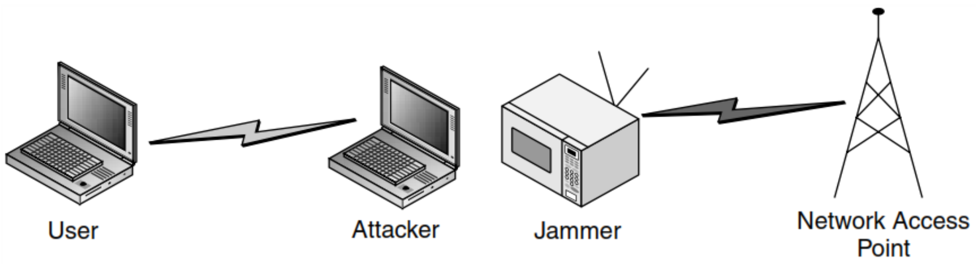
Client Jamming

- Jamming a client station provides an opportunity for a rogue client to take over or impersonate the jammed client.
- Jamming also can be used to DoS the client so that it loses connectivity and cannot access the application.
- A more sophisticated attack may attempt to interrupt connectivity with the real base station to then reattach with a rogue station.



Base Station Jamming

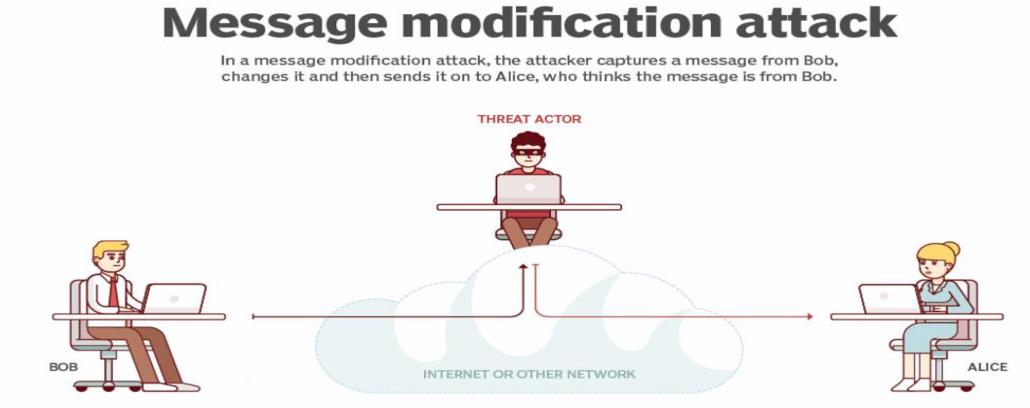
- Jamming a base station provides an opportunity for a rogue base station to stand in for the legitimate base station.
- The jamming can also deprive clients of service or a telecom company from revenue.
- Most of the wireless networking technologies utilize unlicensed frequencies. Therefore, many devices such as cordless phones, baby monitors, and microwave ovens may interfere with wireless networking and effectively jam the wireless communications.



- To prevent this kind of unintentional jamming, site surveys are recommended before spending significant money on wireless equipment.
- These surveys will help to verify that other devices will not interfere with communications and may prevent unneeded capital expenditure on useless equipment.

Injections and Modifications of Data

- Injection attacks occur when an attacker adds data to an existing connection in order to hijack the connection or maliciously send data or commands.
- An attacker can manipulate control messages and data streams by inserting packets or commands to a base station and vice versa.
- Inserting control messages on a valid control channel can result in the disconnection of users from the network.



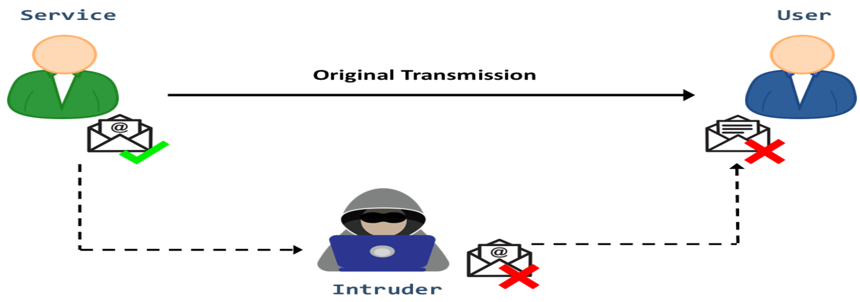
- Injection attacks can be used for DoS.
- An attacker can also flood the network access point with connect messages, tricking the network access point into exceeding a maximum limit, thereby denying authorized users access to the network.

Types of injection attacks

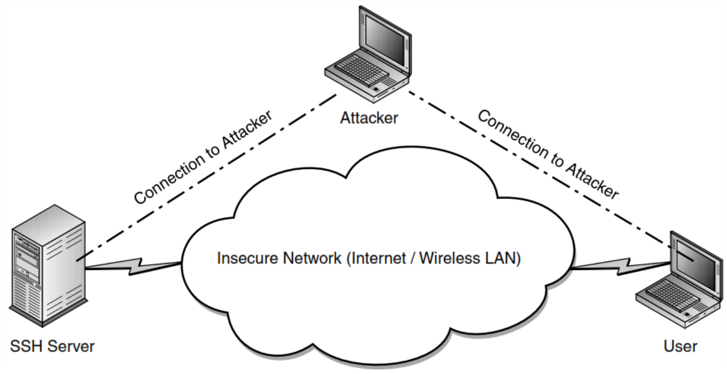
- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Code Injection
- Command Injection
- CCS(Change Cipher Spec) Injection
- CRLF Injection
- Mail Command Injection
- Host Header Injection

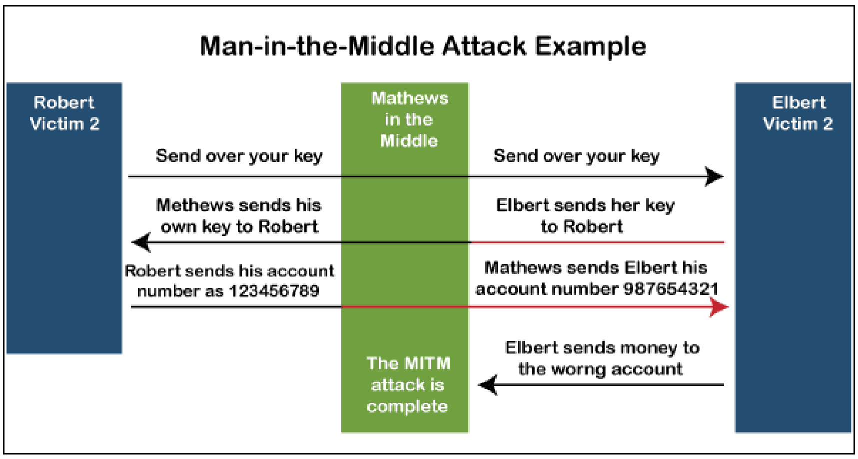
Man-in-the-Middle (MITM) Attack

- Similar to injection attacks are MITM attacks.
- MITM attacks can take many forms and are designed to subvert the confidentiality and integrity of the session.
- MITM attacks are more sophisticated than most attacks and require significant information about the network.
- An attacker will normally impersonate a network resource.



- When a victim initiates a connection, the attacker will intercept the connection, and then complete the connection to the intended resource and proxy all communications to the resource.
- The attacker is now in a position to inject data, modify communications, or eavesdrop on a session that would normally be difficult to decode, such as encrypted sessions.





Types of MITM Attack

- Wi-Fi Eavesdropping
- DNS Spoofing
- IP Spoofing
- HTTPS Spoofing
- ARP Spoofing
- E-mail Hacking
- Session Hacking
- SSL Stripping
- MITB attack

Preventions of Man-in-the-middle attack

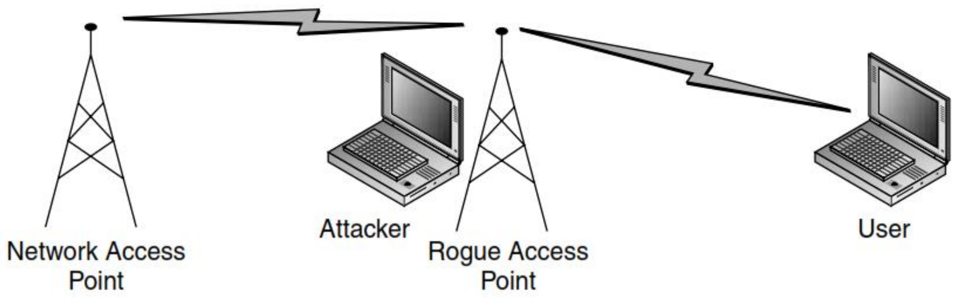
- Wireless access point (WAP) Encryption
- Use a Virtual Private Network (VPN)
- Public Key Pair Authentication
- Strong Network User Credentials
- Communication security
- Using proper hygiene for network protection on all platforms, such as smartphone apps.
- Avoid using public wi-fi

Rogue Client

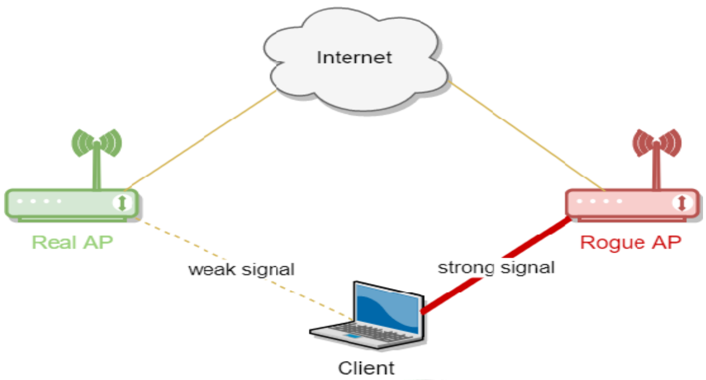
- After studying a client in the field, an attacker may choose to clone the client's identity and attempt to gain access to the network and advertised services.
- The attacker may also be so bold as to steal an access device to attempt to gain access to the network.
- Securing all wireless devices may be very difficult, for convenience and mobility dictate that most wireless devices are very small.
- A common wireless security mechanism was supposed to use layer 2 access controls to limit access to resources.
- This mechanism proved a failure when it was used by cellular phone companies to limit access to phone numbers by using an Electronic Serial Number (ESN).
- Then the failure was repeated by the 802.11 wireless LAN standard with Media Access Controls (MACs) that can be easily circumvented by a skilled attacker.

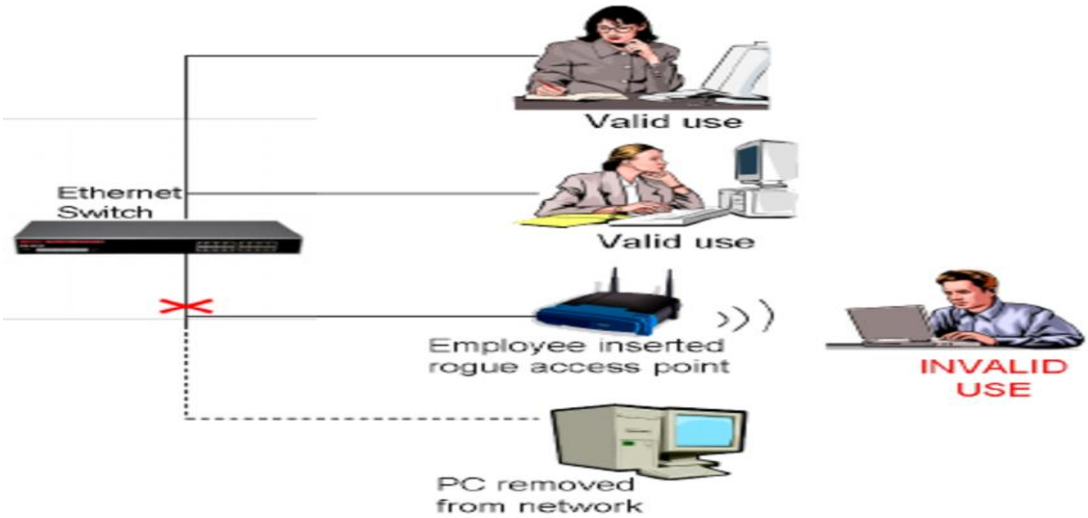
Rogue Network Access Points

- An attacker can set up a rouge access point to impersonate a network resource.
- Clients may unknowingly connect to this false access point and divulge sensitive credentials such as authentication credentials.
- This type of attack can be used in conjunction with directive jamming to block the ears of the legitimate network access point



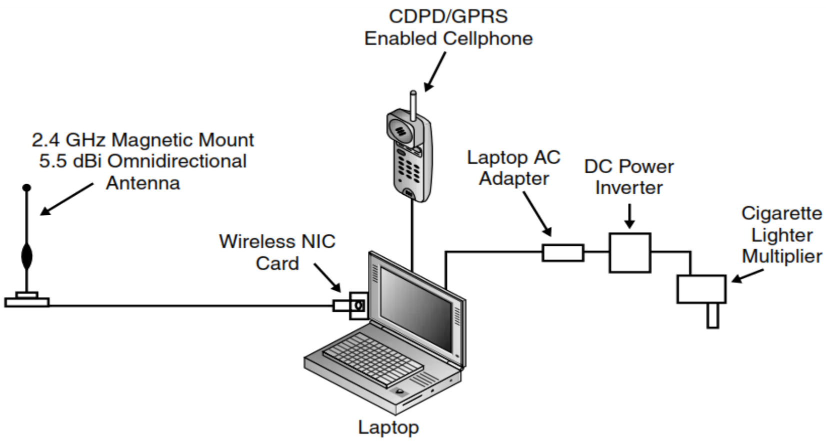
Rogue access point





Attacker Equipment

- The equipment used by the casual attacker can minimally consist of a wireless network interface.
- This can either be a wireless Ethernet Network Interface Card(NIC), a General Packet Radio Service (GPRS), or a Cellular Digital Packet Data (CDPD) cellular telephony handset connected to a laptop either as a Personal Computer Memory Card International Association (PCMCIA) card or through some communications link.
- Advanced attackers will sometimes employ this wireless interface in conjunction with jammers and specialized software.
- Cellular network attackers will generally use a configuration as depicted, because the network coverage is understood and generally covers a large area.

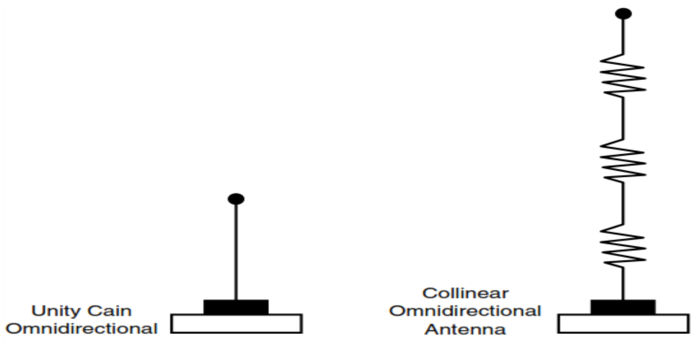


Attacker hardware configuration

- Wireless Ethernet networks generally cover a smaller area.
- Attackers will first detect the networks and determine the coverage area to find the best position to mount an attack.
- The preferred position is one that provides cover sometimes behind landscaping or in a different building and optionally an easy escape route.
- The basic network discovery setup consists of a laptop, a GPS unit, an antenna, an amplifier, and a wireless Ethernet NIC.
- In order to perform long-duration sweeps, extra power can be obtained by using an inverter for converting 12V DC into 120V AC to power the laptop or any other equipment one may be using (such as a jammer or a low-noise amplifier [LNA]).
- Some attackers have been known to remove dashboard cigarette lighters and replace with DC inverters to provide power for an extended period of time.
- Once the basic coverage is determined, the attacker, utilizing various antenna apparatus, determines the best link from which to mount attacks.
- Attackers will utilize various antenna types when mounting an attack, depending on the situation and the desired effect.
- Antenna types are generally characterized by the amount of gain or increase in received or transmitted signal strength and beam width.
- The beam width of an antenna indicates how electromagnetic radiation emanates.
- The three most common antenna types are the omnidirectional antenna, the yagi, and the parabolic.

Omnidirectional Antenna

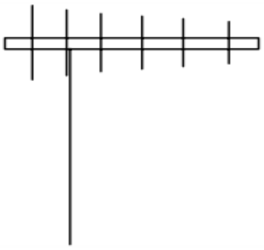
- The omnidirectional antenna has a beam width of 360 degrees and is usually deployed to survey or jam a wide area.
- Electromagnetic radiation is received from all sides and therefore, unless in an array, direction cannot be determined with a single station utilizing an omnidirectional antenna.
- Omnidirectional antennas also have little to no gain, unless they are assembled in a collinear array where gain can be as high as 8 dBi(Decibels relative to isotropic).



Common omnidirectional antenna

Yagi Anteena

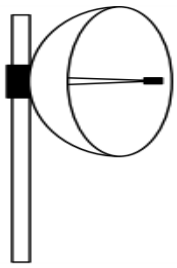
- The yagi antenna has special properties that focus the electromagnetic radiation from a driven element into a directed pattern.
- A yagi antenna, typically exhibits a beam width of 10 to 20 degrees and a gain of 10 to 18dBi.
- The yagi is usually deployed when one cannot gain direct access to the coverage area using an omnidirectional antenna.
- A yagi can also be used when the jamming of a particular device or group of devices sharing a geographical area is desired.
- Using a tripod designed for a camera or a telescope can prove effective for aiming a yagi in the field.



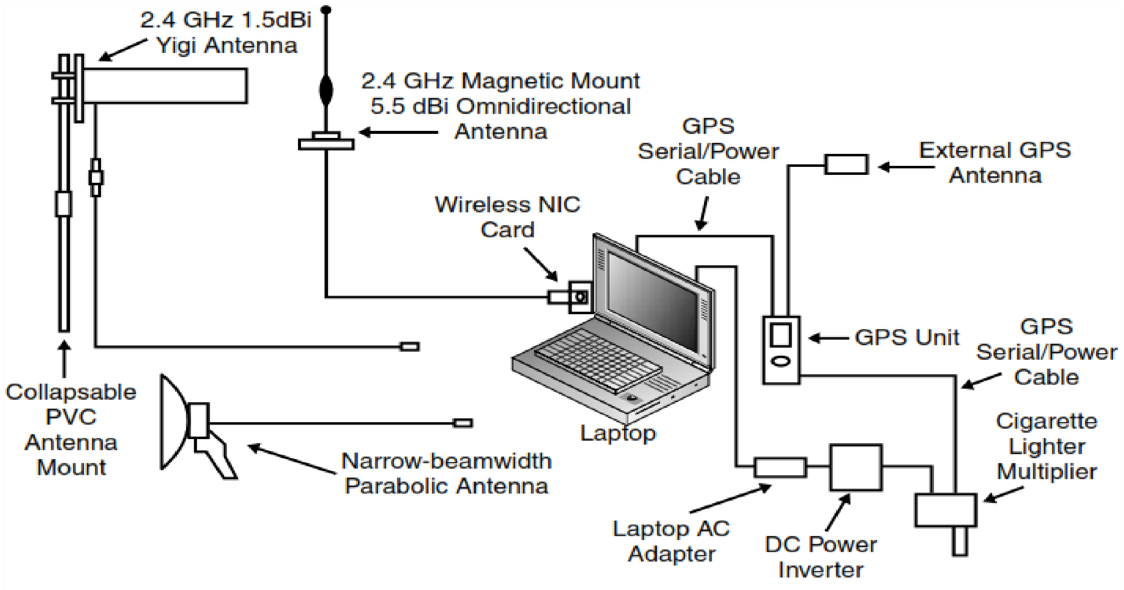
Yagi Anteena

Parabolic Anteena

- The parabolic antenna has the narrowest beam width of all, typically between 4 and 10 degrees and a gain of 20 to 30dBi.
- The parabolic antenna is generally deployed when concealment is of concern and great distances are to be covered.
- The parabolic antenna is difficult to use due to the narrow beam width, but this characteristic can be used to determine location.
- This antenna can also be used to support jamming functions as well as very precise attacks, perhaps to avoid detection systems.



- Survey software for collecting packet reception locations in a log file categorized by longitude and latitude is commonly used to discover the location and coverage of unknown wireless Ethernet networks.
- The longitude/latitude coordinates are supplied by a GPS device.
- Wireless coverage of a given area can then be clearly identified when plotted on a map.



Wireless assessment/war-driving hardware setup

- An antenna is by far the most useful tool for a network designer or an attacker, but an amplifier can also be used to boost reception over a long distance.
- Amplifiers will increase the signal as well as the noise, so getting a good quality amplifier is important.
- Using amplifiers may violate Federal Communications Commission (FCC) regulations, so great care needs to be taken.

UNIT-II

Introduction to Wireless Security Protocols and Cryptography

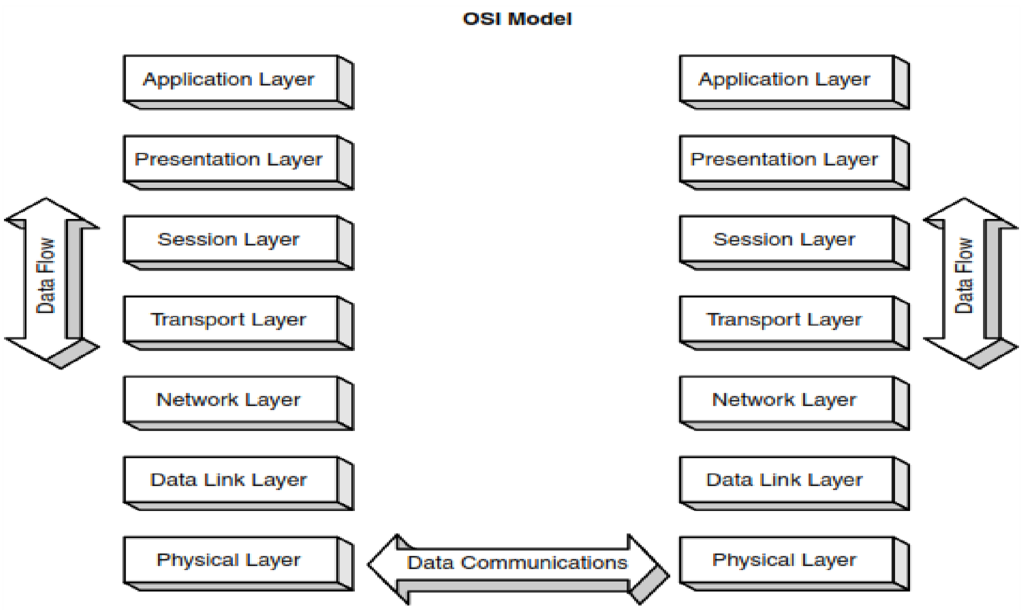
Removing the FUD

- FUD means Fear, Uncertainty and Doubt.
- With the commercial Internet reaching a decade of age, information security professionals and academics have devoted large amounts of time and resources tackling these problems.
- All we need to do is clearly identify the ways to mitigate threats, and this can be done by applying technology and applications that are already in use for other applications on the Internet and in the office.

OSI Model

- OSI stands for Open System Interconnection.
- OSI model is a set of protocols and rules by which communication between two network devices is made possible.
- The network device can be either of mobile device, tablet, laptop, PC, workstation or any other network device.
- OSI model was developed by ISO (International Standard organization).

Layers of OSI model



Application Layer

- The software applications send and receive data over the network.
- The application layer is the user's interface to network communications.
- Examples of application software are Chrome, Firefox, WhatsApp, Office365, Microsoft Edge etc.
- The application layer work on different protocols e.g., File transfer protocol (FTP), Hypertext transfer protocol (HTTP), Simple mail transfer protocol (SMTP), Post office protocol (POL), and Domain name system (DNS)

Presentation layer

- The data move from the application layer to the presentation layer.
- This layer negotiates syntax, so the applications communicating will be able to understand each other.
- The presentation layer encrypts the data so that the size of the data becomes small.
- The data is compressed and encoded in the presentation layer. On the receiver end, the presentation layer then decrypts, uncompressed and decode the data.

Session layer

- In the session layer, the sessions are created. All the data goes through checkpoints.
- This layer is responsible for coordinating communications between applications as well as tracking what data belongs to what data connection.
- Suppose the data link is disconnected then after reconnection the data is again sent through the session so that the previous session is restored and only remaining data is transferred.

Transport layer

- In the transport layer, the data received from the session layer are segmented and then transferred to the network layer.
- Portions of data in this layer are commonly called segments.
- The transport layer must match the connection speed of the sender and receiver.
- Suppose the computer receiving the data has slow connection speed so the transport layer also slows down the data transfer speed of sender.

Network layer

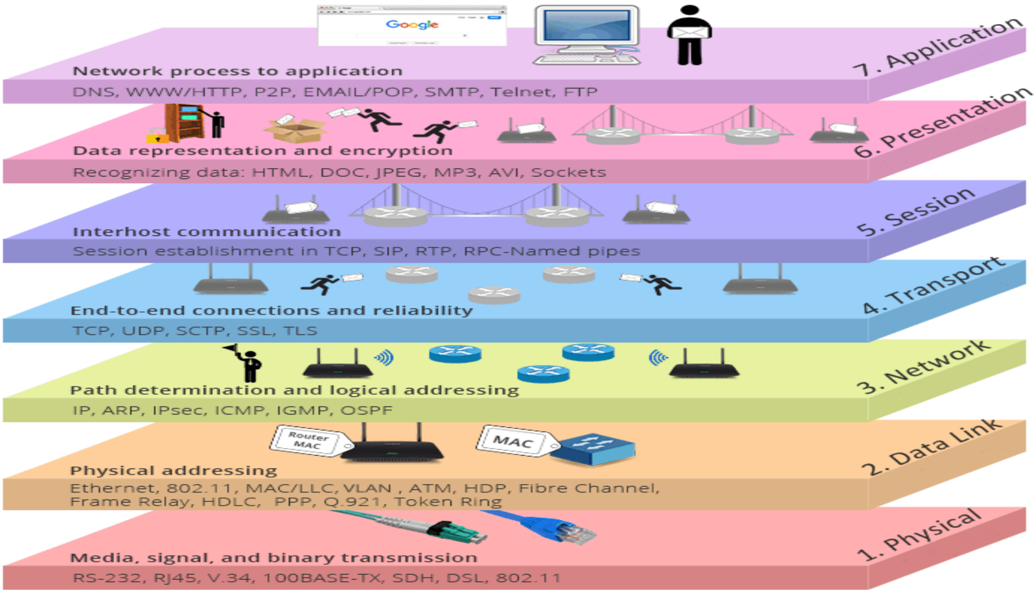
- In the network layer, the segments received from the transport layer are further divided into packets and then transferred to the data link layer.
- On this layer, routing and logical addressing are handled. Portions of data in this layer are commonly called packets.
- The shortest network path is also calculated in the network layer.
- The network layer also identifies the IP addresses of the receiver and sender to transfer data.

Data link layer

- The data link layer further divides the packets received from the network layer into frames.
- This layer also stores the MAC addresses of the sender and receiver.
- The mac addresses are used to identify the sender and receiver devices.
- The error checking of data and synchronization of data frames is also done in this layer.

Physical layer

- The physical layer is responsible for transferring data through physical devices such as wireless devices, cables and network connectors.
- The data frames received from the data link layer are further divided into 0 and 1 form i.e. in bits form then transferred to the physical layer of the receiver.
- The receiver device gets data through the physical layer and goes from the data link layer and all the layers up to the application layer.



OSI Simplified

- In many large enterprises, different groups handle different networking functions.
- For example, let us examine the organization of a large financial institution from the perspective of the customer service application.
- There is a telco group that handles network cabling.
- The desktop/server group is responsible for the network interface cards (NICs) in the end users' PCs and servers, as well as the hubs and switches.
- The network operations group is responsible for the routers in the network, assigning IP addressing, and operating the Domain Name System (DNS) on the network.
- The application development group handles the customer account program that runs over the network.
- The customer service representatives use the application and are responsible for inputting customer data.
- This particular organization maps to the OSI model rather well.

Mapping to the OSI Model

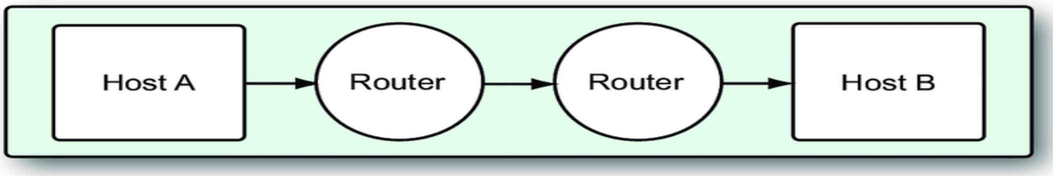
Application	Customer Service
Presentation	Application development
Session	Application development
Transport	Network operations
Network	Network operations
Data link	Desktop/server
Physical	Telco

- This organization may seem overly complicated and you may think that troubleshooting the application can be difficult, but this organization actually makes troubleshooting easier.
- Pulling wires through a drop ceiling and debugging code are two very different disciplines.
- The separation of duties enables each group to become domain experts in their area of responsibility.
- Therefore, when groups are well coordinated, the specialized experienced groups solve problems faster.

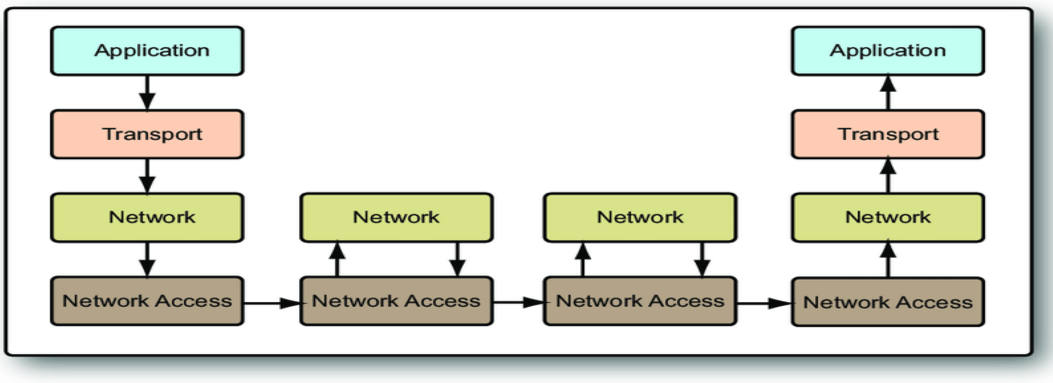
Internet Model

- Internet model is also referred to as the Transmission Control Protocol/Internet Protocol (TCP/IP) model.
- The TCP/IP model is a conceptual framework for how data is transmitted over computer networks.
- Internet Model or TCP/IP Model consists of four layers:
    - Application layer
    - Transport layer
    - Internet layer
    - Network Access layer
- Each layer plays a specific role in the transmission process.

Network Connections View



TCP/IP Model



Application Layer

- The application layer is a combination of the application, presentation, and session layers.
- This layer is responsible for interaction between the user and the application.
- Here, data is formatted, converted, encrypted, decrypted, and set to the user.
- Protocols used by the application layer are: HTTP, SMTP, FTP, DNS, TELNET.

- HTTP->Hypertext transfer protocol allows the users to interact with the World Wide Web through browser applications.
- SMTP->Simple mail transfer protocol is used to send mails.
- FTP->File transfer protocol is used for transmitting files from one system to another.
- DNS->Domain name system is the phonebook of the internet.
- TELNET->Teletype network acts as a client-server protocol. It is used to provide bidirectional connection.

Transport Layer

- The transport layer is responsible for end-to-end communication and provides error-free delivery of data.
- This layer can transport the data through a connection-oriented or connectionless layer.
- The two protocols used in the transport layer are user datagram protocol (UDP) and TCP.

UDP

- This protocol provides connectionless service and end-to-end delivery of transmission.
- It is considered an unstable protocol because it discovers the errors but does not specify them.

TCP

- It provides all transport services to the application layer.
- TCP is a dependable protocol for error detection and retransmission.
- It assures that all segments must be received and recognized before completing the transmission and discarding the virtual circuit.

Network Layer

- The network layer provides host addressing and chooses the best path to the destination network.
- This layer maintains the quality of service and offers connectionless end-to-end networking.
- The protocols in the network layer are: IPV4, ICMPV4, IGMP
- IPV4-> Internet protocol version 4 is employed for packetizing, forwarding, and delivery of packets. IP is an unreliable datagram protocol.
- ICMPV4->Interrupt control message protocol controls all errors. These mistakes are handled by ICMP protocol during the delivery of the message to target problems.
- IGMP->Internet group management protocol helps in multicasting

Network Access layer

- This layer is responsible for transmitting data over physical networks.
- It includes protocols like Ethernet, Wi-Fi, and Bluetooth, which define how data is transmitted over physical media.
- This layer interacts directly with the physical network hardware, such as network interface cards (NICs) and switches.

Equivalent Layers in the OSI and Internet Models

OSI Model	Internet Model
Application layer Presentation layer Session layer	Application layer
Transport layer	Transport layer
Network layer	Internet layer
Data link layer Physical layer	Network interface layer

Wireless LAN Security Protocols

- Wireless Local Area Network (LAN) security protocols are essential to ensure the confidentiality, integrity, and availability of data transmitted over wireless networks.
- These protocols help protect against unauthorized access, data interception, and other security threats.
- Here are some commonly used wireless LAN security protocols: WEP, WPA, WPA2, WPA3.

WEP (Wired Equivalent Privacy)

- WEP was one of the earliest wireless LAN security protocols but is now considered highly insecure.
- It uses a static encryption key for data protection.
- However, due to vulnerabilities in its encryption algorithm and weak key management, WEP can be easily cracked, allowing attackers to gain unauthorized access.

WPA (Wi-Fi Protected Access)

- WPA was introduced as a replacement for WEP to address its security flaws.
- WPA employs stronger encryption mechanisms and key management than WEP.
- There are two versions of WPA: WPA-Personal (WPA-PSK) and WPA-Enterprise.
- WPA-PSK uses a pre-shared key (password) for authentication, while WPA-Enterprise employs a centralized authentication server, such as RADIUS.

WPA2 (Wi-Fi Protected Access II)

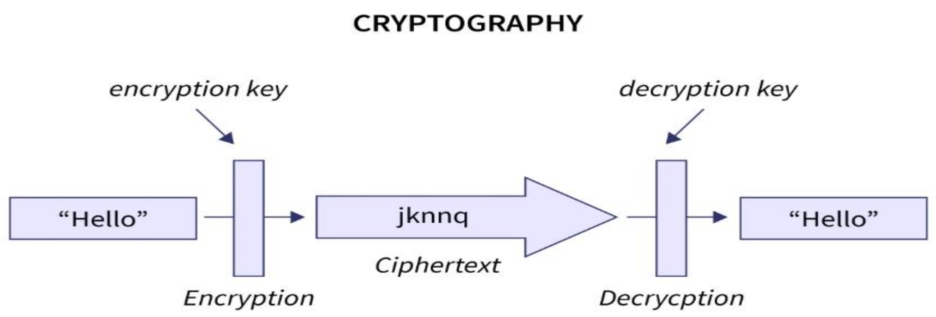
- WPA2 is an improved version of WPA and is widely used for securing wireless networks.
- It provides stronger encryption and security mechanisms, using the Advanced Encryption Standard (AES) for data encryption.
- WPA2-PSK and WPA2-Enterprise are the two main variants, similar to their WPA counterparts.

WPA3 (Wi-Fi Protected Access III)

- WPA3 is the latest iteration of Wi-Fi security, introduced to address vulnerabilities found in WPA2.
- It offers enhanced security features, including protection against brute-force attacks on weak passwords.
- WPA3 also improves security for open networks and introduces a more secure way of connecting Internet of Things (IoT) devices.
- When choosing a wireless LAN security protocol, it's crucial to select the most up-to-date and secure option available.
- WPA3 and WPA2-Enterprise are currently recommended due to their improved security mechanisms.
- Additionally, strong password practices and regular updates to network equipment are important for maintaining the security of your wireless LAN.

Cryptography

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.



Modern cryptography concerns itself with the following four objectives

- Authentication
- Confidentiality
- Non-repudiation
- Integrity

Authentication

The sender and receiver can confirm each other's identity and the origin/destination of the information.

Confidentiality

The information cannot be understood by anyone for whom it was unintended.

Non-repudiation

The creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information.

Integrity

The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

Types of Cryptography

There are three types of cryptography

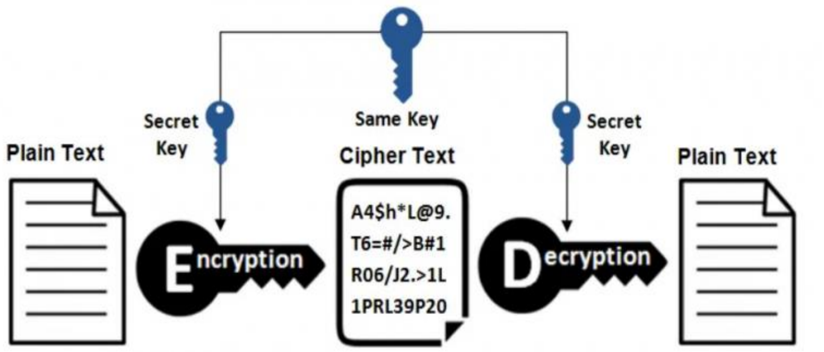
- Symmetric key cryptography
- Asymmetric key cryptography
- Hash Function

Symmetric key cryptography

- It is also known as secret-key cryptography, and in this type of cryptography, you can use only a single key.
- The sender and the receiver can use that single key to encrypt and decrypt a message.
- Advanced Encryption Standard (AES), Data Encryption Standard (DES) and DES3 are the examples of symmetric key cryptography

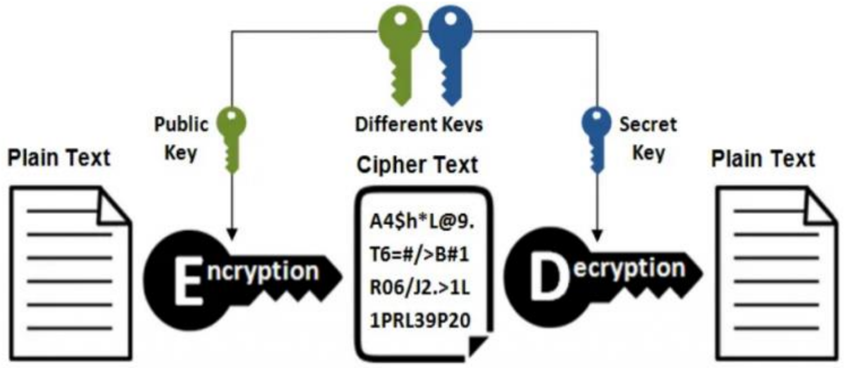
Disadvantage

The two parties must exchange the key in a secure manner.



Asymmetric Key Cryptography

- It is also known as public-key cryptography, and it employs the use of two keys.
- This cryptography differs from and is more secure than symmetric key cryptography.
- In this system, each user encrypts and decrypts using two keys or a pair of keys (private key and public key).
- Each user keeps the private key secret and the public key is distributed across the network so that anyone can use those public keys to send a message to any other user.
- You can use any of those keys to encrypt the message and can use the remaining key for decryption.
- An RSA algorithm, Digital Signature Algorithm (DSA) and Diffie-Hellman key exchange are the examples of asymmetric key cryptography.



Hash Function

- This algorithm makes no use of any keys.
- A hash value with a fixed length is calculated based on the plain text, making it impossible to recover the plain text's contents.
- Many operating systems encrypt passwords using hash functions.

Secure Sockets Layer/Transport Layer Security (SSL/TLS)

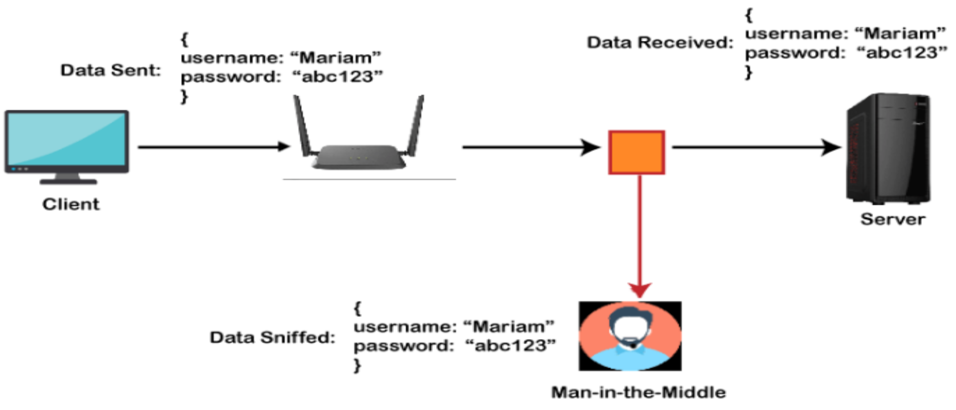
- Secure Sockets Layer (SSL) was originally designed to solve the security problems with web browsers.
- Netscape was the first browser to offer SSL and made the Web safe for commercial transactions and a secure channel could be provided for transmission of data.
- SSL is transparent, which means that the data arrives at the destination unchanged by the encryption/decryption process. Therefore, SSL can be used for many applications.
- SSL and its successor, Transport Layer Security (TLS), are the most widely implemented security protocols on the Internet.
- Originally implemented by Netscape in 1994, SSL/TLS is implemented in nearly every browser and most e-mail clients.
- SSL/TLS has been the basis for other security protocols including Microsoft's Private Communications Technology (PCT), Secure Transport Layer Protocol (STLP), and Wireless Transport Layer Security (WTLS).
- SSL/TLS's primary application is for web traffic or the Hypertext
- Transfer Protocol (HTTP). The process is very basic.
- In normal HTTP communications, a TCP connection is made, a request is sent for a document, and the document is sent.
- With an SSL/TLS HTTP connection, the TCP connection is established, an SSL/TLS connection is established, and then the HTTP connection proceeds over the SSL/TLS connection.
- Two things to note —SSL/TLS relies on TCP for the connection and the addition of the SSL/TLS connection does not change the HTTP communication.
- To prevent confusing standard HTTP servers, HTTP over SSL/TLS is typically implemented over a different TCP port (443) than standard HTTP (80).
- Many of the applications that use SSL/TLS use different ports than the non-SSL/TLS standard protocol.
- SSL/TLS is used to authenticate and encrypt a connection. This is accomplished by using a combination of different technologies that are based on **symmetric and asymmetric algorithms.**
- SSL/TLS has the capability to authenticate the server and client, but in most cases, only server authentication is actually performed.
- The authentication is accomplished by using public-key cryptography and is referred to as a handshake.
- The actual communications using SSL/TLS use a symmetrical encryption algorithm.
- SSL/TLS can be used to secure many varieties of network communications.
- The most common implementations are based on known TCP communication, such as e-mail, news, telnet, and the File Transfer Protocol (FTP). In many cases, different TCP ports are used for the SSL/TLS secured communications.

Secure Shell

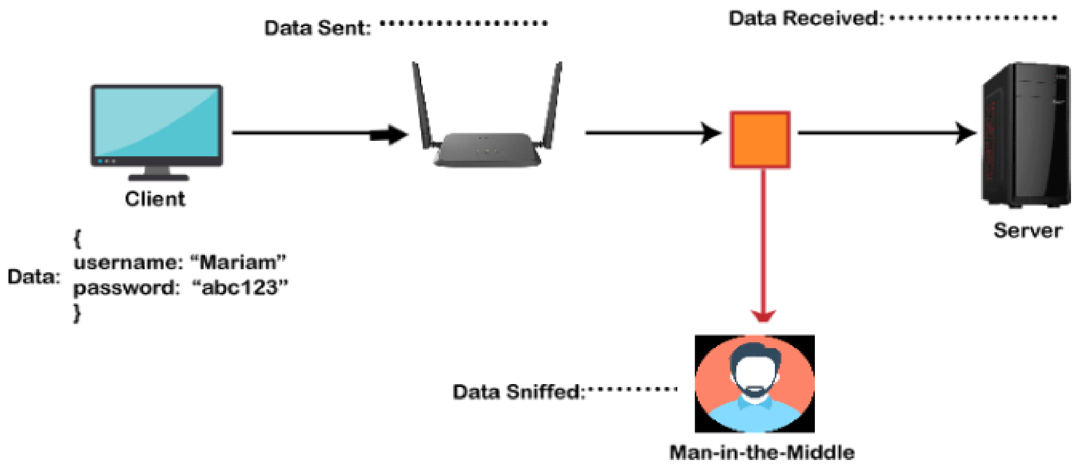
- SSH stands for Secure Shell or Secure Socket Shell.
- SSH was created out of a necessity for secure communication when the only protocols being used were unsecured protocols.
- SSH was originally designed to replace some Unix programs such as telnet, FTP, remote login (rlogin), rshell remote shell (rshell), and remote copy (rcp).
- Besides replacing these programs, SSH can be used to secure otherwise insecure programs over a network.
- Due to its flexibility and ease of use, SSH is a highly used security protocol and comes with the standard installation of many operating systems.
- SSH uses a public-key exchange to secure the initial connection and negotiates a symmetric key for the data transfer during the session.
- SSH can also easily be configured to authenticate both the server as well as the client.

Secure Shell Protocol

- The SSH protocol was developed by SSH communication security Ltd to safely communicate with the remote machine.
- Secure communication provides a strong password authentication and encrypted communication with a public key over an insecure channel.
- The most common implementation of the SSH protocol is the Unix ssh program.
- There are multiple SSH programs available: commercial ssh, Open SSH, putty for Windows platforms, and F-Secure ssh.
- Each of these programs is interoperable with each other, but have their own unique features and configuration options.
- Some of these programs are open source and some are distributed for free.
- You will need to examine the features and support options to determine which program will be appropriate for your application.
- It is used to replace unprotected remote login protocols such as Telnet, rlogin, rsh, etc., and insecure file transfer protocol FTP.
- Its security features are widely used by network administrators for managing systems and applications remotely.
- The SSH protocol protects the network from various attacks such as DNS spoofing, IP source routing, and IP spoofing.



Before SSH



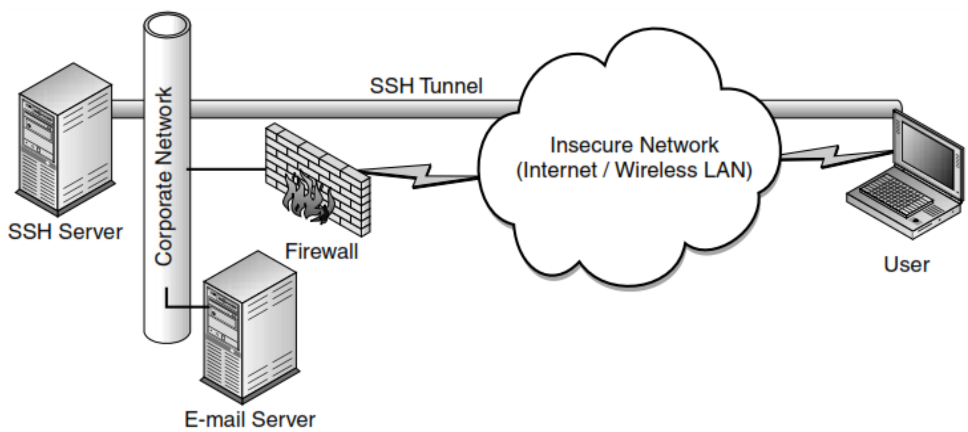
After SSH

Terminal Access and File Transfer

- The most common use of SSH is for replacing telnet. Telnet is a common application used to manage network hosts.
- Telnet sessions can be easily sniffed (revealing sensitive data), hijacked, or data can be injected.
- If properly implemented, SSH eliminates these security concerns. If you are still using telnet for anything, please replace it with SSH immediately.

Port Forwarding

- Some manufacturers are not supporting SSH as a telnet or FTP replacement.
- In these situations SSH can be used to secure otherwise insecure applications such as telnet, FTP, the Post Office Protocol (POP), or even HTTP.
- This can be accomplished by using the port-forwarding feature of SSH.
- Many device and operating manufacturers are starting to include support for SSH.
- Most file transfer protocols such as FTP, the Trivial File Transfer Protocol (TFTP), and the Common Internet File System (CIFS) are very insecure. These protocols suffer from the same sniffing, injection, and hijacking attacks.
- SSH includes the capability to transfer files over an encrypted authenticated session.



SSH Tunnel

- The firewall is configured to only allow traffic from the insecure network to the SSH server.
- No traffic will be allowed to or from the e-mail server to the insecure network.
- In addition to using SSH for terminal access to the SSH server, port forwarding can be used to tunnel e-mail traffic over the insecure network to the SSH server.
- Then the SSH server forwards the packets to the e-mail server.
- From the e-mail server's perspective, the traffic would be coming from the SSH server and packets would be returned to the SSH server for tunneling back to the user.
- E-mail is just one example of the many TCP protocols that can be tunneled over SSH.
- Other common applications for SSH include securing file transfers (Network File System [NFS], FTP and CIFS), web applications (HTTP), and thin client applications (MS Terminal Server and XWindows).

A Word of Caution

- Due to the flexibility and ubiquitous access that SSH enables, great care must be taken when implementing SSH.
- SSH is a tool that is commonly used by attackers.
- In our port forwarding example, we explained how SSH can be used to bypass firewall rules for accessing e-mail or other applications.
- This may be used by legitimate users or by malicious attackers.
- Therefore, make sure that SSH servers and clients are adequately secured and do not forget to secure applications behind the firewall.

Man-in-the-Middle (MITM) of SSL/TLS and SSH

- Some implementations of SSL/TLS and SSH may also be vulnerable to man-in-the-middle (MITM) attacks.
- Both SSL/TLS and SSH use a public key algorithm for establishing symmetric keys for the data transfer.
- A malicious attacker could intercept the handshake and replace the public keys exchanged with counterfeit keys. The attacker would then be able to attack the SSL/TLS or SSH session.
- Implementing a Public Key Infrastructure (PKI) or holding key-signing parties are ways to prevent this type of attack.
- PKI uses complex mathematical algorithms to verify the authenticity of a key by checking it against information from a certificate authority (CA).
- Key-signing parties eliminate the need for a CA, but require all parties that would communicate to meet together and personally exchange keys.
- The error messages in many applications displayed during an SSL/TLS or SSH MITM attack may go unnoticed by users.

WTLS(Wireless Transport Layer Security)

- WTLS is based on SSL/TLS. WTLS is used by Wireless Application Protocol (WAP) devices such as mobile phone handsets and personal digital assistants (PDAs).
- The primary difference between SSL and WTLS is the transport layer. SSL relies on TCP for reliability functions, such as the retransmission of lost packets and out-of-order packets.

- The WAP devices using WTLS cannot use TCP for these functions because WAP devices only use the User Datagram Protocol (UDP).
- UDP is not a connection oriented protocol, so these functions have been included in WTLS.

Three classes can be negotiated during the handshake process

  - WTLS class 1 □ No certificates
  - WTLS class 2 □ Server certificate only
  - WTLS class 3 □ Client and server certificates

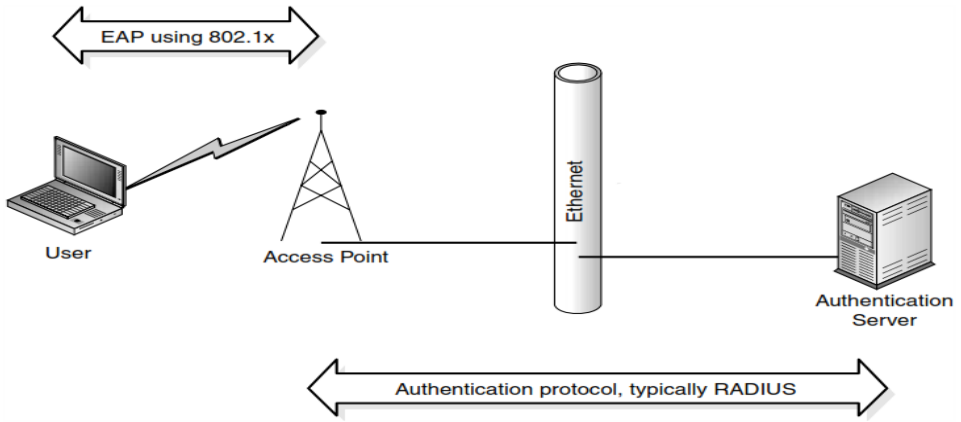
- In class 1, no authentication takes place and the protocol is simply used to set up an encrypted channel.
- In class 2, the client (typically a handset) authenticates the server, in most cases, the certificates are included in the firmware of the handset.
- In class 3, both the client and server are authenticated. This normally involves the implementation of a PKI.
- WTLS is similar to SSL/TLS in that it can be used to secure other protocols, such as Wireless Markup Language (WML).
- WML is much like Hypertext Markup Language (HTML), but it is specifically designed for WAP devices, such as mobile phones and PDAs.

WEP(Wired Equivalent Privacy)

- Wired Equivalent Privacy (WEP) is the security mechanism included in the 802.11 standard and is designed to provide confidentiality and authentication services.
- WEP is based on the RC4 algorithm, which is referred to as a stream cipher.
- Packets are encrypted by generating an RC4 stream with a combination of a 24-bit initialization vector (IV) and a shared key.
- The IV is used to make the RC4 stream generated with the shared key different for many of the data transmissions.
- The data is then XORed with the generated stream and transmitted in a WEP frame with the IV in the header so the receiver can generate the same RC4 stream to XOR the packet for decryption.
- There are problems with the implementation of WEP. WEP can be used as a first line of defense, but cannot be relied on for security because weaknesses have been proven that can compromise the WEP key.
- WEP also presents a number of key management problems. A common WEP key is normally used for all users on a given wireless network, which makes it very difficult to protect the key.
- WEP keys would need to be changed very frequently. Employees are constantly leaving the company or are losing wireless equipment such as laptops.
- Some of the latest implementations of WEP, often bundled in 802.1x functionality upgrades negotiate a WEP key at the time of initial authentication.

802.1x

- 802.1x and its associated protocols are an attempt to increase the security of networks before layer 3 protocols (such as IP) are set up.
- The technology is not specific to 802.11 and can be used on Ethernet, Token Ring, and so on.
- 802.1x is a layer 2 protocol that can be used for a number of operations.
- The basic purpose of 802.1x is to authenticate users and can optionally be used to establish encryption keys.
- When a connection is established, only 802.1x traffic is allowed to pass.
- This means the other protocols such as the Dynamic Host Configuration Protocol (DHCP), IP, and so on are not permitted.
- Extensible Authentication Protocol (EAP) (RFC 2284) is used to authenticate the users.
- EAP was originally designed to solve some of the authentication issues with the Point-to-Point Protocol (PPP), but its main use will probably be solving wireless issues.
- EAP authentication packets are sent to the access point with user login information, in most cases, this will be a username and password.
- The access point can authenticate the user by any means the vendor chooses to support.
- In most cases, this will be via Remote Authentication Dial-in User Service (RADIUS).
- Once the user is authenticated and optional encryption is established, communication will be enabled and protocols such as DHCP will be allowed to pass.

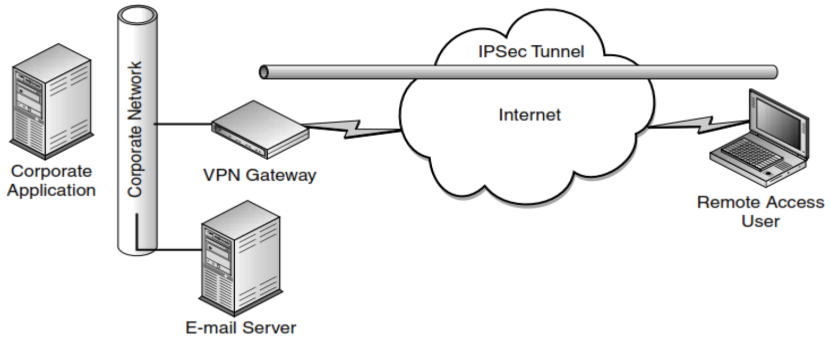


802.1x overview

IP Security (IPSec)

- IP Security (IPSec) was developed by the Internet Engineering Task Force (IETF) working group and continues to evolve.
- The IPSec protocol is lower in the protocol stack than SSL/WTLS, SSH, or WTLS.
- The security is implemented on the IP layer in the Internet model.
- The most common implementations of IPSec are using a tunnel mode that enables all IP traffic to be encrypted and optionally authenticated inside a single session.

- IPSec is the enabling technology behind most virtual private networks (VPNs) used on the Internet today.Due to the flexibility of IPSec and its broad range of application support, many choose to use it for securing their wireless applications.
- IPSec has multiple implementation options that should be used based on the application.
- IPSec can be used to provide encryption by using Encapsulated Security Payload (ESP) or authentication by using Authentication Header(AH).
- AH may be implemented without ESP. This would not provide confidentiality against sniffing, but would prevent tampering with the data and damaging the data in transport, and positively identify the sender.
- ESP can be implemented without AH to provide confidentiality and basic authentication services of data, but many administrators choose to implement both AH and ESP.
- IPSec has many different cryptographic algorithms that can be used for AH and ESP.
- The most commonly used encryption algorithms for ESP are the Data Encryption Standard (DES), Triple DES (TDES), and Advanced Encryption Standard (AES).
- AES is the replacement for DES and TDES, and the IPSec standard mandates that it be implemented in all IPSec implementations.
- The most commonly used authentication algorithms used for AH are Message Digest 5 (MD5) and Secure Hash Algorithm (SHA).
- Two modes can be used by IPSec for encapsulating data.
- Transport mode is normally used when using IPSec to communicate between two hosts. Transport mode only encrypts the data of the IP packet and all the header information remains unencrypted.
- Tunnel mode encrypts the entire IP packet including the headers. Tunnel mode is more flexible for Internet applications because many enterprises utilize private network addressing, as described in RFC 1918.
- The most common implementation of IPSec for secure communications is for remote-access VPNs over the Internet.
- Whenever a public network is used for private networking functions, it can be called a VPN.
- Using this definition, networking technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and X.25 can be considered VPNs, but most people exclusively use the term to refer to encrypted tunnels over the Internet.
- In this application, a gateway is installed on the perimeter of the corporate network.
- Remote-access users will establish an IPSec tunnel to the gateway using tunnel mode with ESP and AH.



UNIT-3

Security Considerations to Wireless Devices: Wireless Device Security Issues, Physical Security, Information Leakage, Device Security Features, Application Security, Detailed Device Analysis, Laptops, Personal Digital Assistants (PDAS), Wireless Infrastructure **Wireless Technologies and Applications:** Introduction to Cellular Networks- FDMA, TDMA, CDMA, Spread Spectrum Primer, Analogy, TDMA Vs CDMA, PDC, Security Threats.

Security Considerations to Wireless Devices:

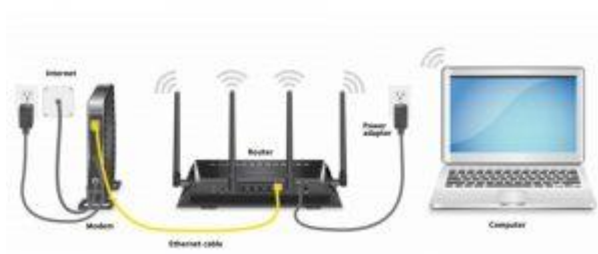
Wireless device security Issues, Physical Security, information Leakage, Device Security Features, Application Security, Detailed Device Analysis, Laptops, Personal Digital Assistance, Wireless Infrastructure

Wireless Standards and Technologies:

Introduction to Cellular Networks: FDMA, TDMA, CDMA, Spread Spectrum, OFDM, CURRENT and FUTURE Standards—IEEE 802 Standards, ETSI, Home RF, Ultra-Wide band Radio(UWB)

WHAT IS A WIRELESS DEVICE?

A wireless device is a device that uses radio waves to send or receive information. Wireless devices can be used for communication, such as in phones, tablets, and computers. They can also be used for entertainment, such as in gaming systems and home theater systems. Wireless devices use different frequencies to send and receive information.



THE WIRELESS REVOLUTION

Wireless technology has revolutionized the way we communicate and access information. Wireless devices allow us to connect to the internet, share files, and stay in touch with friends without having to be connected to a cable or phone line. Wireless devices are also becoming increasingly popular for gaming and entertainment purposes.

The wireless revolution

WIRELESS NETWORKING AND WI-FI

Wireless networking is the process of using radio waves to connect devices that are too far apart to be directly connected with cables. Wireless networking is common in homes and small offices, where it's more convenient and less expensive than using cables.

Wireless Networking and Wi-Fi

Wi-Fi is a type of wireless networking that uses radio waves to connect devices that are within range of each other. Wi-Fi networks use the same frequency as the radios in your computer, phone, or other devices. This means that you can easily connect to a Wi-Fi network without installing any extra software.

WHAT ARE THE DIFFERENT TYPES OF WIRELESS DEVICES?

Wireless devices use radio waves to send and receive information. There are different types of wireless devices, each with its own advantages and disadvantages.

What Are the Different Types of Wireless Devices

WIRELESS ROUTER

A wireless router is a device that allows users to connect to the internet wirelessly. Wireless routers are often found in homes, offices, and schools. They come in a variety of shapes and sizes and can be used for a variety of purposes, such as connecting devices such as laptops, tablets, and smartphones to the internet, sharing files between devices on the same network, or extending the range of a wireless network.

WIRELESS REPEATER

A wireless repeater is a device that amplifies or retransmits signals over a short distance using radio waves. Repeaters are used to extend the range of wireless devices, such as cell phones, laptops and PDAs, in an area where the signal is weak or nonexistent. They can also be used to amplify transmissions from one location to another.

WIRELESS ADAPTERS

Wireless adapters are hardware devices that allow a computer to connect to a wireless network. Wireless adapters come in several different types, including card-based and USB adapters. Card-based adapters are inserted into the computer’s PCI or PCIe slots and connect to the computer’s networking ports. USB adapters connect directly to the computer’s USB ports.

Wireless networks use radio waves to transmit data. Most wireless networks use2 GHz frequency bands because they’re less congested than other frequency bands and they travel farther than networks using5 GHz frequencies. 2 GHz frequency bands are also used by the 802.11b, g, n, and ac standards for wireless networking devices.

WIRELESS PHONES

Wireless devices use radio waves to communicate without the need for a physical connection. Cell phone networks, Wi-Fi networks, and Bluetooth signals are all examples of wireless technologies.

Wireless devices can be used for a variety of purposes, including communication, gaming, navigation, and music streaming. Many wireless devices also have capabilities that are unique to that particular device. For example, a cell phone can be used to make calls and text messages, but it can also be used for navigation purposes thanks to its built-in GPS system.

Wireless technology is constantly evolving and improving. New wireless technologies are being developed all the time, and existing ones are becoming more powerful and versatile. Wireless devices will continue to become more popular as they become increasingly versatile and practical.

WIRELESS DEVICES EXAMPLES

Wireless devices are devices that use wireless technology to send and receive data. Wireless technologies can include radio waves, microwaves, infrared signals, and light waves. Wireless devices can be used for a variety of purposes, including communication, navigation, security, and entertainment. Wireless devices can be powered by batteries or by a nearby electrical outlet.

Wireless Devices Examples

HOW DO WIRELESS DEVICES WORK?

When you think about electronics, you likely think about wires. But there are other ways to connect devices, like with radio waves. Wireless devices use radio waves to transmit data without having to use cables.

Radio waves are invisible, so they travel through walls and other objects without being blocked. That means wireless devices can be placed anywhere in a room without worrying about obstructions.

There are a few different types of wireless signals: Wi-Fi (which is used in homes and businesses), Bluetooth (which is used for connecting accessories like speakers and headphones), and cellular (for connecting phones to the internet). Each type of signal has its own strengths and weaknesses, so it’s important to choose the right one for the task at hand.

LIST OF WIRELESS DEVICES

List of Wireless Devices

Wireless devices use radio waves to connect to devices without having to plug in. Wireless devices can be used for a variety of things, like connecting your phone to the internet, streaming music, or checking your email. There are a lot of different wireless devices out there, so it can be hard to decide which one is right for you. Here are some examples:

COMUNICATION EQUIPMENT

A wireless communication device is an electronic device that allows two or more devices to communicate with each other wirelessly. Wireless devices include cell phones, laptops, tablets, and other portable electronics. Wireless devices are often used to communicate with people in faraway places, as well as with people who are nearby.

HOUSEHOLD ITEMS

When it comes to household items, there are a few that come to mind that use wireless technology. One example is a hair dryer. Most hair dryers now come with a wireless connection so you can control the settings from anywhere in the house. Another example is a remote control for your television. These days, most televisions have remotes that use wireless technology to send commands from across the room.

Computer Peripherals

Computer peripherals include devices that are used to input or output data, such as keyboards, mice, touchpad's, and trackballs. Many computer peripherals also have buttons or switches that allow the user to control how the device works. Peripherals can be connected to a computer using a cable or wireless connection.

Security Concerns

A wireless device is susceptible to security concerns. Wireless devices are vulnerable to being hacked and are often targets for thieves. This is because a wireless device does not require a physical connection to the internet in order to work, which makes it an easy target for thieves. Additionally, wireless devices can be monitored by third parties without the user's knowledge or consent, which can be intrusive and scary.

What are The Advantages of Wireless Devices?

Wireless devices are advantageous because they do not require an outlet or cord to work. They can be placed anywhere in a room without taking up any space, and they are very easy to use. Wireless devices allow for more freedom in movement because there is no need to worry about getting tangled up in cords. They also have a longer battery life than traditional devices, which means that you can use them for longer periods of time without having to recharge them.

What are The Disadvantages of Wireless Devices?

Wireless devices present a number of security and privacy concerns. Wireless networks are notoriously insecure, as anyone within range can access your data. In addition, wireless devices can be tracked by third parties, even when they are not connected to the internet. Finally, many wireless devices emit electromagnetic radiation that may be harmful to your health.

Introduction to Physical Security

These days, tips on how to strengthen your cyber security follow the announcement of every another cyber attack. Don’t forget to backup your data, apply patches over vulnerabilities, monitor firewalls, etc. It is very important to remember that software is not your only weapon when it comes to cyber security. Physical Cyber Security is another tier in your line of defense.

According to Goldstein(2016), Physical Security is critical, especially for small business that does not have many resources to devote to security personnel and tools as opposed to larger firms. When it comes to Physical Security, the same principles apply here:

- Identify and classify your assets and resources.
- Identify plausible threats.
- Identify probable vulnerabilities that threats may exploit.
- Identify the expected cost in case if an attack occurs.

Factors on which Physical Security Depends

1. How many workplaces, buildings or sites are there in an organization?
2. Size of the building of the organization?
3. How many employees are employed in the organization?
4. How many entry and exit points are there in the organization?
5. Points of placement of data centers and other confidential information.

Layers of Physical Security

Layers in Physical Security are implemented at the perimeter and are moving towards an asset. The layers are as follows:

1. Deterrence

The goal of Deterrence methods is to convince a potential attacker that a successful attack is not possible due to strong defenses. For example: By placing your keys inside a highly secure key control system made up of heavy metal like steel, you can help prevent attackers from gaining access to assets. *Deterrence methods are classified into 4 categories:*

- **Physical Barriers:** These include fences, walls, vehicle barriers, etc. They also act as a Psychological deterrent by defining the perimeter of the facility and making intrusion seem more difficult.
- **Combination Barriers:** These are designed to defeat defined threats. This is a part of building codes as well as fire codes.
- **Natural Surveillance:** In this architects seek to build places that are more open and visible to authorized users and security personnel so that attackers are unable to perform the unauthorized activity without being seen. For example- decreasing the amount of dense and tall vegetation.
- **Security Lighting:** Doors, gates or other means of the entrance should be well lit as Intruders are less likely to enter well-lit areas. Keep mind to place lighting in a manner, that is difficult to tamper.

2. Detection

If you are using the manual key control system, you have no way of knowing the exact timestamp of when an unauthorized user requested a key or has exceeded its time limit. Detection methods can of the following types:

- **Alarm Systems and Sensors:** Alarm systems can be installed to alert security personnel in case of an attempt of unauthorized access. They consist of sensors like perimeter sensors, motion sensors, etc.
- **Video Surveillance:** Surveillance cameras can be used for detection if an attack has already occurred and a camera is placed at the point of attack. Recorded video can be used

3. Access Control

These methods are used to monitor and control the traffic through specific access points. Access Control includes the following methods:

- **Mechanical Access Control Systems:** These includes gates, doors, locks, etc.
- **Electronic Access Control:** These are used to monitor and control larger populations, controlling for user life cycles, dates and individual access points.
- **Identification System and access policies:** These includes the use of policies, procedures and processes to manage the access into the restricted area.

4. Security Personnel

They play a central role in all layers of security. They perform many functions like:

- Administering electronic access control.
- Responding to alarms.
- Monitoring and analyzing video footage and many more

Countermeasures and Protection Techniques

1. Protection against Dumpster Diving

Dumpster Diving is the process of finding some useful information about the person or business from the trash that can later be used for hacking purpose. Since the information is in the trash, it is not useful for the owner but deemed useful to the picker. To protect against it, you need to follow certain measures:

- Ensure all important documents are shredded and they are still secure.
- Destroy any CDs/ DVDs containing personal data.
- Make sure that nobody can walk into your building and simply steal your garbage and should have safe disposal policy.
- Firewalls can be used to prevent suspicious users from accessing the discarded data.

2. Employee Awareness Training

A negligent employee can be one of the major causes of a Cyber security breach. Employee awareness training sessions can help in such cases. Employee awareness training should focus on one underlying theme- *avoid the SEP- Somebody else's problem field.*

3. Site Access Control

Lack of Access Control can be highly devastating if a wrong person gets in and gets access to sensitive information. Fortunately nowadays, you have a number of modern tools that will help you to optimize your access control.

- **Envoy** is a tool that will help you to expand access to guests in controlled manner.
- **Open Path** is a mobile system that allows access to only a limited set of people within the directory using smart phones and other devices.

4. Securing Your Windows

If you have the data that hackers would love to get their hands on, they will try any method and might just look through the window. Make sure you are aware of the sight angles to position your screens and other devices. Overlooking from different sight angles to see your credentials is known as *Shoulder Surfing.*

5. Secure Network-Enabled Printers

Network Printers are a very convenient option allowing anyone in the office to get connected, without a need of extra wiring. Unfortunately, they have underlying security risks also. Sometimes, due to default settings, they offer open WiFi access, thus allowing anyone to get in and open vulnerabilities in the process.

- Only connect those to the Internet that actually needs to be.
- Remote access is not necessary for scenarios where only people from your office use the printer.
- You can add passwords to the connection if necessary.

6. Securing Your Backups

Physical backups are critical for business continuity, helping you prevent data loss in the event of disasters, outages, and more. Most businesses secure their servers but they forget that backups are equally important. They are holding the same level of sensitive data as servers. Treat your backups as you treat your sensitive information and secure them.

7. Building Secure Guest Wi-Fi

Guest Wi-Fi is a natural solution when you have guests or visitors. Here are a few tricks to help protect your resources from the external users:

- Segment your network- In this way, it isolates Guest Wi-Fi from your internal devices and data.
- Encrypt your wireless signals and change the default passwords of all devices on the network.

8. Locking up your Servers

Any area in your organization that stores data need to be secured. Locking doors and making sure server area gets extra protection.

9. Accounting for Loss or Stolen Devices

As devices are becoming more mobile, chances for them being stolen or falling out of someone's pocket becomes more frequent. Mobile Device Management can help you to manage such situations and take the necessary precautions. The best solution in such cases is to simply lock down and potentially wipe any lost or stolen devices from the organization remotely.

10. Implementing video systems

To achieve more secure premises, it is advisable to use a Video Surveillance system.

- Mere presence of cameras can deter potential attackers.
- Availability of video footage allows you to have continuous monitoring over the entire premises.
- If an attack happens, you can check the recorded video, easily reconcile the process and catch the perpetrator.

What is Data Leakage?

Data leakage, also referred to as low-profile data theft, involves the unauthorized transfer of electronic or physical data from an organization to external recipients or destinations. Threat actors often leak data using email accounts or the web. They may also use mobile data storage devices like USB keys, laptops, and optical media.

Data leakage can result from purposeful insider action meant to cause harm to the organization, or as part of a bigger scheme to commit payment fraud. It can also be accidental. Cybercriminals look for various types of information in data leaks, including customer information and trade secrets. The scope and the type of leak determines the damage caused to the organization.

This article is part of our series of articles about endpoint security.

Causes of Information Leakage

Here are common causes of information leaks at organizations:

Insider Threats

Insider threats include dissatisfied employees, former employees with access to sensitive systems, or business partners. Their motive may be economic gain, theft of valuable data, or a desire for revenge. Insiders can steal an organization's sensitive data for financial or personal gain.

Payment Fraud

Payment fraud is an attempt to make a fraudulent or illegal transaction. Common scenarios include credit card scams, false returns, and triangle scams. A triangle scam involves an attacker opening an online store with very low prices, tricking customers into providing their payment information, and then using this payment information to buy products at other stores.

Social Engineering

When data leaks are initiated by cybercriminals, they are usually the result of social engineering tactics. Social engineering is the use of psychological manipulation to trick victims into giving over sensitive information. Phishing is the most common type of social engineering attack. Traditionally phishing takes the form of a written message asking the user to provide confidential information or perform an action favorable to the attacker. Increasingly, phishing is performed over the phone (this is known as vishing).

Very often, attackers are after data that does not appear sensitive on its own, but can expand the list of potential victims. This poses a serious threat to data security, because attackers can easily deceive unsuspecting employees, by requesting seemingly harmless information such as phone numbers and social security numbers.

Physical Theft of Sensitive Devices

Company devices contain sensitive information, and misuse of these devices can lead to security breaches and theft of company information.

For example, a cybercriminal can use a stolen device to contact an IT administrator and claim that they have forgotten their login information. With a convincing strategy, attackers can breach the device and gain access to the corporate network.

Unintended Disclosure

Many data breaches are not caused by an attack, but rather by unintentional exposure of sensitive information. For example, employees might view sensitive data and save it to a non-secure location, or IT staff might mistakenly expose a sensitive internal server or cloud system to the Internet.

Malicious Electronic Communications

Many organizations give employees access to the Internet, email, and instant messaging, as part of their role. The problem is that all of these mediums are capable of file transfer or accessing external sources over public networks.

Attackers often target these communication channels and achieve a high success rate. For example, a cybercriminal could spoof a legitimate business email and simply ask an employee to send them sensitive data. If the user is fooled by the message, they could attach the requested files to the email and send them to the attacker.

What Do Cyber Criminals Look for in Data Leaks?

The majority of data leaks involve either personally identifiable information (PII) or protected health information (PHI). Examples of PII are names, social security numbers, and other personal details. PHI is defined in the US HIPAA regulation as any information about an individual's health, now, in the past, or in the future.

Below are a few types of sensitive data that are commonly targeted in data leaks.

Customer Information

This is information about a company's customers, including their names and contact details, credentials, activity history, and payment details.

What damage can it cause?

Exposure of customer information can damage both the company and its customers, cause harm to reputation, and in many cases expose a company to compliance violations and lawsuits.

Company Information

This is information revealing the company's internal operations. It can include emails and internal documents; strategy, marketing, and business plans; and business metrics or forecasts.

What damage can it cause?

Exposure of company information can provide competitors, rivals, or attackers valuable data about a company's operations. This can give third parties an unfair advantage over the company or help them cause direct damage to its operations. Attackers can also use it to plan secondary attacks.

Trade Secrets

This is possibly the most sensitive information a company can lose in a data leak, including intellectual property, plans for future products, source code, and details about proprietary technologies.

What damage can it cause?

Exposure of trade secrets can cause a company to lose large investments in research and development and make its market offering less valuable.

Analytics

This is data used by a business to derive insights about its customers or environment. This can include historical data about customers or prospects in the industry, demographic data, and models that can generate useful predictions in the company's industry.

What damage can it cause?

Analytics is valuable to the business and so is equally valuable to an attacker. Like other types of data leaks it can give third parties an unfair advantage by exposing internal knowledge. If analytics data is not anonymized, it can have the additional impact of exposing PII.

How to Prevent Data Leakage

Ensure Timely Detection

You can avoid or reduce the fallout from a data leak by detecting improper activity fast. Ensure you receive alerts on changes to critical access or configuration parameters, and act quickly to investigate and remediate anomalies. Put in place monitoring for unusual data transfers, such as data loss prevention (DLP), and intervene early on if you discover users copying unusual amounts of data.

Classify Data according to Sensitivity and Value

To prevent data leaks, the first step is to identify which data employees are able to freely share. You should then decide who should have permission to access this data. Using data identification and classification, you can organize your data into categories, protecting sensitive data as required.

Here are a few technologies commonly used to protect sensitive data:

- Data Loss Prevention (DLP)
- Identity and access management (IAM)
- Encryption
- Privileged Access solutions
- Change management and auditing
- User and entity behavior analytics (UEBA)

Discover and Mitigate IT Risks

You can't discover your most vulnerable areas unless you periodically assess your risk. To implement successful risk management and risk assessment, you may wish to use an industry standard such as the National Institute of Standards and Technology (NIST). The NIST SP 800-30 document specifies the protocols for vulnerability assessment, which can help mitigate many risks leading to data leakage.

Discover more best practices in our detailed guide to data leakage prevention (coming soon)

Data Leakage Prevention with Perception Point

Perception Point provides enterprise-grade security to protect email, web browsers, cloud collaboration platforms and proprietary apps from all types of cyber attacks.

Enhanced browser-level DLP capabilities deter malicious insiders, partners and contractors and include:

- Clipboard controls (preventing copy and paste);
- Printing controls;
- Configurable download/upload restrictions;
- Watermarking;

- Smart blur of sensitive web apps/data to prevent accidental external screen capture and shoulder surfing
- User activity monitoring and visibility into all installed browser extensions across the organization
- SaaS app login visibility, enabling the organization's admins and security teams to view the usage of unsanctioned web apps

The all-included managed Incident Response service is available for all customers 24/7. Perception Point's team of cyber security experts will manage incidents, provide analysis and reporting, and optimize detection on-the-fly. The service drastically minimizes the need for internal IT or SOC team resources, reducing the time required to react and mitigate web-borne attacks by up to 75%.

Customers deploying the solution will experience fewer breaches, while providing their users with a better experience as they have the freedom to browse the web, use SaaS applications that they require, and access privileged corporate data, confidently, securely, and without added latency.

Wireless Network Infrastructure definition

Wireless Network Infrastructure (© vege / Fotolia.com)

Wireless networks are networks of computers and other smart devices that utilize a wireless data connection between nodes. This infrastructure today powers a great many of the services, entertainment and products that we rely on and so it pays to have a solid understanding of how it works and of the impact of wireless network infrastructures on your life and your business.

What is a Wireless Network?

Wireless networks are networks that allow for multiple devices to communicate with one another wirelessly and with no need for cables or connections. This is an incredibly useful and important tool and much of modern business, communication and entertainment depends on it.

Most of us have personal wireless networks at home and this depends on the infrastructure that has been put in place. This means that we can have multiple devices connected to the web at any given time, meaning that we might be using a computer upstairs to get work done and answer emails, while still being able to receive online messages through a mobile phone. It also allows us to communicate between devices *on* that wireless network. For instance, you might send a photo to your computer upstairs, or you might stream media to your television from your phone.

Wireless networks become even more important in a range of businesses and industries. Wireless networks are crucial for many companies to communicate internally and conveniently and to exchange information in a manner that is safe and secure. Likewise, wireless networks are used in a range of other institutions and organizations. Hospitals use wireless connections to communicate around the ward and to manage tools and important machinery. Schools and colleges have wireless networks for their students. Police, airlines, government and more all depend on wireless networks.

So with wireless networks being so ubiquitous and fundamental to our way of life, it seems pertinent to understand how they work!

How Do Wireless Networks Work?

So, in any telecommunications network, **nodes** are defined as redistribution points or communication endpoints. In the case of a physical network, nodes might be active electronic devices attached to that network – as long as they are capable of creating, receiving or transmitting information over a communications channel.

Passive distribution points such as patch panels are **therefore** not considered nodes (patch panels are used to connect and route circuits). In the case of **wireless network infrastructure**, nodes are computers, smartphones, games consoles, printers and of course the router itself. Routers, hubs or switches are considered **data communication equipment** whereas **data terminal equipment** includes the devices that we typically interact with.

Networks can be either LAN (**local area network**) or WAN (**wide area network**). WAN networks extend over large geographical distances and essentially allow for multiple LANs to be tied together to transmit communication. Businesses, schools and other organizations use WANs in order to communicate with their members. Likewise, leased telecommunication circuits can be used to form WANs. Even the internet itself can be considered WAN!

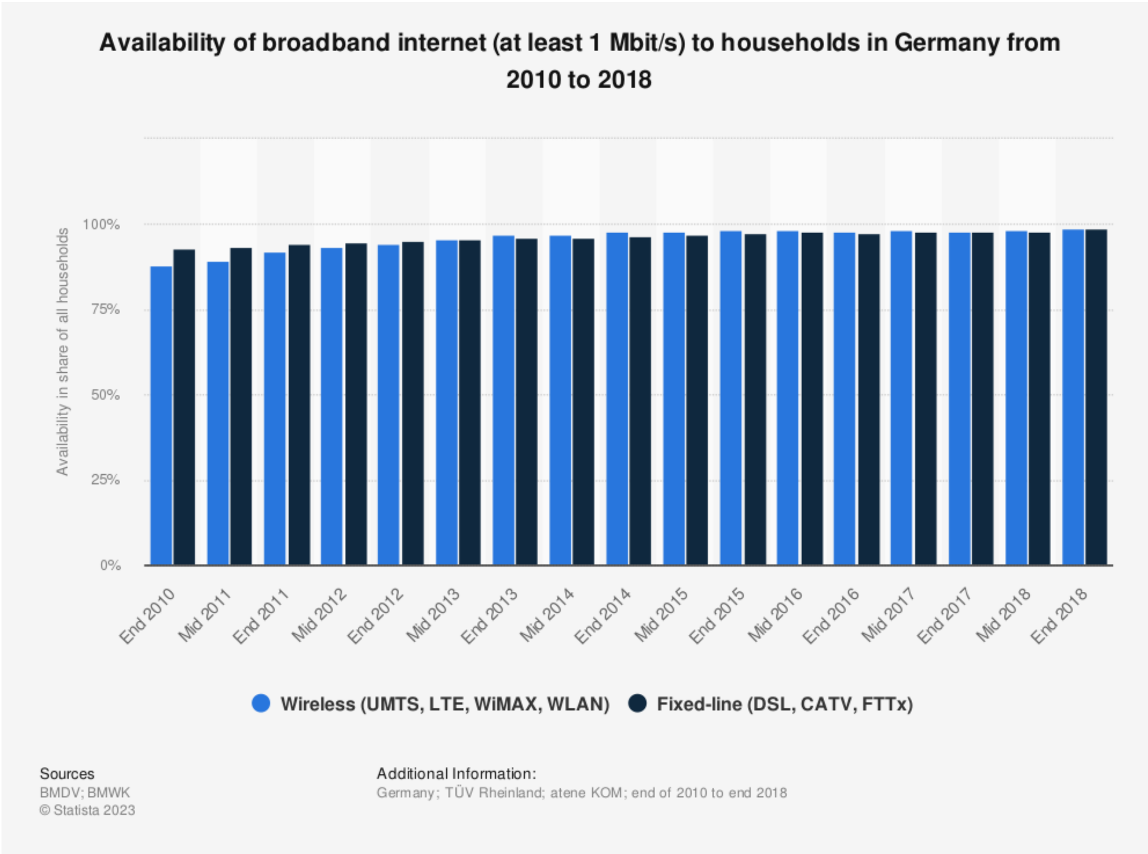
The internet network in your home is most likely a LAN network (for those devices plugged into ethernet ports or powerline adaptors) or a WLAN network (wireless LAN). These use OFDM or spread-spectrum technologies to provide connectivity to the network with no need for a wired connection.

The computers on these networks are described as **host computers** or **internet nodes** and will be given their own IP addresses. These IP addresses are unique to the private network and are called 'private IP' addresses. The router itself also has an IP, which is referred to as the 'public IP address'.

From time to time, the private IPs of your devices will change around. This is handled by the DHCP or '**Dynamic Host Configuration Protocol**'. The public IP however will remain constant. This way, the router acts as a kind of conduit between the devices on your home private network and the internet outside. The router will be connected to a wired cable (perhaps fiber optic) and will then transmit and receive wireless signals to help you communicate with the outside world.

Services are used via specific '**ports**' on the network, which are bound to IP addresses. Because computers are capable of running multiple programs at a time, multiple ports allow for a range of different data services to be carried out simultaneously.

DHCP I just one of several protocols that make up the standardised conceptual model that is the **internet protocol suite.** This series of protocols together provides a 'model' for how networks should be handled and managed on the web and on other computer networks. It is sometimes referred to as **TCP/IP** because the original protocols are the transmission control protocol and internet protocol.



Find more statistics at Statista

Infrastructure

So, while the WLANs that you experience in your home are wireless by name, they still rely on a wired connection that connects the router to the wider internet (the WAN). The infrastructure provided by the local service providers and the council then, will almost certainly provide the limit or bottleneck for your connection speeds and stability.

Some of this will be outside of your control, but other aspects of your wireless infrastructure are your responsibility. For instance, making sure that you have the best router, using wired connections where convenient and tweaking the advanced settings of your router can help you to increase your speed and stability.

openPR-Tip: More importantly, it is up to you to protect your data and to keep your connections as private as possible. Recognize the danger of being on a public network such as coffee shop WiFi and don’t access sensitive private information during this time.

Better yet, consider setting up a VPN or '**virtual private network**'. This works just like a LAN except it is entirely digitized and conceptual. Nevertheless, the IP address you put out to the world will be that of your VPN and *not* the physical location. This is called **spoofing** the physical location.

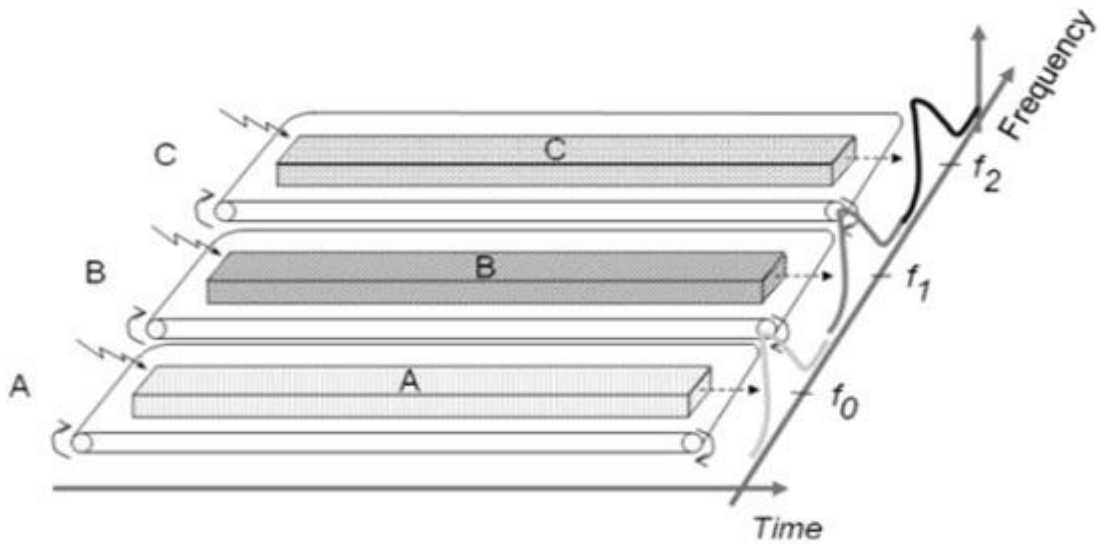
Wireless infrastructure has helped to bring us into the digital age and it will continue to have a transformative impact on our culture and economy. It's up to us to ensure the infrastructure is there and we are using it in a safe and responsibly manner.

Frequency Division Multiple Access (FDMA) is one of the most common analogue multiple access

methods. The frequency band is divided into channels of equal bandwidth so that each conversation is carried on a different frequency (*as shown in the figure below*).

FDMA Overview

In FDMA method, guard bands are used between the adjacent signal spectra to minimize crosstalk between the channels. A specific frequency band is given to one person, and it will received by identifying each of the frequency on the receiving end. It is often used in the first generation of analog mobile phone.



Advantages of FDMA

As FDMA systems use low bit rates (large symbol time) compared to average delay spread, it offers the following advantages −

- Reduces the bit rate information and the use of efficient numerical codes increases the capacity.

- It reduces the cost and lowers the inter symbol interference (ISI)
- Equalization is not necessary.
- An FDMA system can be easily implemented. A system can be configured so that the improvements in terms of speech encoder and bit rate reduction may be easily incorporated.
- Since the transmission is continuous, less number of bits are required for synchronization and framing.

Disadvantages of FDMA

Although FDMA offers several advantages, it has a few drawbacks as well, which are listed below −

- It does not differ significantly from analog systems; improving the capacity depends on the signal-to-interference reduction, or a signal-to-noise ratio (SNR).
- The maximum flow rate per channel is fixed and small.
- Guard bands lead to a waste of capacity.
- Hardware implies narrowband filters, which cannot be realized in VLSI and therefore increases the cost.

TDMA - Technology

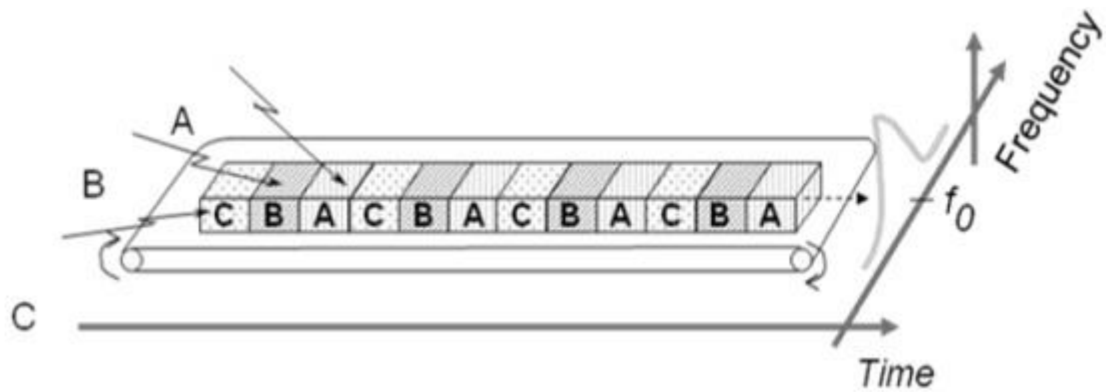
Time Division Multiple Access (TDMA) is a digital cellular telephone communication technology. It facilitates many users to share the same frequency without interference. Its technology divides a signal into different timeslots, and increases the data carrying capacity.

TDMA Overview

Time Division Multiple Access (TDMA) is a complex technology, because it requires an accurate synchronization between the transmitter and the receiver. TDMA is used in digital mobile radio systems. The individual mobile stations cyclically assign a frequency for the exclusive use of a time interval.

In most of the cases, the entire system bandwidth for an interval of time is not assigned to a station. However, the frequency of the system is divided into sub-bands, and TDMA is used for the multiple access in each sub-band. Sub-bands are known as **carrier frequencies**. The mobile system that uses this technique is referred as the **multi-carrier systems**.

In the following example, the frequency band has been shared by three users. Each user is assigned definite **timeslots** to send and receive data. In this example, user **'B'** sends after user **'A,'** and user **'C'** sends thereafter. In this way, the peak power becomes a problem and larger by the burst communication.



FDMA and TDMA

This is a multi-carrier TDMA system. A 25 MHz frequency range holds 124 single chains (carrier frequencies 200) bandwidth of each kHz; each of these frequency channels contains 8 TDMA conversation channels. Thus, the sequence of timeslots and frequencies assigned to a mobile station is the physical channels of a TDMA system. In each timeslot, the mobile station transmits a data packet.

The period of time assigned to a timeslot for a mobile station also determines the number of TDMA channels on a carrier frequency. The period of timeslots are combined in a so-called TDMA frame. TDMA signal transmitted on a carrier frequency usually requires more bandwidth than FDMA signal. Due to the use of multiple times, the gross data rate should be even higher.

Advantages of TDMA

Here is a list of few notable advantages of TDMA −

- Permits flexible rates (i.e. several slots can be assigned to a user, for example, each time interval translates 32Kbps, a user is assigned two 64 Kbps slots per frame).
- Can withstand gusty or variable bit rate traffic. Number of slots allocated to a user can be changed frame by frame (for example, two slots in the frame 1, three slots in the frame 2, one slot in the frame 3, frame 0 of the notches 4, etc.).
- No guard band required for the wideband system.

- No narrowband filter required for the wideband system.

Disadvantages of TDMA

The disadvantages of TDMA are as follow −

- High data rates of broadband systems require complex equalization.
- Due to the burst mode, a large number of additional bits are required for synchronization and supervision.
- Call time is needed in each slot to accommodate time to inaccuracies (due to clock instability).
- Electronics operating at high bit rates increase energy consumption.
- Complex signal processing is required to synchronize within short slots.

CDMA - Introduction

What is CDMA?

Code **D**ivision **M**ultiple **A**ccess (CDMA) is a digital cellular technology used for mobile

communication. CDMA is the base on which access methods such as cdmaOne, CDMA2000, and WCDMA are built. CDMA cellular systems are deemed superior to FDMA and TDMA, which is why CDMA plays a critical role in building efficient, robust, and secure radio communication systems.

A Simple Analogy

Let's take a simple analogy to understand the concept of CDMA. Assume we have a few students gathered in a classroom who would like to talk to each other simultaneously. Nothing would be audible if everyone starts speaking at the same time. Either they must take turns to speak or use different languages to communicate.

The second option is quite similar to CDMA — students speaking the same language can understand each other, while other languages are perceived as noise and rejected. Similarly, in radio CDMA, each group of users is given a shared code. Many codes occupy the same channel, but only those users associated with a particular code can communicate.

Salient Features of CDMA

CDMA, which is based on the spread spectrum technique has following salient features −

- In CDMA, every channel uses the full available spectrum.
- Individual conversations are encoded with a pseudo-random digital sequence and then transmitted using a wide frequency range.
- CDMA consistently provides better capacity for voice and data communications, allowing more subscribers to connect at any given time.
- CDMA is the common platform on which 3G technologies are built. For 3G, CDMA uses 1x EV-DO and EV-DV.

Third Generation Standards

CDMA2000 uses Frequency Division Duplexing-Multicarrier (FDD-MC) mode. Here, multicarrier implies N × 1.25 MHz channels overlaid on N existing IS-95 carriers or deployed on unoccupied spectrum. CDMA2000 includes −

- 1x — uses a spreading rate of 1.2288 Mcps.
- 3x — uses a spreading rate of 3 × 1.2288 Mcps or 3.6864 Mcps.
- 1xEV-DO (1x Evolution – Data Optimized) — uses a spreading rate of 1.2288 Mcps, optimized for the data.
- WCDMA/FDD-DS — Wideband CDMA (WCDMA) Frequency Division Duplexing-Direct Sequence spreading (FDD-DS) mode. This has a single 5 MHz channel. WCDMA uses a single carrier per channel and employs a spreading rate of 3.84 Mcps.

CDMA Development Group (CDG)

The CDMA Development Group (CDG), founded in December 1993, is an international consortium of companies. It works together to lead the growth and evolution of advanced wireless telecommunication systems.

CDG is comprised of service providers, infrastructure manufacturers, device vendors, test equipment vendors, application developers, and content providers. Its members jointly define the technical requirements for the development of complementary systems CDMA2000 and 4G. Further, the interoperability with other emerging wireless technologies are meant to increase the availability of wireless products and services to consumers and businesses worldwide.

IMT-2000 System

	IMT-DS (Direct Sequence)	IMT-MC (Multi Carrier)	IMT-TC (Time Code)	IMT-SC (Single Carrier)	IMT-FT (Frequency Time)
Popular name	W-CDMA	CDMA2000	UTRA-TDD TD-CDMA TD-SCDMA	UWC-136	DECT
Access method	CDMA-FDD	CDMA-FDD	CDMA-TDD	TDMA-FDD	TDMA-TDD
Organization Partners	ARIB/TTC CWTS ESTI T1 TTA	ARIB/TTC CWTS TIA TTA	CWTS ESTI T1 TTA	TIA	ESTI
Body of Technical Spec production	3GPP(FDD)	3GPP2	3GPP(TDD) CWTS	IS-136	DECT

Approved in 2000 as ITU-R M.1457

CDMA - Channels

CDMA channels can be broadly categorized as Forward channel and Reverse channel. This chapter explains the functionalities of these channels.

Forward Channel

The Forward channel is the direction of the communication or mobile-to-cell downlink path. It includes the following channels −

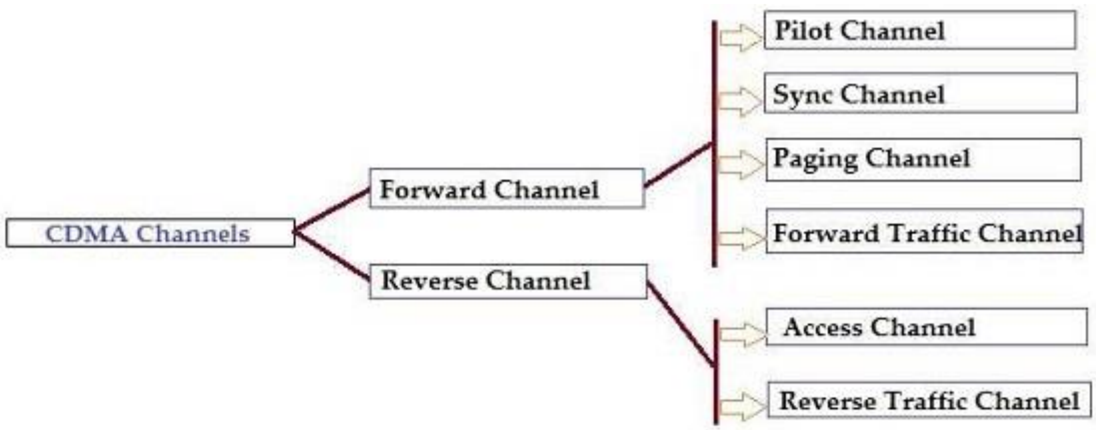
- **Pilot Channel** − Pilot channel is a reference channel. It uses the mobile station to acquire the time and as a phase reference for coherent demodulation. It is continuously transmitted by each base station on each active CDMA frequency. And, each mobile station tracks this signal continuously.
- **Sync Channel** − Synchronization channel carries a single, repeating message, which gives the information about the time and system configuration to the mobile station. Likewise, the mobile station can have the exact system time by the means of synchronizing to the short code.

- **Paging Channel** − Paging Channel's main objective is to send out pages, that is, notifications of incoming calls, to the mobile stations. The base station uses these pages to transmit system overhead information and mobile station specific messages.
- **Forward Traffic Channel** − Forward Traffic Channels are code channels. It is used to assign calls, usually voice and signaling traffic to the individual users.

Reverse Channel

The Reverse channel is the mobile-to-cell direction of communication or the uplink path. It consists of the following channels −

- **Access Channel** − Access channel is used by mobile stations to establish a communication with the base station or to answer Paging Channel messages. The access channel is used for short signaling message exchanges such as call-ups, responses to pages and registrations.
- **Reverse Traffic Channel** − Reverse traffic channel is used by the individual users in their actual calls to transmit traffic from a single mobile station to one or more base stations.



CDMA - Multiple Access Methods

The possibility to operate in either FDD or TDD mode is allowed for efficient use of available spectrum according to frequency allocation in different regions.

Frequency Division Duplex

A duplex method whereby the Uplink and the Downlink transmissions use two separate frequency bands −

- **Uplink** − 1920 MHz to 1980 MHz
- **Downlink** − 2110 MHz to 2170 MHz
- **Bandwidth** − Each carrier is located on the center of a 5 MHz wide band

Channel Separation

Nominal value of 5 MHz that can be adjusted.

Channel Raster

200 kHz (center frequency must be a multiple of 200 kHz).

Tx-Rx Frequency Separation

Nominal value of 190 MHz. This value can be either fixed or variable (minimum of 134.8 and maximum of 245.2 MHz).

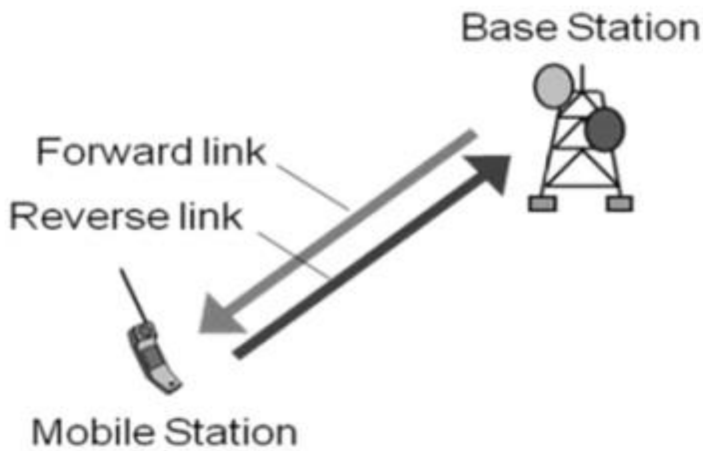
Channel Number

The carrier frequency is designated by the UTRA Absolute Radio Frequency Channel Number (UARFCN). This number is sent by the network (for the uplink and downlink) on the BCCH logical channel and is defined by Nu = 5 * (Frequency uplink MHz) and ND = 5 * (Frequency downlink MHz).

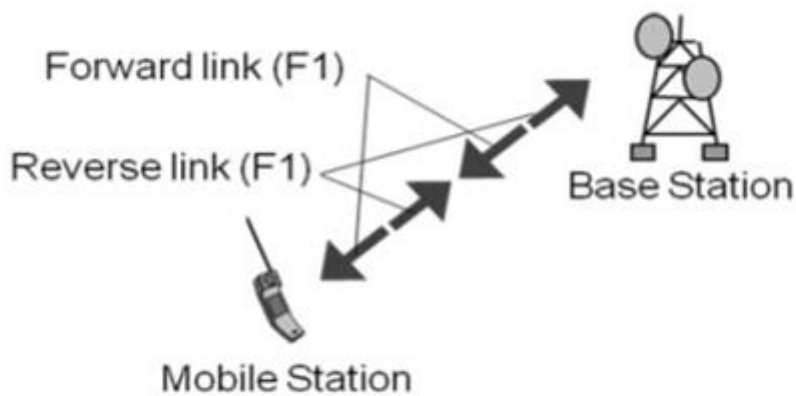
Time Division Duplex

Time division duplex is a technique by which the Uplink and the Downlink transmissions are carried over the same frequency by using synchronized time intervals. The carrier uses a 5 MHz band, although there is a low chip rate solution under study by the 3GPP (1.28 Mcps). The available frequency bands for TDD will be 1900–1920 MHz and 2010 – 2025 MHz.

Duplex Methods of Radio Links



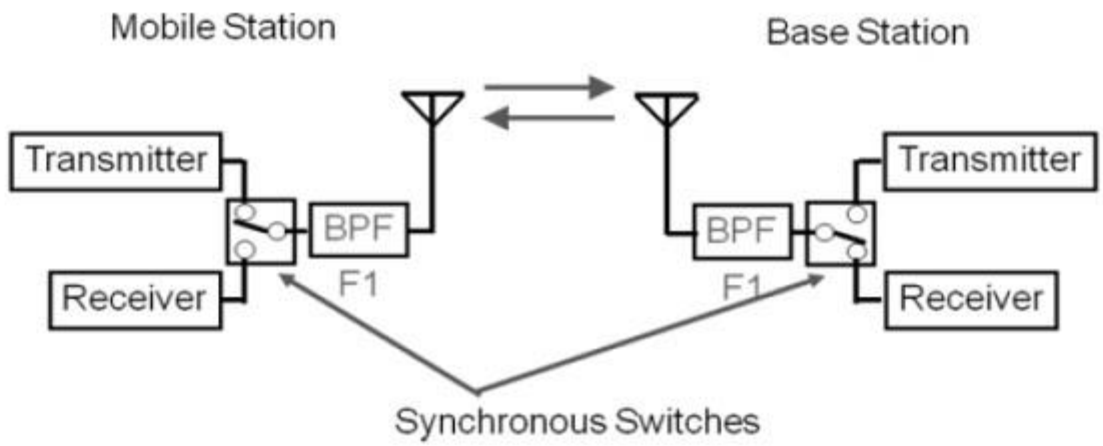
In case of Time Division Duplex, the forward link frequency is same as the reverse link frequency. In each link, signals are transmitted continuously in turns − just like a ping-pong game.



Example of TDD System

TDD uses a single frequency band for both to transmit and to receive. Further, it shares the band by assigning alternate timeslots for transmitting and receiving operations. The information to be transmitted can be voice, video, or computer data in bit-serial format. Each time interval can be 1 byte long or may be a part of several bytes.

TDD alternates the transmission and reception station data over time. Timeslots can be of variable length. Due to the nature of high-speed data, the communicating parties cannot mean that the transmissions are intermittent. Transmissions that appear as simultaneous are actually competing each other. Digitally converted into analog voice, no one can say that it is not a full duplex.



In some TDD systems, alternative time intervals are of same duration or having both DL and UL; however, the system does not need to be symmetric 50/50. The system may be asymmetrical as required.

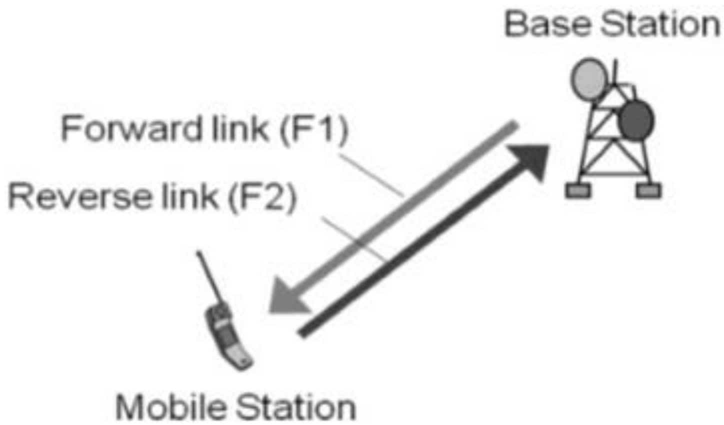
For example, while accessing the Internet, the download speed is usually higher than the upload speed. Most of the equipment work on asynchronous mode where the download speed is higher than the upload speed. When the download speed is higher than the upload speed, less timeslots are needed for uploading. Some TDD formats offer dynamic bandwidth allocation when the number of time intervals or durations is changed on the fly as needed.

The real advantage of TDD is that it is only a single channel of the frequency spectrum and it doesn't require band guards or channel separations as the intervals take place using timeslots. The disadvantage is that the successful implementation of TDD requires a timing system. The precise timing to both the transmitter and the receiver is needed to ensure that the time intervals do not overlap or interfere with another.

Timing is often synchronized to GPS atomic clock standards specific derivative. The guard time is also needed between timeslots to avoid duplication. This time is generally equal to the transmission-reception processing time (transmission-reception switching time) and the transmission delays (latency) on the communications channel.

Frequency Division Duplex

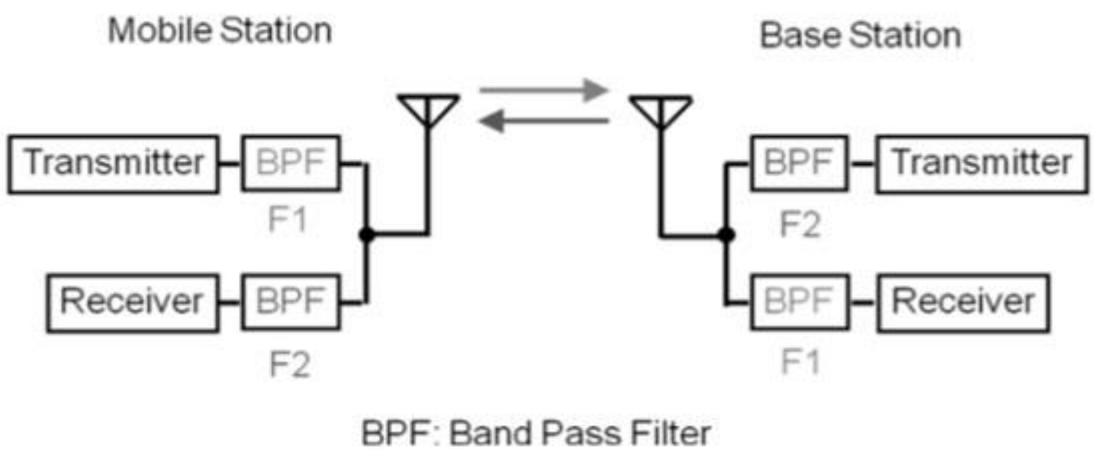
In Frequency Division Duplex (FDD), the forward link frequency is not the same as the reverse link frequency. In each link, signals are continuously transmitted in parallel.



Example of FDD System

FDD requires two symmetrical segments of spectrum for the uplink and downlink channels.

In a cell phone with a transmitter and receiver, operating simultaneously in such close proximity, the receiver has to filter as much of the signal from the transmitter as possible. More separation of the spectrum, the most effective filters.



FDD uses a lot of frequency spectrum, generally twice of the required TDD spectrum. In addition, there must be adequate spectrum separation between transmission and reception of the channels. These bands keep saying − it cannot be used, they are unnecessary. Given the scarcity and cost of the spectrum, they are real disadvantages.

Use of FDD

FDD is widely used in different cellular telephone systems. In some systems, the band 869-894 MHz is used as the downlink (DL) spectrum from the cell site tower to the device. And, the band 824-849 MHz is used as the uplink (UL) spectrum of the handset at the cell site.

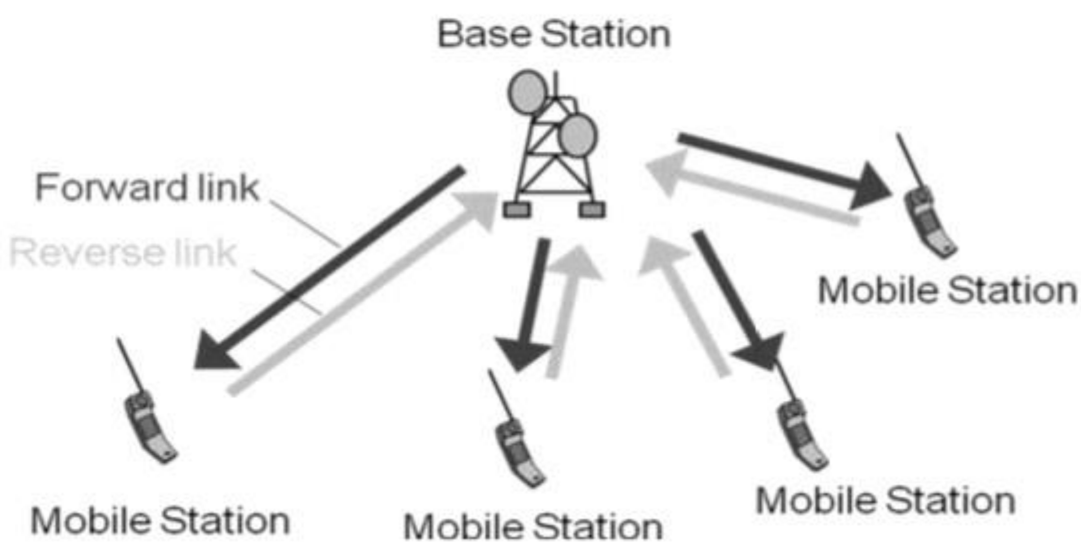
FDD also works on a cable where transmit and receive channels are given different parts of the cable spectrum, as in cable TV systems. And, filters are used to keep the channels separate.

Disadvantage of FDD

The drawback of FDD is that it does not allow special techniques like multiple antennas, multiple input-output (MIMO), and beamforming. These technologies are an essential element of the new strategies Long Term Evolution (LTE) 4G cell phone to increase the data rate. It is difficult to make broad enough bandwidth to cover both sets of antenna spectrum. Circuit complex dynamic adjustment is required.

Multiple Access Methods

The radio channel is a communication medium shared by several users in a geographic area. Mobile stations are in competition with one another for the frequency resource to transmit their information flow. Without other measures to control concurrent access of several users, collisions can occur. Since collisions are undesirable for connection oriented communication such as mobile phones, personal/mobile subscriber stations need to be allocated the dedicated channels on request.

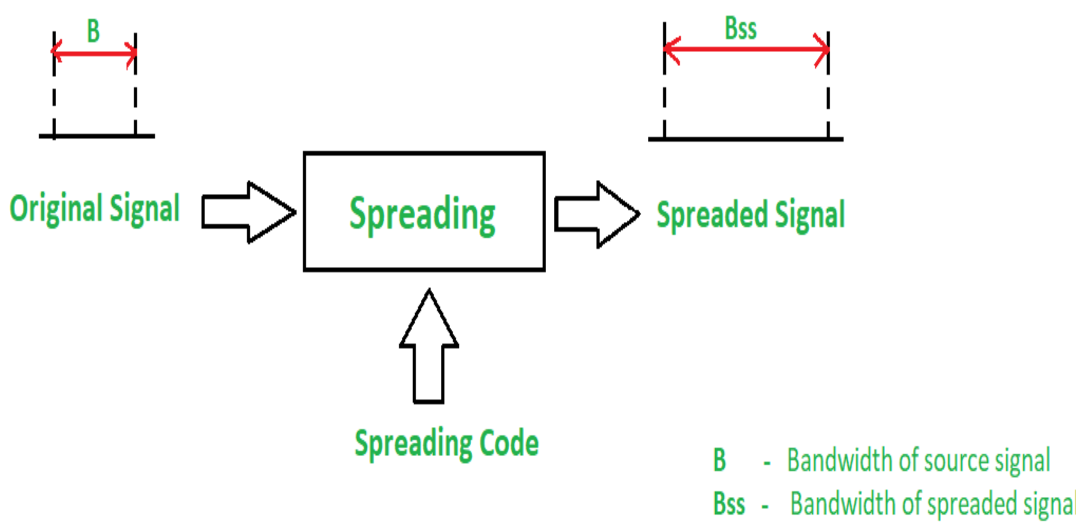


The mobile communication, sharing wireless resources on all users, must be communicated to identify the user. While identifying the user, it is referred to as "multiple access" (Multiple Access) that is receiving a radio wave of a number of transmitting stations in a receiving station (as shown in the following image).

What is Spread Spectrum?

The increasing demand for wireless communications has problems due to limited spectrum efficiency and multipath propagation. The use of spread spectrum communication has simplified these problems. In the spread spectrum, signals from different sources are combined to fit into **larger bandwidth**.

Most stations use air as the medium for communication, stations must be able to share the medium without an interception and without being subject to jamming from a malicious intruder. To achieve this, spread-spectrum techniques add redundancy means it uses **extended bandwidth** to accommodate signals in a protective envelope so that more secure transmission is possible. The spread code is a series of numbers that looks random but are actually a pattern. The original bandwidth of the signal gets **enlarged** (spread) through the spread code as shown in the figure.



Spread Spectrum

Principles of Spread Spectrum process:

1. To allow redundancy, it is necessary that the bandwidth allocated to each station should be much larger than needed.
2. The spreading process occurs after the signal is created by the source.

Conditions of Spread Spectrum are:

1. The spread spectrum is a type of modulation where modulated signal BW is much larger than the baseband signal BW i.e. spread spectrum is a wide band scheme.
2. A special code (pseudo noise) is used for spectrum spreading and the same code is to be used to despread the signal at the receiver.

Characteristics of the Spread Spectrum are:

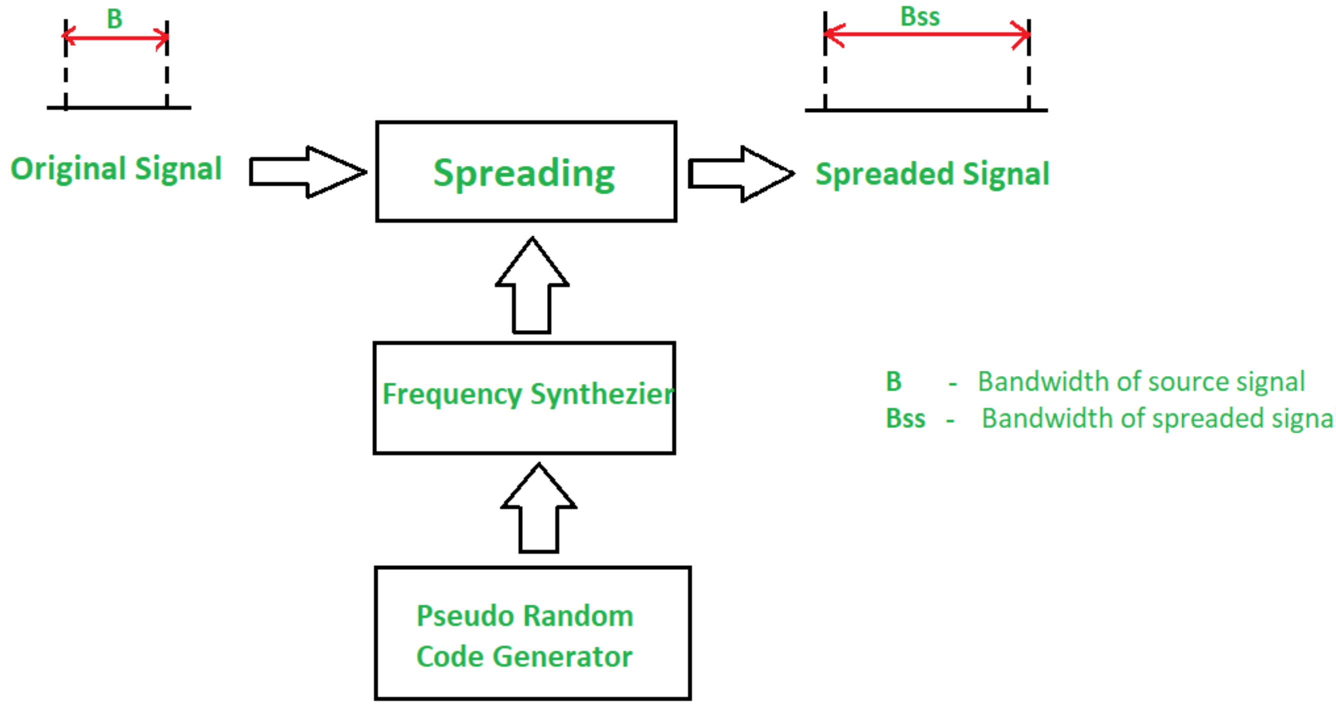
1. Higher channel capacity.
2. Ability to resist multipath propagation.
3. They cannot easily intercept any unauthorized person.
4. They are resistant to jamming.
5. The spread spectrum provides immunity to distortion due to multipath propagation.
6. The spread spectrum offers multiple access capabilities.

Two types of techniques for Spread Spectrum are:

1. Frequency Hopping Spread Spectrum (FHSS)
2. Direct Sequence Spread Spectrum (DSSS)

Frequency Hopping Spread Spectrum (FHSS):

In Frequency Hopping Spread Spectrum (FHSS), different carrier frequencies are modulated by the source signal i.e. M carrier frequencies are modulated by the signal. At one moment signal modulates one carrier frequency and at the subsequent moments, it modulates other carrier frequencies. The general block diagram of FHSS is shown in the below figure.



Frequency Hopping Spread Spectrum

A pseudorandom code generator generates Pseudo-random Noise of some pattern for each hopping period $\mathbf{T_h}$. The frequency corresponding to the pattern is used for the hopping period and is passed to the frequency synthesizer. The synthesizer generates a carrier signal of that frequency. The figure above shows the spread signal via FHSS.

Advantages of FHSS:

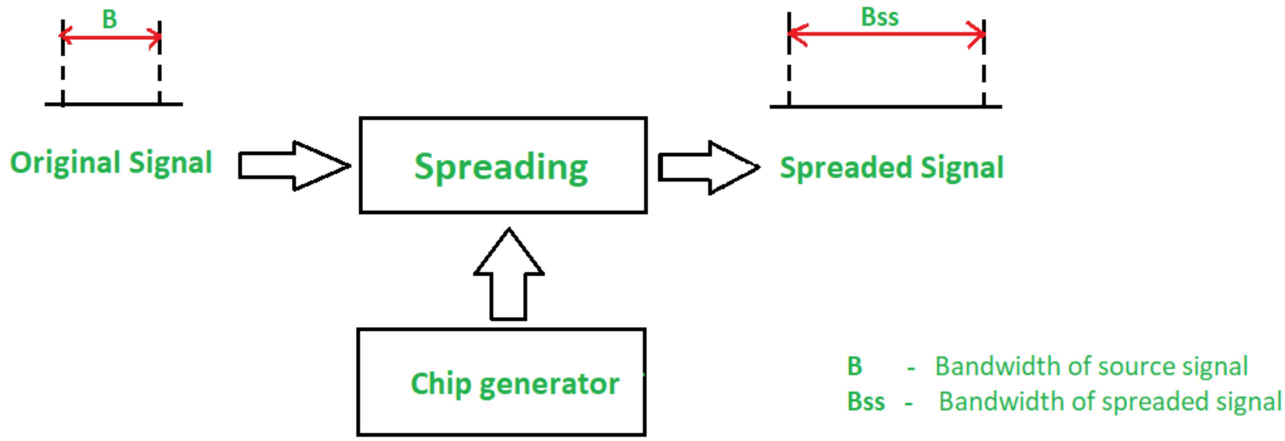
- Synchronization is not greatly dependent on distance.
- Processing Gain is higher than DSSS.

Disadvantages of FHSS:

- The bandwidth of the FHSS system is too large (in GHz).
- Complex and expensive Digital frequency synthesizers are required.

Direct Sequence Spread Spectrum (DSSS):

In DSSS, the bandwidth of the original signal is also expanded by a different technique. Here, each data bit is replaced with n bits using a spreading code called **chips,** and the bit rate of the chip is called as **chip-rate**. The chip rate is n times the bit rate of the original signal. The below Figure shows the DSSS block diagram.



Direct Sequence Spread Spectrum

In wireless LAN, the sequence with n = 11 is used. The original data is multiplied by **chips** (spreading code) to get the spread signal. The required bandwidth of the spread signal is 11 times larger than the bandwidth of the original signal.

Advantages of DSSS:

- The DSSS System combats the jamming most effectively.
- The performance of DSSS in presence of noise is superior to FHSS.
- Interference is minimized against the signals.

Disadvantages of DSSS:

- Processing Gain is lower than DSSS.
- Channel Bandwidth is less than FHSS.
- Synchronization is affected by the variable distance between the transmitter and receiver.

Types Of Attacks

Due to the massive architecture of a cellular network, there are a variety of attacks that the infrastructure is open to.

1. Denial Of Service (DOS): This is probably the most potent attack that can bring down the entire network infrastructure. This is caused by sending excessive data to the network, more than the network can handle, resulting in users being unable to access network resources.
2. Distributed Denial Of Service (DDOS): It might be difficult to launch a large scale DOS attack from a single host. A number of hosts can be used to launch an attack.
3. Channel Jamming: Channel jamming is a technique used by attackers to jam the wireless channel and therefore deny access to any legitimate users in the network.
4. Unauthorized Access: If a proper method of authentication is not deployed then an attacker can gain free access to a network and then can use it for services that he might not be authorized for.
5. Eavesdropping: If the traffic on the wireless link is not encrypted then an attacker can eavesdrop and intercept sensitive communication such as confidential calls, sensitive documents etc.
6. Message Forgery: If the communication channel is not secure, then an attacker can intercept messages in both directions and change the content without the users ever knowing.
7. Message Replay: Even if communication channel is secure, an attacker can intercept an encrypted message and then replay it back at a later time and the user might not know that the packet received is not the right one.
8. Man In The Middle Attack: An attacker can sit in between a cell phone and an access station and intercept messages in between them and change them.
9. Session Hijacking: A malicious user can highjack an already established session, and can act as a legitimate base station.

wireless networks are dependent on other private networks, which are managed by others, so after these issues, the users have less control of security procedures. These security issues are:

Denial of Service (DOS) attacks

The denial of services or DOS attacks is one of the most common attacks of all kinds of networks and especially in a wireless network. It prevents users from using network services because the attacker sends a large amount of unnecessary data or connection requests to the communication server. It causes a slow network, and therefore the users cannot get benefitted from using its service.

Traffic Analysis

Traffic analysis is used to identify and monitor communication between users. In this process, the service provider listens the traffic flowing in the wireless channel to access the private information of users affected by the attacker.

Eavesdropping

It specifies that the attacker can log on to the wireless network and access sensitive data if the wireless network was not secure enough. This can also be done if the information is not encrypted.

Session Interception and Messages Modification

It specifies that the attacker can intercept the session and modify the transmitted data in this session. This scenario is called "man in the middle." It inserts the attacker's host between the sender and receiver host.

Spoofing

In this security issue, the attacker impersonates him as an authorized account of another user and tries to access the sensitive data and unauthorized services.

Captured and Retransmitted Messages

In this security issue, the attacker can get some of the network services by getting unauthorized access. After capturing the message, he/she can reply to it with some modifications to the same destination or another.

PDC (Personal Digital Cellular)

Personal Digital Cellular (PDC) is a digital cellular telecommunications system that was primarily used in Japan. Developed in the 1990s, PDC was designed to offer improved voice quality and enhanced features compared to its predecessor, the analog cellular system. In this article, we will explore the key aspects of PDC, including its technical specifications, network architecture, and impact on the telecommunications industry.

PDC was introduced by the Japanese telecommunications company NTT DoCoMo in 1993 and quickly gained popularity in the country. It was based on the IS-95 standard, which was also used in the United States for the Code Division Multiple Access (CDMA) technology. PDC operated in the 800 MHz frequency band, providing efficient and reliable communication services to mobile phone users.

One of the main advantages of PDC over the analog cellular system was its ability to carry digital voice signals, resulting in improved call quality and reduced background noise. PDC utilized a speech coding algorithm called Adaptive Transform Coding (ATC), which compressed voice signals while maintaining acceptable audio quality. This compression allowed for more efficient use of network resources, enabling higher call capacity within the available frequency spectrum.

PDC also introduced several advanced features that enhanced the user experience. It supported Short Message Service (SMS) for text messaging, enabling users to send and receive text-based messages directly from their mobile phones. PDC also supported data services, allowing users to access basic internet services such as email and basic web browsing. While the data speeds were relatively slow compared to modern standards, it laid the foundation for the future development of mobile data technologies.

In terms of network architecture, PDC utilized a cellular network structure consisting of multiple base stations that provided coverage over specific geographic areas called cells. Each base station was equipped with antennas that transmitted and received signals from mobile devices within its coverage area. The base stations were interconnected through a wired network, allowing seamless communication across the entire PDC network.

To manage the allocation of network resources and ensure efficient call handling, PDC employed a system known as cell selection and handover. When a user moved from one cell to another while making a call, the system automatically transferred the call to a new base station without interrupting the conversation. This feature was critical in maintaining call quality and reducing dropped calls, especially when users were traveling or moving between different coverage areas.

PDC faced some challenges during its deployment and operation. One of the major limitations was its incompatibility with other cellular systems used globally. Since PDC operated on a unique frequency band and utilized different technical specifications, mobile phones designed for PDC were not compatible with networks outside of Japan. This limited the international roaming capabilities of PDC users and hindered its global adoption.

Another challenge was the rapid advancement of mobile technologies during the same period. While PDC provided significant improvements over the analog cellular system, it was soon overshadowed by the emergence of Global System for Mobile Communications (GSM) and its subsequent upgrades, such as General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE). These technologies offered higher data speeds, improved call quality, and global compatibility, eventually becoming the de facto standards for digital cellular communication worldwide.

Despite these challenges, PDC played a crucial role in the development of digital cellular technologies, particularly in Japan. It paved the way for subsequent generations of mobile networks, including 3G, 4G, and 5G, which brought significant advancements in data speeds, capacity, and multimedia capabilities.

WNS UNIT-4

Introduction to Wireless Data Networks: Cellular Digital Packet Data (CDPD), CDPD Architecture, CDPD Security, Mobitex- Mobitex Architecture, Mobitex Security Architecture, Security Issues, Gateway, Security Model Wireless Standards and Technologies: Current and Future Technologies-Infrared, Radio, Spread Spectrum, OFDM, Current and Future Standards- IEEE 802 Standards, ETSI, Home RF, Ultra-wide band Radio (UWB)

Introduction:

As we know AMPS (Advanced Mobile Phone System) cellular network has been developed for voice communication in 1980s. Due to long established setup times and modem handshaking requirement packet data communication was not supported by AMPS. In order to support packet data, CDPD has been introduced in 1993.

Cellular Digital Packet Data (CDPD) was developed by IBM (along with a consortium of Regional Bell Operating Companies) and other organizations to leverage the existing installed base of AMPS cellular equipment in the United States to provide low-cost, packet-switched data services. CDPD was first offered in 1994 by Bell Atlantic Mobile.

CDPD stands for Cellular Digital Packet Data. Though it has its own infrastructure it utilizes vacant AMPS assigned channels or gaps between the channels for packet communication. CDPD architecture is explained below. It co-exist with AMPS network architecture. Hence it supports both data and voice communication.

CDPD technology features:-

Following are the features of CDPD (Cellular Digital Packet Data).

• Communication between BS (Base station i.e. MDBS) and MS (i.e. M-ES) is full duplex.

• It utilizes or seizes 30 KHz channel from existing AMPS/GSM networks for transmitting data at 19.2 Kbps. The net data rate is 9.2 Kbps due to large amount of overhead.

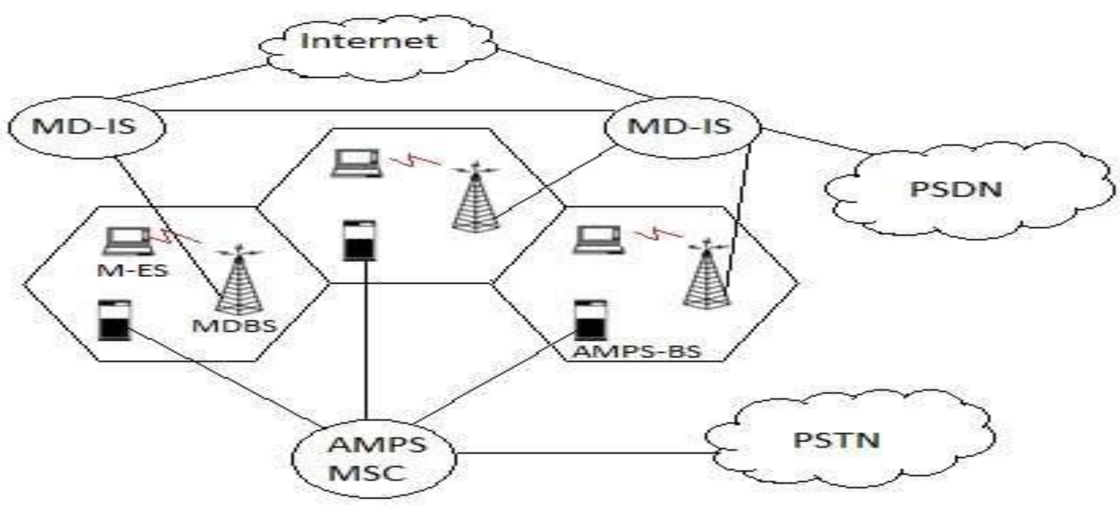
• It utilizes same frequency band as used by AMPS i.e. 824 MHz and 894 MHz for uplink and downlink. Both uplink and downlink are separated using FDMA.

• There are two types of handsets or phones available viz. single mode and dual mode. In single mode phone can initiate data call or voice call. In dual mode phone can switch between data call and voice call due to simultaneous registration on both AMPS and CDPD networks.

• It utilizes DSMA (Digital Sense Multiple Access) technique. In this technique CDPD mobile checks for flag bit in downlink channel which informs whether uplink slot is idle or busy. If idle, it utilizes for transmission. If busy, it waits for random period instead of transmitting in the next time slot.

• It supports different types of services and has access to internet backbone.

CDPD network architecture:-



CDPD Network Architecture

The figure depicts CDPD network architecture. As shown it consists three major system elements M-ES, MDBS and MD-IS. Moreover CDPD co-exist with AMPS network and hence will have fall back to AMPS for voice call. Figure shows AMPS-BS and AMPS-MSC which are part of AMPS network connected with PSTN for voice connectivity.

There are three CDPD interfaces viz. E-interface, I-interface and A-interface. E-interface exists between CDPD and fixed network external to CDPD. I-interface exists between two CDPD networks. A-interface exists between BS and MS. It is also known as Air interface.

Let us understand network elements used in CDPD architecture.

M-ES: It functions similar to subscriber or mobile unit used in any cellular system. It requires SIM for operation which can be housed in laptop, mobile or PDA. It interfaces with radio equipment at 19.2 Kbps. Each M-ES has unique NEI (Network Equipment Identifier) which is associated with its home MD-IS.

MDBS: It functions similar to Base Station. It broadcasts available channels for M-ES. It takes care of radio activities such as channel allocation, usage etc. These MDBSs co-exist with AMPS Base Stations and hence share the same antenna and site together.

MD-IS: It provides connectivity with internet and PSDN. It has functionalities of both frame relay switch and packet router. It does buffering of packets routed for M-ES. It also supports roaming management as it contains registration directory.

How CDPD Works:-

Cellular Digital Packet Data makes use of idle times between calls in cellular phone network channels for interleaving packets of digital data. In other words, CDPD makes use of the «bursty» nature of typical voice transmission on the AMPS cellular system. Voice communication has gaps or pauses where packet data can be inserted and transmitted without interfering with the communication taking place between customers.

Although CDPD supports data transmission rates of 19.2 Kbps and higher, actual data throughput is usually around 9.6 Kbps. This is because of the large overhead added by CDPD to each data block transmitted. This overhead is designed to ensure that communications are reliable and to maintain synchronization between the modems at each end of the transmission. In addition, a color code is added to every data block to detect interference resulting from transmissions on the same channel from neighboring cell sites.

CDPD uses the Reed-Solomon forward-error-correcting code to encode each block or burst of data sent, and includes built-in RC4 encryption to ensure security and privacy of the transmitted data. CDPD is also based on the industry standard Internet Protocol (IP), allowing data to be transmitted to and from the Internet.

A typical implementation of CDPD consists of three components:

- **Mobile-End System (M-ES):** A user device such as a laptop equipped with a cellular modem. This system communicates in full-duplex mode with a Mobile Data Base Station (MDBS) using the Digital Sense Multiple Access protocol, which prevents collisions of data streams from multiple Mobile-End Systems.
- **Mobile Data Base Station (MDBS):** A telco device for receiving and transmitting CDPD data.
- **Mobile Data Intermediate System (MDIS):** Provides the central control for a CDPD network.

CDPD is typically used to provide wireless access to public packet-switched networks such as the Internet so that mobile users can access their e-mail and other services. Multiple users can share the same channel; the user's modem determines which packets are destined for the user's machine. CDPD also supports IP multicasting and is an open standard based on the Open Systems Interconnection (OSI) reference model for networking.

CDPD advantages and disadvantages:-

Following are the advantages of CDPD:

• Utilizes existing channels of the AMPS network and hence easy to install and start using the existing channels if not in use.

• It has cellular like architecture and hence can support larger capacity due to ease in upgrading the network.

• There is no delay in establishing data call as CDPD phone is already registered with the CDPD network.

Following are the disadvantages of CDPD:

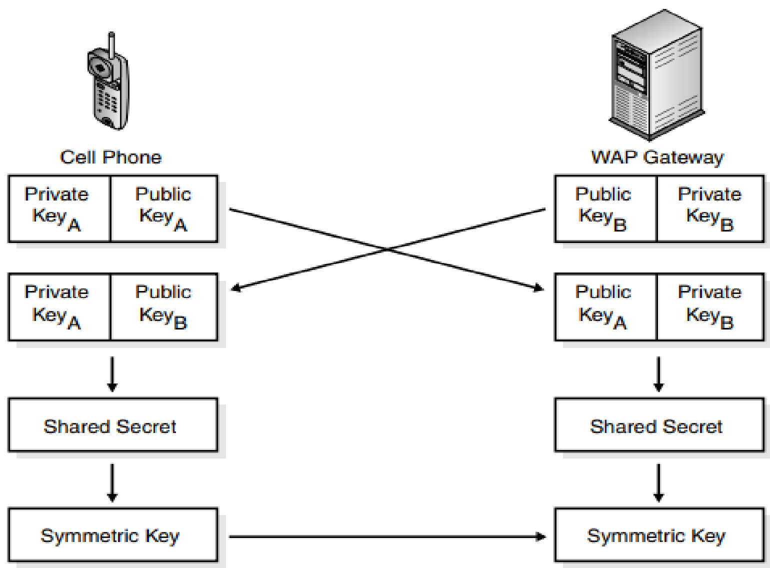
• There is no mesh connectivity in CDPD. Hence M-ES and M-ES can not communicate directly. Communication between them occurs via MDBS.

• CDPD cell size is limited to less than 10 miles.

CDPD Security:-

- The security requirements of CDPD are similar to those of a wireless voice network.
- CDPD devices are programmed at the time of manufacture with a unique numeric value called the Network Entity Identifier (NEI)
- The value is stored in the memory of the CDPD device and is used to authenticate the device on the CDPD network.
- The CDPD security architecture differs from a voice network in one significant manner. Whereas as a voice network utilizes a challenge response protocol over an unencrypted channel, CDPD establishes an encrypted channel first before progressing with authentication.
- This authentication is based on a widely used security protocol called the Diffie-Hellman key exchange. Diffie Hellman is not a mechanism that encrypts data, but is a mechanism that enables two unknown parties to exchange private keys that can be used to encrypt data.
- This makes Diffie-Hellman ideally suited for the CDPD architecture. Because the Diffie-Hellman protocol is used in some WAP implementations.
- In an asymmetric system, each party has a private and public key. In the protocol, the device sends its public key to the network, and vice versa. Because the keys are public, they can be transmitted over an insecure link. Each party now combines its private key with the received public key.
- Through this mechanism, each party can generate a secret session key that can be utilized for establishing an encrypted session.

- There are two issues worth knowing about the Diffie-Hellman protocol. First, Diffie-Hellman does not authenticate the participants; it merely establishes a session key between two parties. For this reason, Diffie Hellman is susceptible to a so-called man-in-the-middle attack.
- In this attack, an intermediate party intercepts the device's public key during transmission, replaces it with a different public key, and sends that value to the intended recipient. The intermediary conducts the same process with the recipient's public key.
- Through this process, the intermediary can then decrypt and read all traffic. There is protection against man in-the-middle attacks in the Diffie-Hellman key exchange; however, this protection typically requires the use of a more elaborate public key infrastructure (PKI) architecture.
- Getting back to the topic of CDPD, once the Diffie-Hellman protocol has been completed, the M-ES and MD-IS create two ciphering keys. Because Diffie-Hellman has provided each party with the same shared secret, that secret can be utilized to generate a symmetric key.
- All CDPD encryption utilizes a variable key size stream cipher called RC4. To authenticate itself to the CDPD network, the mobile device transmits its NEI along with some additional unique identifiers to the MD-IS. The MD-IS forwards this information to an authentication server that compares the results, if the results match, the device is authenticated and allowed onto the network. As an additional level of security, the CDPD devices utilize something called a shared history record (SHR).



Mobitex:-

- Mobitex is a wireless data technology developed by Ericsson in the mid 1980.
- All Mobitex networks operate in one of four frequency families: 80 MHz, 400 MHz, 800 MHz, or 900 MHz.
- Mobitex is a packet-based switching technology and is capable of throughput rates of up to 8 Kbps. Mobitex data is transmitted in 512-byte blocks.

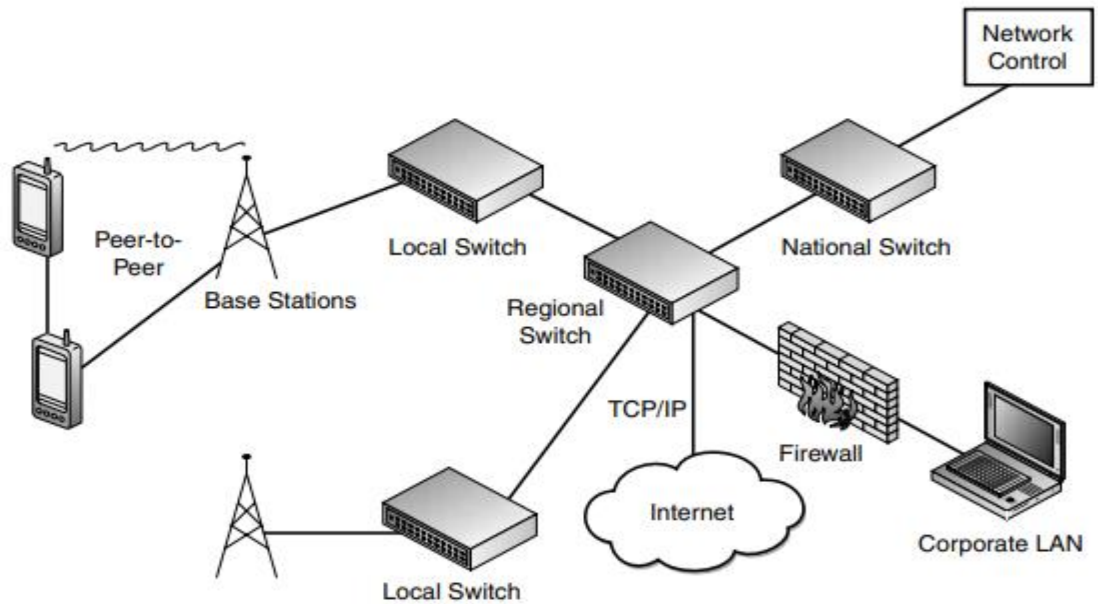
Mobitex Architecture:-

- The design of Mobitex networks is similar to traditional cellular voice networks. Each Mobitex hand-held device connects to a base station, which in turn connects to a local switch.
- The local switch connects to the Mobitex operator's network backbone, but it can also connect to external networks (such as a corporate local area network [LAN] or gateway).
- In addition to the local switches, Mobitex networks utilize regional switches (which control a set of local switches) as well as a Network Control Center (NCC), which handles billing, monitors usage, and oversees network performance.

- One unique feature of Mobitex is its capability to offer peer-to-peer communication between two Mobitex devices. With peer-to-peer communication, two devices communicate without engaging the entire Mobitex network infrastructure.
- the base station coordinates all the communication and then ultimately forwards the activity back to the NCC.
- The main advantage of this approach is that it minimizes the back-haul network traffic.

Mobitex Security Architecture:-

- The Mobitex security architecture is quite similar to other wireless data networks. The main difference is that the Mobitex security specifications are not widely published and have not been subjected to the same level of scrutiny as other standards.
- The same general authentication principles that are used in cellular networks are used in Mobitex. Each Mobitex device contains a unique serial number and another value called the Mobitex Access Number
- These values are stored locally in the Mobitex hand-held device and are transmitted over the air to the base station where they are forwarded onto the NCC for authentication.
- Mobitex is a packet-based network, it is possible to utilize some of the security features available in wired networks to encrypt data at the application layer.
- This exchange is then used to create a pair of DES-X keys (a variant of the Data Encryption Standard [DES]) that can be used to establish an encrypted session between the device and the network.
- GPRS is based on the same fundamental GSM security architecture, GPRS introduces several new security threats that have to be considered and for which appropriate countermeasures must be created.



Security Issues:-

- GPRS is based on the same fundamental GSM security architecture, GPRS introduces several new security threats that have to be considered and for which appropriate counter measures must be created.
- The single biggest security threat to GPRS is the network's connection to public networks (such as the Internet) means that wireless networks are susceptible to attack from the back end. Previous wireless voice-only networks were closed networks, making access to them considerably harder. This means that operators must take added measures to protect the connection between the GPRS gateway (GGSN) and the Internet.
- Another significant development is that GPRS is packet and IP based. This means that GPRS is now susceptible to some of the same security threats facing the wired Internet, including the following:

    i. **Denial of service (DoS):-** This attack consists of sending thousands or millions of simultaneous requests to an individual web server. These requests overwhelm the web server and it crashes, making it unable to provide service to valid users (hence, DoS). In GPRS, it is theoretically possible to launch a DoS attack against the GGSN (thereby stopping all GPRSs for all subscribers) or even against an individual mobile phone to prevent it from operating.

ii. **IP address spoofing:-** In this attack, a hacker successfully determines the valid numeric IP address for a given web site. The hacker can then create data packets that appear genuine and send them to unsuspecting users. Because the subscriber cannot tell if the content has been hijacked, hackers can use this attack to retrieve passwords, credit-card numbers, and other sensitive data from users.

WAP Gateway:-

- WAP(Wireless Application Protocol) is not a wireless standard like GPRS or CDPD (in fact, it can operate over most network interfaces), WAP is another important component to wireless data services.
- The WAP primary goal was to develop a common architecture for accessing the wireless Internet and collectively promote the benefits of WAP. Although the WAP worked on developing a series of technical specifications starting with WAP v1.0 in early 1998.
- The WAP gateway serves as the central interface to the Internet. All requests and data from the wireless devices must pass through the WAP gateway before proceeding onto the Internet.
- The WAP gateway was always managed and maintained by the network operator. Depending on the subscriber base, an operator might utilize multiple WAP gateways for load balancing.
- The WAP gateway serves several key functions:-

  i. **Protocol converter:-**Converts WAP protocols (such as the Wireless Data Protocol [WDP] and Wireless Transport Layer Security [WTLS]) to wired protocols (like TCP and TLS).

ii. **Content converter:-** Translates HTML web pages into WML compatible content.

iii. **Performance optimization and overhead reduction :-** Given the low bandwidth and throughput of the phone, the WAP gateway's routines are designed to compress data as much as possible and minimize the number of roundtrips that must take place between the client and the gateway.

- When a WAP gateway receives a request for content from a WAP device, the WAP gateway will translate that request into HTTP and retrieve the content from the original web server. Although the WAP gateway is capable of converting HTML to WML dynamically, in most WAP implementations, the content provider creates a subset of data in the WML format.
- Given WML's interoperability with HTML, this is not an enormous task, but it does point out that some effort must be expended to enable existing web content for wireless device.

WAP Security Model:-

- The WAP security layer is different from the wired world. Rather than relying on the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol, the WAP specification adopted WTLS.
- This protocol was designed to provide authentication, data encryption, and privacy for WAP users. WTLS was included in the WAP 1.1 specification.
- Traditional SSL is not suitable for wireless networks primarily for performance reasons. SSL works fine in a PC world where the client PC has significant processing power, ample battery supply, and a relatively fast connection to the web server. A WAP device has none of these features, which explains the reason for developing WTLS.
- The WAP specification also created a WMLScript function called SignText that provides capabilities for providing digital signatures on WAP devices.

- SignText-compliant products are just being introduced into the market, the SignText capability will add significant value to existing WAP environments by providing a level of nonrepudiation that can be used for security-sensitive transactions.
- The WAP specification introduces three different classes of authentication:-
    i. Class 1 authentication is anonymous. Neither client nor gateway can authenticate each other.
    ii. Class 2 authentication is server authentication only. This is equivalent to shopping over a SSL link from a wired browser. The SSL protocol authenticates the server (so that the user knows it really is the corporation's web site).
    iii. Class 3 authentication is both client and server authentication. This requires the use of a PKI(Public Key Infrastructure)
- Although Class 3-capable devices introduce the possibility of a true wireless public key infrastructure (WPKI), they also introduce a whole host of unresolved business issues.
- Specifically, in Class 3 devices, the critical issue is how the user's public/private key is going to be managed, installed, supported, and so on.
- Again, the WTLS protocol specified a process to minimize the amount of communication required between the client and server. The Class 2 authentication process completes itself in four steps:
    1. The WAP device sends a request to the WAP gateway.
    2. The gateway responds and sends a copy of its certificate (containing the gateway's public key) to the WAP device.
    3. The WAP device retrieves the certificate and public key, generates a unique random value, and encrypts it with the gateway's public key.
    4. The WAP gateway receives the encrypted value and decrypts it with its corresponding private key.

- Unfortunately, the WTLS protocol only encrypts data from the WAP device to the WAP gateway. From the WAP gateway to the content web server, information is transmitted over standard SSL. Because the data must be converted from WTLS to SSL, there is a brief millisecond in time when data is unencrypted on the gateway.
- This brief millisecond soon became known as the WAP Gap. Even though the practical risks of this gap were extremely minor, the press and analysts used the gap to proclaim that WAP was insecure.

Wireless Standards and Technologies:-

Current and Future Technologies:-

- Currently, wireless technologies use either radio or light waves to move information from one point to another. Most of us have been wireless users for years with our mobile/cordless phones and television remote controls.
- However, wireless technologies continue to evolve. For example, mobile phones, the veterans of the wireless world, are beginning to delve into the world of data transmission. Let's look at the basics of how these technologies work.
- **Infrared:-**
  - **i.** Infrared radiation (IR) involves electromagnetic waves in the spectrum just below visible light. Being close to visible light lends infrared a number of the same properties that visible light has.
  - **ii.** For example, like light waves, infrared travels in straight lines and bounces off objects, but it cannot penetrate physical or opaque objects. Data can be transmitted over infrared in much the same way that light is used to transmit data in fiber optics—by pulsing it (turning it on or off)
  - **iii.** This is the same type of technology used in many remote control units for TVs, VCRs, and so on.

- **Radio:-**
    i. Radio is the use of electromagnetic waves that are emitted when an alternating current is input to an antenna. This can be used to transmit data invisibly through the air to devices such as radios, televisions, and mobile phones
    ii. Radio is the most widely used technology for wireless communications. As with anything good, only a limited amount of usable radio frequencies is available, and radio is used in an almost endless number of ways in today's world.
    iii. Many of the frequencies in the radio spectrum require a license. Some frequencies allocated in the radio spectrum have been made available for use without a license.
    iv. One of these groups of unlicensed frequencies is known as the industrial, scientific, and medical (ISM) band because it is allocated for use by the industrial, scientific, and medical fields.
    v. Specific allocation of radio frequencies for wireless LAN use, radio frequency availability is still limited. Therefore, a number of interesting ways to fit more data into the existing available frequencies have come into use.
    vi. Some of these include the use of spread spectrum techniques and Orthogonal Frequency Division Multiplexing (OFDM).
- **Spread Spectrum:-**
    i. Spread spectrum refers to the method of dividing data and sending it over a "spread" or wideband of different frequencies.
    ii. Spread spectrum signals use multiple frequencies (wideband) and appear to be radio noise to narrowband devices
    iii. This kind of noise can be easily filtered out, which is what enables the coexistence of narrowband devices.

iv. Some common spread spectrum methods are frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS).

v. In FHSS systems, the transmitter and the receiver hop from one frequency to another in prearranged synchronized patterns. The hops occur frequently with very little time being spent on any one frequency. This reduces the possibility of interference with other devices and enables several overlapping FHSS systems to be operational at the same time.

vi. DSSS pushes data through a binary encoding process that spreads the data by combining it with a multibit pattern or pseudo-noise code. The resulting data is now somewhat hidden and inflated. For example, if the bit pattern is 11 bits long (which is typical for most DSSS wireless applications), then 1 bit of data would now be 11 bits long. This data is modulated and then sent out over multiple frequencies (which typically consist of about 22 MHz of bandwidth) at the same time. Since the original data bit was encoded into 11 bits, the data is more resilient to air loss because the data has a tremendous amount of redundancy.

- **OFDM:-**

i. OFDM is a multicarrier modulation method that divides a communications channel into a number of equally spaced frequency bands. Each band is then used to transmit a portion of the user information.

ii. Each band is independent of, or orthogonal, to every other band. This multicarrier approach also reduces multipath problems where the reflected radio signals bounce back from different sources with slightly different timing.

iii. At the same time, it increases the performance and data throughput.

Current and Future Standards:-

- A number of standard-setting organizations exist, but the two that are having the most impact on wireless technologies are the Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standards Institute (ETSI).

IEEE 802 Standards:-

The IEEE (www.ieee.org) develops standards in a wide range of electrical/electronic fields. The 802 Local and Metropolitan Area Networks Standards Committee (LMSC) of the IEEE Computer Society defines specifications related to LANs.

IEEE Standard	Description
IEEE 802	For LAN/MAN networks
IEEE 802.1	Standards for LAN/MAN management and bridging and remote media access control bridging.
IEEE 802.2	For Logical Link Control connectivity.
IEEE 802.3	Standards for CSMA/CD.
IEEE 802.4	Standards for the token passing bus access.
IEEE 802.5	For communication between LAN and MAN, and standard for token ring access.
IEEE 802.6	For exchanging information between systems
IEEE 802.7	For broadband LAN cable
IEEE 802.8	For Fiber-optic connection
IEEE 802.9	For integrated services, like voice-over video, etc.

IEEE 802.10	For security implementation in LAN/MAN
IEEE 802.11	For WiFi or Wireless Networking
IEEE 802.12	For demand Priority Access Method
IEEE 802.14	For Cable TV broadband communications
IEEE 802.15.2	For Bluetooth and Wifi co-existence mechanism
IEEE 802.15.4	For Wireless Sensors or Control Systems
IEEE 802.15.6	For Wireless Body Area Network, like Bluetooth low energy
IEEE 802.16	For Wireless Network connectivity, like WiMax
IEEE 802. 24	To facilitate collaboration and coordination among all IEEE 802 standards

802.11:-

- IEEE 802.11 standard, popularly known as **WiFi**, lays down the architecture and specifications of wireless **LANs** (**WLANs**). WiFi or WLAN uses high frequency radio waves for connecting the nodes.
- There are several standards of IEEE 802.11 WLANs. The prominent among them are 802.11, 802.11a, 802.11b, 802.11g, 802.11n and 802.11p. All the standards use carrier-sense multiple access with collision avoidance (CSMA/CA).
- IEEE 802.11 was the original version released in 1997. It provided 1 Mbps or 2 Mbps data rate in the 2.4 GHz band and used either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS). It is obsolete now.

a) IEEE 802.11a:-

- 802.11a was published in 1999 as a modification to 802.11, with orthogonal frequency division multiplexing (OFDM) based air interface in physical layer instead of FHSS or DSSS of 802.11.

- It provides a maximum data rate of 54 Mbps operating in the 5 GHz band. Besides it provides error correcting code.
- As 2.4 GHz band is crowded, relatively sparsely used 5 GHz imparts additional advantage to 802.11a.

b) <u>IEEE 802.11b:-</u>

- 802.11b is a direct extension of the original 802.11 standard that appeared in early 2000. It uses the same modulation technique as 802.11, i.e. DSSS and operates in the 2.4 GHz band.
- It has a higher data rate of 11 Mbps as compared to 2 Mbps of 802.11, due to which it was rapidly adopted in wireless LANs.
- However, since 2.4 GHz band is pretty crowded, 802.11b devices faces interference from other devices.

c) <u>IEEE 802.11g:-</u>

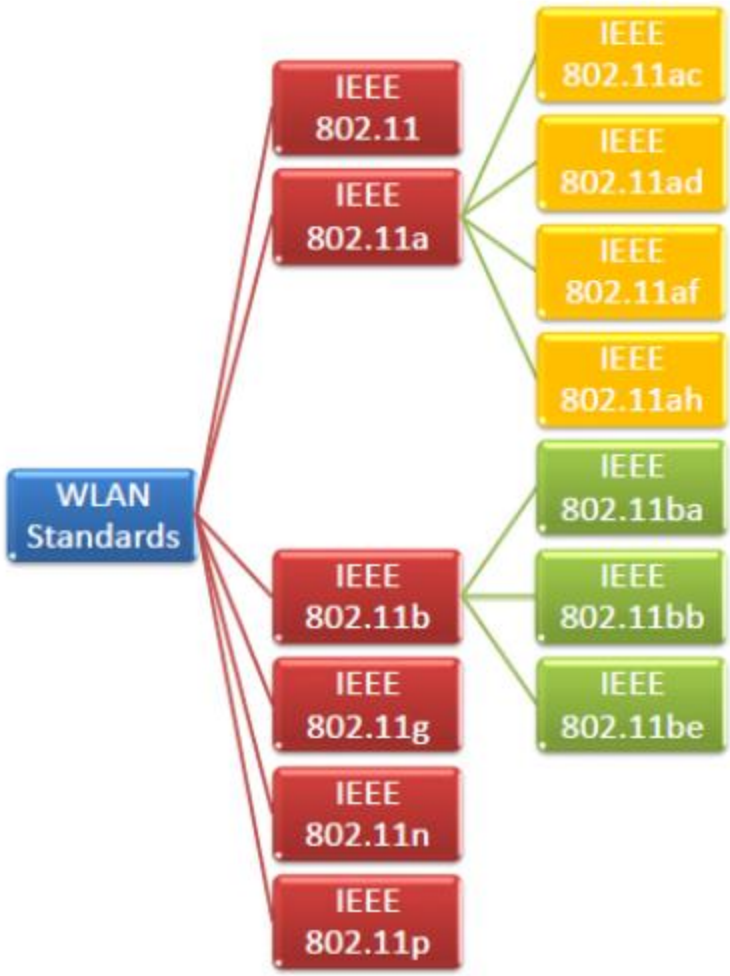
- 802.11g was indorsed in 2003. It operates in the 2.4 GHz band (as in 802.11b) and provides a average throughput of 22 Mbps. It uses OFDM technique (as in 802.11a).
- It is fully backward compatible with 802.11b. 802.11g devices also faces interference from other devices operating in 2.4 GHz band.

d) <u>IEEE 802.11n:-</u>

- 802.11n was approved and published in 2009 that operates on both the 2.4 GHz and the 5 GHz bands. It has variable data rate ranging from 54 Mbps to 600 Mbps.
- It provides a marked improvement over previous standards 802.11 by incorporating multiple-input multiple-output antennas (MIMO antennas).

e) <u>IEEE 802.11p:-</u>

- 802.11 is an amendment for including wireless access in vehicular environments (WAVE) to support Intelligent Transportation Systems (ITS).
- They include network communications between vehicles moving at high speed and the environment. They have a data rate of 27 Mbps and operate in 5.9 GHz band.



Advantages:-

1. The data communication system is faster than the speed of transportation.
2. Multi-path propagation increases the transmission rate and reduces error incidence.
3. Manually fix the modulation used by the transmission.
4. Developing standards for the computer and electronic industry.
5. It is a non-profit professional association and works for the benefit of Humanity.

Disadvantages:-

1. It requires periodic maintenance.
2. Network security needs to stay secure.
3. It has unauthorized use.

ETSI:-

- ETSI stands for European Telecommunications Standards Institute.
- ETSI (www.etsi.org) is the European counterpart to IEEE.
- **HiperLAN/1:-**
  1. In 1991, ETSI formed the Subtechnical Committee RES10 to develop a HiperLAN. The resulting standard was the HiperLAN/1 standard (approved in 1996) and defines the PHY and MAC specifications for wireless high-speed communications
  2. HiperLAN/1 uses gaussian minimum shift keying (GMSK) and specifies data rates of up to 20 Mbps between portable devices.
  3. One advantage of HiperLAN/1 is that it works in a dedicated bandwidth (5.1 to 5.3 GHz, which is allocated only in Europe) so it doesn't have to use spread spectrum technologies in order to coexist with other radio usage as is the case in the 2.4 GHz ISM range.
  4. Also, the protocol uses a variant of CSMA/CA and includes optional encryption and power savings.
  5. Another nice feature of HiperLAN/1 is ad-hoc routing. For example, if your destination is out of reach, intermediate nodes will automatically forward it through the best route within the HiperLAN/1 network (the routes are automatically recalculated regularly).

- **HiperLAN/2:-**
  1. In 1997, ETSI formed the Broadband Radio Area Network (BRAN) group to work on HiperLAN/2.HiperLAN/2 is a redesign of HiperLAN/1 and was the first standard to use OFDM.
  2. HiperLAN/2 and IEEE 802.11a are similar in their use of the 5 GHz band and OFDM to attain data rates as high as 54 Mbps. However, a key

difference between the two standards is in the MAC portion of the systems.

iii. HiperLAN/2 uses Time Division Multiplexing (TDM),whereas 802.11a/g use CSMA/CD. Because of this, HiperLAN/2 can provide QoS, while IEEE 802.11a does not currently include it.

iv. HiperLAN/2 is regarded as wireless Asynchronous Transfer Mode (ATM).

v. It is possible that a joint standard may exist between ETSI and IEEE because a joint project, referred to as the 5 GHz Unified Protocol (5-UP) project, is currently being worked on.

vi. The objective of the project is to provide a single universal standard in the 5 GHz range for wireless LANs

HomeRF:-

- HomeRF (www.homerf.org) is a label for a group of manufacturers that came together in 1998 to develop a standard for wireless connectivity between personal computers and electronic devices.
- The standard that resulted is the Shared Wireless Access Protocol (SWAP), which allows for voice and data transmission with data rates of up to 1.6 Mbps.
- Targeting the home market, the premise behind HomeRF was that 802.11 devices would be too costly and complicated for home/consumer markets.
- HomeRF is working on SWAP 2.0, which will use wideband frequency hopping (WBFH) to increase the data rate of the standard.
- It is also trying to differentiate HomeRF from the other wireless standards by promoting it as a standard for wireless communication between not just data but also voice and multimedia devices.

Ultrawideband Radio (UWB):-

- The FCC approved the use of ultrawideband (UWB) radio in the 3.1 through 10.6 GHz band, opening the way for the use of radio impulse technology in wireless LANs.
- Instead of traditional sine waves, UWB radio broadcasts digital pulses that are timed very precisely on a signal across a very wide spectrum at the same time.
- The transmitter and receiver must be coordinated to send and receive pulses with an accuracy of trillionths of a second. This actually sidesteps the multipath issues typically associated with radio signals.
- With the current power restrictions mandated by the FCC, UWB signals appear as radio noise to other frequency users. This is why UWB has been approved for use in the 3.1 to 10.6 GHz range.
- UWB also has a low power consumption, making this a very desirable technology for many portable wireless applications.

UNIT V:

Wireless Deployment Strategies: Implementing Wireless LAN's- Security Considerations Common Wireless Network Applications, Enterprise Campus Designs, Wireless IST Design, Retail and Manufacturing Design, Small Office/Home Office Design (SOHO)

Implementing wireless LAN's- Security Considerations:

To properly understand and counter the risks, the functional goals of the wireless network must be fully understood. We will explore the security considerations that should be applied to different layers of the wireless network— namely, the physical, network, and application layers. The physical section will cover radio frequency (RF) coverage, equipment placement, and building construction. The network section will cover the general network architecture, wireless local area network (LAN) medium access protections, and mobility and virtual private network (VPN) considerations. The application section will cover application communications tunnelling encryption.

Common Wireless Network Applications:

We examine the various common network configurations where wireless Ethernet is deployed. Many companies use wireless Ethernet as a drop-in replacement for Ethernet when mobility is needed or when wiring is difficult or impossible. Some historic buildings are very limited in wiring possibilities so wireless Ethernet is the only option for network connectivity. Another common way to bridge networks over short distances between buildings is to use a wireless bridge and directional antennae.

Wireless Internet service providers (ISPs) generally provide last-mile wireless access to fixed-point locations to either a home or business. This configuration is called point-to-multipoint, where the customers connect to the ISP upstream access point via a client adapter at the customer premises. Because the network is not designed with mobility in mind, it operates similarly to point-to-point configuration, differing only in that multiple clients can connect to one access point. The last two scenarios involve client roaming between access points. Roaming occurs because the wireless user moves out of range from the access point that was providing network services.

As the client moves out of range, the link deteriorates and is eventually lost because no other access point is in the vicinity. When the existing link begins to deteriorate, the client may also search for another access point to roam to. The roaming process drops the existing Transmission Control Protocol (TCP) connection and requires a new network connection upon association with the new access point. This leaves the wireless network designer with the problem of maintaining the TCP state during network disassociation and reassociation. Networks that permit roaming are often large and cover vast distances. When designed poorly, they can be a network administrator's nightmare.

However, if designed with security and performance in mind, the administrator will be rewarded with a high-performance, dynamic wireless environment that can also facilitate wireless network incident response.

Physical Security Considerations:

Good security engineering examines the problem from all angles, and when building a wireless network, you must begin at the physical layer. Control over the wireless coverage will reward the administrator with fewer headaches down the road. Understanding the boundaries of your network makes network incident response a less daunting task and can actually lead to better network performance. Key points on infrastructure placement also assist the designer and implementer in successfully deploying a wireless network that eliminates areas without coverage and focuses radio signals into needed areas.

Site Survey

A site survey is used to determine the physical environment in which a wireless LAN is installed. The site survey has two components: the physical walkthrough and the signal strength and access point placement evaluation. Having a site plan for the building or area that will be surveyed is recommended, but it is not always needed. During the physical walkthrough, the engineer takes note of the surrounding areas and the obstacles that need to be overcome. For example, dense vegetation, out buildings, large metal objects, large open distances, and building construction must all be noted. The buildings must be carefully evaluated. Outer- and inner-wall construction, window treatments, and window glass material must all be identified and considered when determining the placement of the access point and antenna.

The second component of the site survey is performed with access points and a roaming wireless client. An access point is installed in a potential service location and the wireless client is walked around while the user monitors the signal strength. Network coverage is evaluated and fine-tuned for optimal performance and security. A proper design for directional antennae occurs in this phase. After the general coverage is determined, the overall signal strength of the access point can be adjusted to contain wireless network exposure inside a controllable range.

Equipment Placement

You should follow several guidelines when deploying equipment in the field:

- Ensure that the access point is installed out of the normal reach of employees. Where possible, conceal the access point from sight.
- If the access point is installed outdoors, make sure the equipment is properly secured, discouraging tampering.
- When appropriate, sector network areas with directional antennae. This places RF where you intend it to be. It also quantifies areas where users are when connected to that cell. This is very useful when tracking down problems or running through incidence-response procedures.
- Name the access points so that they can be tracked down easily during frantic troubleshooting events.

Once the access points are in the best possible configuration, you should perform a perimeter sweep to ensure that excess radiation isn’t bleeding into unintended areas. Most access points designed for corporate and enterprise use have an adjustable power output and can be trimmed down to remove excess bleeding.

RF Containment

The objective of RF containment is to attenuate or limit the scope of your network within the known boundaries. This is very important in large networks where roaming is necessary, but it also deprives would-be attackers from detecting the network or certain portions of the network, which lowers your drive-by profile. When combined with directional antennae, it also normally has a performance benefit.

In addition to attenuating the transmit power on the access point, you can also perform the following physical tasks to limit the amount of RF bleed out of buildings and rooms. When designing a new facility, specific rooms can be designed to prevent the leakage of excessive RF energy by installing metallic film or foil under the drywall. Metallic paint can also be applied to walls to add a layer of attenuation. Metallic window blinds provide better attenuation over cloth or plastic blinds. These simple details may result in the difference between a wireless perimeter extending tens of feet from the intended area to hundreds of feet.

Network Security Considerations:

The needs of the enterprise drive the majority of the network architecture, and security and performance must be considered from the onset of the project. In the following sections, we will discuss the major wireless network scenarios, provide best practices, and share some thoughts on how you would build a network to meet your goals in a secure manner.

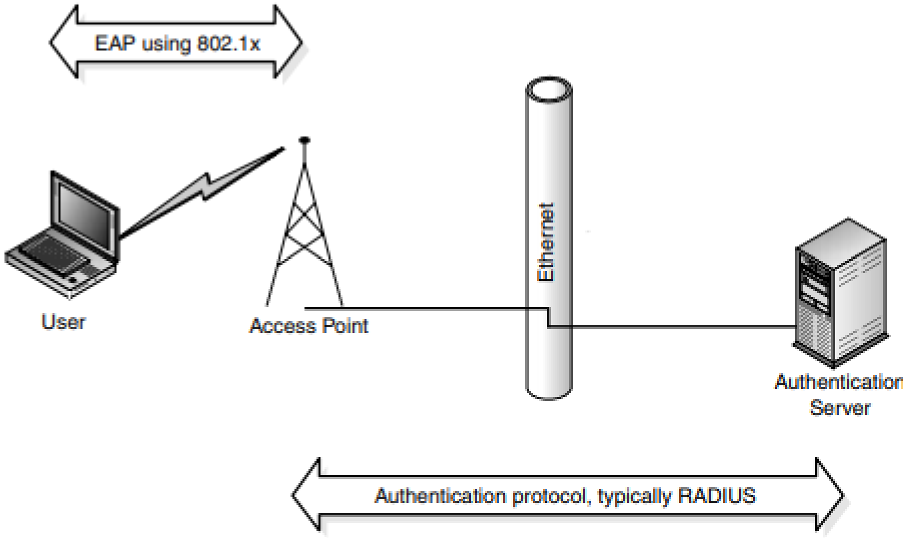
The general consensus is to treat all wireless networks as untrusted anonymous hosts just like the traffic originating on the Internet. Access is granted once the host successfully presents the qualifying credentials to an authentication server and all communications travel over an encrypted tunnel between the two systems. This still holds true to a point, but, when possible, you should segment the networks in order to minimize physical layer denial of service (DoS) attacks to shield critical networks from the external threats. As stated before, segmenting can also significantly assist in incident-response activities.

Segmenting off administrative communications channels is difficult with access points because the administrative interfaces are often limited to the Ethernet port. Some access points have out-of-band management through a serial port, but that can also be difficult to manage in large distributed networks; however, it is the only secure method. Most access points do not allow you to push configurations across many access points through the serial interface, but you can usually do it over the Ethernet or wireless interface. If possible, configuration capabilities over the wireless interface should be disabled to prevent attackers from tampering with the configuration. Management of the access point should be considered when choosing a brand of access point. Telnet, cleartext Hypertext Transfer Protocol (HTTP), and unencrypted Simple Network Management Protocol (SNMP) should be avoided. Instead, try using Secure Shell (SSH) or Secure Sockets Layer (SSL) for managing network devices. Some terminal servers with SSH capabilities can be configured to access the serial port on access points.

Physical and Data Link Layer Security Controls

The International Organization for Standardization (ISO) model as set forth in the earlier chapters by looking at the physical and data link layers. The 802.11 wireless Ethernet standard has minimal and flawed authentication and packet encryption methods defined within.

However, as mentioned previously, when used in conjunction with Wired Equivalent Privacy (WEP), 802.1x augments and corrects some of the standard's pitfalls.



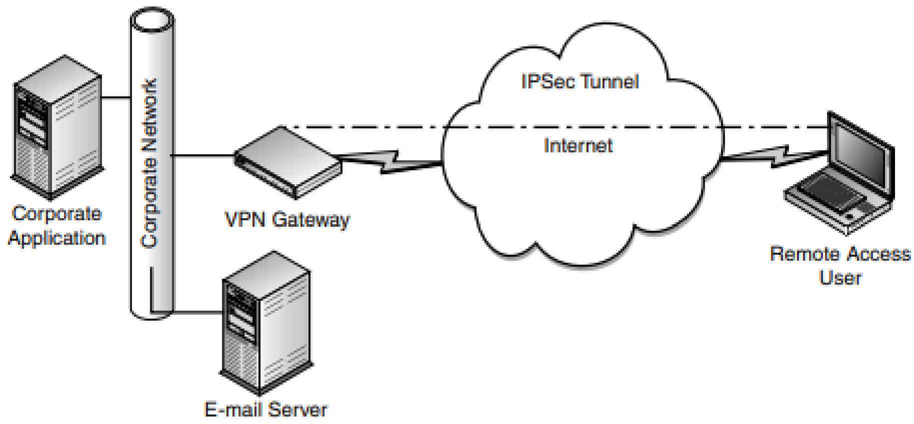
Using 802.1x with dynamic WEP keys eliminates most of the attacks against WEP, as defined in 802.11-1999 and 802.11b, as long as keys are rotated frequently. Shared authentication should never be used; always use an open system because the shared authentication scheme leaks WEP key information to attackers through known plaintext methods. One of the downfalls of 802.1x is that it requires more back-end equipment and a Remote Access Dial-In User Service (RADIUS) server with 802.1x capabilities. This additional management overhead should be considered.

Recently, many vendors have implemented WEP key hashing. Key hashing is the process of hashing the initialization vector (IV) and shared key before generating the RC4 stream. This is a highly effective way to prevent someone from recovering the WEP key by using passive attacks. At the time of this writing, all key-hashing features of wireless devices are vendor proprietary and not interoperable. Another common 802.11-based security mechanism is the use of Media Access Control (MAC) access control lists. A MAC access control list is a list of physical addresses that are allowed to access the wireless network. This security mechanism is found in almost all access points. It enables the network administrator to enter lists of valid MAC addresses into an access control list, limiting network access. With some access points, the list can then be pushed out to all participating access points. The downfall of this practice is that the MAC addresses of all wireless clients and access points are sent in the clear, even when WEP is enabled.

Changing the MAC address of a network card is a trivial task. Many times, it is a configuration option in the driver. An eavesdropper can easily compile a listing of valid MACs, detect when one disassociates, and attach to the network with that valid MAC address. Even with their limitations, MAC access controls are still useful in some circumstances. They can be powerful tools in preventing roaming clients from accidentally attaching to an open wireless network. However, the administrative overhead needs to be considered because keeping track of valid MACs and updating all access points with the valid address can be a time-consuming task.

VPN Tunnelling

As alluded to in the previous chapters, VPN tunnelling works extremely well in many environments. It is a proven technology and many companies are already equipped with a VPN gateway. Sometimes adding access to the VPN from the wireless network can be as simple as adding a network card to the VPN gateway or changing some firewall rules. When roaming is required, network designers need to take network subnetting into consideration. The IP address must remain the same for it to work seamlessly. In many cases, the VPN tunnel will drop when roaming and will reset TCP connections. This may require the user to renter authentication credentials.



MobileIP may be used for roaming. MobileIP may prevent the VPN connection from getting torn down when traversing between access points. MobileIP can also be used across different wireless network types. You can use MobileIP on cellular telephone data services, eliminating the enterprise's requirement of a separate infrastructure to support mobile tele□phony applications.

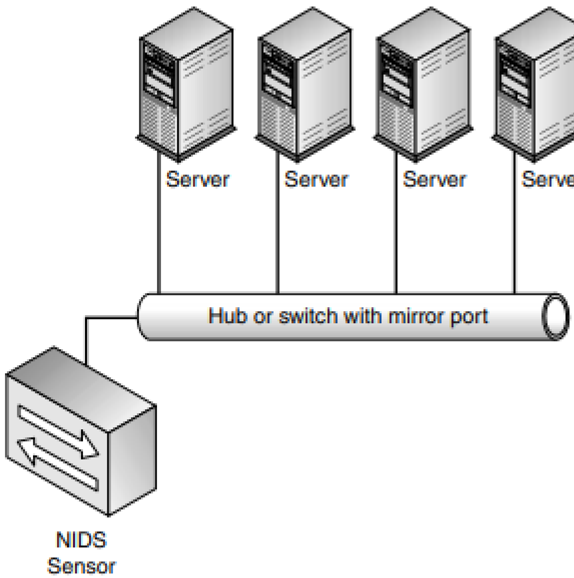
Intrusion Detection Systems (IDSs):

Your network will never be 100 percent secure. Not all attacks can be stopped and excessive security measures can sometimes be prohibitive to business. In other words, attempting to prevent all possible attacks is not only an exercise in futility, but it may not be worth the effort. Many people who want to secure their houses install alarms instead of bars on the windows to notify the police in the event of a break-in. The equivalent to home alarms in the digital arena is intrusion detection systems (IDSs). IDSs take many forms, but they normally break down into two categories: host based and network based.

A host-based IDS (HIDS) is normally a piece of software that monitors the system for suspicious activity. This involves monitoring system files for changes or the installation of new software, drivers, or kernel modifications. Sometimes an HIDS also monitors the network connections, looking for suspicious connections and new programs, listening for incoming connections, and initiating new outgoing connections. Some personal firewall software has an HIDS component.

A network-based IDS (NIDS) is based on a modified packet sniffer. It is installed on a network and has the capability to examine network traffic. The NIDS either monitors for suspicious activity by comparing network traffic to signatures of known attacks or monitors for anomalies. Anomaly IDS systems have a learning mode in which they build rules based on the normal network traffic patterns. Then they monitor traffic with the created rules and alert any suspicious activity. Some systems are a hybrid of the two technologies. Many commercial IDS systems and some open-source systems are available.

One of the benefits of using NIDS over HIDS is that a single NIDS sensor can monitor a network containing many hosts, thus simplifying the installation and configuration of the IDS. Some HIDS can dramatically decrease the performance of the host operating system. Be sure to fully test the impact of different IDSs on your applications before deploying them to the entire network. Various forms of IDSs are included in the designs discussed in the following sections.



Due to the administrative overhead of monitoring IDS sensors and keeping IDS signatures up-to-date, many companies choose to outsource this service. An outsourced IDS service provides or sells sensors to be placed on the network and monitors them from the Internet or a dedicated telco link. The monitoring service is responsible for updating changes and alerting administrators of any suspicious activity. These services are expensive and are not for every enterprise. You should evaluate your in-house security and monitoring expertise before deciding to use an outsourced IDS provider.

Some people feel that an IDS can also involve reviewing logs for suspicious events. Regularly reviewing and archiving logs should be the standard practice on any network. Many intrusion-related events do not produce suspicious-looking logs during the event so the effectiveness of these systems as IDSs is limited.

Additional IDS resources include

www.snort.org

www.sourcefire.com

www.nfr.com

www.enterasys.com/ids/

Application Security Considerations

Wireless networks are often set up to offer a specific application. This may include roaming agents in airports, inventory tracking in warehouses, email, or service of the “killer app” to end users. Many times, these applications have already been hardened to work on a hostile network: the Internet. In these cases, wireless security precautions, such as WEP and IP Security (IPsec) may not be needed. Instead, SSL/Transport Layer Security (SSL/TLS) and SSH may be good ways to secure an existing application.

Enterprise Campus Designs:

The following section deals with the security needs of the enterprise campus. Many applications are available for wireless networking on a campus. In some cases, these designs can be combined into a hybrid design to solve multiple business problems. Key design concepts are highlighted as best practices. Use these best practices when evaluating your current design or when creating a hybrid design for your application.

Enterprise Design 1

One of the most difficult challenges that wireless network designers face is the need to support many different platforms, operating systems, and hardware vendors with a single infrastructure. The following design was used in a campus that needed to support a large population of engineers and salespeople. Many of the engineers used different operating systems such as Windows, Linux, Berkeley Software Distribution (BSD), which is a Unix-like operating system, and Solaris. To make matters worse, many of the engineers used their personal laptops, which had a wide variety of wireless network cards. Due to the highly sensitive nature of the data being transmitted on the network and the network resources, security was a key concern. Because the users were not very technical, ease of use also played an important role.

The solution to the problem proved to be easier than first anticipated. The company already had an infrastructure for providing access from a hostile network (the Internet) with the corporate VPN. The network 200 Part 3 Wireless Deployment Strategies designers remembered the pain and agony that it took to meet the engineers’ functional requirements with the VPN and did not want a repeat with the wireless network. The decision was made to build a completely separate wireless network that would not have Internet connectivity and the internal network would only be accessible through the corporate VPN.

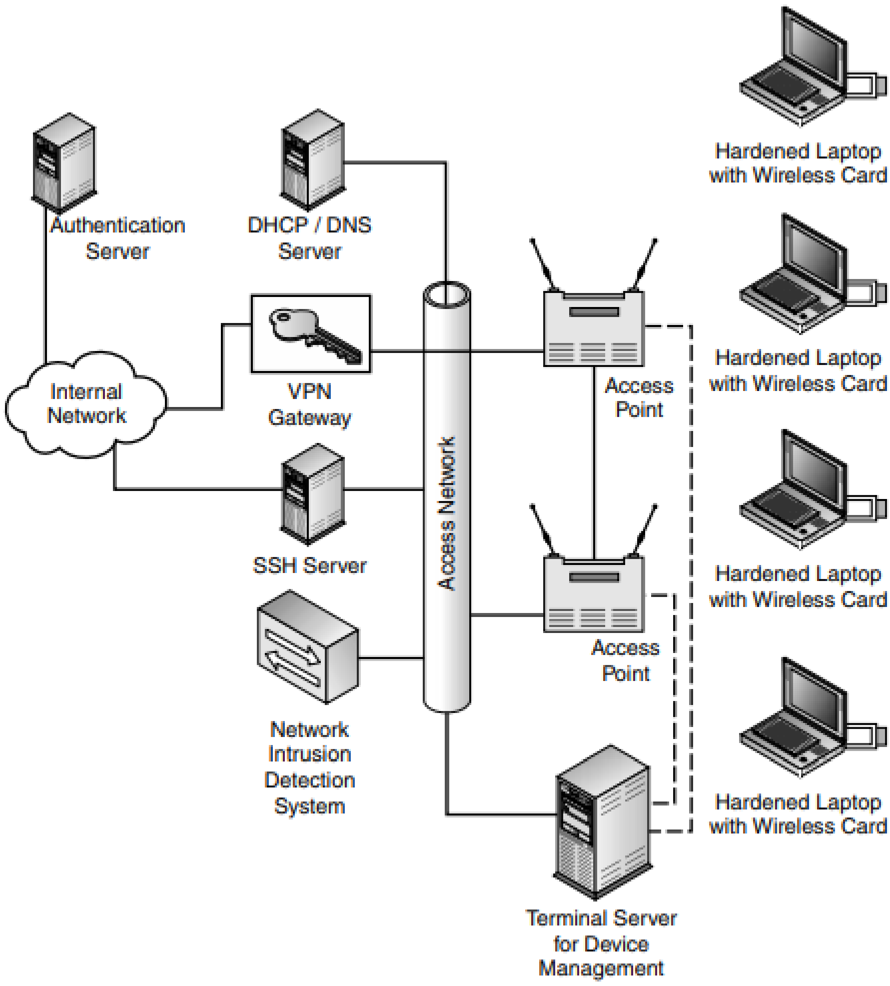
The corporate VPN consisted of an IPsec appliance and an SSH gateway that was configured for port forwarding. Token-based one-time passwords (OTPs) were used on the IPSec appliance and the SSH gateway. The corporate VPN already had a requirement for using a company approved secure build or utilizing a personal firewall with a company standard rule set.

The installation proved to be easy. Additional network cards were added to the IPSec appliance and the SSH gateway for connectivity to the wireless network, as shown in Figure 8-4. Only a few more machines were needed to make the network fully functional. A server was added to provide Dynamic Host Configuration Protocol (DHCP) and Domain Name Server (DNS) services to the wireless users because the VPN and SSH clients were configured to connect to a hostname, not an IP address. Another server was added to the wireless segment as a NIDS and a syslog server to capture logs from the access points and DHCP server. Finally, a terminal server was installed to manage the access points and Ethernet switches because the only network-based management options offered by the vendor were cleartext (telnet and HTTP). The best practices include the following:

- Segment the hostile wireless network from the rest of the internal network.
- Disable the management of access points with the wireless interface.
- Harden the DHCP/DNS server.

Enterprise Design 2

Another option for implementing a secure wireless network is to use 802.1x. At the time of this writing, 802.1x is still in draft form and vendor interoperability is limited at best. However, 802.1x is a valid option for adding security to a wireless network. It is a new technology and still has not had the time in the market or been under public scrutiny to show what implementation-specific caveats and details need to be addressed.



However, 802.1x shows great promise and should be considered in a wireless network designer’s toolkit.

This design does not suffer from the limitations of the previous design. In this case, the users were exclusively using Windows and all hardware was provided by the company, so using a vendor-specific implementation was not a problem. The vendor chosen was one that the network designers were very comfortable with: Cisco.

The 802.1x implementation used the existing corporate directory services. However, a new RADIUS server was necessary for the vendor's 202 Part 3 Wireless Deployment Strategies Access Network Access Point Access Point Terminal Server for Device Management Network Intrusion Detection System SSH Server VPN Gateway DHCP / DNS Server Authentication Server Hardened Laptop with Wireless Card Hardened Laptop with Wireless Card Hardened Laptop with Wireless Card Hardened Laptop with Wireless Card Internal Network Figure 8-4 Enterprise design 1 802.1x implementation of EAP over RADIUS, and additional features were required. 802.1x not only provided authentication services, but it was also used for dynamically creating WEP keys. RADIUS session timeouts of three hours were used to force the changing of WEP keys on a frequent basis. The implementation also used the key-hashing features mentioned earlier in this chapter.

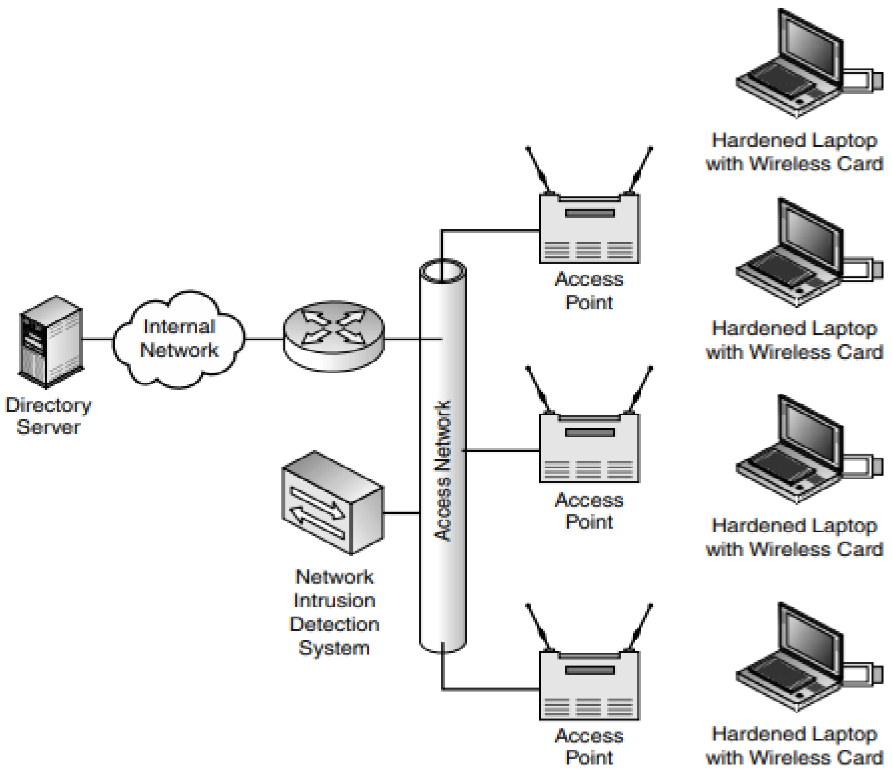
The best practices include the following:

■ Use 802.1x for authentication and encryption.

■ Change keys frequently; three-hour timeouts are used.

■ Use key-hashing features.

■ Advanced proprietary integrity checking features are used



■ The wireless network is kept segmented from the rest of the network to enable future network changes.

■ NIDS is used on the wireless network.

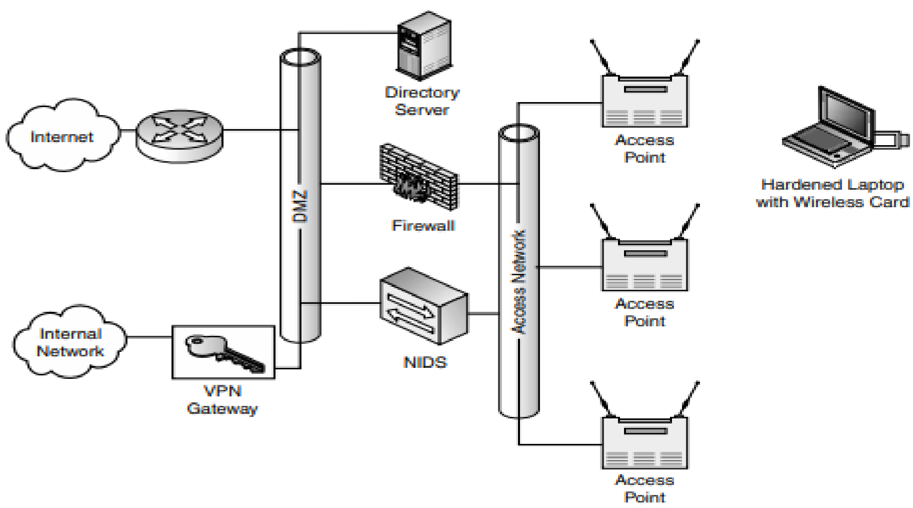
Enterprise Guest Network

Another application for a wireless network at an enterprise campus is for a guest network. A similar configuration can also be used at universities or training centers. At one corporation, contractors and vendors frequently needed access to the Internet. The information security team did not want people attaching to the network who had not signed the acceptable use policy so a guest network was set up. This was a separate network set up to protect the enterprise's intellectual property.

The first implementation of this guest network was adding data connections in strategic locations, such as conference rooms and visitor cubicles. After one visitor infected machines on the internal (nonguest) network with a virus by accidentally plugging into the wrong jack in a conference room, the network architects began searching for another solution. The decision was made to set up a wireless network that would be used by guests needing Internet access.

A process was followed to set up the guest network during its initial implementation without wireless, but the design evolved into a wireless network. Functional requirements were presented to the network architects. The guests needed the applications of web surfing and VPN access. The security group was concerned that an open network may give free Internet access to malicious attackers. After considering the functional requirements and the concerns of the security group, a design was proposed and approved.

The network was set up with a web proxy that required a username, password, and a packet filter that allowed VPN connections, as shown in Figure 8-6. The access points that were used offered DHCP services so a DHCP server was not needed. The proxy server was used to capture logs from the access points and provided DNS services. An NIDS was also added to the network. The help desk has a supply of wireless cards that can be checked out for guests and visitors. When a wireless card is checked out, a username and password are created on the proxy server and an instruction sheet with configuration instructions is provided. Each username and password expire after one week



The best practices include the following:

■ The guest network is segmented and firewalled from the rest of the network.

■ NIDS is installed on the hostile guest network.

■ Users must agree to an acceptable use policy in order to use the network.

■ Network uses 802.11 standards to give the maximum hardware support.

■ Corporate laptops are hardened before using the wireless network.

Enterprise Point-to-Point Configuration

The cost savings of replacing a traditional telco point-to-point connection with a wireless link can be tremendous; wireless links can also be set up much faster than traditional telco links. Existing wireless networking technologies can be used to create these point-to-point links. In many cases, ranges can be extended by using directional antennae and amplifiers. The security benefit of using a directional antenna is that it makes the link much more difficult to sniff or jam. This link is trivial to secure because both ends of the link are static and known.

In this commonly found scenario, you can easily use traditional IPsec based VPN-tunnelling software or appliances to protect all traffic flowing between one end of the bridge to the other. These VPNs can be set up using VPN appliances, routers, or software-based VPNs.

The best practices include the following:

■ Use directional antennae to eliminate signal loss and boost power.

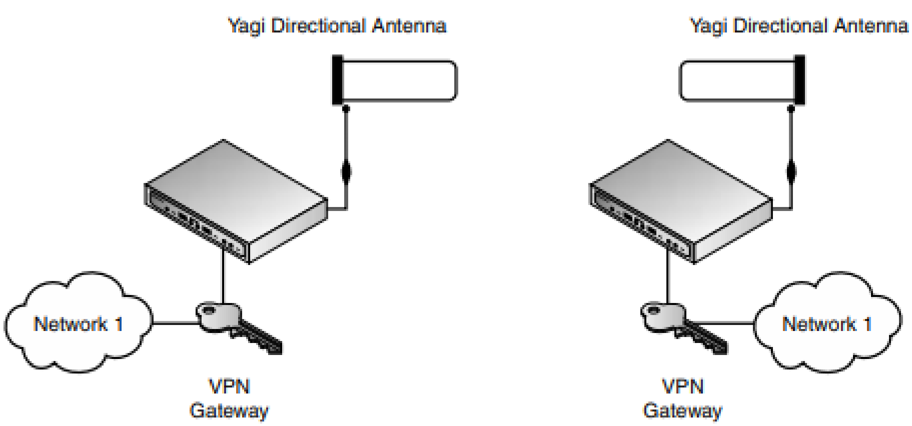
■ Configure access points to only connect to the other end of the connection; many times this is accomplished with entering a MAC address.

■ Use WEP.

■ Use IPsec tunnel mode.

■ Use a strong form of encryption, such as Advanced Encryption Standard (AES) or Triple Data Encryption Standard (TDES).

■ Rekey the VPN frequently.



Wireless ISP Design

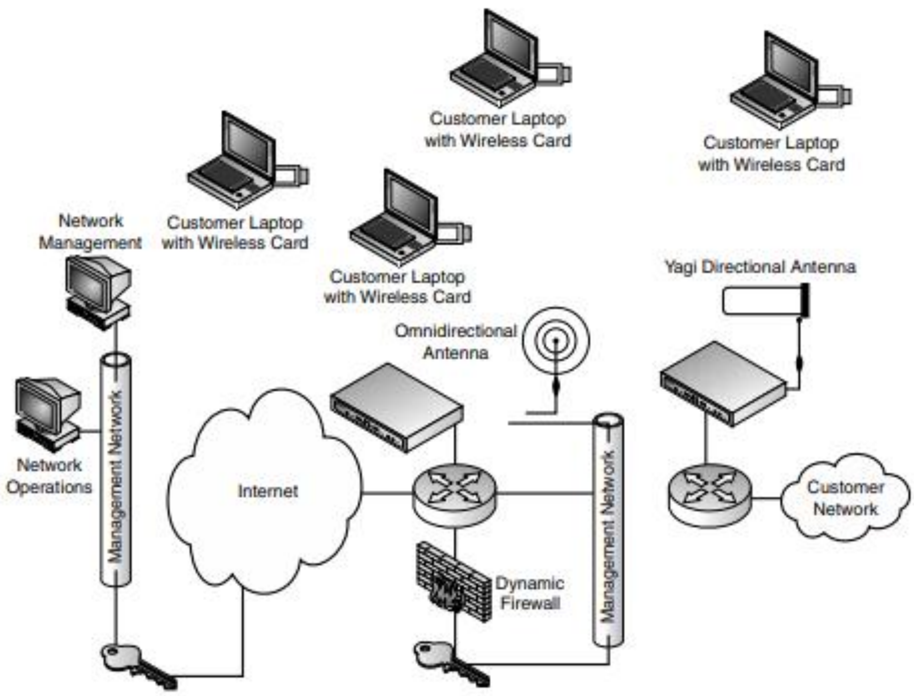
Metropolitan area networks (MANs) have seen a rebirth from almost certain doom with the adoption of wireless network technologies. Many regional and specialty ISPs are starting to offer wireless Internet access. This Internet access can be limited to a small area or can be offered in coffee shops, hotels, or airports. In order to prevent customer support calls and improve the customer experience, the network needs to be open. In this scenario, you don't know who is going to join the network. Therefore, network resources need to be well protected.

In order to meet customer requirements, an open design is required. The network administrators chose to implement a separate back-end network for management. During implementation, careful consideration was given to finding a vendor that had features for securing managing network devices, such as access points and routers. Unfortunately, no vendor was offering this during the buildout of the network so a separate management network was necessary. The management network had the added benefit of giving the network designers a lot of flexibility to roll out new applications.

The network was set up with a dynamic firewall that would open up holes for Internet access after users authenticated to the billing server. This was an off-the-shelf product that had some security holes, but building a custom solution would be cost-prohibitive. A VPN was used to access the management network for the network operation and management functions.

Retail and Manufacturing Designs

Wireless networking has proven to be a killer app for many network retail and manufacturing companies. The return on investment (ROI) for wireless applications has proven to be significant. Unlike the corporate campus, the common workstations for a retail or manufacturing wireless application are personal digital assistants (PDAs), bar-code scanners, and other thin clients. The following network designs were used in these environments.



Kiosk/Roaming Agent Design

Wireless applications can dramatically increase customer satisfaction. Customer-service applications are often wired to a desk or service point that may not be in the most convenient place for the customer, or a new application may need to be rapidly deployed into an existing store, or kiosk, and wiring constraints may prevent the adoption of the application.

This wireless design is for an application that has a very large user population that does not have much technical expertise, so the equipment and user experience needed to be simple. PDAs with bar-code scanners were chosen as the equipment for this application. The PDA had all the necessary functionality, but needed the capability to add a small printer. A quick proof-of-concept application was created using a wide-open wireless network and a modified web browser. All the functionality was there, but the security concerns needed to be addressed.

The application designers tried using off-the-shelf software modified for the particular environment, but after initial testing, the decision was made to customize an application. The application programmers were able to port the Mini browser application to IPsec using a cryptographic toolkit from a commercial vendor. The toolkit was designed to handle all the sophisticated cryptographic functions without the programmer needing to learn how to write IPsec software. Due to the highly public environment of the application, the designers chose to harden the application and use WEP and MAC access controls. A pair of VPN gateways and servers providing DHCP, DNS, and logging were set up for the entire network, serving hundreds of stores. An IDS system was also set up for network monitoring and detecting suspicious activity.

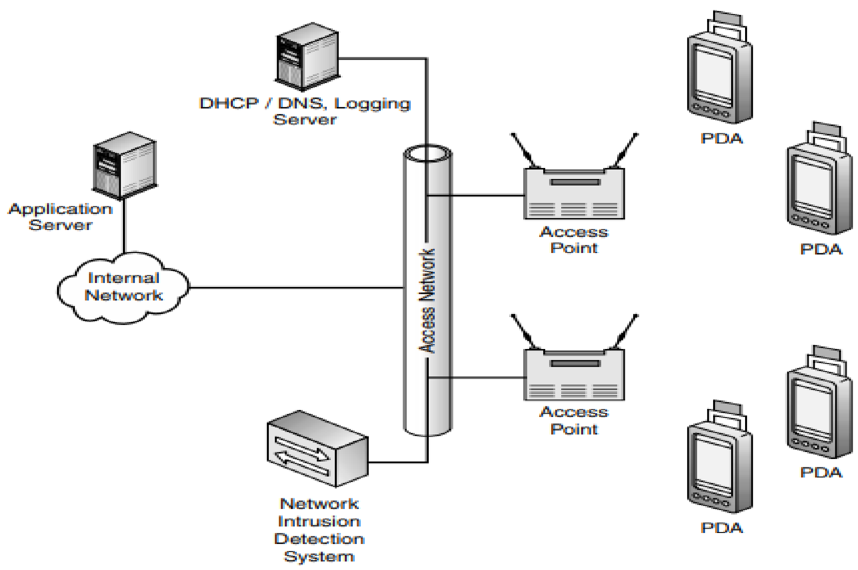
The best practices include the following:

■ All traffic is authenticated and encrypted.

■ An IDS system is used for watching the network.

■ Standard-based 802.11 security features are used, but are not relied on.

■ A hardened server provides network services (DHCP and DNS).



Warehouse Design

The early adopters of wireless technology included the manufacturing and warehousing industries. Wireless was adopted mainly for the mobility that it provides and to prevent significant wiring changes that are frequently needed in a warehouse. Internet and e-mail are not common applications in the industry. The most common are inventory tracking and shipping applications. Many times, these run off a PDA or connect to a thin client or terminal. Many of these early implementations used telnet or a simple browser for user input in conjunction with a bar-code scanner or magnetic-strip reader. WEP was used to secure these applications because cleartext protocols were being used. After the shortfalls of WEP were publicized, a network redesign was needed.

Once the wireless network was installed, there was no going back, but security was still needed. The network was redesigned to keep the functionality and ease of use while adding security. If a malicious attacker were to attack the network, downtime could be very expensive. Troubleshooting wireless networks is also expensive because in many cases the staff is not immediately available and often must travel to the site. Many warehouses and manufacturing companies lose money if products cannot be delivered on time. During the network redesign, using a technology that uses licensed frequencies was considered, but it was cost prohibitive and not available in all locations.

The existing network was used with a few modifications. Shared key authentication was replaced with an open system. WEP keys were rotated on a monthly basis. MACs were utilized when the feature was not previously enabled. Then an IDS was added to the network. SSH was used to replace the telnet application and port forwarding to the e-mail server that was added for the program. The network was also designed to allow the addition of thin clients using an encrypted protocol.

The best practices include the following:

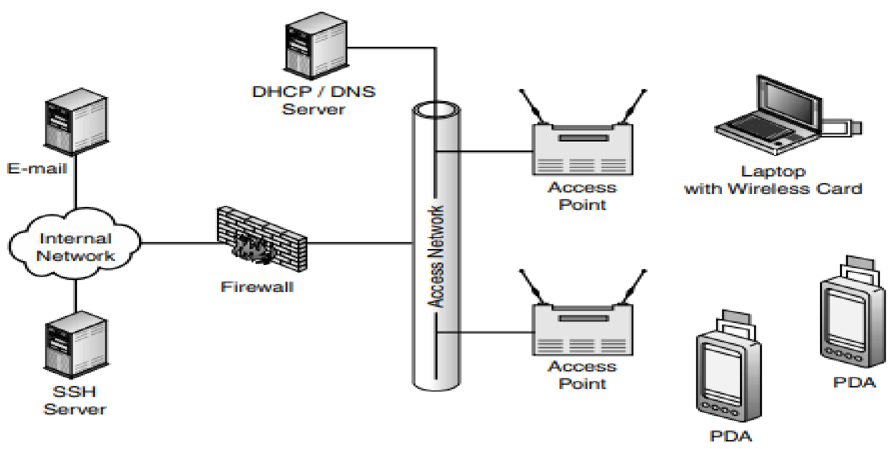
■ Use encrypted protocols.

■ Use a firewall or packet filter to limit network exposure.

■ Monitor for potential failure conditions or attacks.

■ Regularly change WEP keys.

■ Use MAC access controls.



Small Office/Home Office Design (SOHO)

One of the biggest challenges in securing a Small Office/Home Office (SOHO) wireless network is deciding how much security to use. You would not buy a million-dollar safe to protect a thousand-dollar diamond. To make matters more difficult, SOHO configurations are often implemented with inexpensive hardware that does not offer many security features. However, achieving adequate security for your SOHO is still possible. The decision about security should be made before purchasing hardware to ensure that the hardware has the necessary features.

The primary question that needs to be answered is how will adding wireless to your SOHO change the current threats? Some SOHO networks are connected directly to the Internet through a broadband connection. If this is the case, then adding a wireless connection to the network does not significantly change the threat to the already Internet-connected machine. However, a new threat to the network bandwidth is being introduced. A malicious user could attach to the wireless connection for free Internet access.

To make matters worse, this malicious user may attack other sites or use your Internet connectivity to introduce a new virus on the Internet with your connection. Therefore, steps must be taken to secure the wireless connection. Very destructive viruses, such as the Melissa virus, have been introduced to the Internet using stolen Internet access accounts. Although the authorities were eventually able to track down the writer, the person with the stolen AOL account went through much heartache. Tracking down a wireless user who attached to someone's unprotected access point could be very difficult, if not impossible, and may leave the negligent owner liable. By the way, make sure that your desktop computer has a virus-scanning program and it is kept up-to-date.

Now let's take a step back and examine the threats toward the SOHO machines. As stated before, many times these machines are directly connected to the Internet. In some cases, these may be protected by a firewall or router, which provide a level of protection. In either case, if you add a wireless connection to a SOHO network, the machines on the network must be hardened. Hardening hosts may involve many different processes, but this normally involves disabling unnecessary services, using strong passwords, deleting unused accounts, or adding firewall software.

Reasonable steps should be taken to secure a SOHO wireless network. Use the security features of the access point, which may include WEP and MAC access controls. Consider purchasing a high-end access point with advanced security features. Cisco produces access points with very advanced security features (such as LEAP, an 802.1x implementation) that cost just a little bit more than most access points and will give you much better performance and radio coverage. It is money well spent.

The best practices include the following:

■ Access point—use WEP and MAC access controls. This will significantly increase the level of complexity of an attack.

■ Network hosts—add personal firewall software to machines and add strong passwords to the printer and router.

- Turn off the equipment when it is not in use.