CWSP Guide to Wireless Security

Foundations of Wireless Security

Objectives

- List the advantages and disadvantages of a wireless local area network
- Describe the functions of the wireless LAN standards and regulatory agencies
- List wireless networking and security certifications
- Define information security and tell why it is important in wireless networks
- List the five types of IEEE WLANs

Wireless in Our World

- Wireless LAN applications
  - Can be found in every industry whose employees need or want to conduct business without being confined to a specific location

Business

- “Flatter” organizations
  - Employees are involved in team meetings that occur away from their desks
- Wireless technology
  - Has dramatically changed how and where business meetings take place
    - Has made the meetings more focused and productive
- Wireless LANs benefits
  - Increased productivity, time/financial savings

Business (continued)

- Voice over wireless LAN (VoWLAN)
  - Emerging wireless technology
  - Uses the existing data WLAN to make and receive telephone calls
  - VoWLAN devices can forward business calls to their mobile phones during regular business hours

Business (continued)

Table 1-1 Business plans for WLANs

Application	Percentage planning to implement
Employee mobility	66%
Conference-room access	56%
Voice over WLAN	24%
Asset tracking	22%
Wired port replacement	21%
Other	12%
Unsure	5%

Travel

- Travel industry is a leader in adopting wireless technologies
  - Most airports provide wireless access hotspots
  - Some airports use wireless technology to keep track of passenger luggage
- Wireless PDAs now replace walkie-talkies
- WLAN technology is used to communicate with the aircraft
  - Once it has parked or is taxiing on the ground
- WLAN technologies are not restricted to airplanes

Education

- WLANs are ideal for colleges and schools
- Educational institutions were early users of WLANs
- Wireless LAN connections offer teachers and students an important degree of freedom
  - Teachers create classroom presentations on laptops
  - Can access the school network wirelessly from almost any location
- Most schools publish maps showing the location of wireless access points

Education (continued)

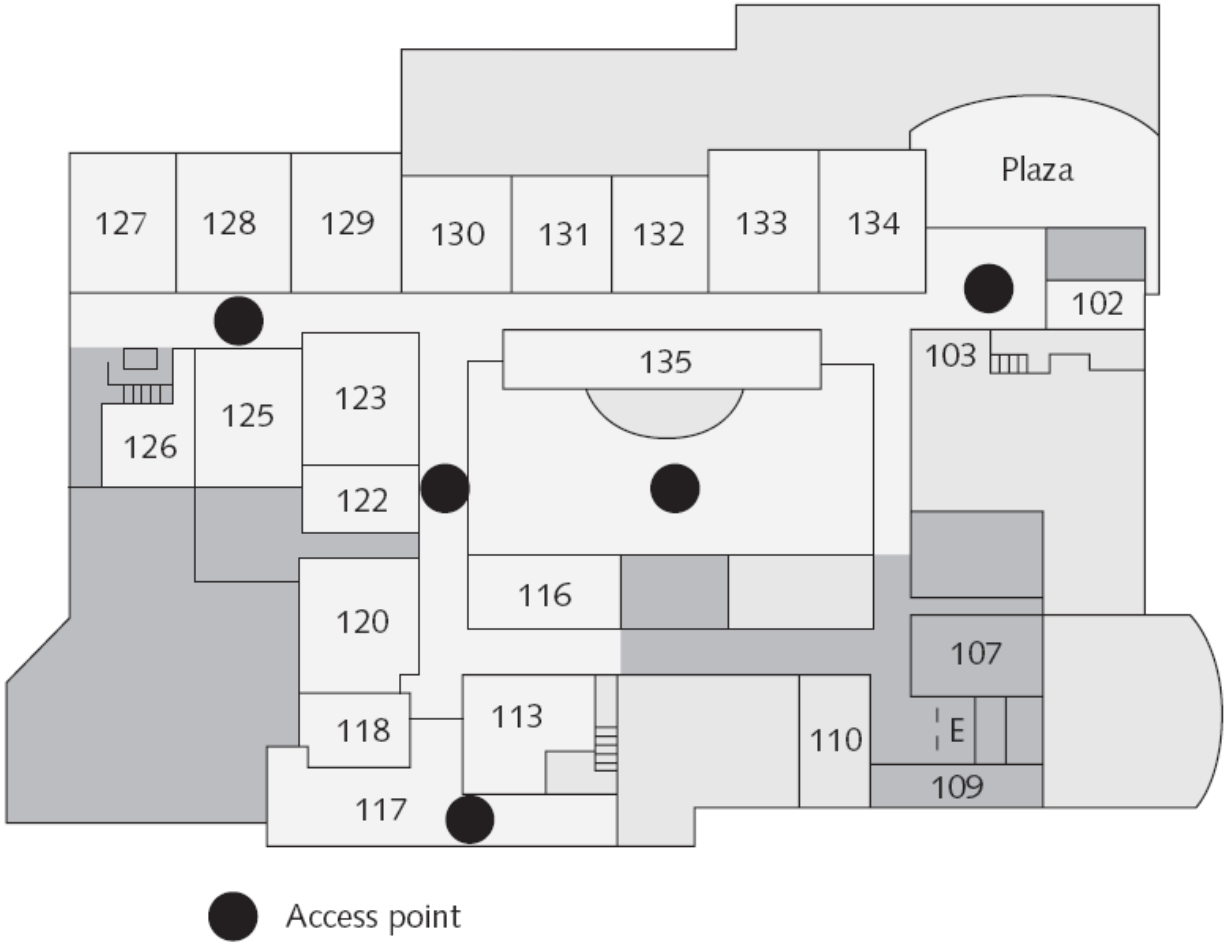


Figure 1-1 Campus access point locations

Education (continued)

- WLAN technology translates into a cost savings for colleges as well
  - Classrooms become fully accessible computer labs
  - Colleges no longer have to consider the expense of adding multiple open computer labs
  - Wireless networks are also used to promote safety and security

Health Care

- The health care industry has embraced wireless technology to improve patient care
- Wireless LAN point-of-care computer systems
  - Allow medical staff to access and update patient records immediately
  - Verify that medication is being administered to the correct patient in the correct dosage

Wireless Advantages and Disadvantages

- With any technology, there are advantages and disadvantages to be considered
  - Wireless LANs are no exception

Advantages

- Mobility
  - Primary advantage of wireless technology
  - Enables individuals to use a laptop computer that is always in contact with the network
- Easier and less expensive installation
  - Installing network cabling can be expensive
  - Significant time required to install network cabling
  - Wireless technologies allow creation of an office in a space where the traditional infrastructure doesn’t exist

Advantages (continued)

- Increased reliability
  - Wireless LAN technology eliminates cable failures and increases the overall reliability of the network
- Disaster recovery
  - Hot site has all the equipment needed for an organization to continue running
    - Generally run by a commercial disaster recovery service
  - Cold site provides office space but the customer must provide and install all the equipment
  - Many businesses use cold sites and WLANs as a major piece of their disaster recovery plan

Disadvantages

- Radio frequency interference
  - Signals from other devices can disrupt wireless
- Health risks
  - High levels of RF can produce biological damage through heating effects
  - It is not known if or to what extent lower levels of RF might cause adverse health effects
- Security
  - Greatest disadvantage to wireless LANs
  - Attacks on wireless networks: denial-of-service, stealing passwords, altering messages

Information Security and Wireless LANs

- Knowing how to defend a wireless network against a wide array of attacks
  - Begins with an understanding of what information security is

What is Information Security?

- Information security
  - The tasks of guarding digital information
  - Ensures that protective measures are properly implemented
  - Cannot completely prevent attacks or guarantee that a system is totally secure
  - Intended to protect information
- Characteristics of secure information
  - Confidentiality, integrity, and availability

What is Information Security? (continued)

- Information security protects devices that store, manipulate, and transmit the information
- Information security is achieved through a combination of three entities
  - Innermost layer consists of the products that provide the necessary security
  - Middle layer is people
  - Outmost layer consists of procedures

What is Information Security? (continued)

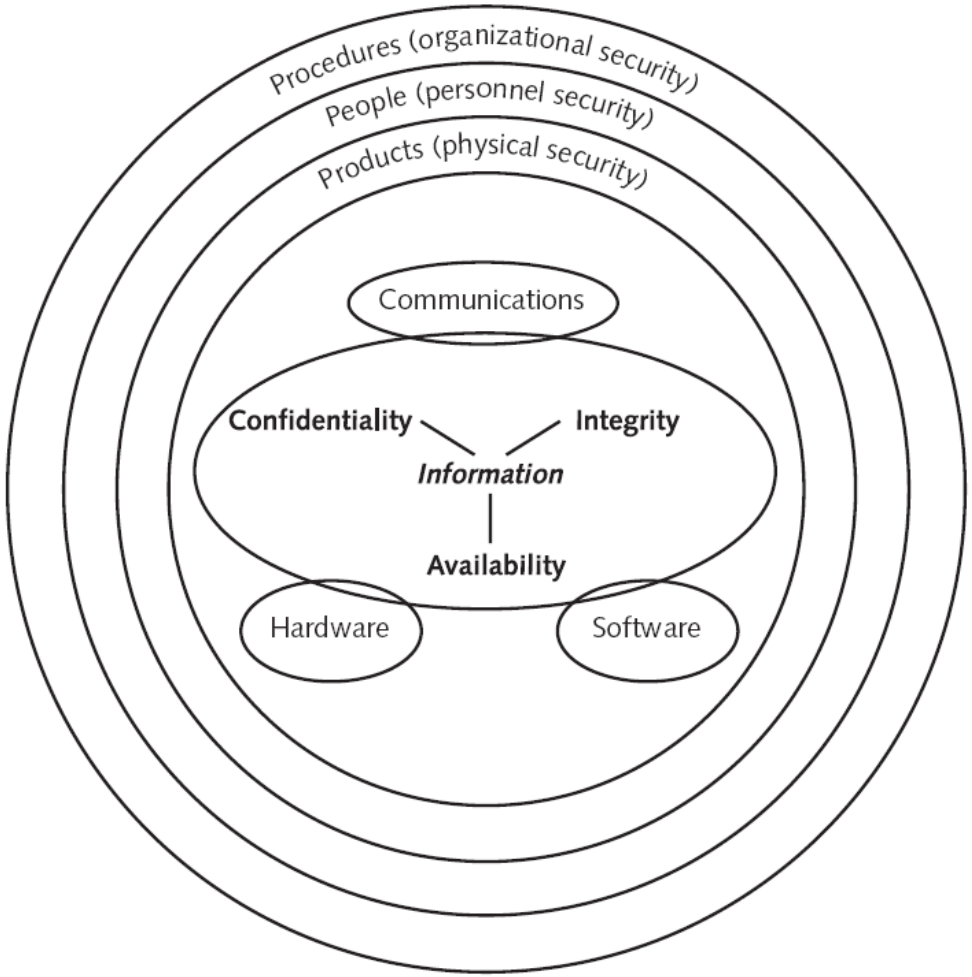


Figure 1-2 Information security components

Difficulties in Defending against Attacks

- Factors that make security increasingly difficult
  - Speed of attacks
  - Sophistication of attacks
  - Attackers now detect weaknesses faster
  - Distributed attacks
  - User confusion
- Zero day attacks
  - Attacker discovers and exploits a previously unknown flaw

Why Wireless Security is Important

- Unique challenges
  - Unauthorized users can access the network
  - Attackers can view transmitted data
  - Employees can weaken installed security protections
  - Attackers can easily crack existing wireless security
- Attackers can:
  - Steal personal data
  - View wireless transmissions
    - With freely available wireless packet sniffer
  - Inject malware

Why Wireless Security is Important (continued)

- Attackers can (continued):
  - Download harmful content
  - Cause loss of equipment
  - Cause violation of an ISP agreement
  - Identify “weak link” users

Why Wireless Security is Important (continued)

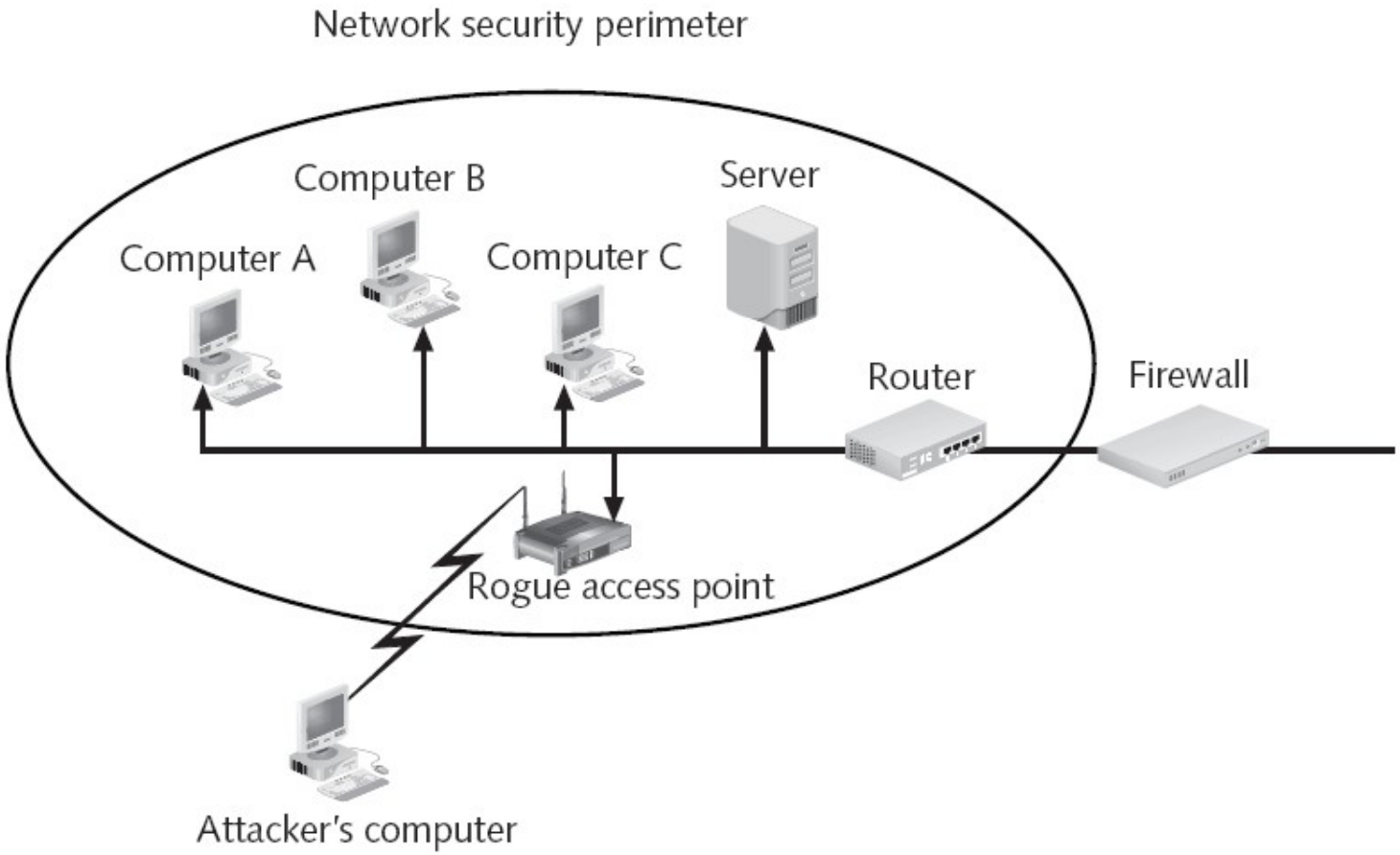


Figure 1-3 Rogue access point

Wireless Standards Organizations and Regulatory Agencies

- Three primary standard-setting and regulatory bodies
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Wi-Fi Alliance
  - U.S. Federal Communications Commission (FCC)

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE
  - The most widely known and influential organization
  - Dates back to 1884
  - Establishes standards for telecommunications
  - World's largest technical professional society
  - Technical, educational, and professional activities
  - Project 802
    - Computer network architecture standards
    - Quickly expanded into several different categories of network technology

Institute of Electrical and Electronics Engineers (IEEE) (continued)

Table 1-2 Current IEEE 802 task groups

Task Group	Description	Comments
802.11a	54 Mbps WLAN at 5 GHz	Ratified 1999, but devices did not appear until 2001
802.11b	11 Mbps WLAN at 2.4 GHz	Ratified 1999, also known as "Wi-Fi"
802.11c	Bridge connections	Moved to 802.1 Working Group
802.11d	Worldwide compliance with regulations for use of wireless signal spectrum	Adds features and restrictions to allow WLANs to operate within the countries that have wireless spectrum conflicts; ratified 2001
802.11e	Quality of Service	Ratified in 2005
802.11F	Inter-Access Point Protocol (IAPP)	Handles the registration and exchange of information between different vendors' access points; ratified 2003
802.11g	54 Mbps WLAN at 2.4 GHz	Ratified 2003
802.11h	Enhanced version of 802.11a	Supplement to the MAC layer to comply with European regulations for 5 GHz WLANs
802.11i	Wireless security	Also known as Robust Security Network, ratified 2004
802.11j	Enhancements to 5 GHz signaling	Proposed addition that incorporates Japanese regulatory extensions to the 802.11a standard

Institute of Electrical and Electronics Engineers (IEEE) (continued)

Table 1-2 Current IEEE 802 task groups (continued)

Task Group	Description	Comments
802.11k	Wireless LAN management system	In progress
802.11l	Not used	Omitted to avoid confusion with "802.11i"
802.11m	Maintenance of 802.11 documentation	In progress
802.11n	Future 300+ Mbps WLAN	In progress, anticipated ratification 2007
802.11p	Wireless Access for the Vehicular Environment (WAVE)	WLANs for automobiles
802.11r	Handoffs between mobile clients	As a major support to VoWLANs, it is designed to speed the handoff of wireless phones between wireless networks
802.11s	Mesh wireless network	A mesh network can determine the optimum route for a packet to travel across the WLAN based on the quality required
802.11t	Wireless Performance Prediction (WPP)	Standardized test methods and metrics for WLAN performance
802.11u	Interworking with non-802 networks (e.g., cellular)	Standards for how WLANs connect to external networks such as the Internet or cellular networks

Institute of Electrical and Electronics Engineers (IEEE) (continued)

Table 1-2 Current IEEE 802 task groups (continued)

Task Group	Description	Comments
802.11v	Wireless management	Creates efficient mechanisms to simplify wireless network deployment and management
802.11w	Protected Management Frames	Increases security of management frames

Wi-Fi Alliance

- Wireless Ethernet Compatibility Alliance (WECA)
  - Consortium of wireless equipment manufacturers and software providers, formed in 1999
  - Goals
    - To encourage wireless manufacturers to use the IEEE 802.11 technologies
    - To promote and market these technologies
    - To test and certify that wireless products adhere to the IEEE 802.11 standards
  - In October 2002, WECA changed its name to Wi-Fi (Wireless Fidelity) Alliance

Wi-Fi Alliance (continued)



Figure 1-4 Wi-Fi Certified seal

Federal Communications Commission (FCC)

- FCC
  - Controls and regulates wireless transmissions for use by citizens in the United States
  - Serves as the primary regulatory agency for wireless communications
  - Independent government agency that is directly responsible to Congress
  - Established by the Communications Act of 1934
  - Process applications for licenses
  - Represents US in negotiations with other nations about telecommunications issues

Federal Communications Commission (FCC) (continued)

- Radio frequency spectrum
  - Entire range of all radio frequencies
  - Divided into over 450 different sections or bands
- License-exempt spectrum or unregulated bands
  - Available nationwide to all users, without a license
  - Devices can be either fixed or mobile
  - Devices can interfere with each other
- Bands used for WLANs
  - Industrial, Scientific and Medical (ISM)
  - Unlicensed National Information Infrastructure (UNII)

Federal Communications Commission (FCC) (continued)

Table 1-3 Unlicensed bands

Unlicensed Band	Frequency	Total Bandwidth	Common Uses
Industrial, Scientific and Medical (ISM)	902-928 MHz 2.4-2.4835 GHz 5.725-5.85 GHz	234.5 MHz	Cordless phones, WLANs, Wireless Public Branch Exchanges
Unlicensed Personal Communications Systems	1910-1930 MHz 2390-2400 MHz	30 MHz	Wireless Public Branch Exchanges
Unlicensed National Information Infra-structure (UNII)	5.15-5.25 GHz 5.25-5.35 GHz 5.725-5.825 GHz	300 Mhz	WLANs, Wireless Public Branch Exchanges, campus applications, long outdoor links
Millimeter Wave	59-64 GHz	5 GHz	Home networking applications

Wireless LAN Standards and Types

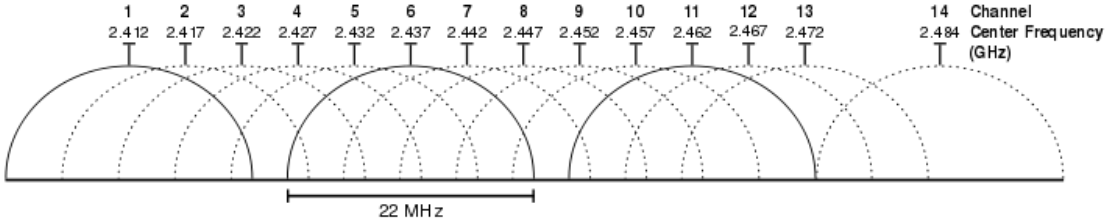
- Since the late 1990s, the IEEE has approved four standards for wireless LANs
  - –802.11b
  - –802.11a
  - –802.11g
  - –802.11n

IEEE 802.11

- Standard for WLANs operating at 1 and 2 Mbps
- Specified that wireless transmissions could take place in one of two ways
  - Through infrared light
  - By sending radio signals
- Today infrared transmissions are generally used in specialized applications

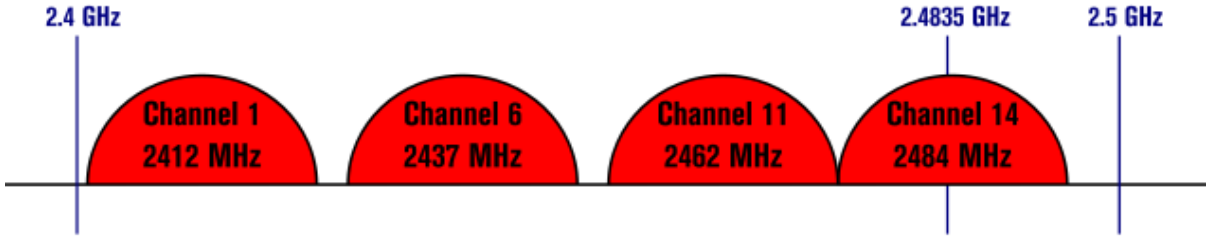
IEEE 802.11b

- Added two higher speeds (5.5 Mbps and 11 Mbps)
- 802.11b uses the ISM band
- Can support wireless devices that are up to 115 meters (375 feet) apart
  - Devices that are that far apart might not be transmitting at 11 Mbps
- Radio waves decrease in power over distance



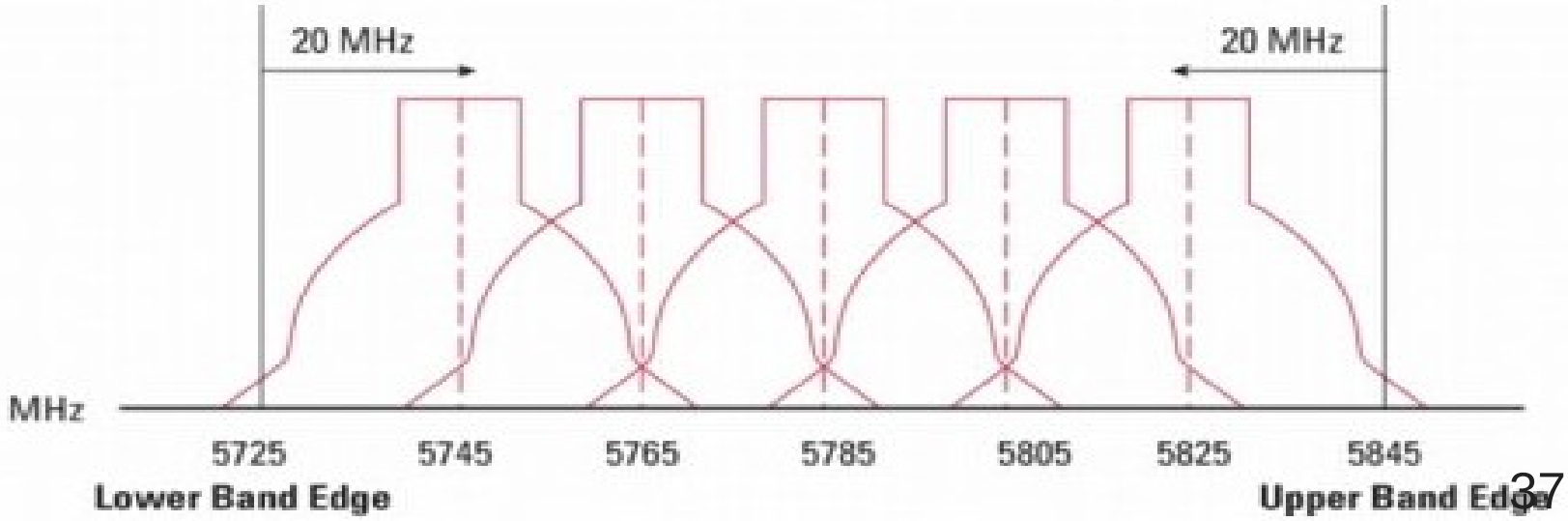
Non-Overlapping Channels for 2.4 GHz WLAN

802.11b (DSSS) channel width 22 MHz



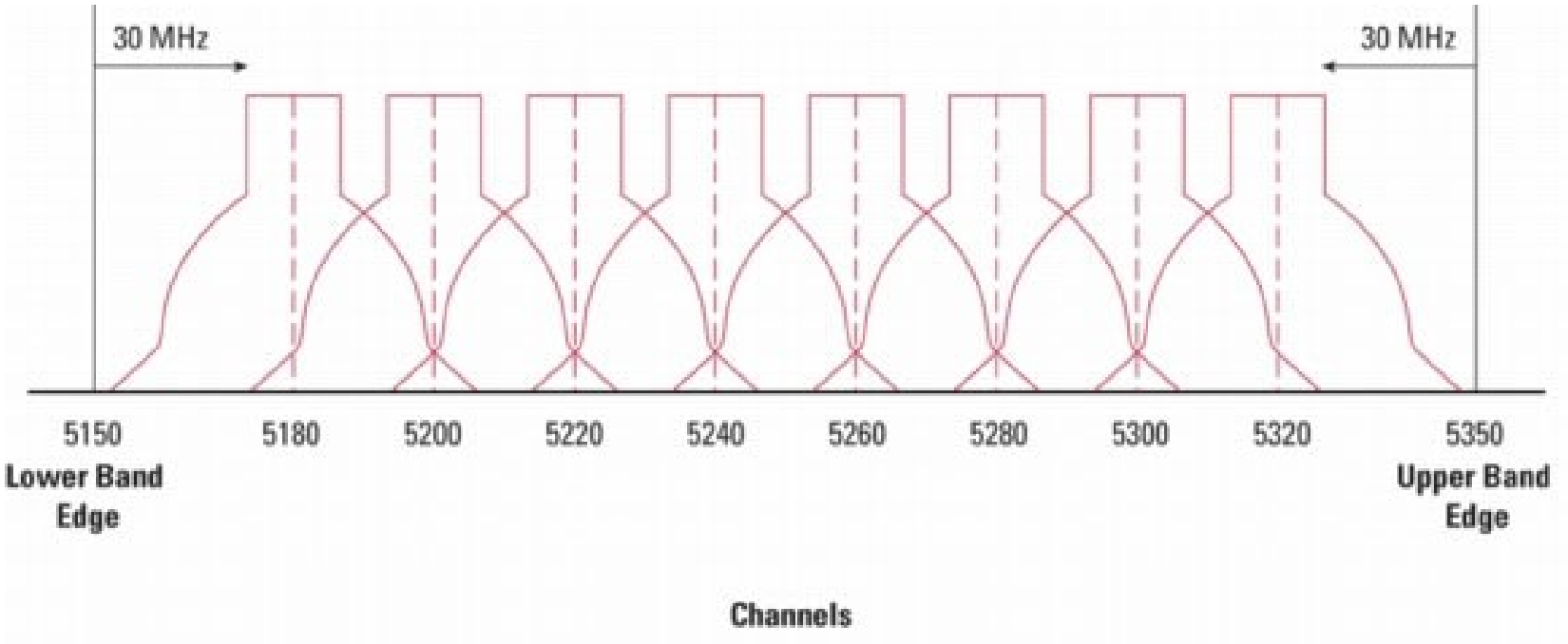
IEEE 802.11a

- 802.11a and 802.11b specifications were published at the same time by IEEE
  - 802.11b products started to appear almost immediately
  - 802.11a products did not arrive until late 2001
    - Because of the high development costs
- Supports devices that are no more than 30 meters (100 feet) apart



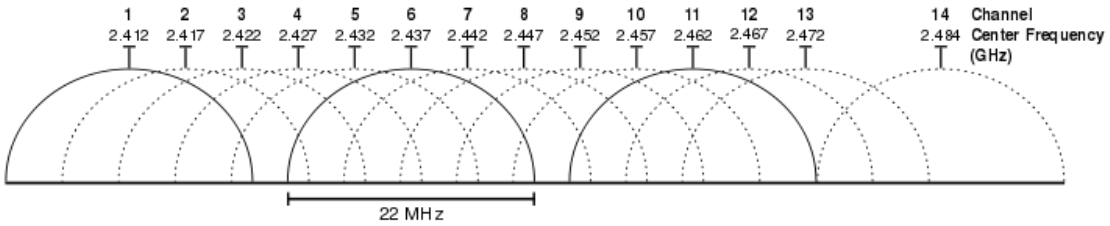
IEEE 802.11a

- Specifies a maximum rated speed of 54 Mbps
  - Also supports 48, 36, 24, 18, 12, 9, and 6 Mbps transmissions using the UNII band

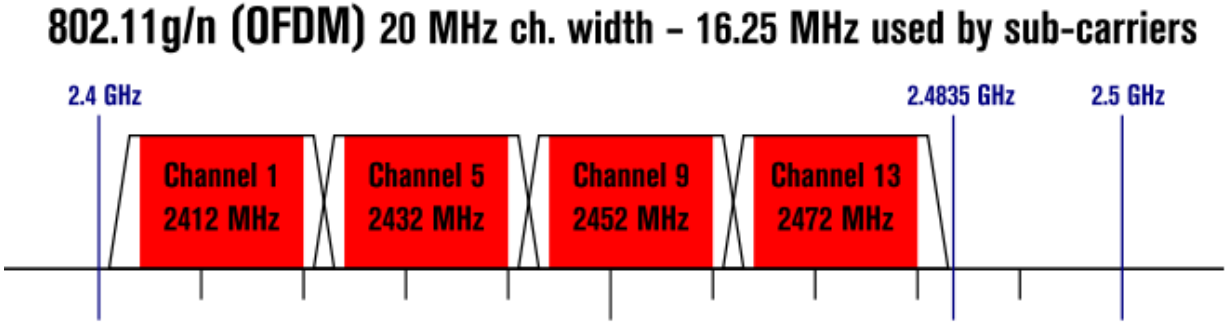


IEEE 802.11g

- Combines the best of 802.11a and 802.11b worlds
- 802.11g is backward-compatible with 802.11b
- Devices operate entirely in the ISM frequency
- Supports devices that are farther apart with higher speeds
  - Up to 115 meters (375 feet) apart

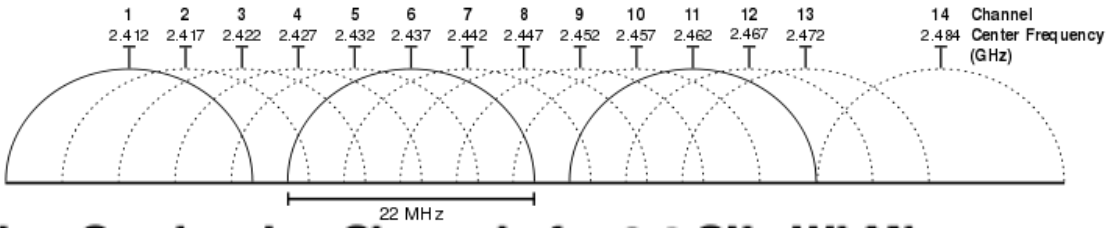


802.11b vs. 802.11g



Projected IEEE 802.11n

- Known as Multiple-Input, Multiple-Output Enhanced WLAN (MEW)
  - Or simply Multiple-Input, Multiple-Output (MIMO)
- Set standards for transmissions are to exceed 300 Mbps
- Top speed of the 802.11n standard is anywhere from 300 Mbps to 600 Mbps

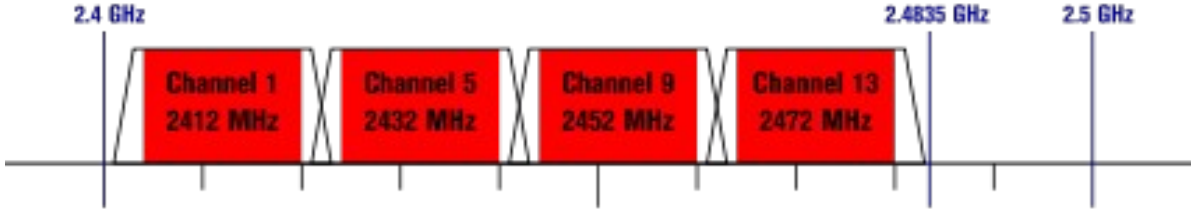


Non-Overlapping Channels for 2.4 GHz WLAN

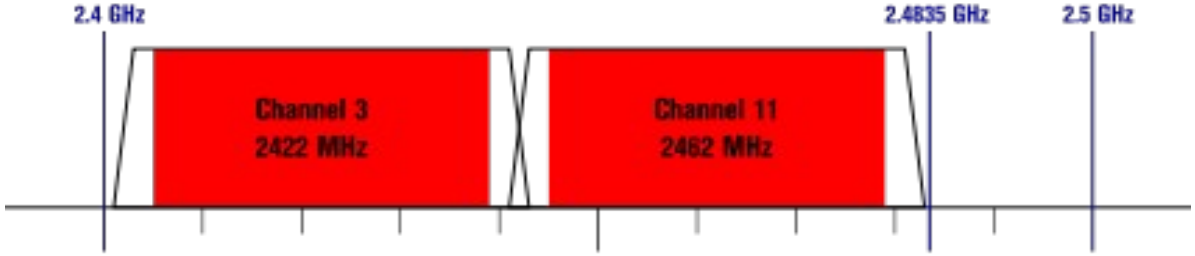
802.11b (DSSS) channel width 22 MHz



802.11g/n (OFDM) 20 MHz ch. width – 16.25 MHz used by sub-carriers



802.11n (OFDM) 40 MHz ch. width – 33.75 MHz used by sub-carriers



Projected IEEE 802.11n (continued)

Table 1-4 Summary of IEEE standards

IEEE Standard	Frequency Band	Bandwidth
802.11	ISM	2 Mbps
802.11b	ISM	11 Mbps
802.11a	UNII	54 Mbps
802.11g	ISM	54 Mbps
802.11n (proposed)	ISM	300+ Mbps

Wireless Certifications

- Certified Wireless Network Professional (CWNP)
  - The most well-known wireless certifications
  - Offered by Planet3 Wireless
  - Certifications
    - Wireless#
    - Certified Wireless Network Administrator (CWNA)
    - Certified Wireless Security Professional (CWSP)
    - Certified Wireless Analysis Professional (CWAN)
    - Certified Wireless Network Expert (CWNE)
    - Certified Wireless Network Trainers (CWNT)

Wireless Certifications (continued)

- AreTec
  - Promotes standardization in wireless technologies
  - Administers another wireless certification
  - Certifications
    - AreTec Certified Wireless Professional (AceWP)
    - AreTec Certified Wireless Developer (AceWD)
    - AreTec Certified Wireless Expert (AceWE)
- National Association of Radio and Telecommunications Engineers (NARTE)
  - Offers the Wireless System Installers Certification

Wireless Certifications (continued)

- National Association of Radio and Telecommunications Engineers (NARTE) (continued)
  - Certifications
    - Wireless Installer Technician
    - Wireless Installer Engineer
- The best-known vendor-specific certification is offered by Cisco Systems
  - Certifications
    - Cisco Wireless LAN Design Specialist
    - Cisco Wireless LAN Sales Specialist
    - Cisco Wireless LAN Support Specialist

Quiz

1. _____ uses the existing data WLAN to make and receive telephone

calls.

2. A(n) _____ has all the equipment needed for an organization to

continue running, including office space and furniture, telephone jacks, computer

equipment, and a live telecommunications link.

3. A(n) _____ provides office space, but the customer must provide and

install all the equipment needed to continue operations.

4. The greatest disadvantage to wireless LANs is

_____.

1. _____ is a general term used to describe worms, viruses, spyware, or other types of software with a malicious intent.

2. The _____ is the entire range of all radio frequencies.

Summary

- Wireless LAN applications can be found in almost every industry
- WLANs have several advantages and disadvantages
- Information security is frequently used to describe the tasks of guarding information that is in a digital format
- Wireless security presents a number of challenges
  - Unauthorized users accessing the network
  - Attackers viewing transmitted data
  - Employees installing rogue access points
  - Weaknesses of older wireless security defenses

Summary (continued)

- Primary standard-setting and regulatory bodies
  - IEEE
  - Wi-Fi Alliance
  - The U.S. FCC
- Since the late 1990s, the IEEE has approved four standards for wireless LANs
  - 802.11
  - 802.11b
  - 802.11a
  - 802.11g
  - 802.11n