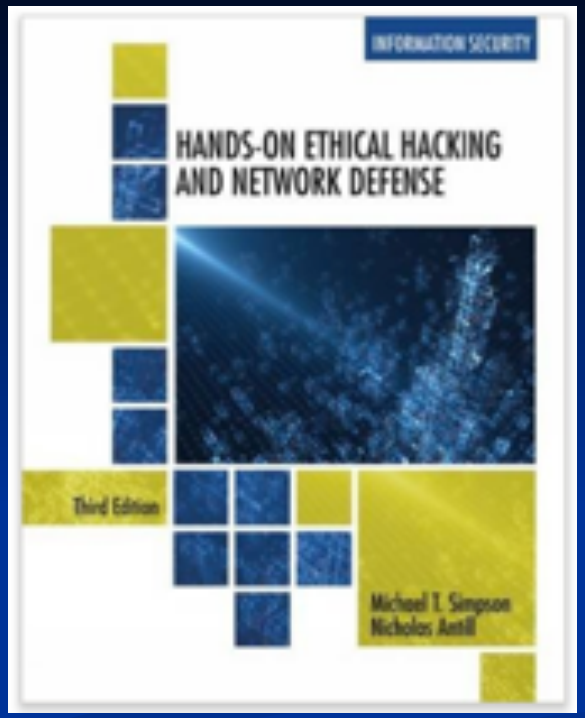
THOMSON
COURSE TECHNOLOGY

Hands-On Ethical Hacking and Network Defense



Chapter 11
Hacking Wireless Networks

Last revised 1-11-17

Objectives

- Explain wireless technology
- Describe wireless networking standards
- Describe the process of authentication
- Describe wardriving
- Describe wireless hacking and tools used by hackers and security professionals

Understanding Wireless Technology

- For a wireless network to function, you must have the right hardware and software
- Wireless technology is part of our lives
  - Baby monitors
  - Keyless entry systems
  - Cellphones and smartphones
  - GPS
  - Remote controls
  - Garage door openers
  - Two-way radios
  - Bluetooth speakers

Components of a Wireless Network

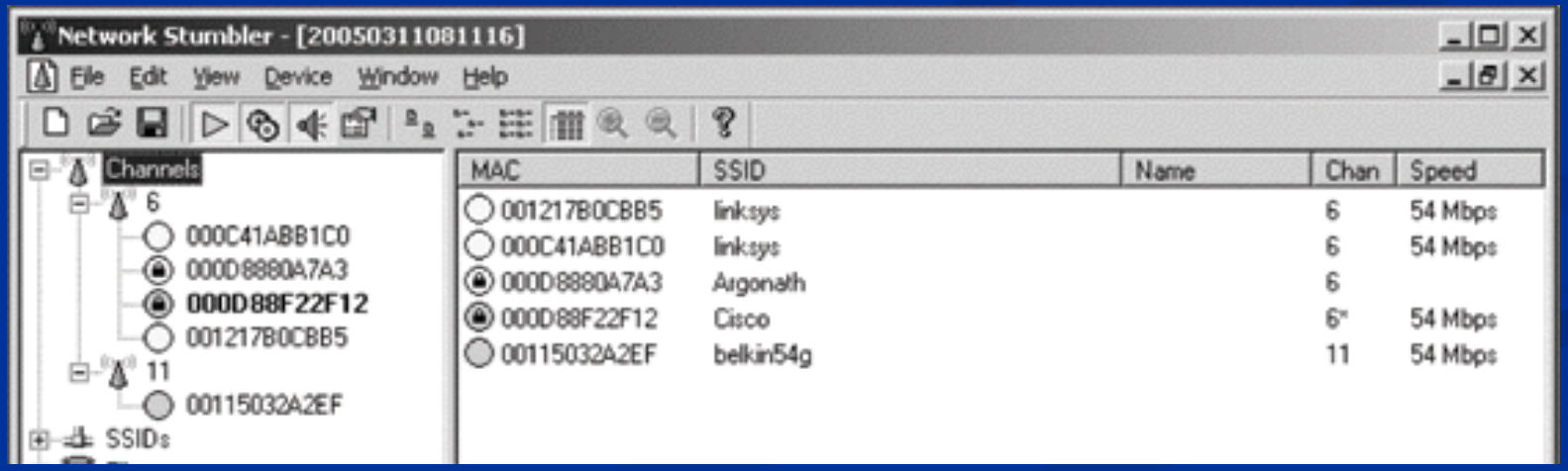
- A wireless network has only three basic components
  - Access Point (AP)
  - Wireless network interface card (WNIC)
  - Ethernet cable

Access Points

- An access point (AP) is a transceiver that connects to an Ethernet cable
  - It bridges the wireless network with the wired network
    - Not all wireless networks connect to a wired network
  - Most companies have Wireless LANs (WLANs) that connect to their wired network topology

Access Points

- The AP is where channels are configured
- An AP enables users to connect to a LAN using wireless technology
  - An AP is available only within a defined area

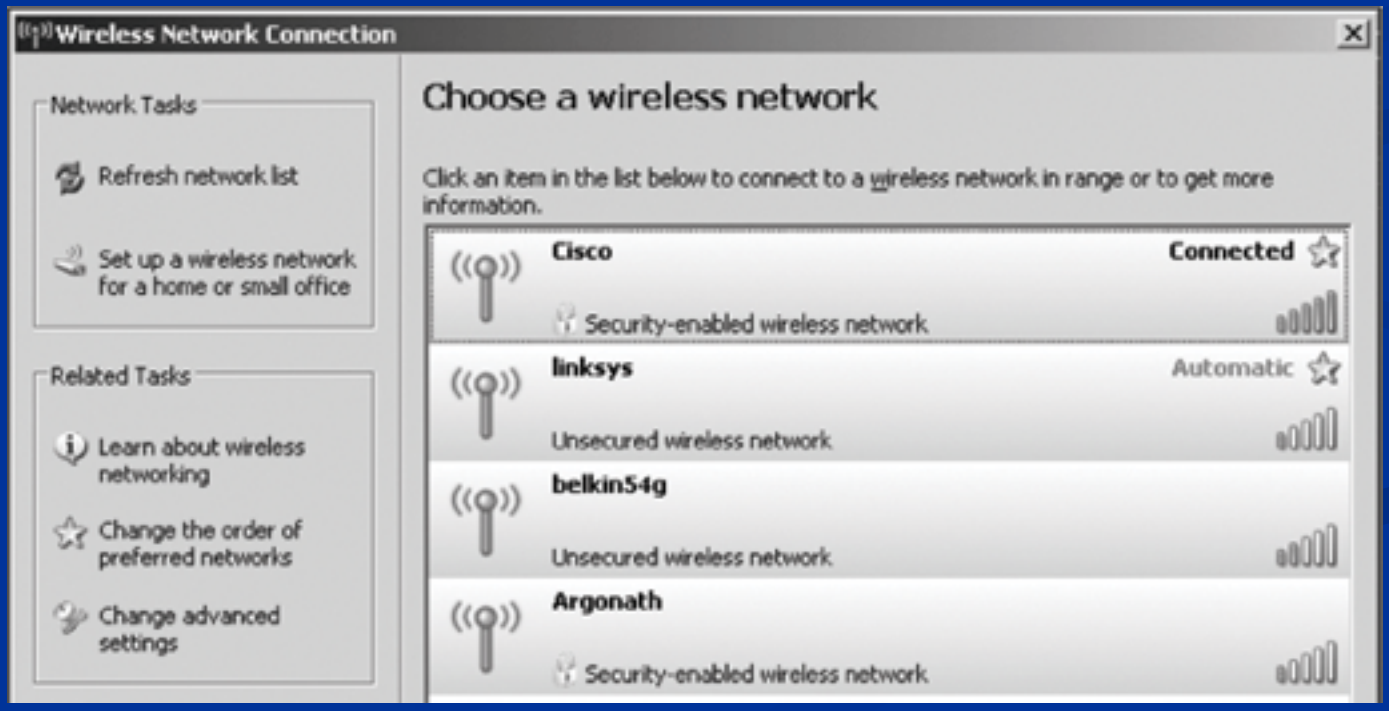


Service Set Identifiers (SSIDs)

- Name used to identify the wireless local area network (WLAN)
- The SSID is configured on the AP
  - Unique 1- to 32-character alphanumeric name
  - Name is case sensitive
- Wireless computers need to configure the SSID before connecting to a wireless network

Service Set Identifiers (SSIDs)

- SSID is transmitted with each packet
  - Identifies which network the packet belongs
- The AP usually broadcasts the SSID



Service Set Identifiers (SSIDs)

- Many vendors have SSIDs set to a default value that companies never change
- An AP can be configured to not broadcast its SSID until after authentication
  - Wireless hackers can attempt to guess the SSID
- Verify that your clients or customers are not using a default SSID

Table 11-1 Default SSIDs

Vendor	Default SSIDs
3Com	3Com
Apple	Airport Network
Belkin (54G)	Belkin54g
Cisco	Tsunami
Compaq	Compaq
D-Link	WLAN, default
Dell	Wireless
Intel	Intel, 101, xlan, 195
Linksys	linksys, Wireless, linksys-g
Microsoft	MSNHOME
Netgear	Wireless, NETGEAR
SMC	WLAN, BRIDGE, SMC
Symantec	101
US Robotics	WLAN, USR9106, USR808054

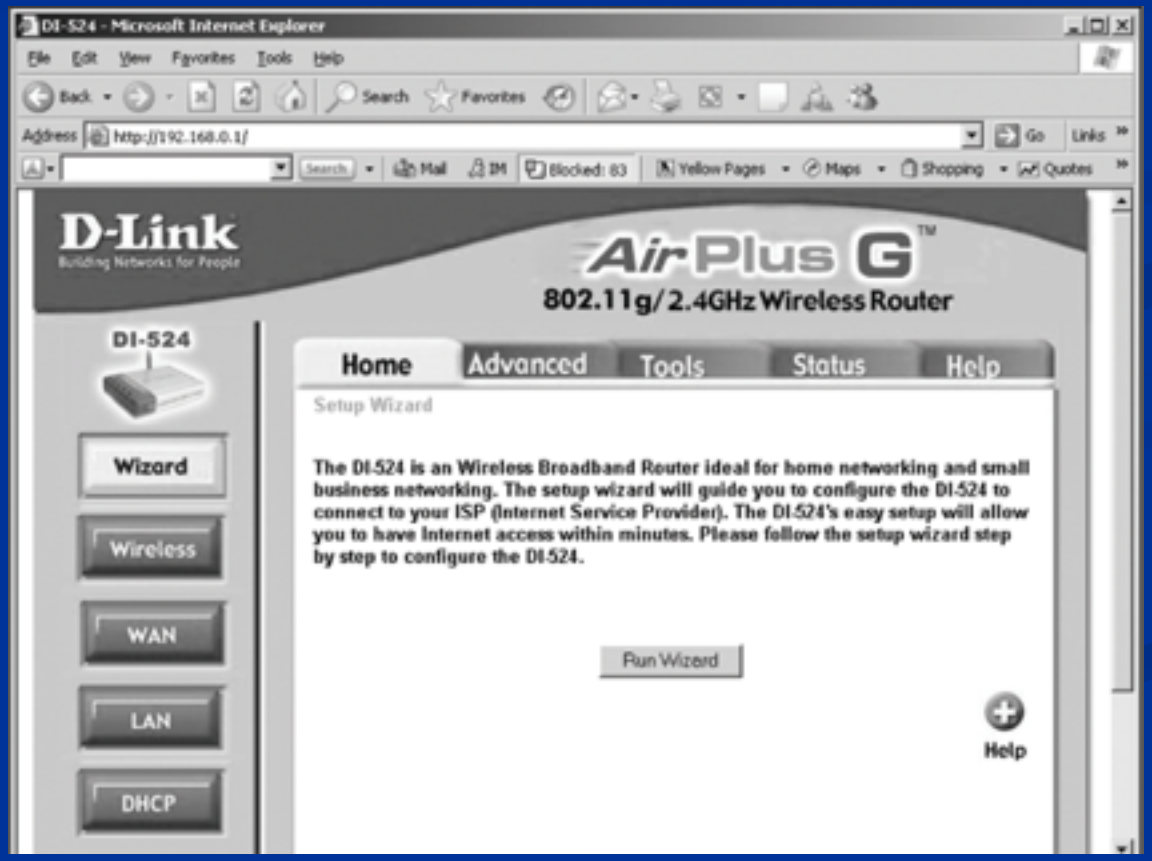
- See links Ch 11a, b

Configuring an Access Point

- Configuring an AP varies depending on the hardware
  - Most devices allow access through any Web browser
  - Enter IP address on your Web browser and provide your user logon name and password

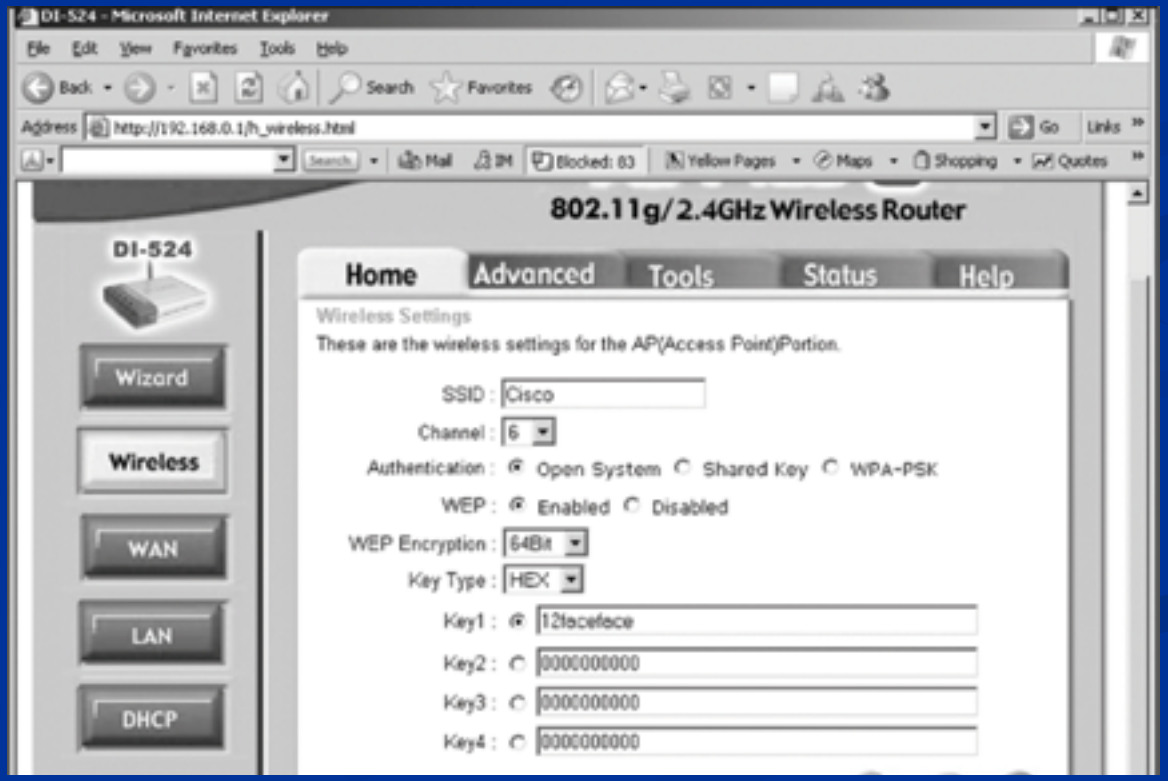
Wireless Router

- A wireless router includes an access point, a router, and a switch



Configuring an Access Point

- Wireless Configuration Options
  - SSID
  - Wired Equivalent Privacy (WEP) encryption
  - WPA (WiFi Protected Access) is better



Configuring an Access Point (continued)

- Steps for configuring a D-Link wireless router (continued)
  - Turn off SSID broadcast
  - You should also change your SSID

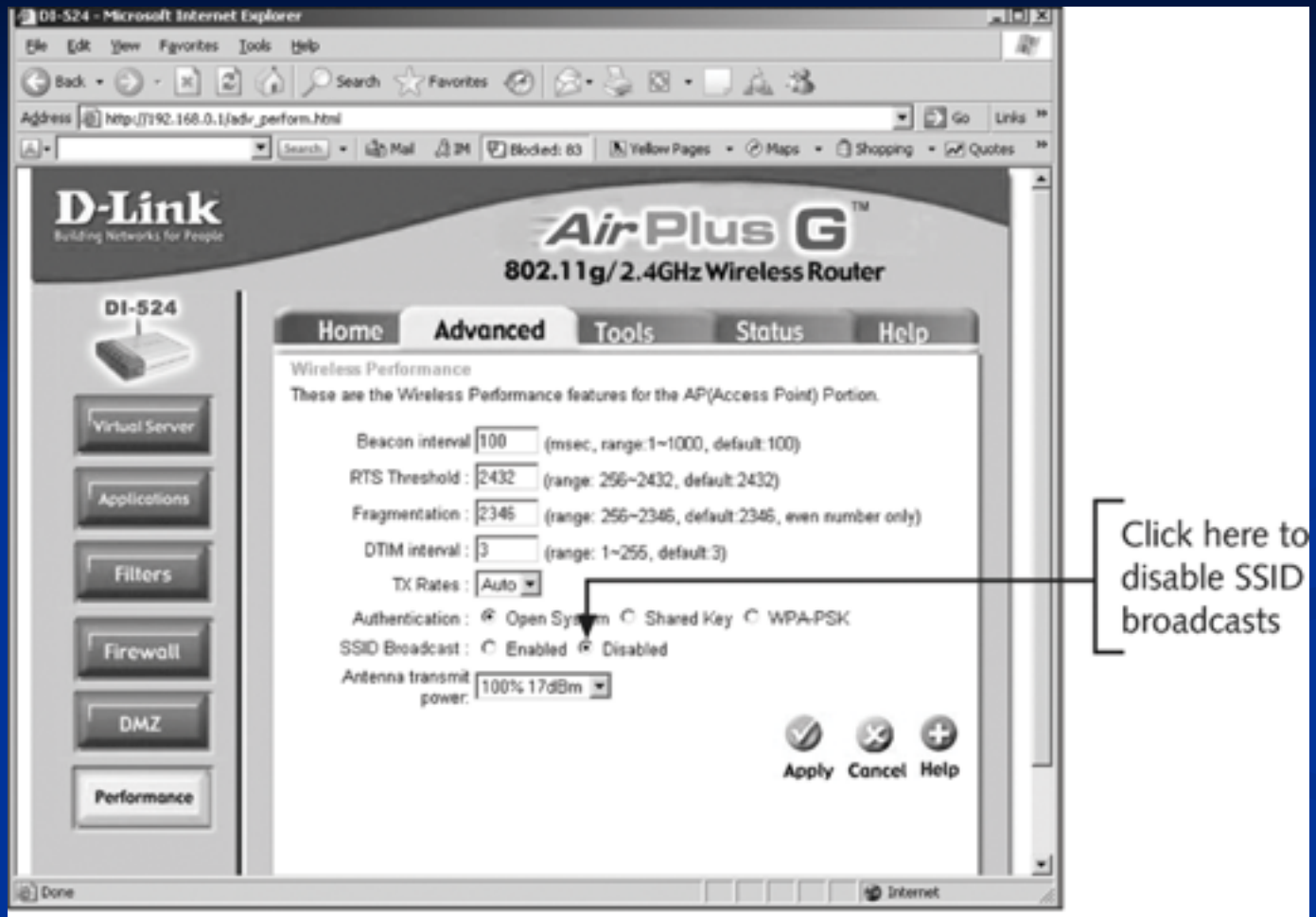


Figure 11-8 Disabling SSID broadcasts

Wireless NICs

- For wireless technology to work, each node or computer must have a wireless NIC
- NIC's main function
  - Converting the radio waves it receives into digital signals the computer understands

Wireless NICs

- There are many wireless NICs on the market
  - Choose yours depending on how you plan to use it
  - Some tools require certain specific brands of NICs
    - Cracking WEP requires NICs that can use monitor mode or perform packet injection

Understanding Wireless Network Standards

- A standard is a set of rules formulated by an organization
- Institute of Electrical and Electronics Engineers (IEEE)
  - Defines several standards for wireless networks

IEEE Standards

- Standards pass through these groups:
  - Working group (WG)
  - Sponsor Executive Committee (SEC)
  - Standards Review Committee (RevCom)
  - IEEE Standards Board
- IEEE Project 802
  - LAN and WAN standards

The 802.11 Standard

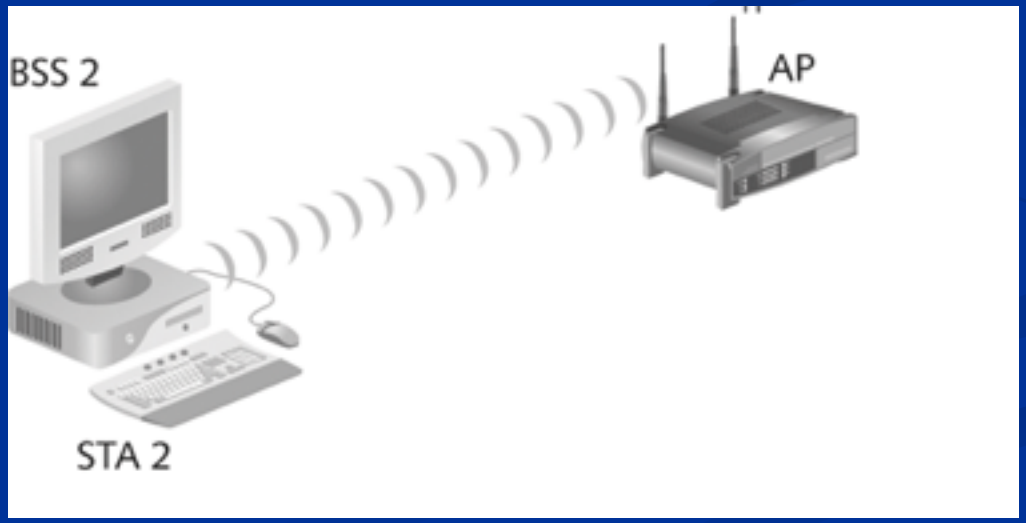
- The first wireless technology standard
- Defined wireless connectivity at 1 Mbps and 2 Mbps within a LAN
- Applied to layers 1 and 2 of the OSI model
- Wireless networks cannot detect collisions
  - Carrier sense multiple access/collision avoidance (CSMA/CA) is used instead of CSMA/CD

Addressing

- Wireless LANs do not have an address associated with a physical location
  - An addressable unit is called a station (STA)

The Basic Architecture of 802.11

- 802.11 uses a basic service set (BSS) as its building block
  - Computers within a BSS can communicate with each other



The Basic Architecture of 802.11

- To connect two BSSs, 802.11 requires a distribution system (DS)

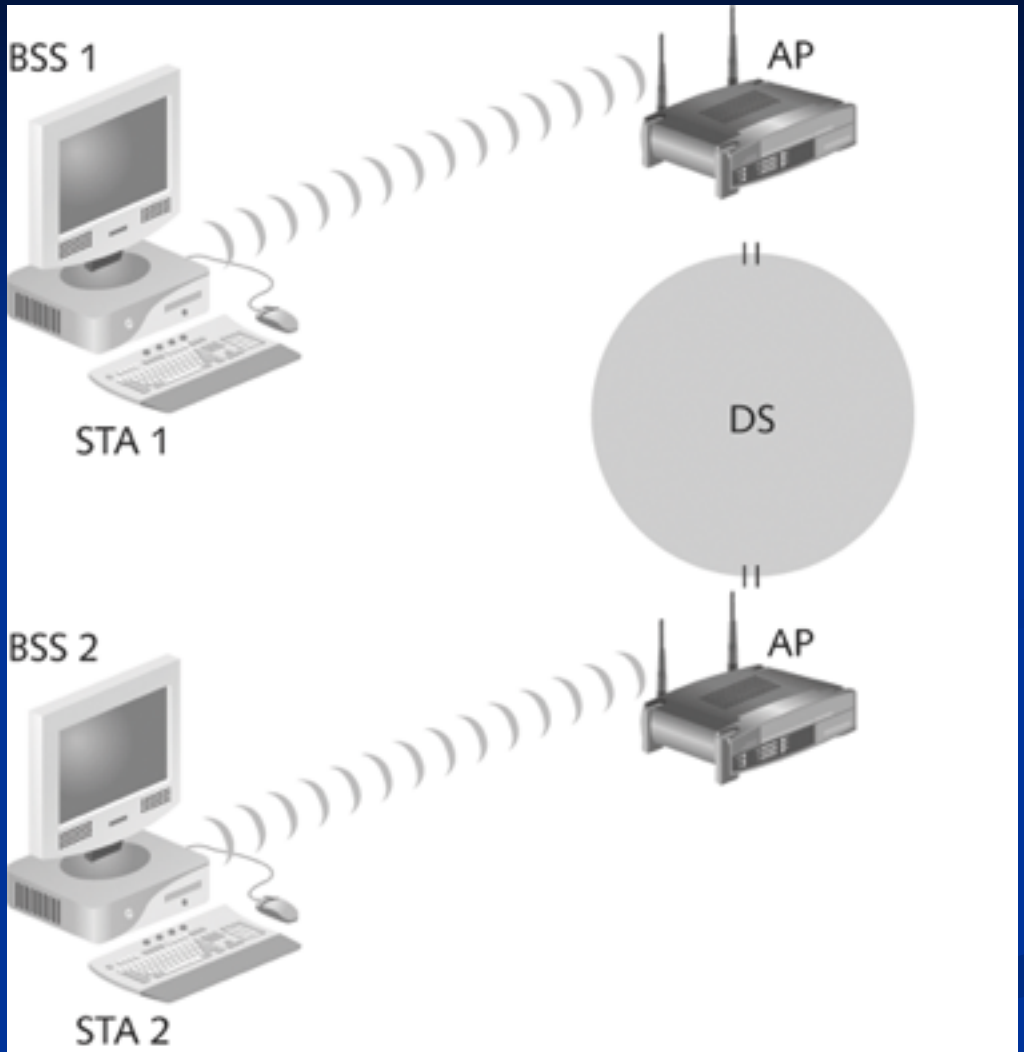
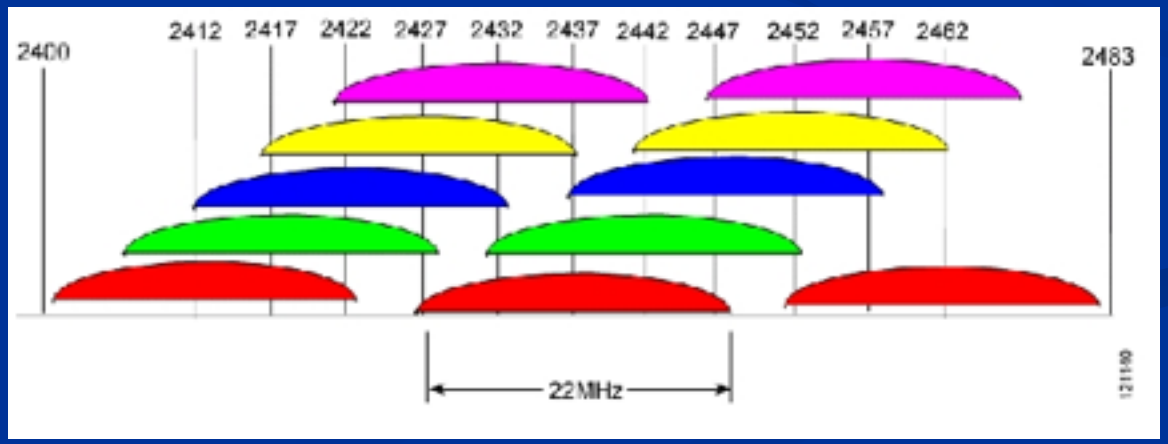


Figure 11-9 Connecting two wireless remote stations

Frequency Range

- In the United States, Wi-Fi uses frequencies near 2.4 GHz
  - (Except 802.11a at 5 GHz)
  - There are 11 channels, but they overlap, so only three are commonly used
    - See links Ch 11c & Ch 11zh



Infrared (IR)

- Infrared light can’t be seen by the human eye
- IR technology is restricted to a single room or line of sight
- IR light cannot penetrate walls, ceilings, or floors
  - Image: IR transmitter for wireless headphones

IEEE Additional 802.11 Projects

- 802.11a
  - Created in 1999
  - Operating frequency 5 GHz
  - Throughput 54 Mbps

IEEE Additional 802.11 Projects (continued)

- 802.11b
  - Operates in the 2.4 GHz range
  - Throughput 11 Mbps
  - Also referred as Wi-Fi (wireless fidelity)
  - Allows for 11 channels to prevent overlapping signals
    - Effectively only three channels (1, 6, and 11) can be used in combination without overlapping
  - Introduced Wired Equivalent Privacy (WEP)

IEEE Additional 802.11 Projects (continued)

- 802.11e
  - It has improvements to address the problem of interference
    - When interference is detected, signals can jump to another frequency more quickly
- 802.11g
  - Operates in the 2.4 GHz range
  - Throughput increased from 11 Mbps to 54 Mbps

IEEE Additional 802.11 Projects (continued)

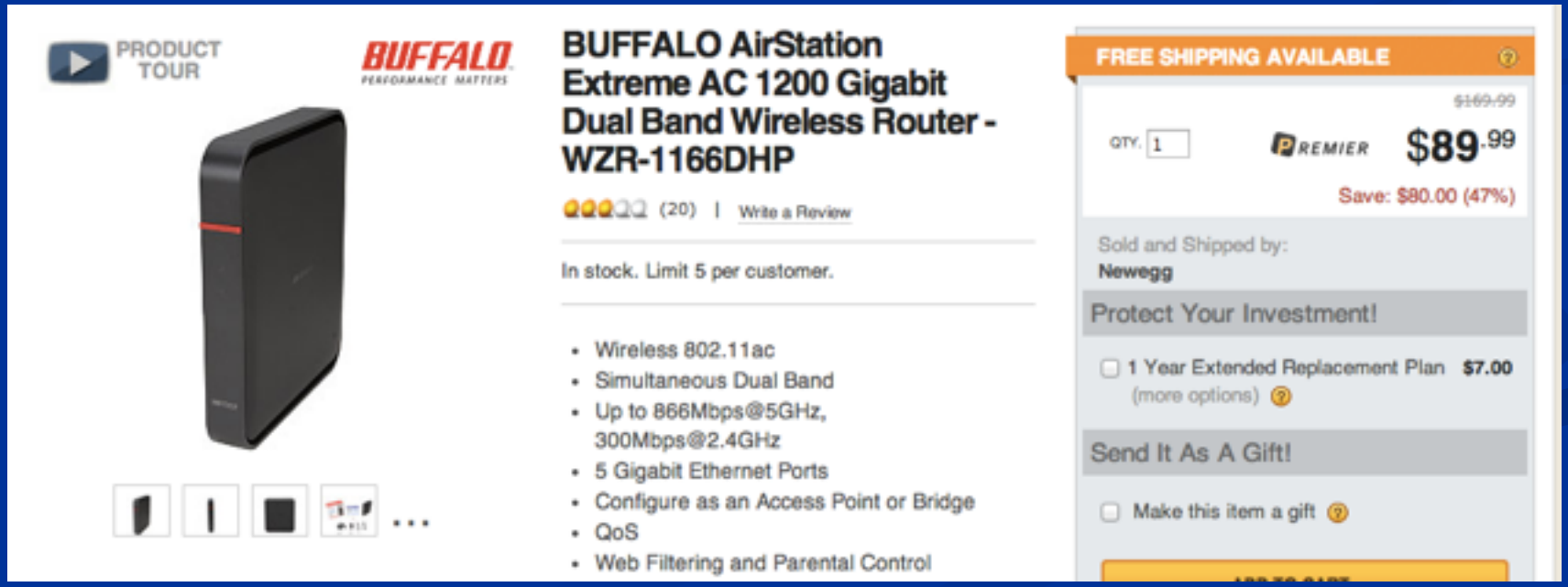
- 802.11i
  - Introduced Wi-Fi Protected Access (WPA)
  - Corrected many of the security vulnerabilities of 802.11b
- 802.11n
  - Finalized in 2009
  - Can use up to four spatial streams with multiple antennas
  - Speeds up to 600 Mbps
    - Link 11zh

802.11n Devices

- Images from newegg.com

802.11ac

- Like 802.11n, but wider bands, more spatial channels
- For sale at Newegg on 4-12-14



802.11ac on MacBook Air

- Starting with the 2013 model

802.11ad (WiGig)

- New physical layer
- 60 GHz, up to 7 Gbps
- Short-range (up to 30 feet) (Link Ch 11zq)


appleapple.top/iphone-8-will-get-support-for-the-new-802-11-ad-standard-wigig-at-a-speed-of-8-gbps/
iPhone 8 will get support for the new 802.11 ad standard, WiGig at a speed of 8 Gbps
25.10.2016
0 Comments
Search
Google™ Custom Search

IEEE Additional 802.11 Projects (continued)

- HiperLAN2
  - European WLAN standard
  - It is not compatible with 802.11 standards

IEEE Additional 802.11 Projects (continued)

- 802.15
  - Addresses networking devices within one person's workspace
    - Called wireless personal area network (WPAN)
  - Bluetooth is one of six 802.15 standards
    - Image from ubergizmo.com

IEEE Additional 802.11 Projects (continued)

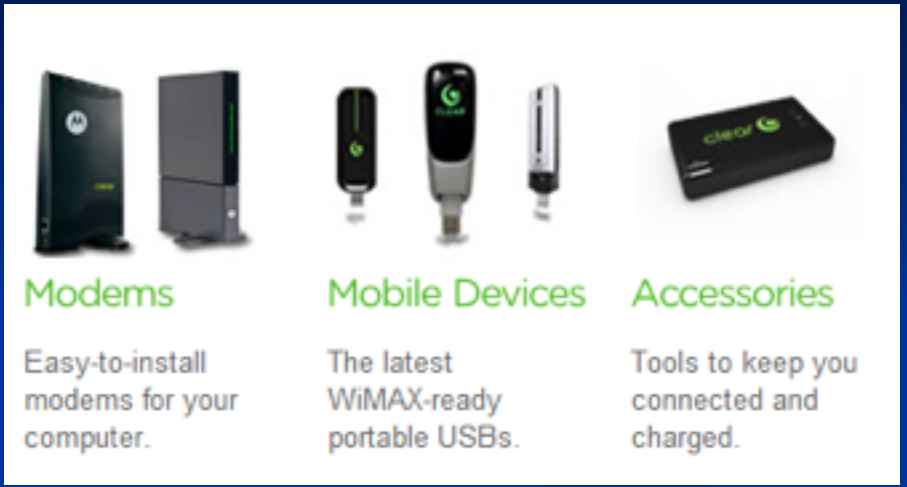
- Bluetooth
  - Defines a method for interconnecting portable devices without wires
  - Maximum distance allowed is 10 meters
  - It uses the 2.45 GHz frequency band
  - Throughput of up to 2.1 Mbps for Bluetooth 2.0
    - Up to 24 Mbps for Bluetooth 3.0 (not 12 Mbps as stated in the textbook, p. 316)
    - Link Ch 11zg

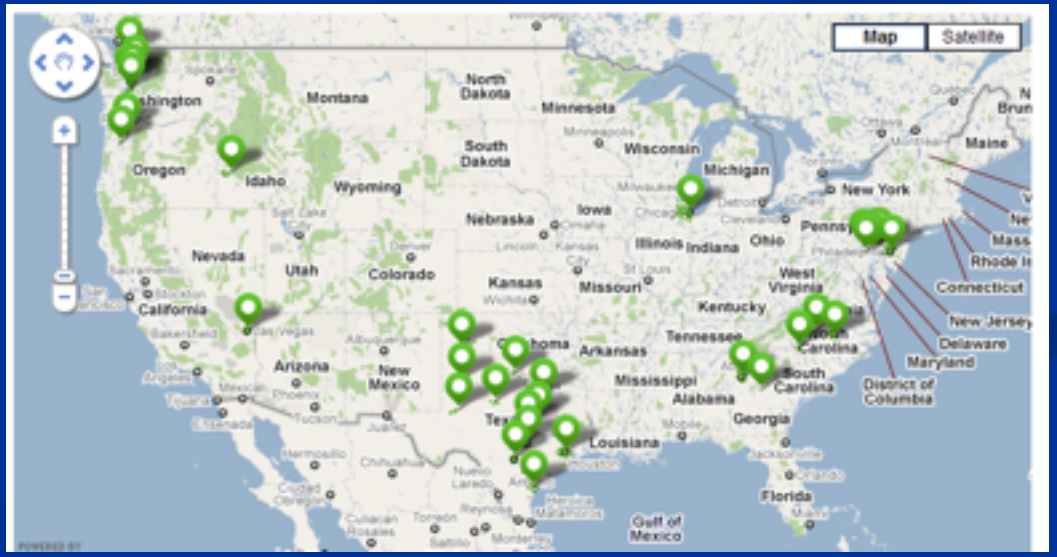
IEEE Additional 802.11 Projects (continued)

- 802.16 (also called WIMAX)
  - Addresses the issue of wireless metropolitan area networks (MANs)
  - Defines the WirelessMAN Air Interface
  - Range of up to 30 miles
  - Throughput of up to 120 Mbps
- 802.20
  - Addresses wireless MANs for mobile users who are sitting in trains, subways, or cars traveling at speeds up to 150 miles per hour

WIMAX

- Rolled out, then rolled back
- Sprint abandoned WiMax as of 2016 (link Ch 11zs)



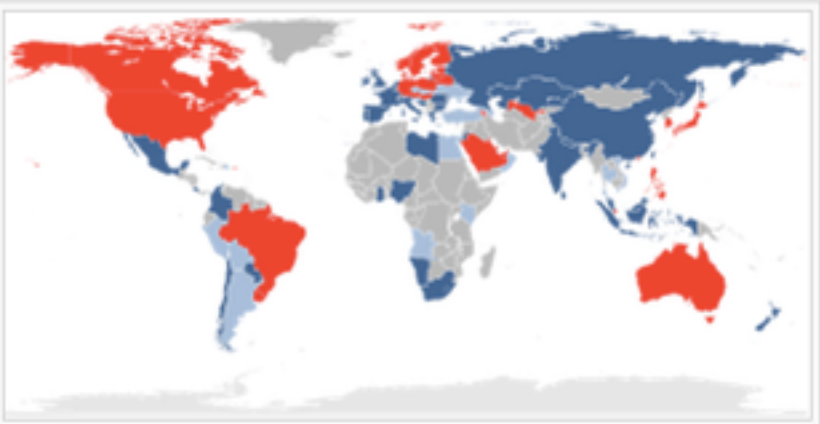


LTE

3GPP Long Term Evolution

From Wikipedia, the free encyclopedia

3GPP Long Term Evolution, referred to as **LTE** and marketed as **4G LTE**, is a standard for wireless communication of high-speed data for mobile phones and data terminals. It is based on the GSM/EDGE and UMTS/HSPA network technologies, increasing the capacity and speed using new modulation techniques.[1][2] The



Adoption of LTE technology as of January 5, 2012.

Countries with commercial LTE service

Countries with commercial LTE network deployment on-going or planned

Countries with LTE trial systems (pre-commitment)

Standard	Frequency	Maximum rate	Modulation method
802.11	2.4 GHz	1 or 2 Mbps	FHSS/DSSS
802.11a	5 GHz	54 Mbps	OFDM
802.11b	2.4 GHz	11 Mbps	DSSS
802.11g	2.4 GHz	54 Mbps	OFDM
802.11n	2.4 GHz	600 Mbps	OFDM
802.15	2.4 GHz	2 Mbps	FHSS
802.16 (WiMAX)	10–66 GHz	120 Mbps	OFDM
802.20 (Mobile Wireless Access Working Group)	Below 3.5 GHz	1 Mbps	OFDM
Bluetooth	2.4 GHz	24 Mbps	Gaussian frequency shift keying (GFSK)
HiperLAN/2	5 GHz	54 Mbps	OFDM

One Day in Oct 2013 on CCSF Wireless

Top operating systems

#	OS	# Clients ▾	% Clients	Usage	% Usage
1	Apple iPhone	2394	29.0%	1.21 TB	25.1%
2	Android	1596	19.3%	636.23 GB	12.9%
3	Mac OS X	1173	14.2%	842.44 GB	17.1%
4	Apple iPad	1062	12.9%	816.13 GB	16.5%
5	Windows 7	789	9.6%	564.99 GB	11.5%
6	Windows 8	504	6.1%	489.22 GB	9.9%
7	Apple iPod	321	3.9%	190.58 GB	3.9%
8	Apple iOS	87	1.1%	3.07 GB	0.1%
9	Windows XP	63	0.8%	54.99 GB	1.1%
10	Windows Vista	45	0.5%	21.31 GB	0.4%

Wireshark Monitor Mode

- Use a Mac
- In Wireshark, Capture, Options
- In the en0 line, on the far right, enable Monitor
- Restart Wireshark
- In the en0 line, Link-Layer Header, select "802.11 plus radiotap header"

Understanding Authentication

- Wireless technology brings new security risks to a network
- *Authentication*
  - Establishing that a user is authentic—authorized to use the network
  - If authentication fails, anyone in radio range can use your network

The 802.1X Standard

- Defines the process of authenticating and authorizing users on a WLAN
- Basic concepts
  - Point-to-Point Protocol (PPP)
  - Extensible Authentication Protocol (EAP)
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)

Point-to-Point Protocol (PPP)

- Many ISPs use PPP to connect dial-up or DSL users
- PPP handles authentication with a user name and password, sent with PAP or CHAP
  - PAP (Password Authentication Protocol) sends passwords unencrypted
    - Vulnerable to trivial sniffing attacks
- See link Ch 11f

CHAP Vulnerability

- CHAP (Challenge-Handshake Authentication Protocol)
  - Server sends a Challenge with a random value
  - Client sends a Response, hashing the random value with the secret password
- This is still vulnerable to a sort of session hijacking attack (see links Ch 11e)
  - "Pass the hash"

Extensible Authentication Protocol (EAP)

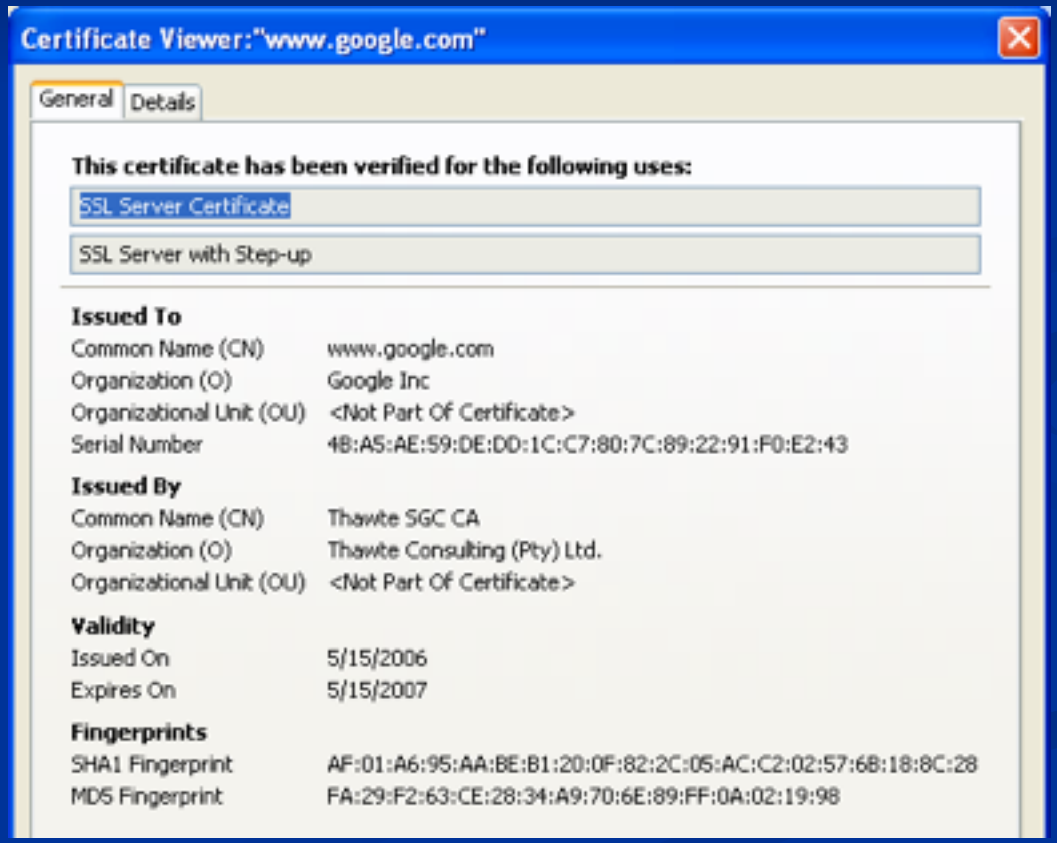
- EAP is an enhancement to PPP
- Allows a company to select its authentication method
  - Certificates
  - Kerberos
    - Kerberos is used on LANs for authentication
    - Uses Tickets and Keys
    - Used by Windows 2000, XP, and 2003 Server by default
    - Not common on WLANS

X.509 Certificate

- Record that authenticates network entities
- Identifies
  - The owner
  - The certificate authority (CA)
  - The owner's public key
    - See link Ch 11j

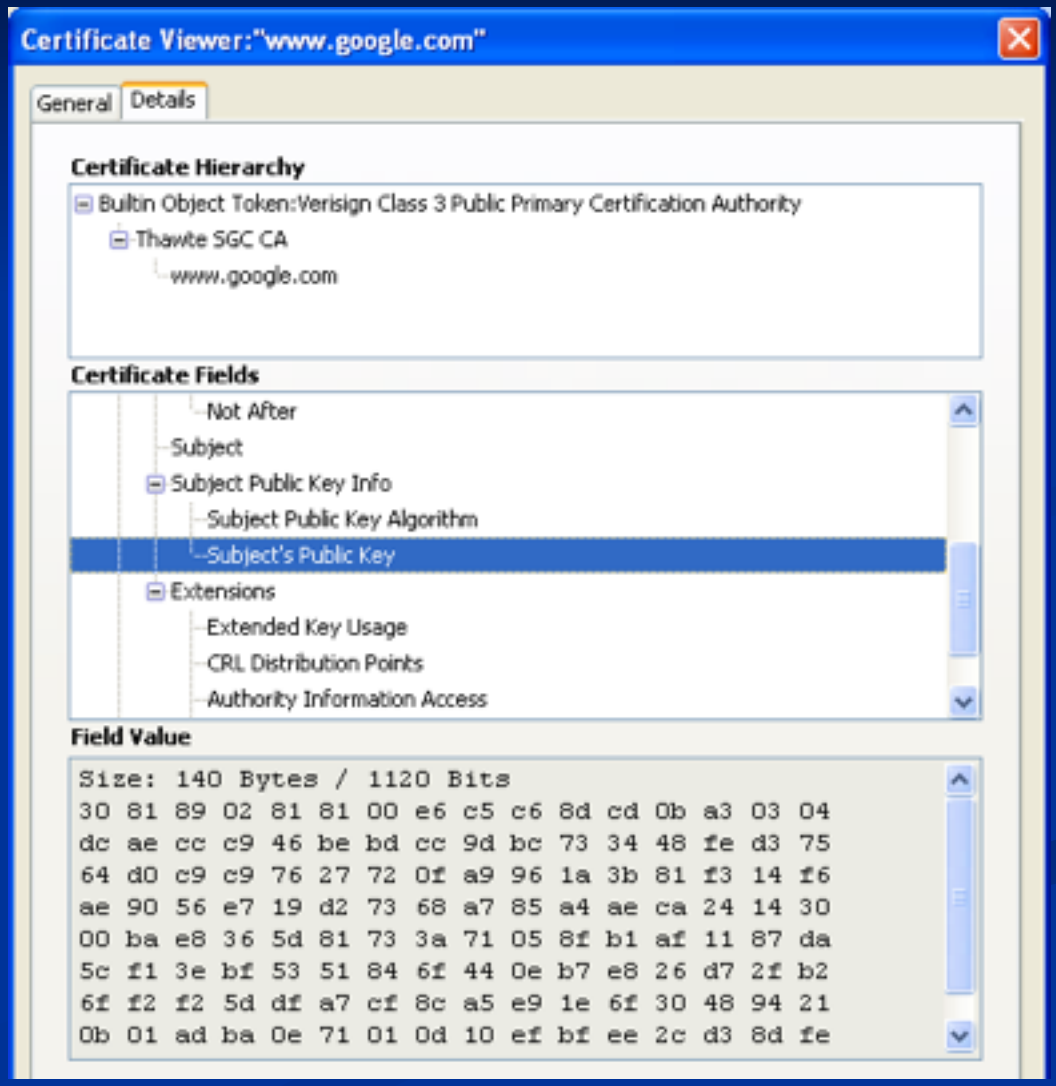
Sample X.509 Certificate

- Go to gmail.com
- Double-click the padlock



Public Key

- Your browser uses the Public Key to encrypt data so only Gmail can read it



LEAP

- Lightweight Extensible Authentication Protocol (LEAP)
  - A Cisco product
  - Vulnerable, but Cisco didn't care
  - Joshua Wright wrote the ASLEAP hacking tool to crack LEAP, and forced Cisco to develop a better protocol
    - See link Ch 11g

Reaction to ASLEAP

- *“Within months, some "helpful" person invested their time into generating a cracker tool. Publicizing the threat was a service to everyone, but I leave it as an exercise for readers to determine what satisfaction is obtained by the authors of tools that turn threat into reality and lay waste to millions of dollars of investments.”*
- --"Real 802.11 Security", William Arbaugh and Jon Edney, as quoted in link Ch 11g

Narcisstic Vulnerability Pimps

Verizon dubs sec researchers 'narcissistic vulnerability pimps'

In defense of full-disclosure

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Security, 23rd April 2010 19:51 GMT

Updated In an official blog post, an employee in Verizon's Risk Intelligence unit has taken aim at researchers who disclose security flaws, calling them "Narcissistic vulnerability pimps" and comparing them to criminals.

"Have you ever heard of a terrorist referred to as a 'demolition engineer?'" the unnamed author of the rant asked, one presumes rhetorically. "How about a thief as a 'locksmith?' No? Well, that's because most fields don't share the InfoSec industry's ridiculous yet long-standing inability to distinguish the good guys from the bad guys."

- Link Ch 11zk

More Secure EAP Methods

- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
  - Secure but rarely used, because both client and server need certificates signed by a CA
- Protected EAP (PEAP) and Microsoft PEAP
  - Very secure, only requires server to have a certificate signed by a CA
- See link Ch 11h

802.1X components

- Supplicant
  - The user accessing a WLAN
- Authenticator
  - The AP
- Authentication server
  - Checks an account database to see if user's credentials are acceptable
  - May use RADIUS (Remote Access Dial-In User Service)
- See link Ch 11k

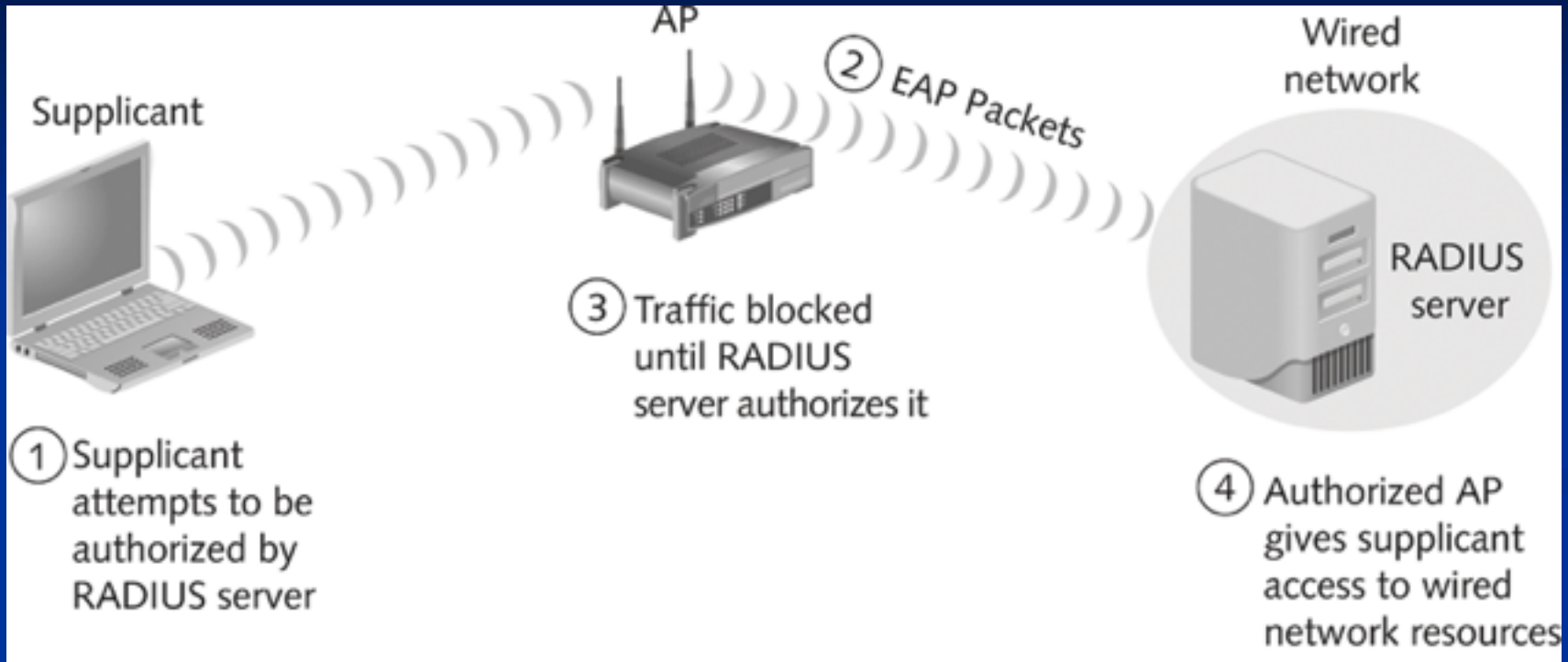


Figure 11-11 A supplicant connecting to an AP and a RADIUS server

Wired Equivalent Privacy (WEP)

- Part of the 802.11b standard
- Encrypts data on a wireless network
- WEP has many vulnerabilities
- To crack WEP, see links Ch 11l, 11m

Wi-Fi Protected Access (WPA)

- Specified in the 802.11i standard
- Replaces WEP
- WPA improves encryption by using Temporal Key Integrity Protocol (TKIP)

TKIP Enhancements

- Message Integrity Check (MIC)
  - Prevent attacker from injecting forged packets
- Extended Initialization Vector (IV) with sequencing rules
  - Prevent replays (attacker re-sending copied packets)

TKIP Enhancements

- Per-packet key mixing
  - MAC addresses are used to create a key
  - Each link uses a different key
- Rekeying mechanism
  - Provides fresh keys
  - Prevents attackers from reusing old keys

WPA Adds 802.1x

- WPA also adds an authentication mechanism implementing 802.1X and EAP
  - This was not available in WEP

WPA Versions

- WPA and WPA-2
  - WPA only implements part of 802.11i, using TKIP
    - Can run on older hardware
  - WPA2 implements the full IEEE 802.11i security standard, using CCMP
    - More secure
      - Link Ch 11zj

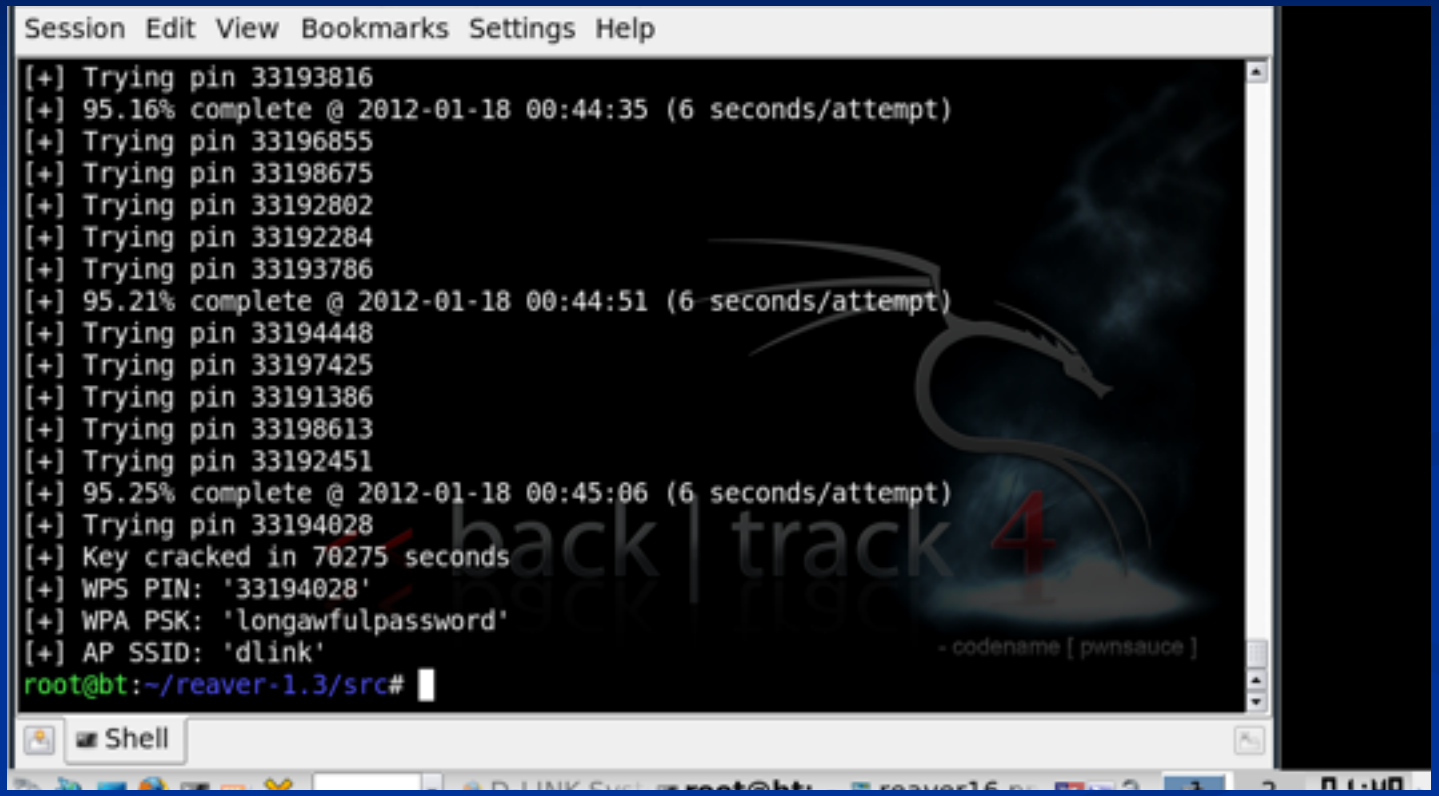
Pre-Shared Key v. 802.1x

- Both WPA and WPA-2 can run in either mode
- Pre-Shared Key uses a passphrase the user types into each device
  - Less secure because the user might choose a guessable passphrase, and all devices on the WLAN use the same passphrase
- 802.1x uses a server to manage keys
  - Each user has a different key
  - More secure
    - Link Ch 11zj

Hacking WPA

- In 2008 and 2009, some new WPA attacks were developed, for its weakest form (TKIP)
  - These attacks allow injection of spoofed packets for limited periods of time
    - Up to 18 minutes
  - They don't find the WPA key, but they are a warning that it's time to go to WPA-2

Attacking WPS



- Link Ch 11zo

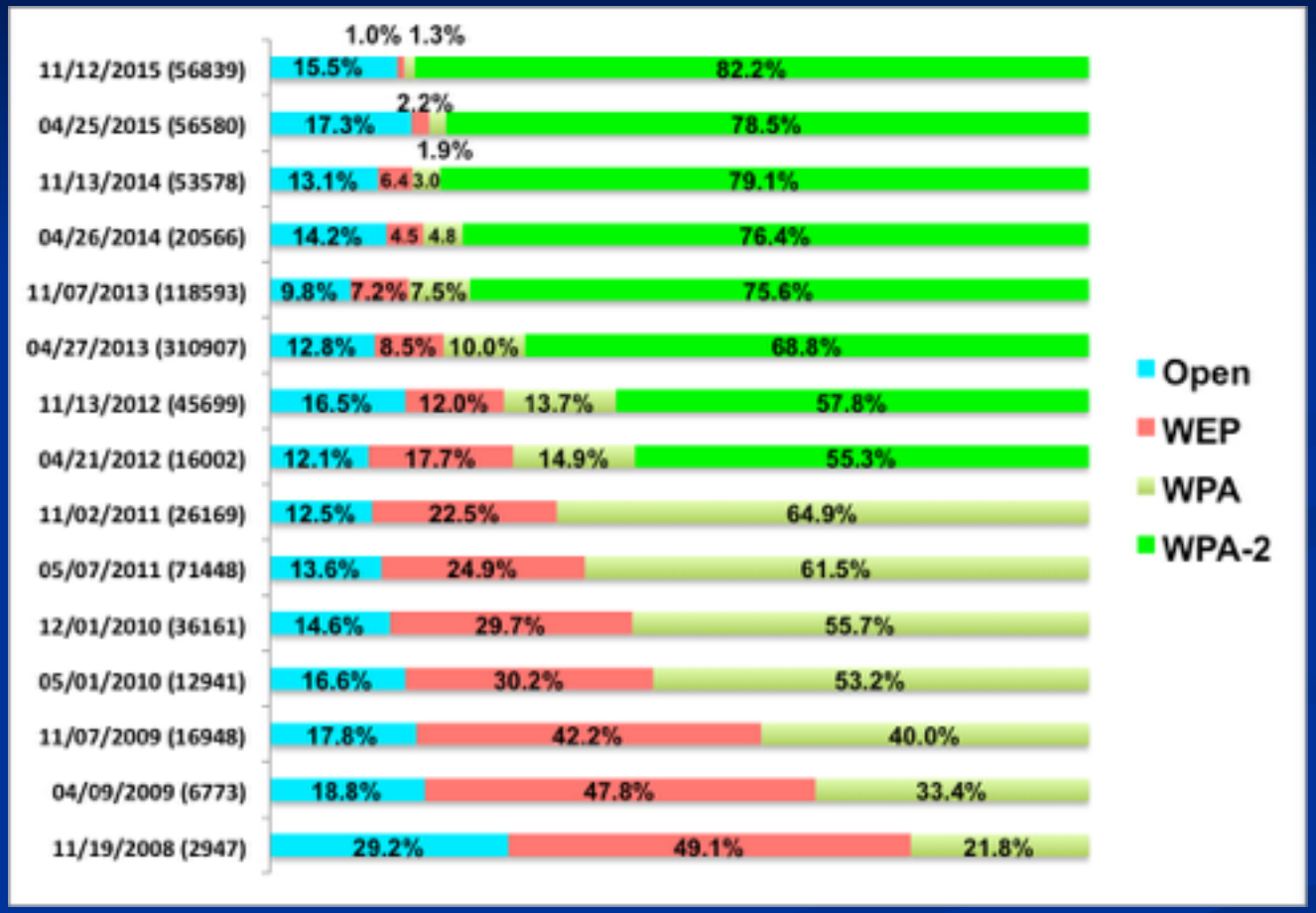
Understanding Wardriving

- Hackers use wardriving
  - Finding insecure access points
  - Using a laptop or palmtop computer
- Wardriving is not illegal
  - But using the resources of these networks is illegal
- Warflying
  - Variant where an airplane is used instead of a car

CCSF Wardriving

- No wardrive this semester

Wardriving Results



- Link Ch11zt

How It Works

- An attacker or security tester simply drives around with the following equipment
  - Laptop computer
  - Wireless NIC
  - An antenna
  - Software that scans the area for SSIDs
- Not all wireless NICs are compatible with scanning programs
- Antenna prices vary depending on the quality and the range they can cover

How It Works (continued)

- Scanning software can identify
  - The company's SSID
  - The type of security enabled
  - The signal strength
    - Indicating how close the AP is to the attacker

NetStumbler

- Shareware tool written for Windows that enables you to detect WLANs
  - Supports 802.11a, 802.11b, and 802.11g standards
- NetStumbler was primarily designed to
  - Verify your WLAN configuration
  - Detect other wireless networks
  - Detect unauthorized APs

NetStumbler

- NetStumbler is capable of interface with a GPS
  - Enabling a security tester or hacker to map out locations of all the WLANs the software detects

NetStumbler

- NetStumbler logs the following information
  - SSID
  - MAC address and Manufacturer of the AP
  - Channel
  - Signal Strength
  - Encryption (but not level of encryption)
- Can detect APs within a 350-foot radius
  - With a good antenna, they can locate APs a couple of miles away

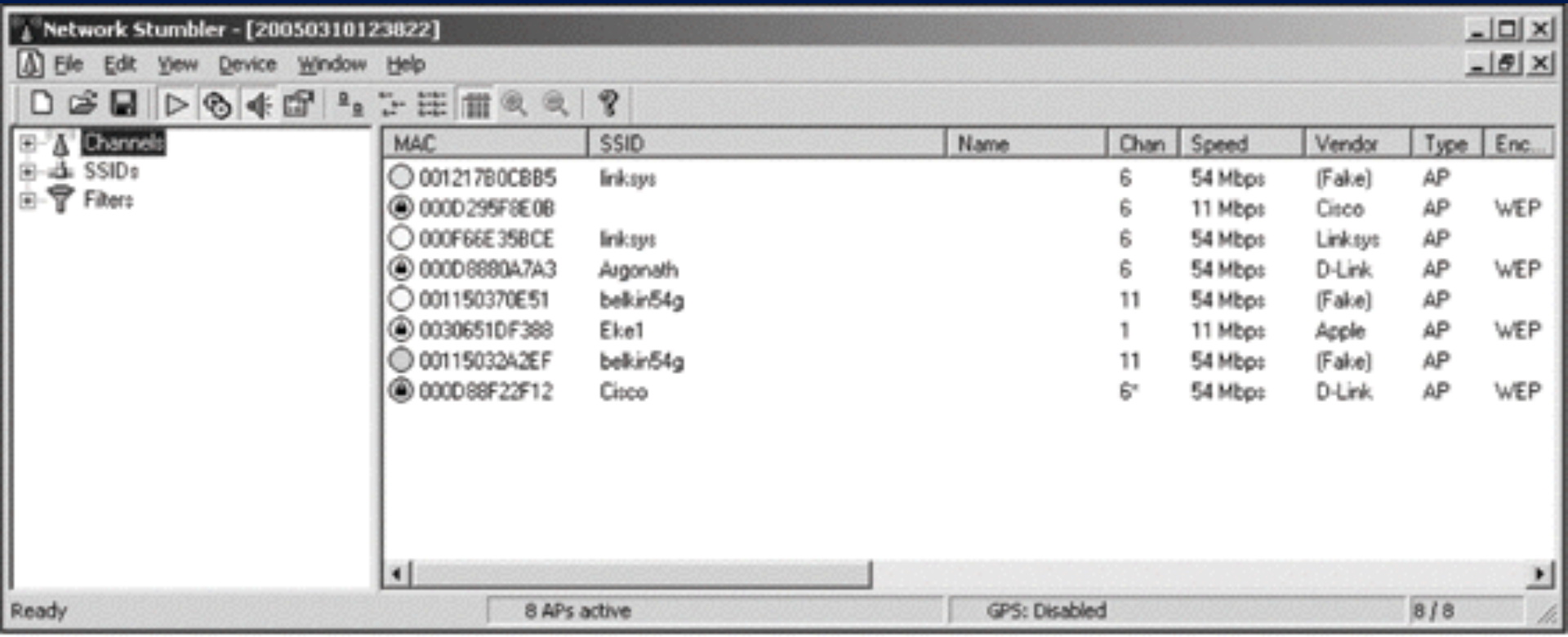


Figure 11-14 The Network Stumbler main window

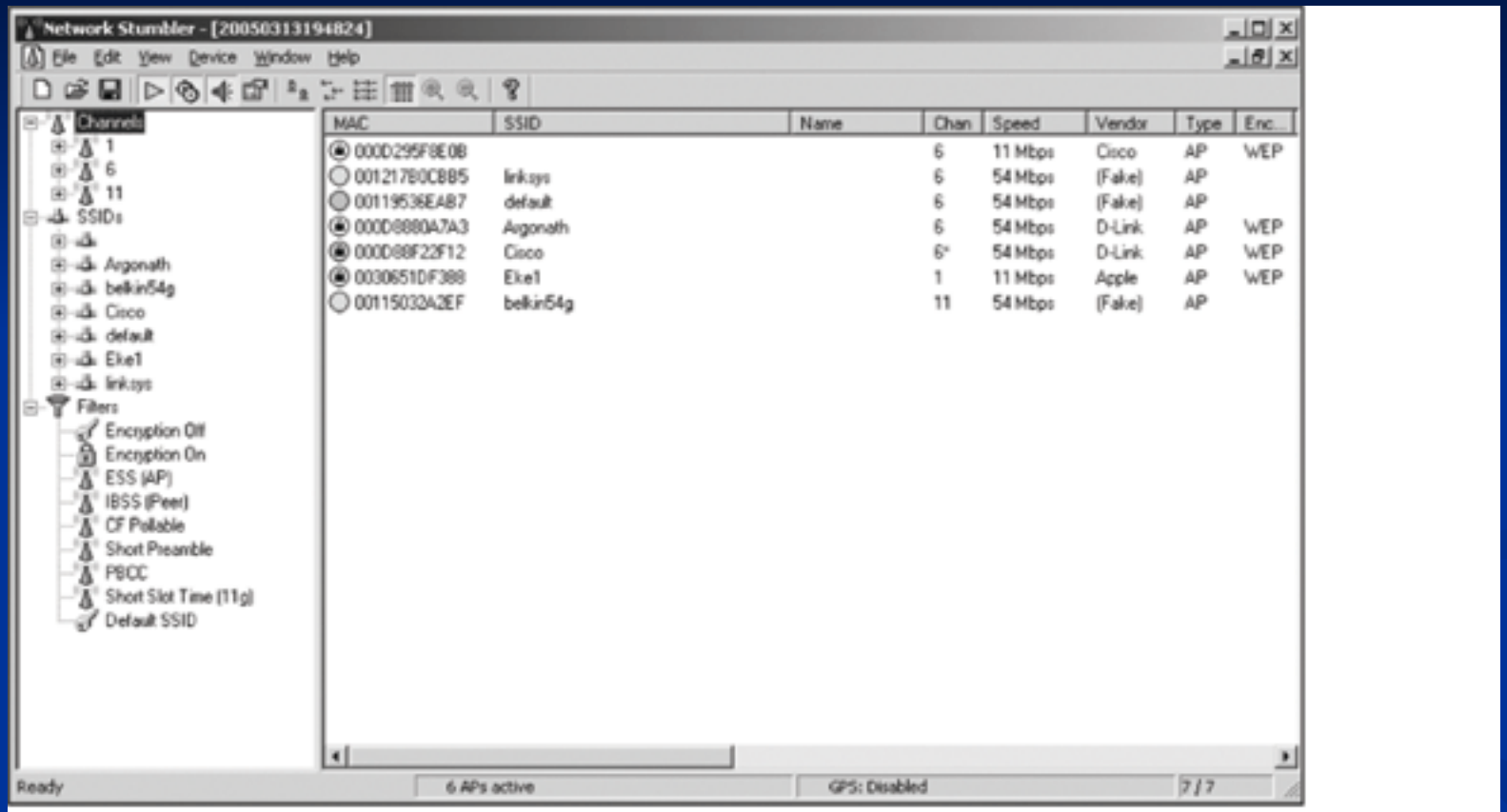


Figure 11-15 Viewing SSIDs, channels, and filters in Network Stumbler

Kismet

- Another product for conducting wardriving attacks
- Runs on Linux, BSD, MAC OS X, and Linux PDAs
- Kismet is advertised also as a sniffer and IDS
  - Kismet can sniff 802.11b, 802.11a, and 802.11g traffic

Kismet features

- Ethereal- and Tcpdump-compatible data logging
- AirSnort compatible
- Network IP range detection

Kismet features (continued)

- Hidden network SSID detection
- Graphical mapping of networks
- Client-server architecture
- Manufacturer and model identification of APs and clients
- Detection of known default access point configurations
- XML output
- Supports more than 25 card types

Understanding Wireless Hacking

- Hacking a wireless network is not much different from hacking a wired LAN
- Techniques for hacking wireless networks
  - Port scanning
  - Enumeration

Tools of the Trade

- Equipment
  - Laptop computer
  - A wireless NIC
  - An antenna
  - Sniffer software

AirCrack NG

- Popular WEP-cracking tool
- Included in Kali

WEP-Cracking Project

- No longer worth the bother
- WEP is almost extinct in the SF Bay area

WI-Fi Pineapple

Secure https://wifipineapple.com

COMPREHENSIVE WIFI AUDITING

The WiFi Pineapple® NANO and TETRA are the 6th generation auditing platforms from Hak5. Thoughtfully developed for mobile and persistent deployments, they build on over 8 years of WiFi penetration testing expertise.

- WiFi man-in-the-middle platform
- Highly effective rogue AP suite
- Over-the-air apps and modules
- Advanced client and AP filtering
- Intuitive web interface
- Simplified auditing workflow
- Live reconnaissance view
- At-a-glance intelligence
- Device tracking and alerting
- Reports emailed at set intervals
- Built on embedded Linux
- Free software updates

Countermeasures for Wireless Attacks

- Anti-wardriving software makes it more difficult for attackers to discover your wireless LAN
  - Honeypots
    - Servers with fake data to snare intruders
  - Fakeap and Black Alchemy Fake AP
    - Software that makes fake Access Points
      - Link Ch 11s

Countermeasures for Wireless Attacks

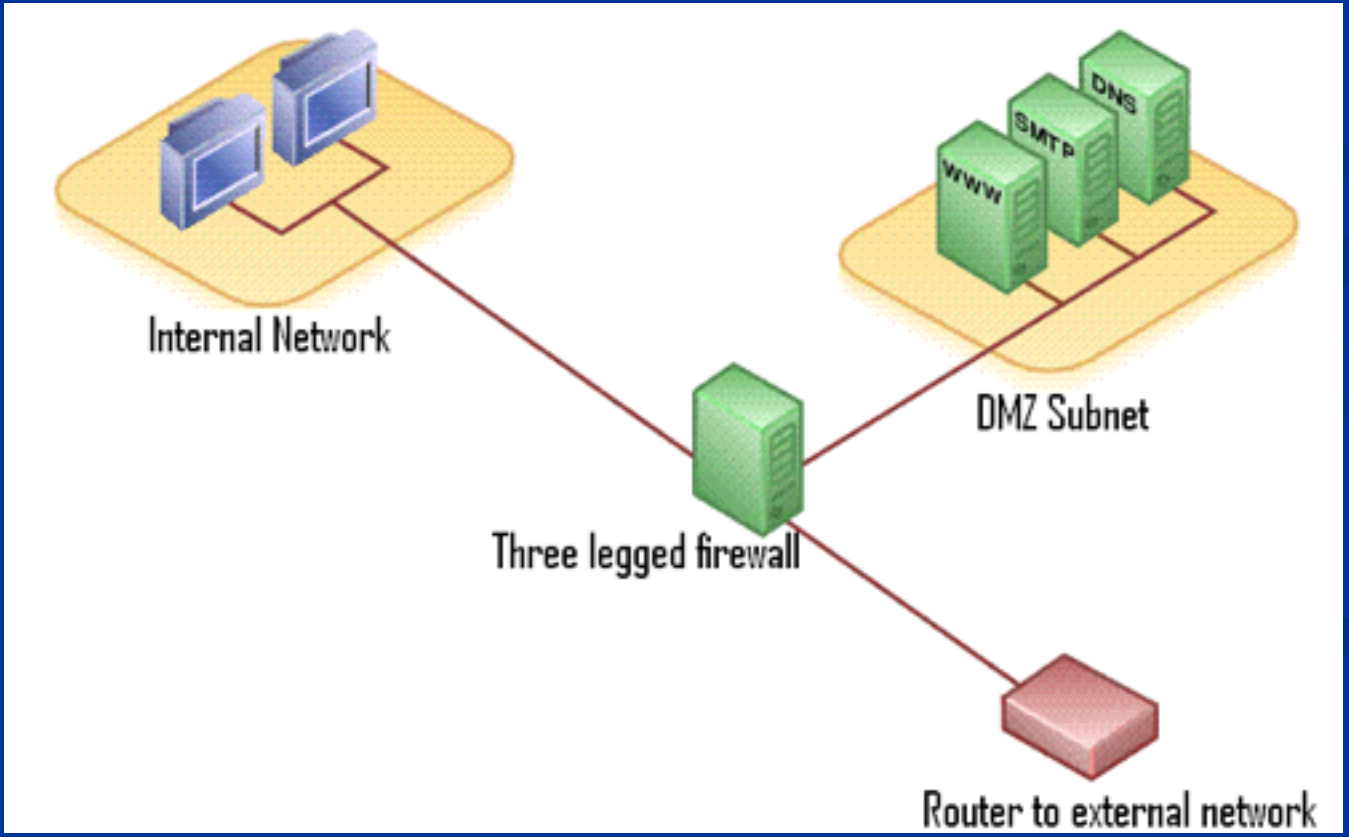
- Use special paint to stop radio from escaping your building
- Allow only predetermined MAC addresses and IP addresses to have access to the wireless LAN
- Use an authentication server instead of relying on a wireless device to authenticate users

Countermeasures for Wireless Attacks

- Use an EAP authentication protocol
- If you use WEP, use 104-bit encryption rather than 40-bit encryption
  - But just use WPA instead
- Assign static IP addresses to wireless clients instead of using DHCP
- Don’t broadcast the SSID

Countermeasures for Wireless Attacks

- Place the AP in the demilitarized zone (DMZ) (image from wikipedia)



Demo: Defeating MAC Address Filtering

- Link Ch 11zf