

# Chapter 8

# Hacking Wireless Networks

# 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
- Countermeasures

# **EXPLAIN WIRELESS TECHNOLOGY**

# 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
  - Cell and cordless phones
  - Pagers
  - GPS
  - Remote controls
  - Garage door openers
  - Two-way radios
  - Wireless PDAs

# Wireless terminology

- GSM
- Bandwidth
- BSSID
- ISM Band
- Access Point
- Hotspot
- Association



# Revolution of WiFi



802.11g lets consumers stream music at 54 Mbps

1999

802.11b released, featuring wireless speeds of 11 Mbps



2003



802.11ac breaks the gigabit per second barrier

2012

2009

802.11n boosts range and throughput for video streaming



2015

Next-Gen AC introduced



# 802.11 Wireless Standards

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

1980s

2014

2020

1G

2G  
100Kbps

3G  
10Mbps

LTE /4G  
1Gbps

5G and beyond  
multi-Gbps or higher



Analog

Digital

+ Data

+ HD Video

Voice

+ Message

+ Internet

+ Apps

+ VoIP

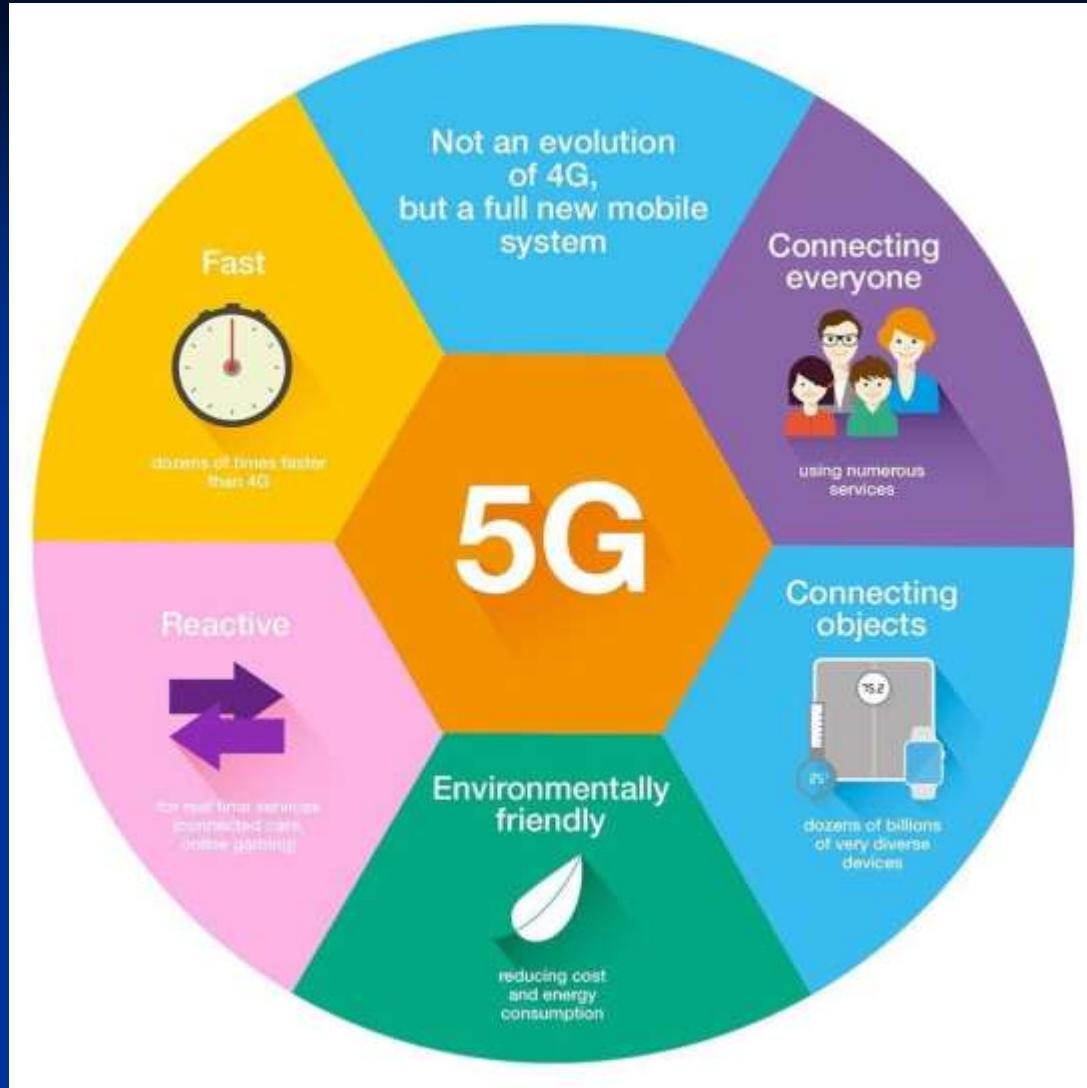
+ Position

+ High Mobility

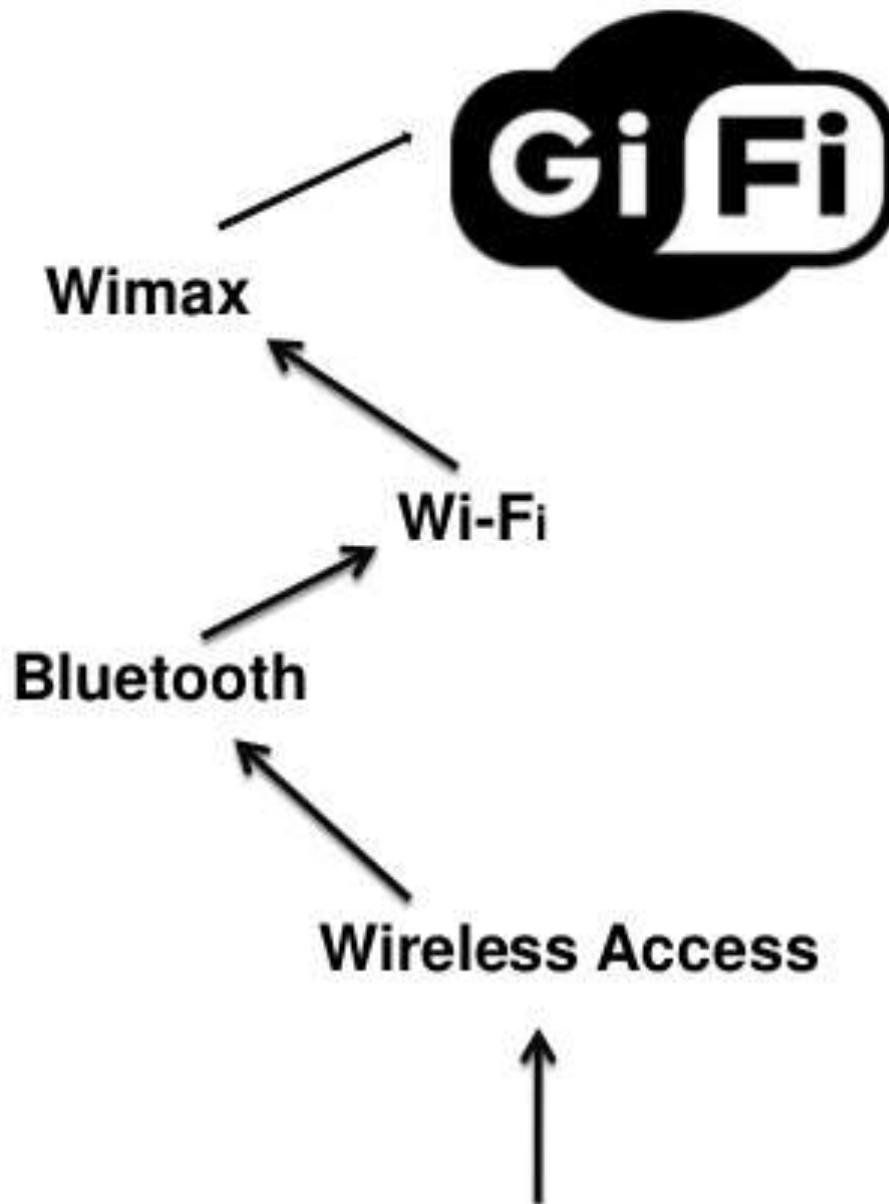


### 5G Vision

- Always on, data centric
- 1000x today's traffic volume
- 10-100x today's typical user data rate
- 100x connected devices
- Content rich, anytime, anywhere
- Connecting everything
- Green



# NETWORK EVOLUTION





100 Times Faster than Wi-Fi



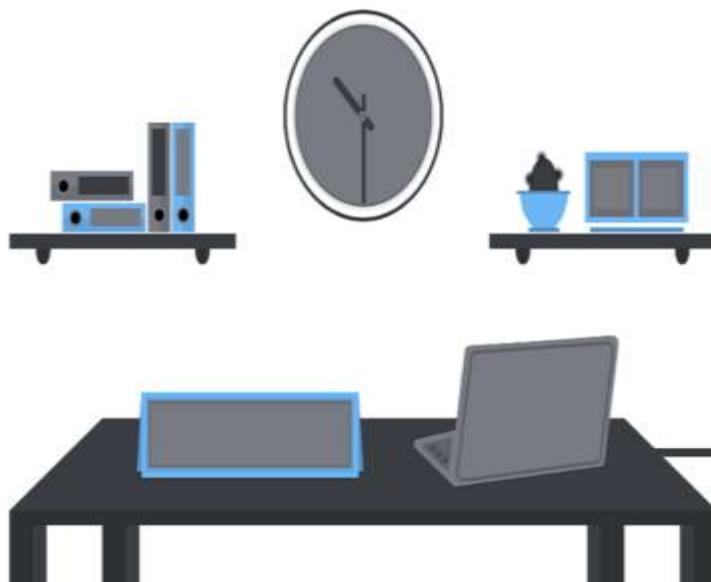
An LED will flicker light at extremely high speed that goes undetected by human eyes, nonetheless, a photodetector will pick it up easily. In the next step, it converts the received signal into electric current to provide you ultra-high speed.

Streaming content ➔

Lamp Driver



Receiver Dongle



Amplification and Processing

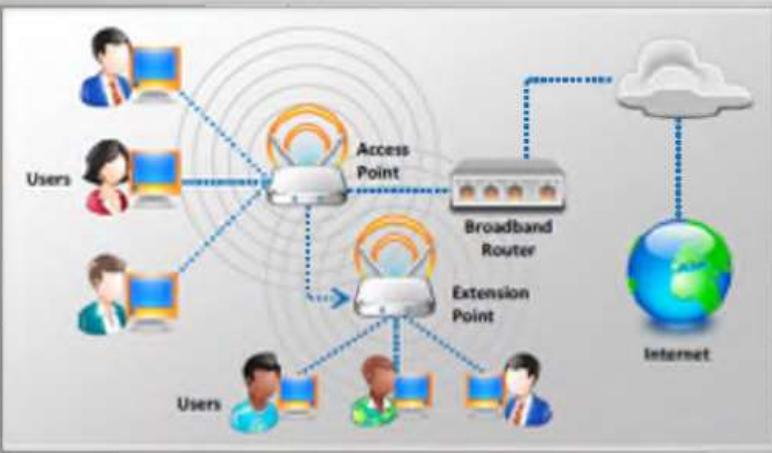


Received data

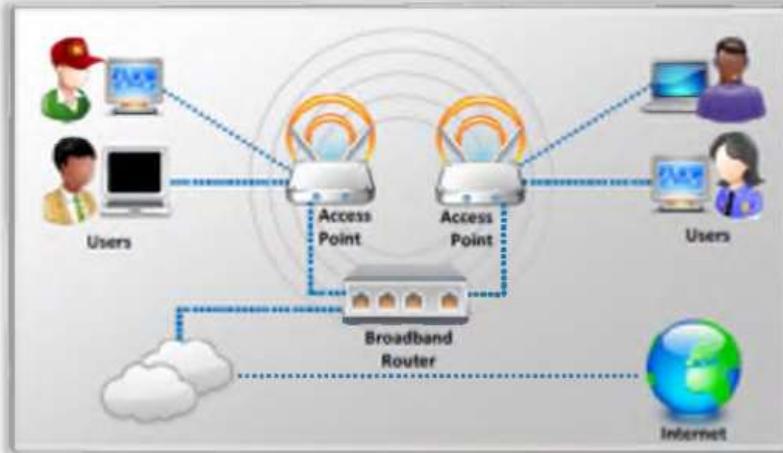




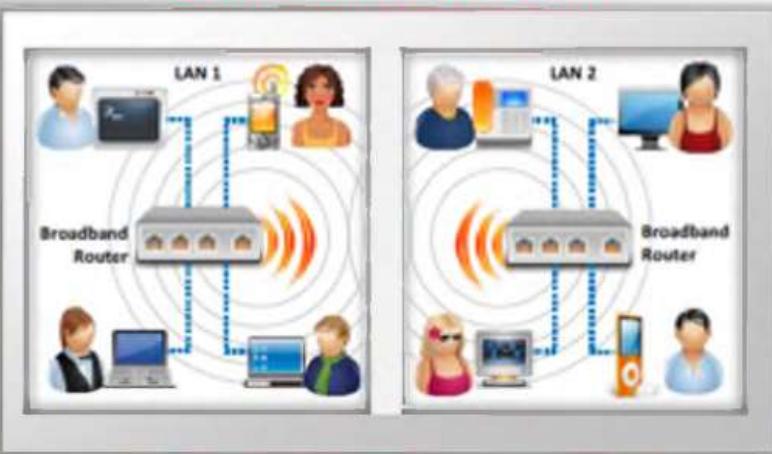
# Type of wireless Network



Extension to a Wired Network



Multiple Access Points



LAN-to-LAN Wireless Network



3G/4G Hotspot

# Components of a Wireless Network

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

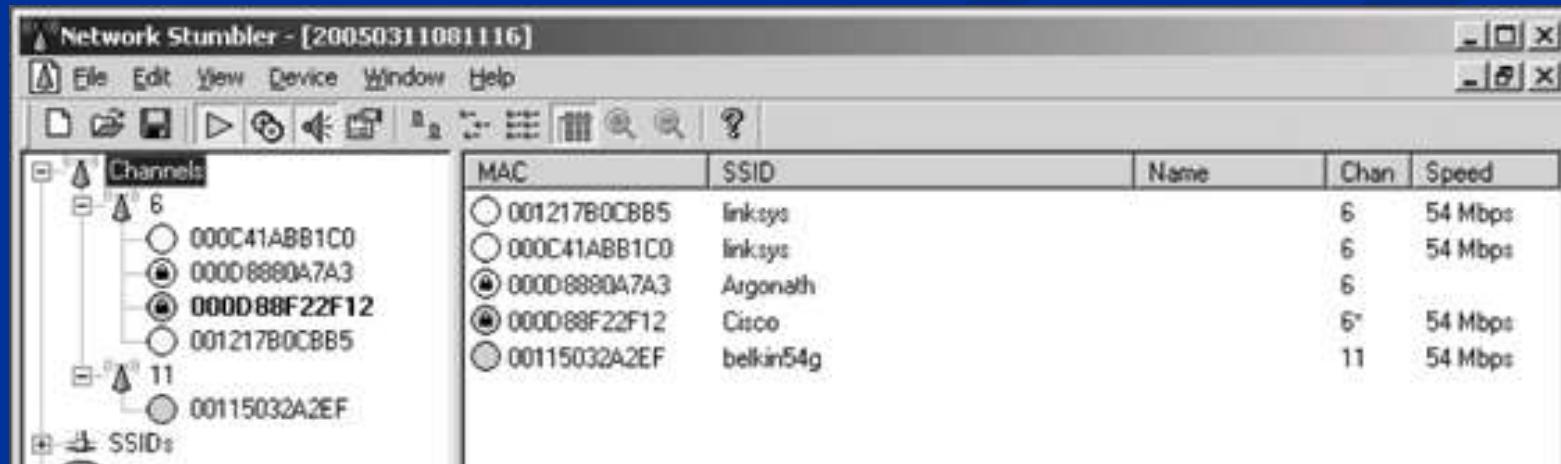
# Access Points



- 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

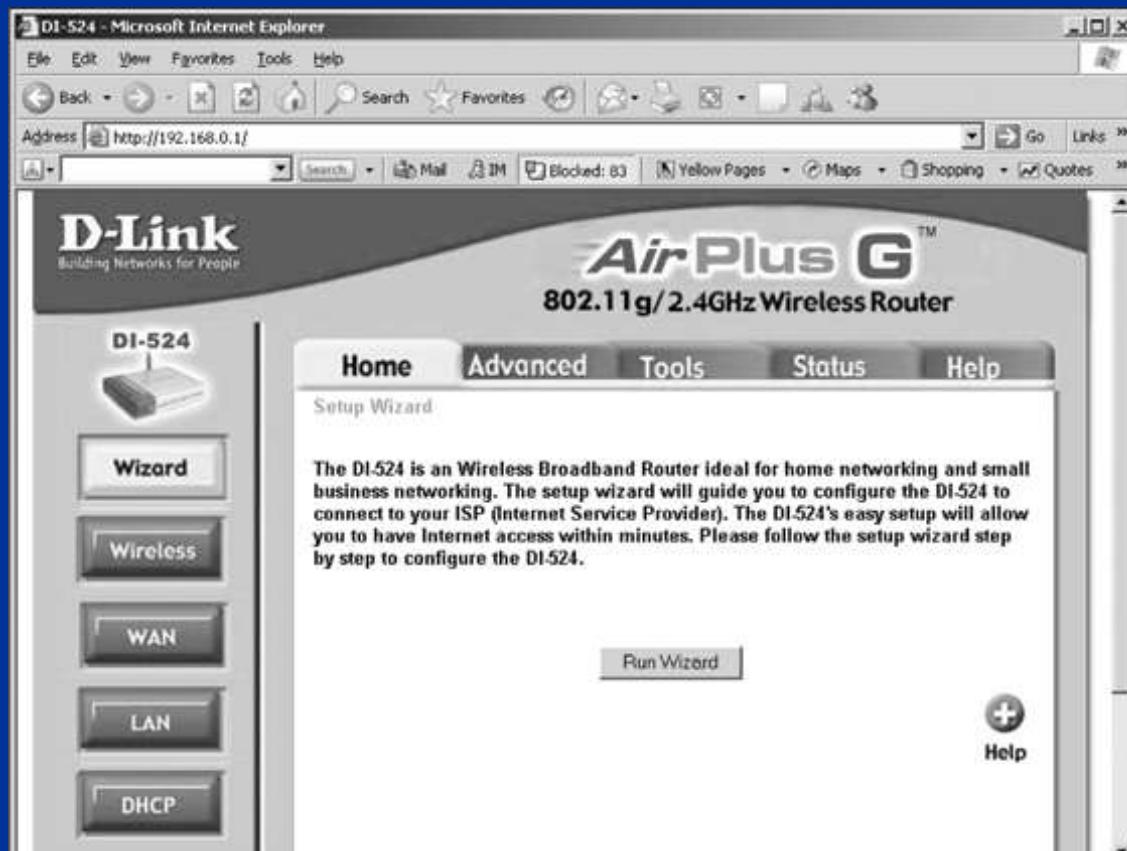
Vendor	Default SSIDs
3Com	3Com
Apple	Airport Network
Belkin (54G)	Belkin54g
Cisco	Tsunami
Compaq	Compaq
D-Link	WLAN, default
Dell	Wireless
Intel	Intel, 101, xlan, 195
Linksys	linksys, Wireless, linksys-g
Microsoft	MSNHOME
Netgear	Wireless, NETGEAR
SMC	WLAN, BRIDGE, SMC
Symantec	101
US Robotics	WLAN,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

# 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

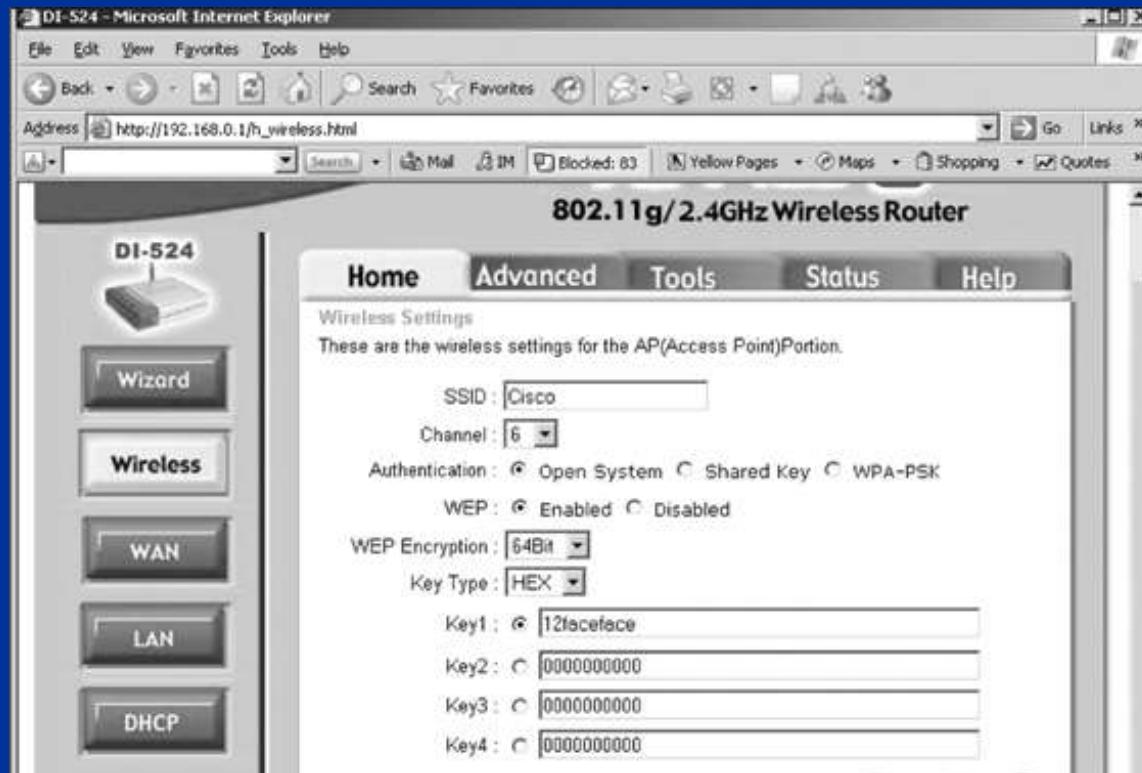
# Wireless Router

- 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

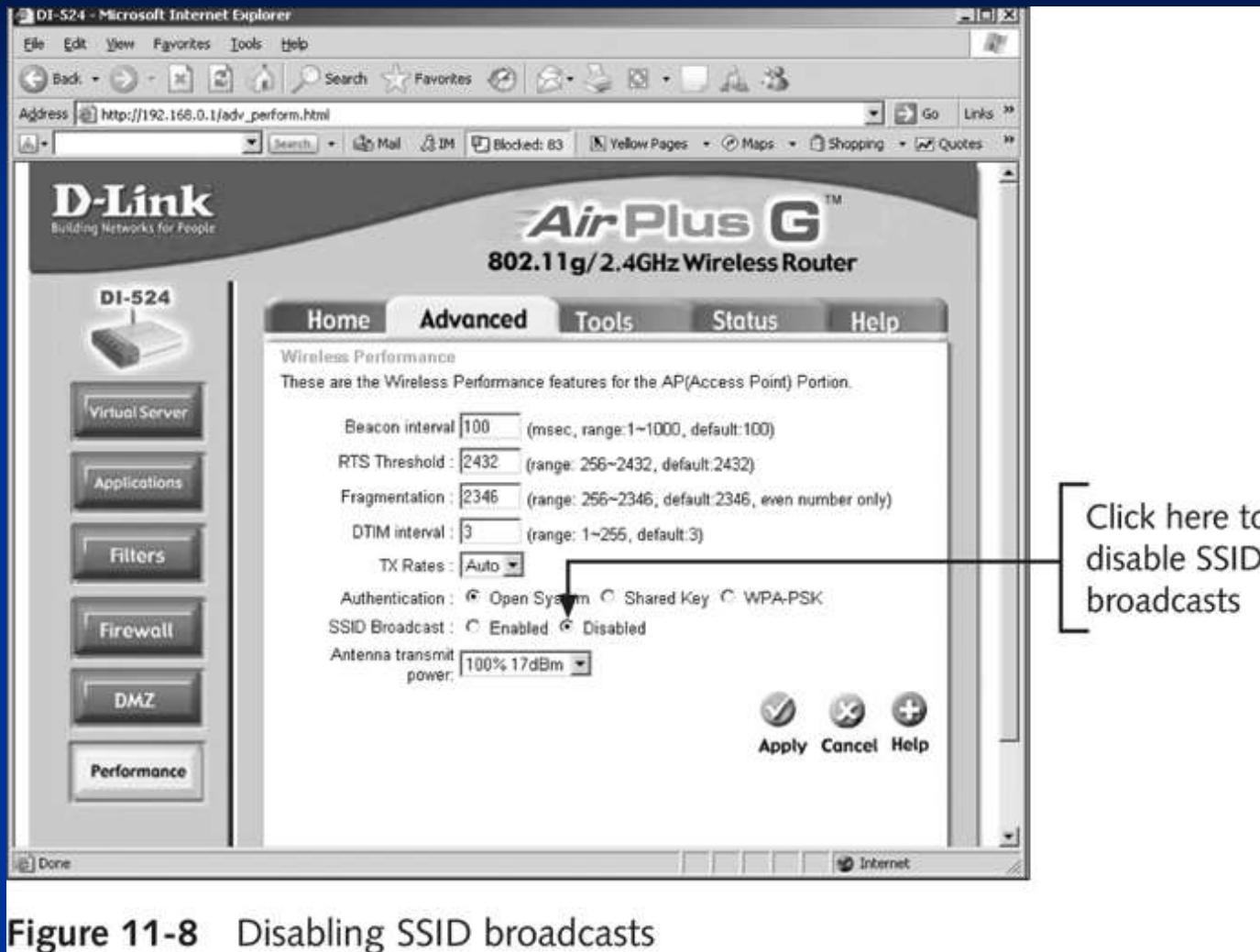


Figure 11-8 Disabling SSID broadcasts

# 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

# **DESCRIBE WIRELESS NETWORKING STANDARDS**

# 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

# Wireless Standard

Amendments	Freq. (GHz)	Modulation	Speed (Mbps)	Range (ft)
802.11a	5	OFDM	54	25 – 75
802.11b	2.4	DSSS	11	150 – 150
802.11g	2.4	OFDM, DSSS	54	150 – 150
802.11i	Defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	OFDM	54	~100
802.16 (WiMAX)	10 - 66		70 – 1000	30 miles
Bluetooth	2.4		1 - 3	25

# The 802.11 Standard

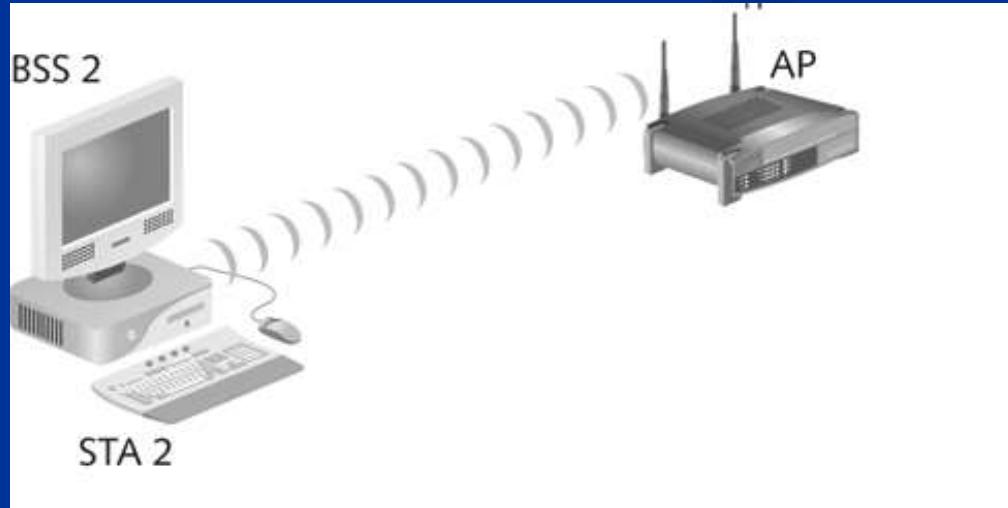
- The first wireless technology standard
- Defined wireless connectivity at 1 Mbps and 2 Mbps within a LAN
- Applied to layers 1 and 2 of the OSI model
- Wireless networks cannot detect collisions
  - Carrier sense multiple access/collision avoidance (CSMA/CA) is used instead of CSMA/CD

# 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)

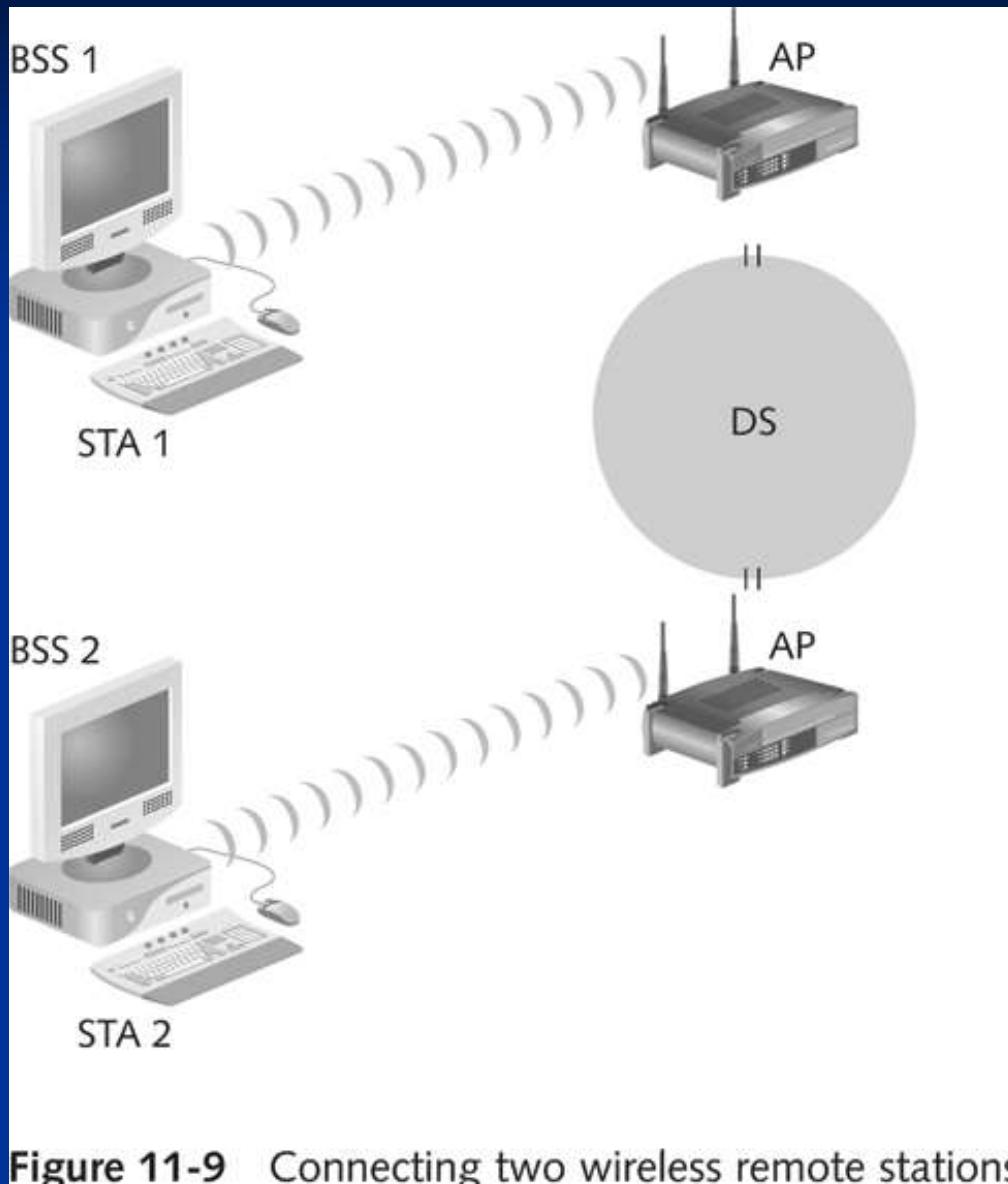
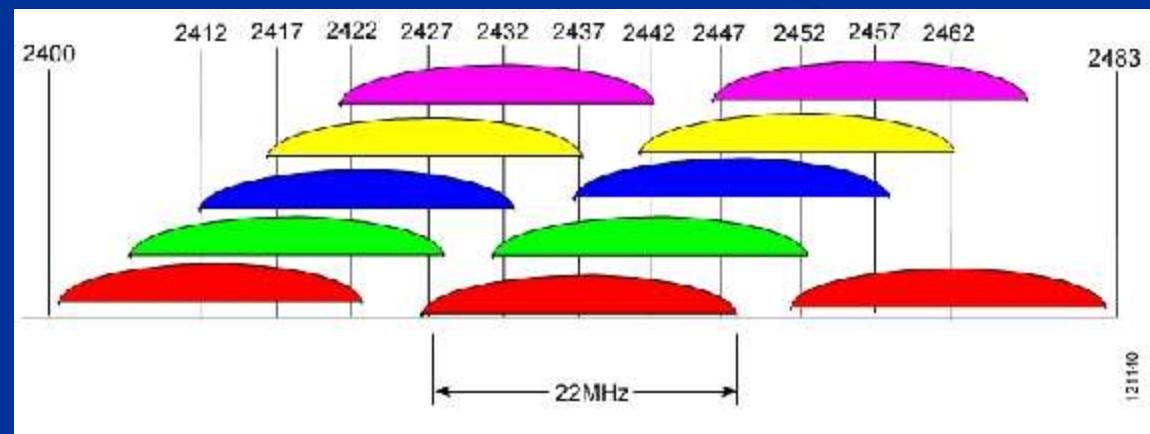


Figure 11-9 Connecting two wireless remote stations

# 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

[PRODUCT TOUR](#)

**BUFFALO**  
PERFORMANCE MATTERS

**BUFFALO AirStation  
Extreme AC 1200 Gigabit  
Dual Band Wireless Router -  
WZR-1166DHP**

(20) | Write a Review

In stock. Limit 5 per customer.

- Wireless 802.11ac
- Simultaneous Dual Band
- Up to 866Mbps@5GHz, 300Mbps@2.4GHz
- 5 Gigabit Ethernet Ports
- Configure as an Access Point or Bridge
- QoS
- Web Filtering and Parental Control

FREE SHIPPING AVAILABLE

\$169.99

QTY. 1  PREMIER \$89.99

Save: \$80.00 (47%)

Sold and Shipped by:  
Newegg

Protect Your Investment!

1 Year Extended Replacement Plan \$7.00  
(more options)

Send It As A Gift!

Make this item a gift

[ADD TO CART](#)

# 802.11ac on MacBook Air

- Starting with the 2013 model



## New 802.11ac Wi-Fi support. The next generation of wireless.

With the latest 802.11ac technology, MacBook Air takes Wi-Fi speeds over the top. Connect to an 802.11ac base station — including the new AirPort Extreme or AirPort Time Capsule — and experience wireless performance up to 3x faster than the previous generation. 802.11ac also delivers expanded range, so you can work more freely than ever.

[Learn more >](#)

# 802.11ad (WiGig)

- New physical layer
- 60 GHz, up to 7 Gbps
- Short-range (up to 30 feet) (Link Ch 11zq)
- Not common yet (in 2014)

# 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](http://ubergizmo.com)



# IEEE Additional 802.11 Projects (continued)

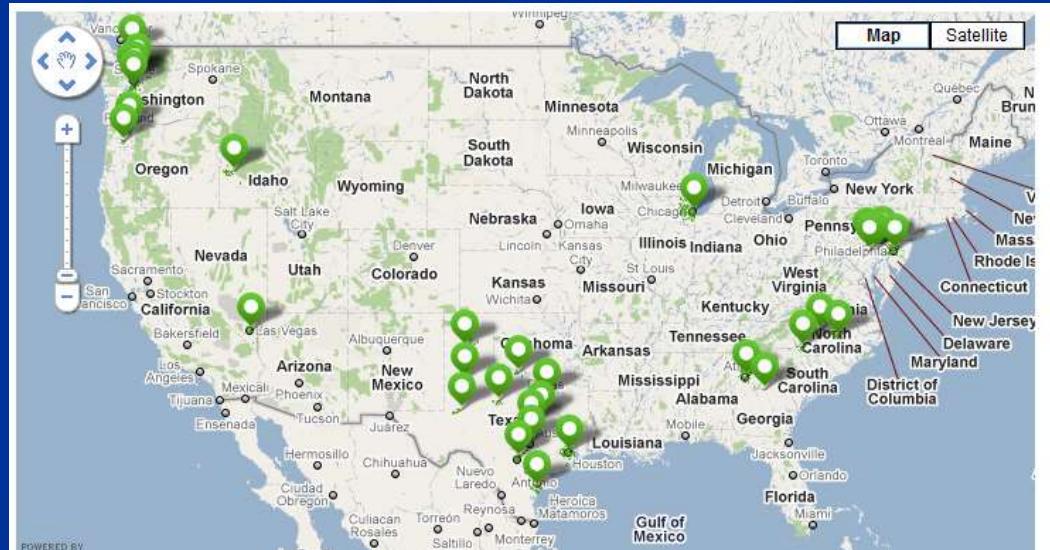
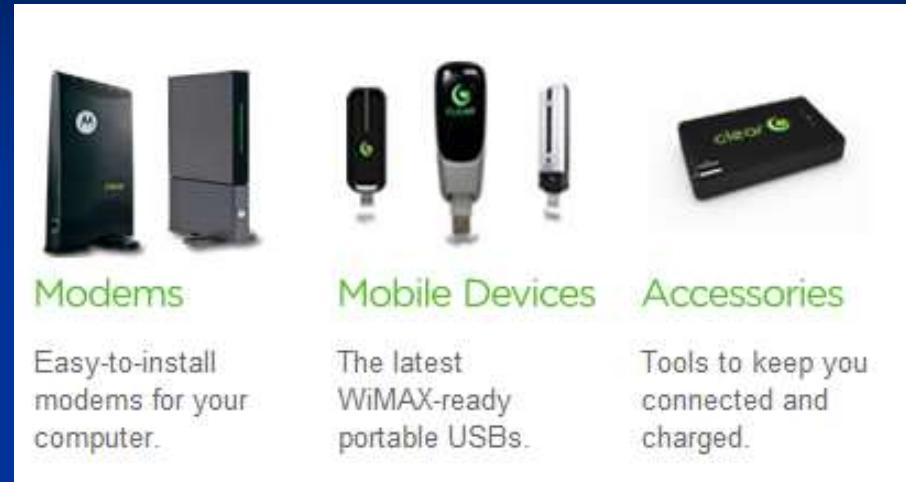
- Bluetooth
  - Defines a method for interconnecting portable devices without wires
  - Maximum distance allowed is 10 meters
  - It uses the 2.45 GHz frequency band
  - Throughput of up to 2.1 Mbps for Bluetooth 2.0
    - Up to 24 Mbps for Bluetooth 3.0 (not 12 Mbps as stated in the textbook, p. 316)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

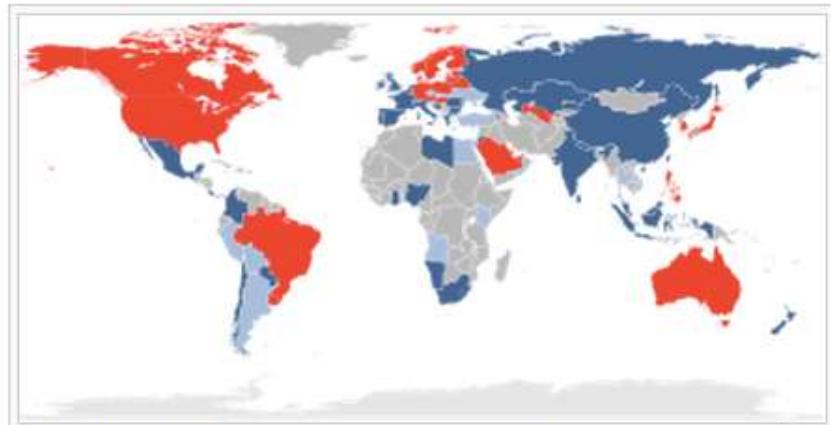


# LTE

## 3GPP Long Term Evolution

From Wikipedia, the free encyclopedia

**3GPP Long Term Evolution**, referred to as **LTE** and marketed as **4G**, 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.<sup>[1][2]</sup> The



Adoption of LTE technology as of January 5, 2012.

Red: Countries with commercial LTE service

Blue: Countries with commercial LTE network deployment ongoing or planned

Light Blue: Countries with LTE trial systems (pre-commitment)

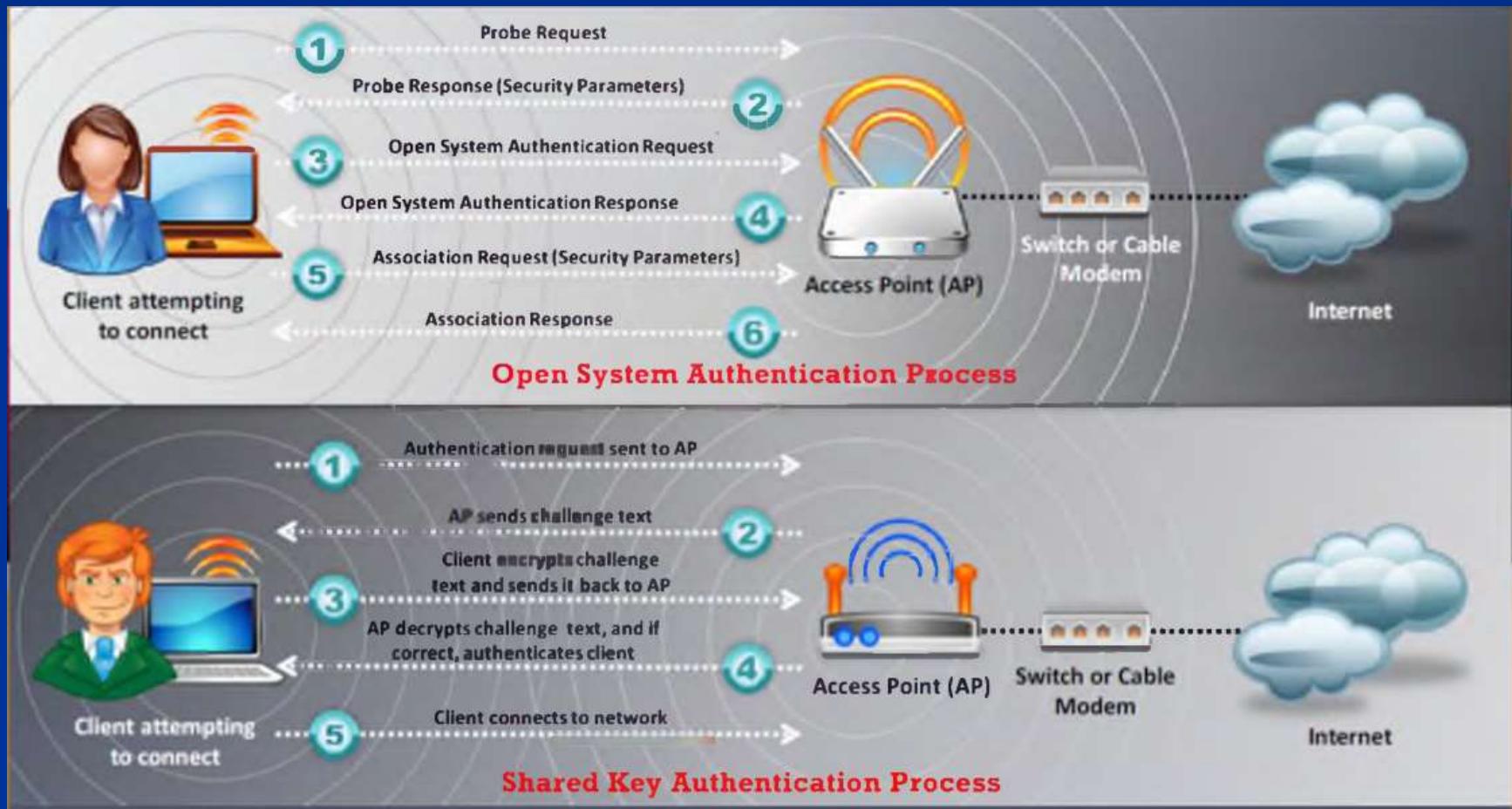
<b>Standard</b>	<b>Frequency</b>	<b>Maximum rate</b>	<b>Modulation method</b>
802.11	2.4 GHz	1 or 2 Mbps	FHSS/DSSS
802.11a	5 GHz	54 Mbps	OFDM
802.11b	2.4 GHz	11 Mbps	DSSS
802.11g	2.4 GHz	54 Mbps	OFDM
802.11n	2.4 GHz	600 Mbps	OFDM
802.15	2.4 GHz	2 Mbps	FHSS
802.16 (WiMAX)	10–66 GHz	120 Mbps	OFDM
802.20 (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

**DESCRIBE THE PROCESS OF  
AUTHENTICATION**

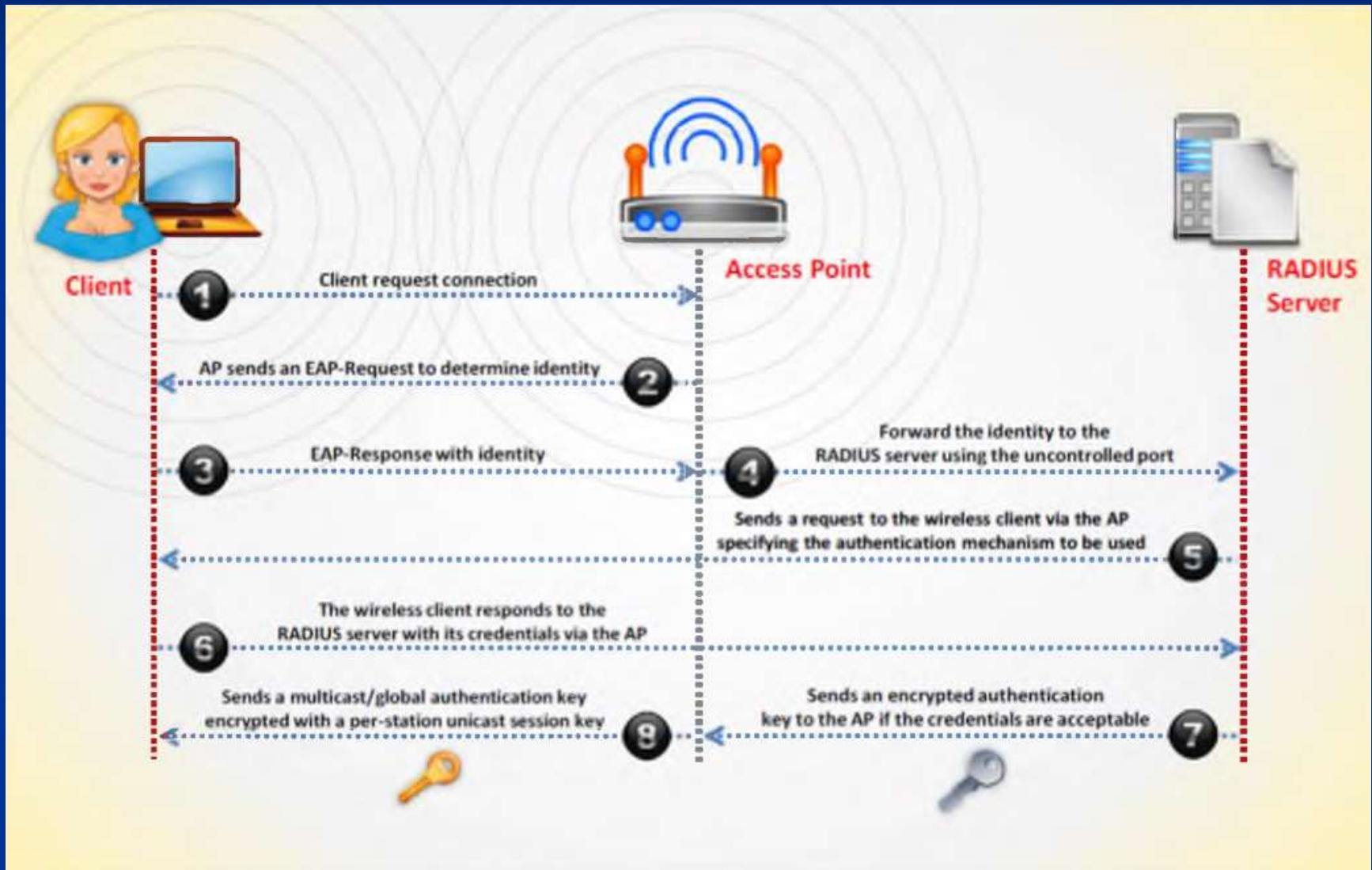
# Understanding Authentication

- 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

# Authentication Modes



# Centralized Authentication Server



# 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

# 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
  - "Pass the hash"

# Extensible Authentication Protocol (EAP)

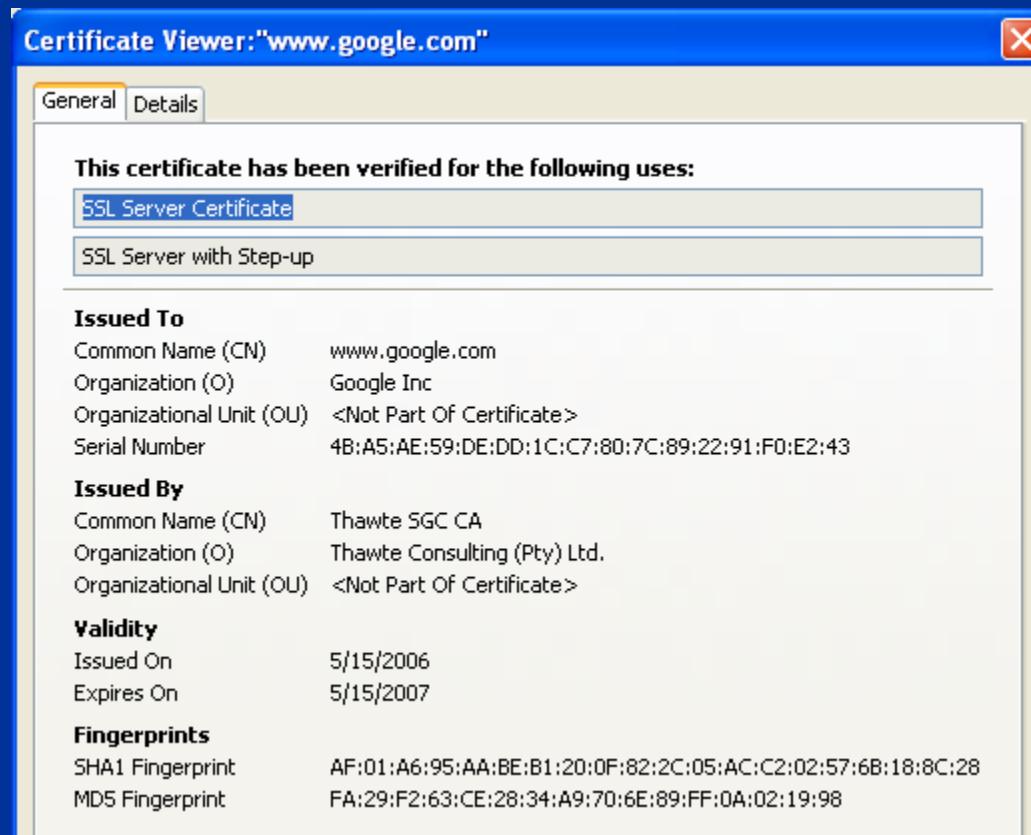
- EAP is an enhancement to PPP
- Allows a company to select its authentication method
  - Certificates
  - Kerberos
    - Kerberos is used on LANs for authentication
    - Uses Tickets and Keys
    - Used by Windows 2000, XP, and 2003 Server by default
    - Not common on WLANS

# X.509 Certificate

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

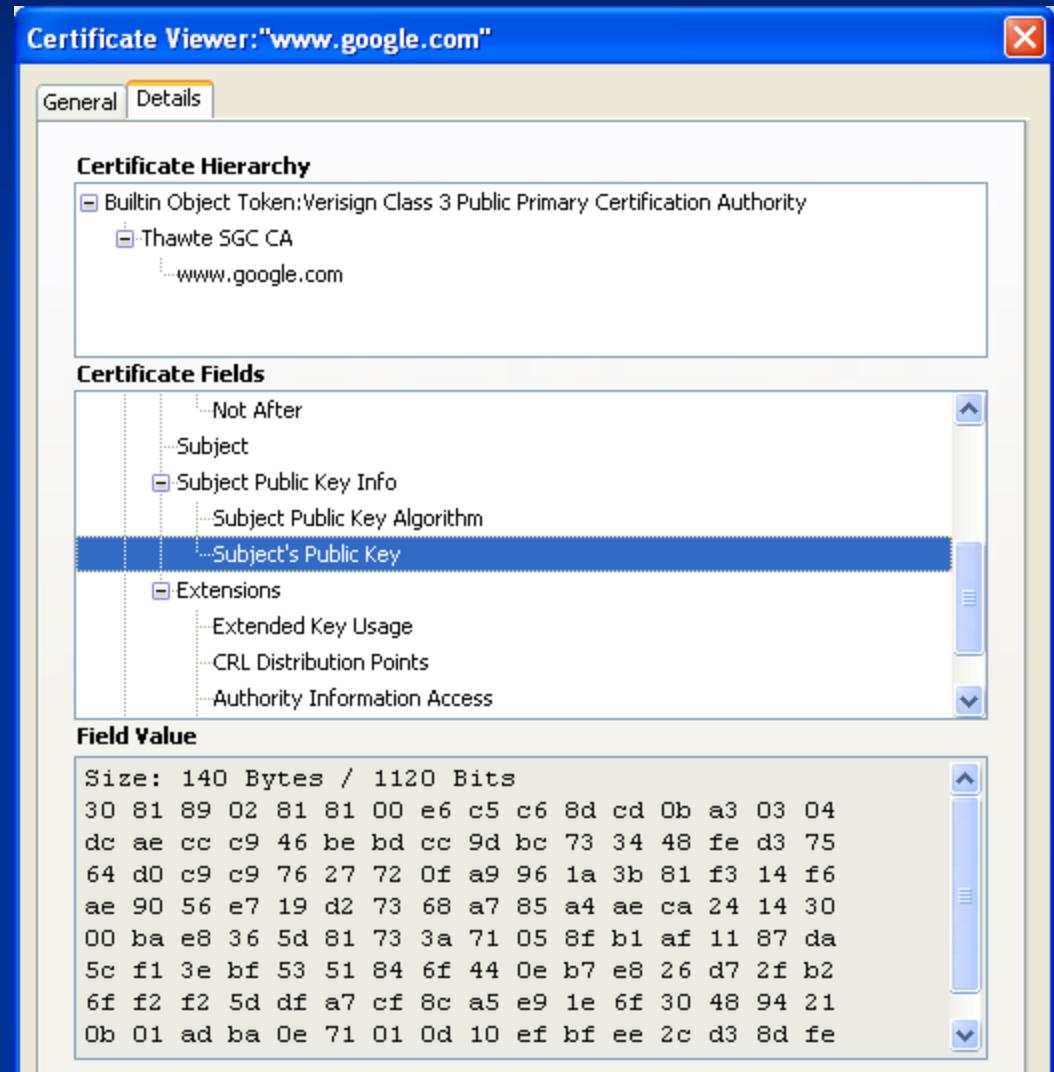
# Sample X.509 Certificate

- 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



JOSHUA WRIGHT

# 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,

# Narcissistic 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

[Free whitepaper – The realities of SaaS and security](#)

**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.

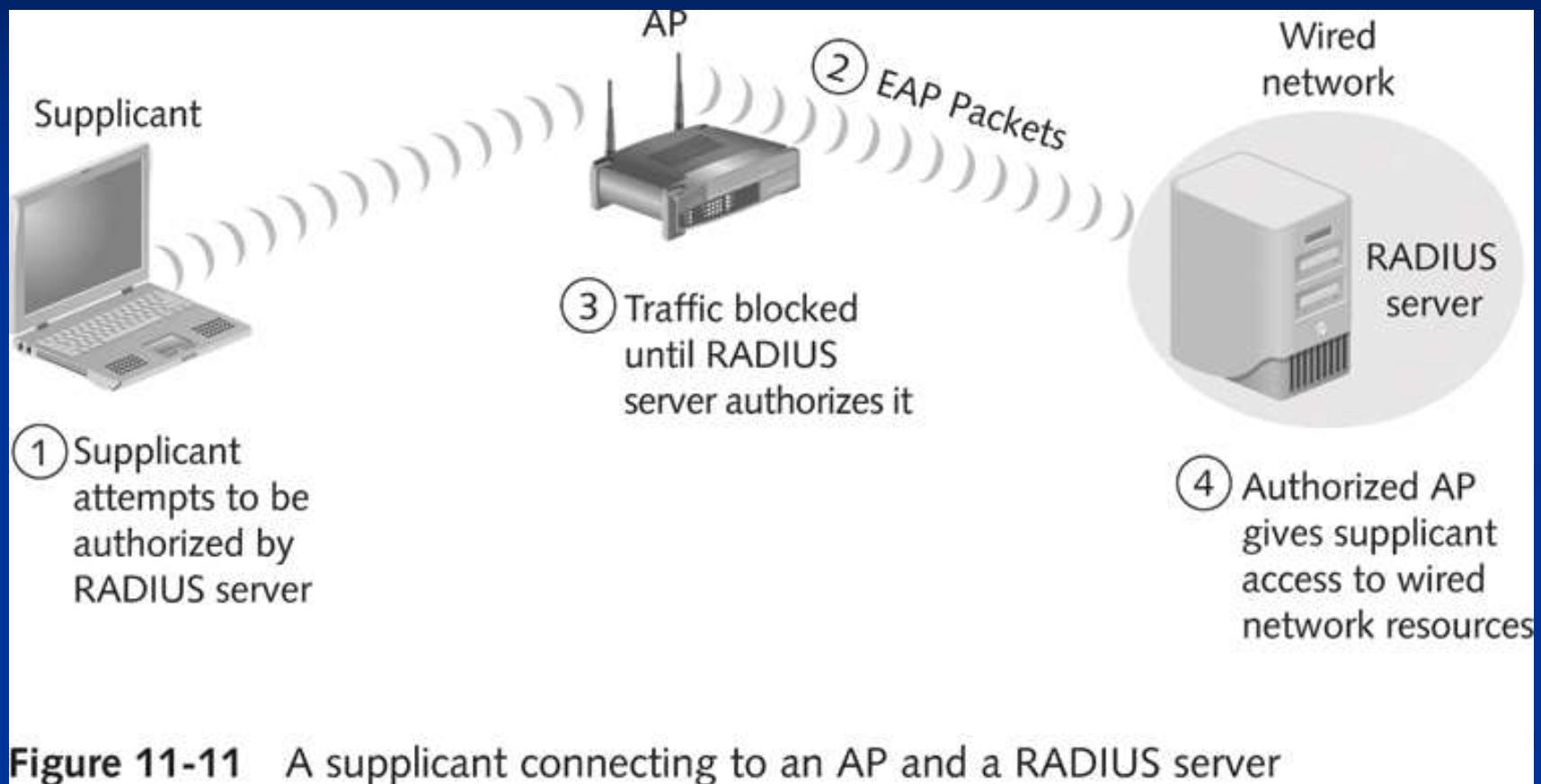
"Have you ever heard of a terrorist referred to as a 'demolition engineer?'" the unnamed author of the [rant](#) asked, one presumes rhetorically. "How about a thief as a 'locksmith?' No? Well, that's because most fields don't share the InfoSec industry's ridiculous yet long-standing inability to distinguish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

# 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

# 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)



**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

# 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

# How Vulnerable Your Wireless?



# WiFi PROTOCOLS



- **WEP**
- **WPA**
- **WPA 2**
- **WPA/WPA2**

Encryption standard	Fast facts	How it works	Should you use it?
<b>WIRED EQUIVALENT PRIVACY (WEP)</b>	First 802.11 security standard; easily hacked due to its 24-bit initialization vector (IV) and weak authentication.	Uses RC4 stream cipher and 64-or 128-bit keys. Static master key must be manually entered into each device.	No
<b>WI-FI PROTECTED ACCESS (WPA)</b>	An interim standard to address major WEP flaws. Backwards compatible with WEP devices. It has two modes: personal and enterprise.	Retains use of RC4, but adds longer IVs and 256-bit keys. Each client gets new keys with TKIP. Enterprise mode: Stronger authentication via 802.1x and EAP.	Only if WPA2 is not available
<b>WPA2</b>	Current standard. Newer hardware ensures advanced encryption doesn't affect performance. Also has personal and enterprise modes.	Replaces RC4 and TKIP with CCMP and AES algorithm for stronger authentication and encryption.	Yes

# WEP vs WPA vs WPA2

	WEP	WPA	WPA2
Cipher	RC4	128 bits encryption	AES
Key Size	40 bits	64 bits authentication	128 bits
Key Life	24 bits IV	24 bits IV	24 bits IV
Packet Key	concatened	Mixing Function	Not Nedeed
Data Integrity	CRC-32	Michael	CCMP
Header Integrity	none	Michael	CCMP
Replay Attack	none	IV sequence	IV sequence
Management Key	none	EAP-based	EAP-based

# WPA3 ?

TECHSPOT

TRENDING FEATURES REVIEWS THE BEST DOWNLOADS PRODUCT FINDER FORUMS

SAP Litmos® LMS Software - Training In The Now

We're The #1 Training Platform For Customer-Focused Enterprises.

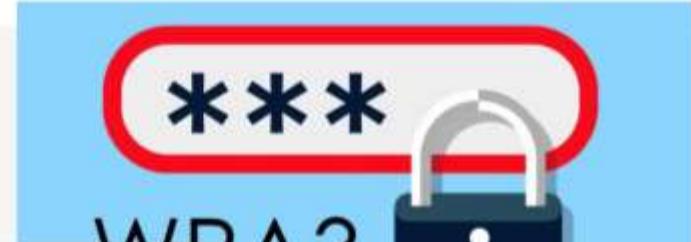
Visit Site

INDUSTRY SECURITY MFT WPA3

## Security researchers disclose WPA3 security flaws that allow attackers to swipe sensitive data

Hackers can steal passwords, emails, and more

By Cohen Cederly on April 11, 2018, 8:02 PM



**DESCRIBE WIRELESS HACKING  
AND TOOLS USED BY HACKERS  
AND SECURITY PROFESSIONALS**

# 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

The screenshot shows a terminal window titled "Shell" running on a Backtrack 4 operating system. The window displays the output of a WPS attack using the Reaver tool. The text in the terminal indicates the following process:

- [+] Trying pin 33193816
- [+] 95.16% complete @ 2012-01-18 00:44:35 (6 seconds/attempt)
- [+] Trying pin 33196855
- [+] Trying pin 33198675
- [+] Trying pin 33192802
- [+] Trying pin 33192284
- [+] Trying pin 33193786
- [+] 95.21% complete @ 2012-01-18 00:44:51 (6 seconds/attempt)
- [+] Trying pin 33194448
- [+] Trying pin 33197425
- [+] Trying pin 33191386
- [+] Trying pin 33198613
- [+] Trying pin 33192451
- [+] 95.25% complete @ 2012-01-18 00:45:06 (6 seconds/attempt)
- [+] Trying pin 33194028
- [+] Key cracked in 70275 seconds
- [+] WPS PIN: '33194028'
- [+] WPA PSK: 'longawfulpassword'
- [+] AP SSID: 'dlink'

The terminal prompt shows the user is root on the machine, located at `root@bt:~/reaver-1.3/src#`. The background of the desktop shows the Backtrack 4 logo.

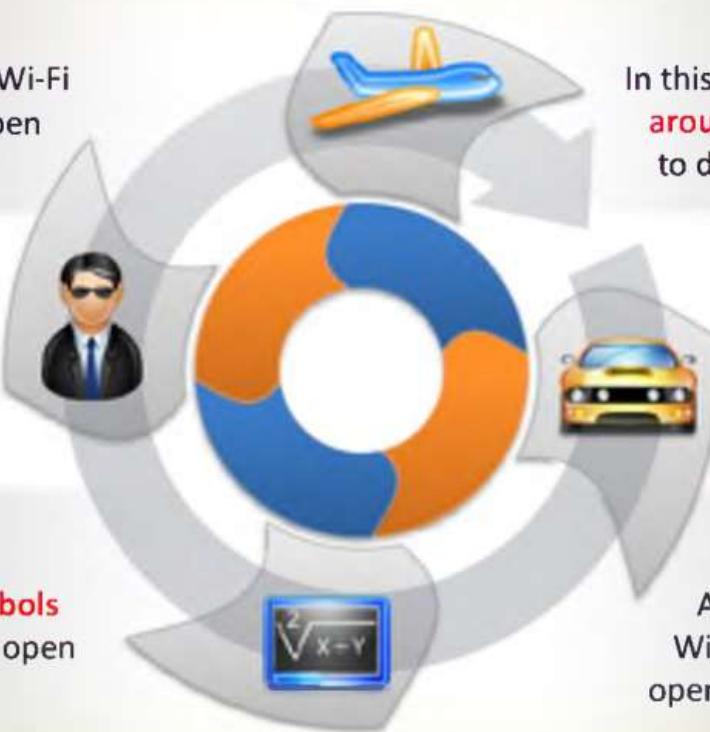
### WarWalking

Attackers **walk around** with Wi-Fi enabled laptops to detect open wireless networks



### WarChalking

A method used to **draw symbols in public places** to advertise open Wi-Fi networks



### WarFlying

In this technique, attackers **fly around** with Wi-Fi enabled laptops to detect open wireless networks



### WarDriving

Attackers **drive around** with Wi-Fi enabled laptops to detect open wireless networks

# 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

# 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

Network Stumbler - [20050310123822]

File Edit View Device Window Help

Channels SSIDs Filters

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc.
001217B0C6B5	linksys		6	54 Mbps	(Fake)	AP	
000D295F8E0B			6	11 Mbps	Cisco	AP	WEP
000F66E35BCE	linksys		6	54 Mbps	Linksys	AP	
000D8880A7A3	Argonath		6	54 Mbps	D-Link	AP	WEP
001150370E51	bellin54g		11	54 Mbps	(Fake)	AP	
0030651DF388	Eke1		1	11 Mbps	Apple	AP	WEP
00115033A2EF	bellin54g		11	54 Mbps	(Fake)	AP	
000D88F22F12	Cisco		6	54 Mbps	D-Link	AP	WEP

Ready 8 APs active GPS: Disabled 8 / 8

Figure 11-14 The Network Stumbler main window

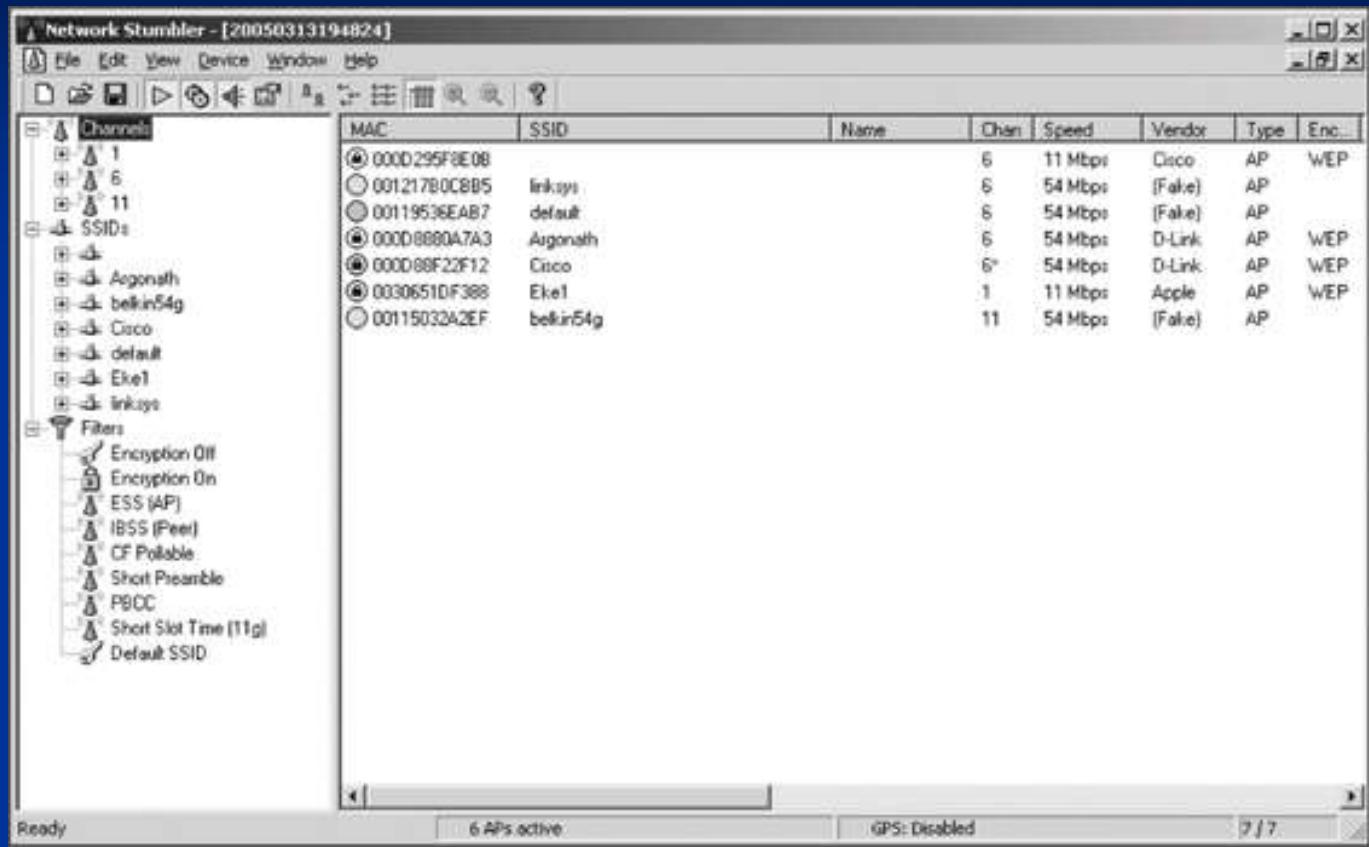


Figure 11-15 Viewing SSIDs, channels, and filters in Network Stumbler

# 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

# COUNTERMEASURES

# 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

# Countermeasures for Wireless Attacks

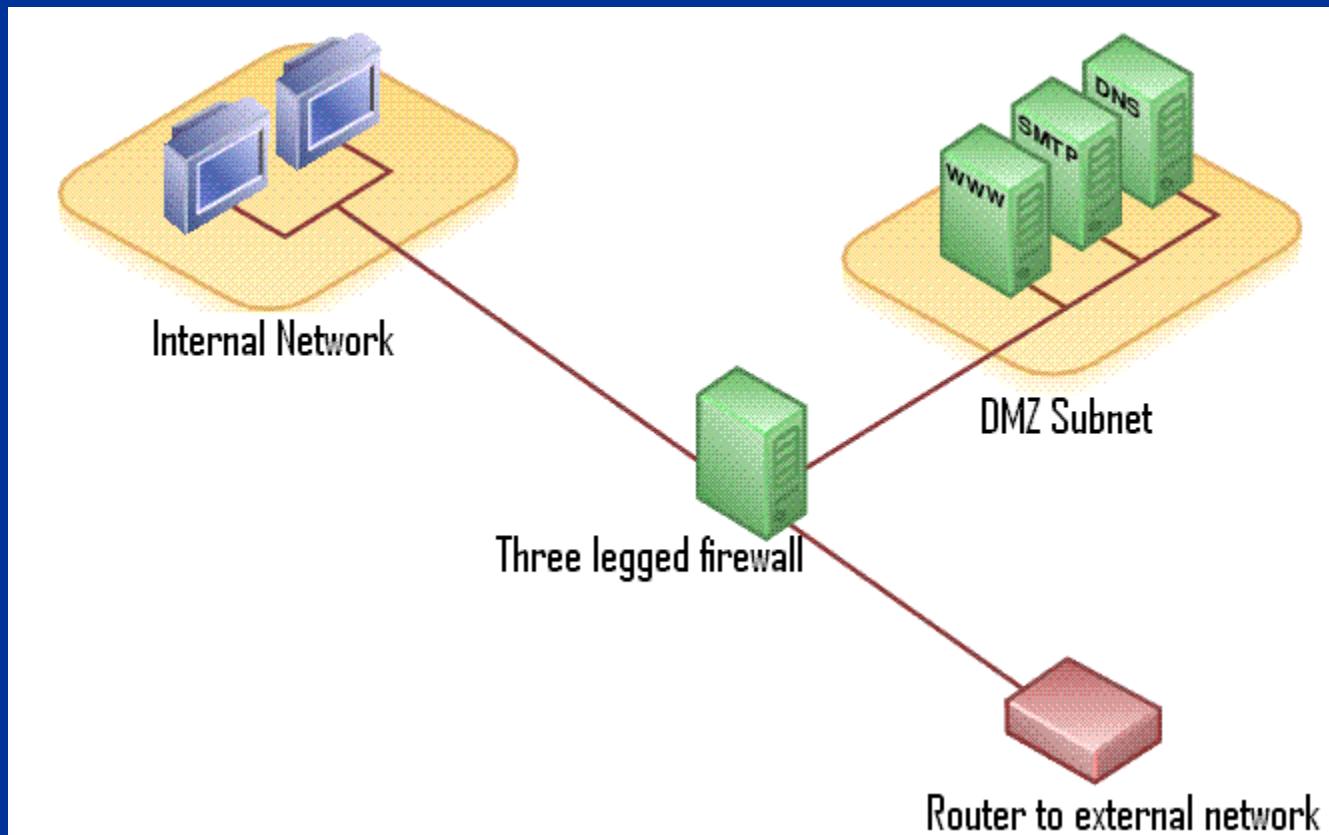
- Use special paint to stop radio from escaping your building
- Allow only predetermined MAC addresses and IP addresses to have access to the wireless LAN
- Use an authentication server instead of relying on a wireless device to authenticate users

# 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)



# SUMMARY

- Get to know the different between Wi-Fi standard
- Each authentication used by Wi-Fi have it own vulnerability, each improvement on the Wi-Fi security is just to slow down the attack
- Wi-Fi can be exploit by several attacking method and tool
- The countermeasures introduce in this chapter can be used to increase the Wi-Fi security

**THE END**