

Introduction to Wireless Networks

- Wi-Fi refers to a wireless local area networks supported IEEE 802.11 standard
- It is widely used technology for wireless communications across a radio channel
- Devices like a private computer, video-game console, Smartphone. Use Wi-Fi to attach to a network resource like the web via a wireless network access point

Advantages:

- Installation is fast and straightforward and eliminates wiring through walls and ceilings
- It is easier to supply connectivity in areas where it's difficult to get cable
- Access to the network are often from anywhere within range of an access point
- Public places like airports, libraries, schools offers you constant Internet connections using Wireless LAN

Disadvantages:

- Security may be a big issue and should not meet expectations
- As the number of computers on the network increases, the bandwidth suffers
- Wi-Fi enhancement can require new wireless cards and / or access points
- Some equipment can interfere with the Wi-Fi networks

Wireless Terminologies

GSM:

Global System for Mobile Communication (GSM) may be a standard by European Telecommunication Standards Institute. it's a second generation (2G) protocol for digital cellular networks. 2G was developed to exchange 1G (analog) technology. This technology has been replaced by 3G UMTS standard and followed by 4G LTE standard.

Access Point:

In Wireless networks an Access point (AP) may be a hardware device that permits wireless connectivity to the top devices. The access point can either integrated with a router or a separate device connected to the router.

SSID:

Service Set Identifier (SSID) is the name of an Access Point.

BSSID:

MAC address of an Access Point.

Wireless Terminologies

ISM Band:

ISM band also called the unlicensed band may be a frequency band dedicated to the commercial, Scientific and Medical purpose. The 2.54 GHz waveband is dedicated to ISM. Microwave ovens, cordless phones, Military radars and industrial heaters are a number of the equipment that uses this band.

Orthogonal Frequency Division Multiplexing (OFDM):

Orthogonal frequency-division multiplexing (OFDM) could be a method of digital encoding on multiple carrier frequencies. it's utilized in digital televisions, audio broadcasting, DSL internet and 4G communication.

Frequency-hopping Spread Spectrum (FHSS):

FHSS may be a technique of transmitting radio signals by switching or hopping the carrier of various frequencies.

Wireless Technology Statistics

Why Wireless Technology Matters?



More than half of all open Wi-Fi networks are susceptible to abuse

There will be more than **7 billion** new Wi-Fi enabled devices in the next 3 years

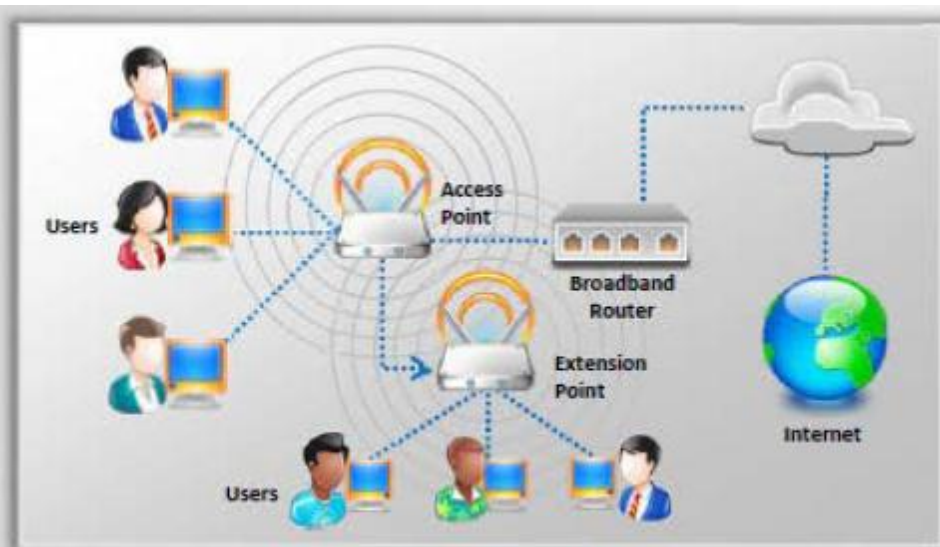
90% of all smartphones are equipped with Wi-Fi capabilities

A Wi-Fi attack on an open network can take less than **2 seconds**

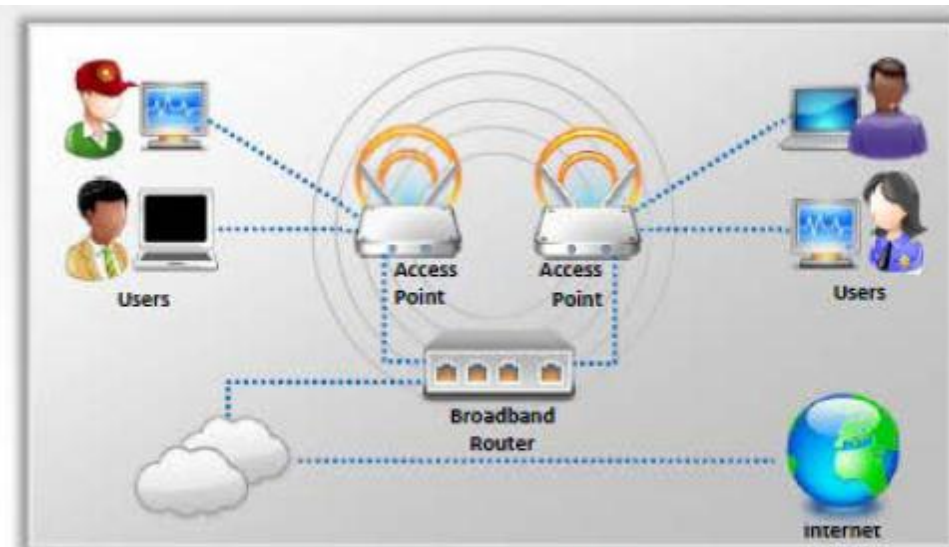
By 2017, **60%** of carrier network traffic will be offloaded to Wi-Fi

71% of all mobile communications flows over Wi-Fi

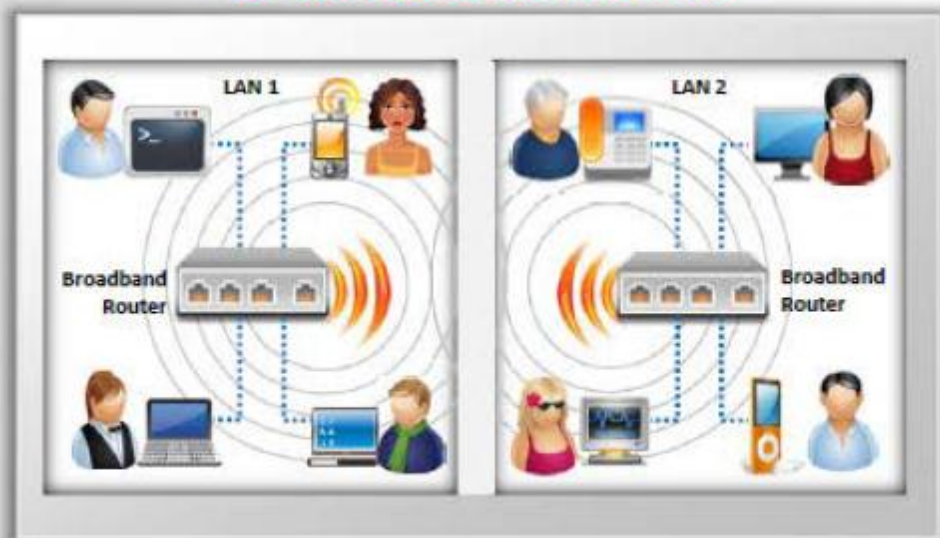
Types of Wireless Networks



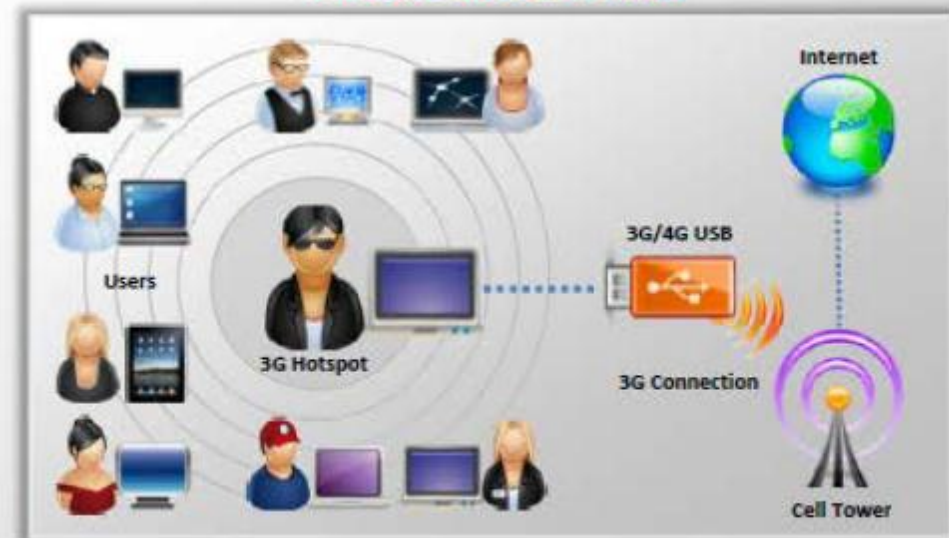
Extension to a Wired Network



Multiple Access Points



LAN-to-LAN Wireless Network



3G/4G Hotspot

Wireless Standards

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

Service Set Identifier (SSID)

- SSID may be a token to spot a 802.11(Wi-Fi) network, by default it's the a part of the frame header sent over a wireless local area network (WLAN)
- It acts as one shared identifier between the access points and clients
- Access points continuously broadcasts SSID, if enabled for the client machines to spot the presence of wireless network
- SSID may be a human-readable text string with a maximum length of 32 bytes
- If SSID of the network is modified reconfiguration of the SSID on every host is required, every user of the network configures SSID into their system
- Security concerns arise when the default values aren't changed, as these units are often compromised
- The SSID remains secret only on closed networks with no activity, that's inconvenient to the legitimate users
- A non-secure access mode allows clients to attach to the access points using the configured SSID, a blank or an SSID configured as "any"

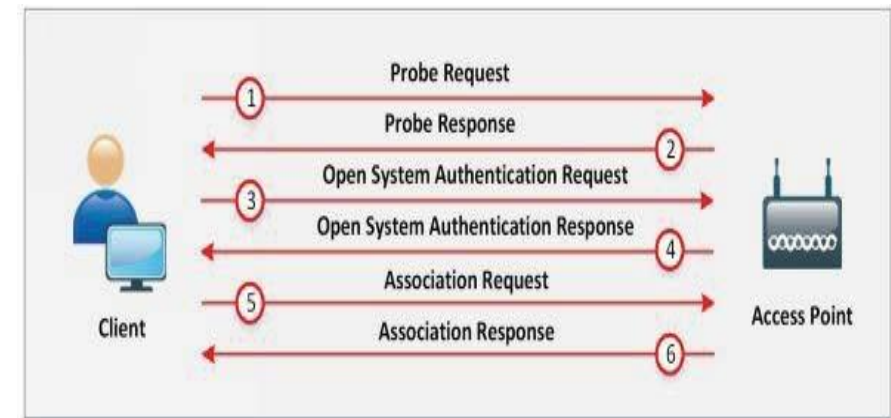
Wi-Fi Authentication Modes

- There are 2 types authentication in Wi-Fi based networks:
 1. Open Authentication
 2. Shared Key Authentication

Open system authentication process

Open system authentication process involves six frame communications between client and therefore the responder to finish the method of authentication

- The client sends an open authentication request to the access point with the sequence 0x0001 to line authentication open.
- The Open authentication request is replied by access point with response having sequence 0x0002
- Access point responds with an invitation to finish the method of association and client can start sending data.



Wi-Fi Authentication Modes

Shared Key Authentication:

Shared Key authentication mode involves four frames to finish the method of authentication

- first frame is that the initial authentication request frame that sent by client to the responder or access point.
- Access point responds to authentication request frame with the authentication reply frame.
- The client will encrypt the text with the shared secret key & send it back to the responder.
- Responder decrypts the text with the shared secret key. If the decrypted text matches with the challenge text, successful authentication response frame is shipped to the client.



Major Components of 802.1xWLAN Security Solution

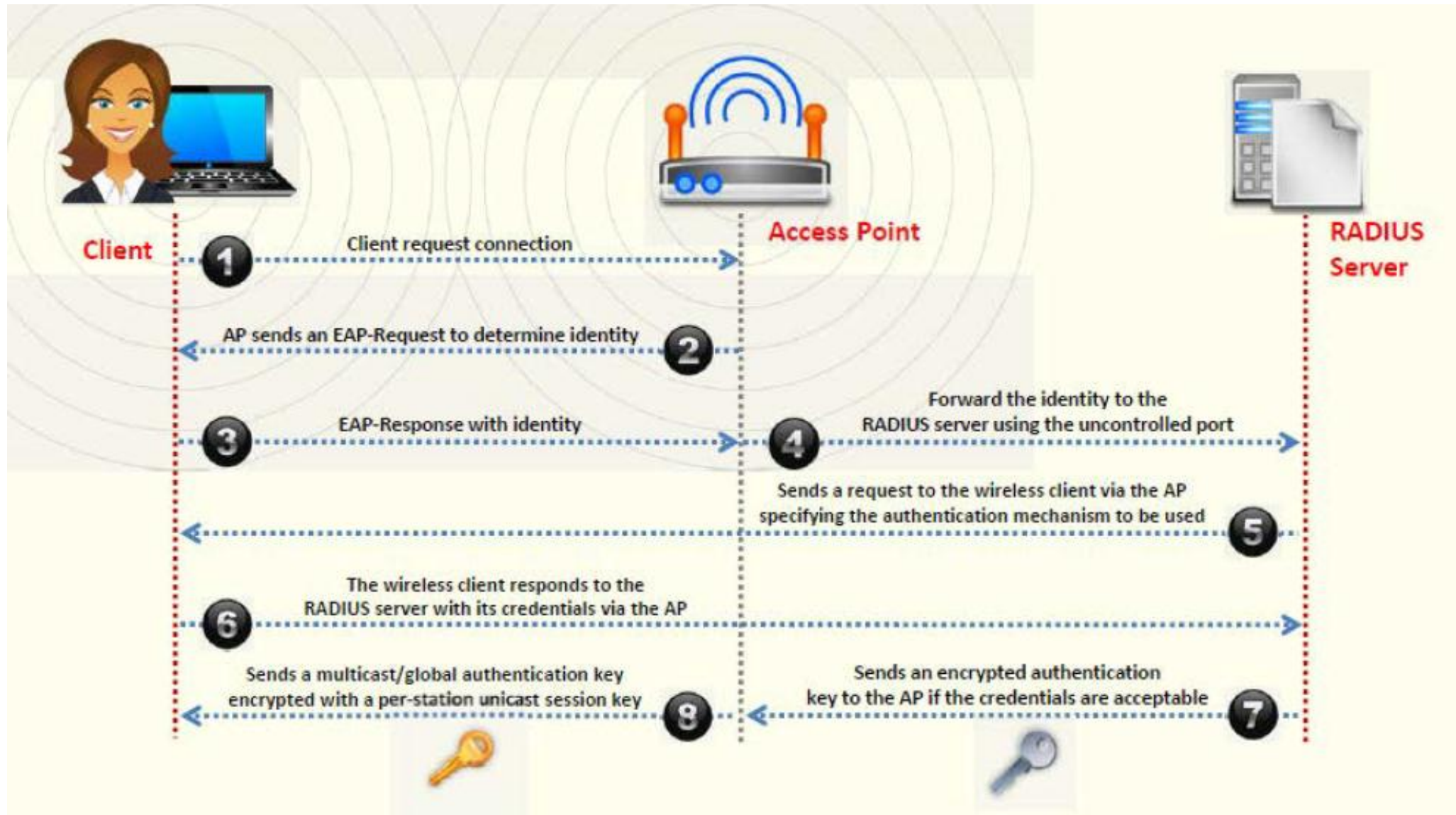
The major components on which enhanced WLAN Security solution IEEE 802.1x with EAP depends are: -

Authentication: Mutual Authentication process between Endpoint User & Authentication Server RADIUS, i.e., commonly ISE or ACS

Encryption: Encryption keys are dynamically allocated after authentication process.

Central Policy: Central policy offers management & Controlling over re-authentication, session timeout, regeneration and encryption keys, etc.

Wi-Fi Authentication with Centralized Authentication Server



Types of Wireless Encryption

WPA2 Enterprise: It integrates EAP standards with WPA2 encryption

WPA2 : WPA2 uses AES(128-bit) and CCMP for wireless data encryption

WEP : WEP is an encryption algorithm for IEEE 802.11 wireless networks

It is an old & original wireless security standard which can be cracked easily

EAP : Supports many authentication methods, such as token cards, Kerberos, certificates

802.11i : It is an IEEE amendment that specifies security mechanisms for 802.11 wireless networks

RADIUS: It is a centralized authentication and authorization management system

TKIP: A security protocol used in WPA as a replacement for WEP

CCMP: CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection

AES: It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP

WPA: It is a advanced wireless encryption protocol using TKIP, MIC, and AES encryption

Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security

LEAP: It's a proprietary WLAN authentication protocol developed by Cisco

WEP Encryption

- Wired Equivalent privacy is an IEEE 802.11 wireless protocol which provides security algorithms for data confidentiality during wireless transmission
- WEP uses 24-bit initialization vector (IV) to make stream cipher RC4 for confidentiality, and therefore the CRC-32 checksum for integrity of wireless transmission

WEP encryption can be easily cracked

64-bit WEP uses a 40-bit key
128-bit WEP uses a 104-bit key size
256-bit WEP uses 232-bit key size

WEP Flaws

It was developed without:

- 👤 Academic or public review
- 👤 Review from cryptologists

It has significant vulnerabilities and design flaws

WPA Encryption

Wi-Fi Protected Access (WPA) is another encoding technique that's popularly used for WLAN network supported 802.11i Standards. Deployment of WPA needs firmware upgrade for Wireless network interface cards that are designed for WEP. WPA also contains Message Integrity Check as an answer of Cyclic Redundancy Check (CRC) that's introduced in WEP to beat the flaw of strong integrity validation.

Temporal Key Integrity Protocol

Temporal Key Integrity Protocol (TKIP) could be a protocol that's utilized in IEEE 802.11i Wireless networks. This protocol is used in Wi-Fi Protected Access (WPA). TKIP has introduced three security features:


1. Secret root key & Initialization Vector (IV) Mixing before RC4.
2. Sequence Counter to make sure receiving so as to stop replay attacks.
3. 64-bit Message Integrity Check (MIC).

WPA2 Encryption

- WPA2 provides enterprise & Wi-Fi users with stronger data protection and network access control
- Provides government grade security by implementing the NIST, FIPS 140-2 complaint AES encryption algorithm

Encryption	Encryption Algorithm	IV Size	Encryption Key	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-Bits	CRC-32
WPA	RC4 , TKIP	48-bits	128-Bits	Michael Algorithm and CRC-32
WPA2	AES , CCMP	48-bits	128-Bits	CBC-MAC

WEP vs. WPA vs. WPA2

Encryption	Attributes			
	Encryption Algorithm	IV Size	Encryption Key Length	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bit	CRC-32
WPA	RC4, TKIP	48-bit	128-bit	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bit	128-bit	CBC-MAC

WEP



Should be replaced with more secure WPA and WPA2

WPA, WPA2



Incorporates protection against forgery and replay attacks

WEP / WPA Cracking Tools



WepAttack

<http://wepattack.sourceforge.net>



Wesside-ng

<http://www.aircrack-ng.org>



Reaver Pro

<https://code.google.com>



WEPCrack

<http://wepcrack.sourceforge.net>



WepDecrypt

<http://wepdecrypt.sourceforge.net>



Portable Penetrator

<http://www.secpoint.com>



CloudCracker

<https://www.cloudcracker.com>



coWPAtty

<http://wirelessdefence.org>



Wifite

<http://code.google.com>



WepCrackGui

<http://wepcrackgui.sourceforge.net>

How to Defend Against Wireless Attacks

Configuration Best Practices:

- Change the default SSID after WLAN configuration
- Set the router access password and enable firewall protection
- Disable SSID broadcasts
- Disable remote router login and wireless administration
- Enable encryption on access point and change passphrase often

SSID Settings Best Practices:

- Use SSID cloaking to stay certain default wireless messages from broadcasting the ID to everyone
- Do not use your SSID, company name, network name, or any easy to guess string in passphrases
- Place a firewall or packet filter in between the AP and therefore the corporate intranet
- Check the wireless devices for configuration
- Implement a further technique for encrypting traffic like IPSEC over wireless

How to Defend Against Wireless Attacks

