

**Wireless Networking**



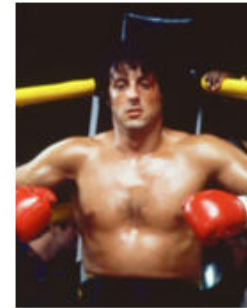
# Objectives

- Quick Recap: Wired and Wireless connectivity
- Wired connectivity (Ethernet connection)
- Wireless Connectivity
- Wireless (Pros and Cons)
- Wireless standards (802.11a, b, g, n)
- Wireless components (clients, access points)
- Wireless Access Points
- Antennas
- WLAN Topologies (ad-hoc & infrastructure)
- Wireless security methods (Open, Shared Key, WEP, WPA, WPA2)
- Site Survey

# So Let's Recap...

In order for communication to occur, a source, destination and some channel (path) must be present

In one corner we have guided or bound media i.e. “The Wire”  
(some physical means e.g. cable that guides the data signal along a specific path)



In the other corner we have unguided or unbound media i.e. “Wireless”  
(data signals travel but there is nothing to guide them along a specific path (use radio waves))



Wireless networks allow the transmission of information between hosts without cables

Similar to a wired LAN, except that radio waves, infrared light beams or lasers are used instead of wires



## **Connect via Ethernet Connection**

Cabling protocol for transmitting data across LAN's (connect computers to hubs/switches/routers)

Wired connection (fast data transfer speeds within the LAN or your networking sensitive data)

Cable installation can be labor intensive and expensive

Ethernet Network = NIC + Ethernet cables



## **Ethernet Connection**

**(transmit data at one of four standard speeds)**

Around since the 70's with slow networks running at 10Mbps  
(Ethernet is a tenth of Fast Ethernet)



Years later 100 Mbps (Fast Ethernet) became practical  
(operates at a tenth of the gigabit speed)

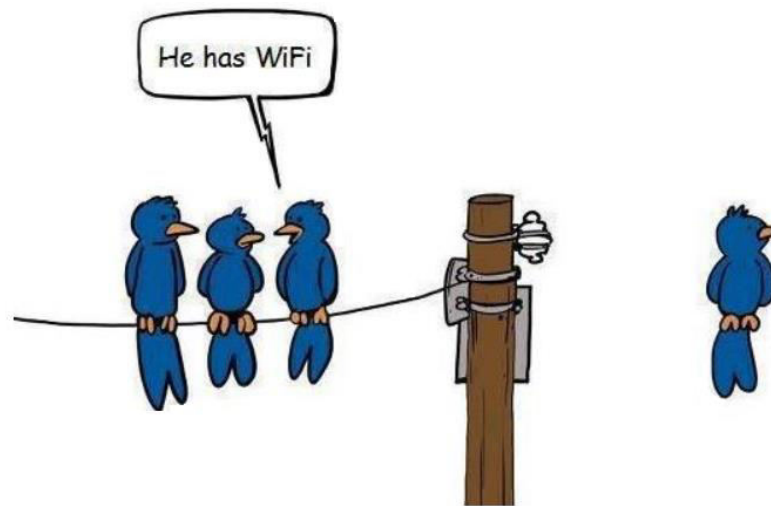


1000 Mbps (Gigabit (1G) Ethernet)



10 Gigabit Ethernet (10G Ethernet)

Ethernet or wired networks (except 10 Mbps Ethernet standard) are **faster** than most wireless networks  
(Gigabit Ethernet however, 802.11ac is getting fast at 1.3 Gbps)



**More reliable** (no wireless signal cutting in and out)

Nothing will delay or stop the signal moving through Ethernet cabling.  
Signals transmitted are seldom subject to fluctuations in bandwidth & interference.  
e.g. Ideal for high volume streaming of movies



**More secure** (no way to intercept signals/steal the data through the air)

(Major companies/universities have stayed with wired due been more secure)



**More useful** over very large distances where wireless signals are not strong enough.



**More control:** business is in full control of who and what gets online  
i.e. physical layout and more layers of security





## Connect via Wireless

Use radio frequency (RF) signals to connect all of devices together

Most popular wireless technology for home networks = **Wi-Fi (Wireless Fidelity)**

"Wi-Fi" is a type of wireless networking protocol that allows devices to communicate without cords or cables

Multiple Wi-Fi protocols with each operating at different frequencies, speeds and distances

(pretty much compatible w ith each other)



Each computer must have a wireless adapter installed/connected to it i.e. adapter is a miniature transmitter for those RF signals

Wireless devices transmit/receive radio frequencies (RF) signals at a specific frequency



# On a Positive Note

## Wireless connectivity is convenient

(Coffee shops, schools or universities, libraries, cell phones, iPads)



## Adds Mobility

(Provides users with access to information from anywhere in their organization)



## Flexible

(Allows new clients/devices to be added quickly and effortlessly)

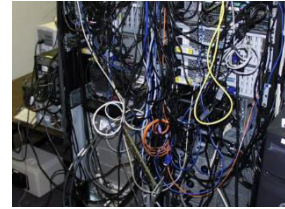


## Scalable

(Can easily be resized/expanded to meet current needs (allow more users to connect))



**Simpler to install**  
(reduced installation time)



**Cost Effective**  
(Networking media for use in areas that are too costly to wire)



**Reliable in harsh environments**  
(Easy to install in emergency & hostile environments)



# ON THE NEGATIVE SIDE

## Lack of security

(Intercepting the wireless connection is easy as broadcasting your data over public airwaves)

## Limited throughput

i.e. subject to interference & dropped connections due to distance & range issues

Speeds are slower than with a wired connection

## Signals can be affected by outside influences

(Walls, floors and other electronic items)

You know what's worse  
than slow internet?

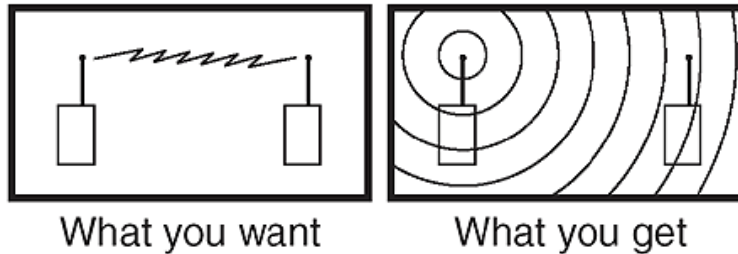


In BED, it's 6AM...  
you close your eyes for 5 minutes... it's 7:45.  
At WORK, it's 1:30...  
You close your eyes for 5 minutes... it's 1:31.



## Limited Range

Inside a building, range of wireless components might be limited to 100 – 200 feet  
To ensure full, reliable coverage across a building install plenty of **access points**



## Lack of control

Wireless networks can be protected, there is usually one point of vulnerable outside access.  
Non-company owned devices can subject the network to malware.

# Combo is good.....

## **Combination of Wired and Wireless**

Business can satisfy the needs of its mobile workers

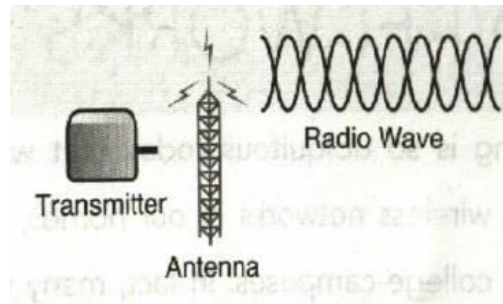
+

Ensure all security, control and reliability requirements

Wireless devices transmit/receive radio frequencies (RF) signals at a specific frequency



Radio waves are generated when a transmitter oscillates at a specific frequency  
(faster the oscillation the higher the frequency)



Antenna is used to amplify and broadcast the signal over long distances

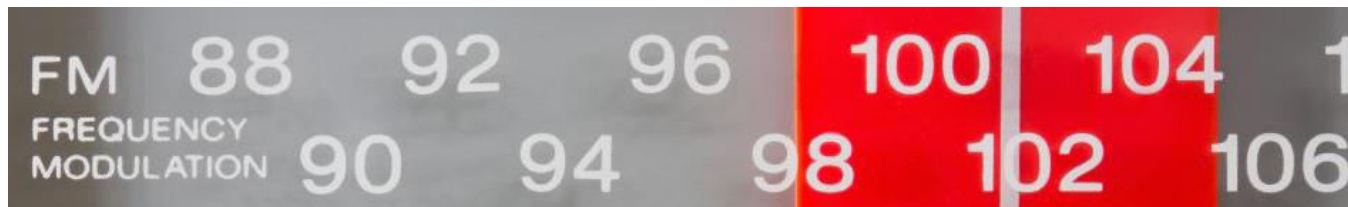


To receive a radio signal, you need a radio receiver which is tuned to a specific frequency to receive signals

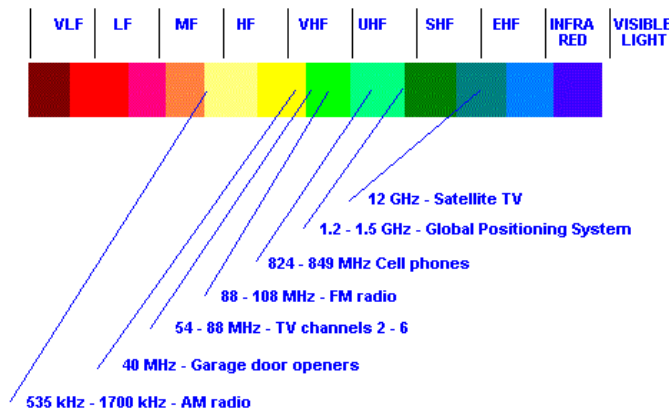
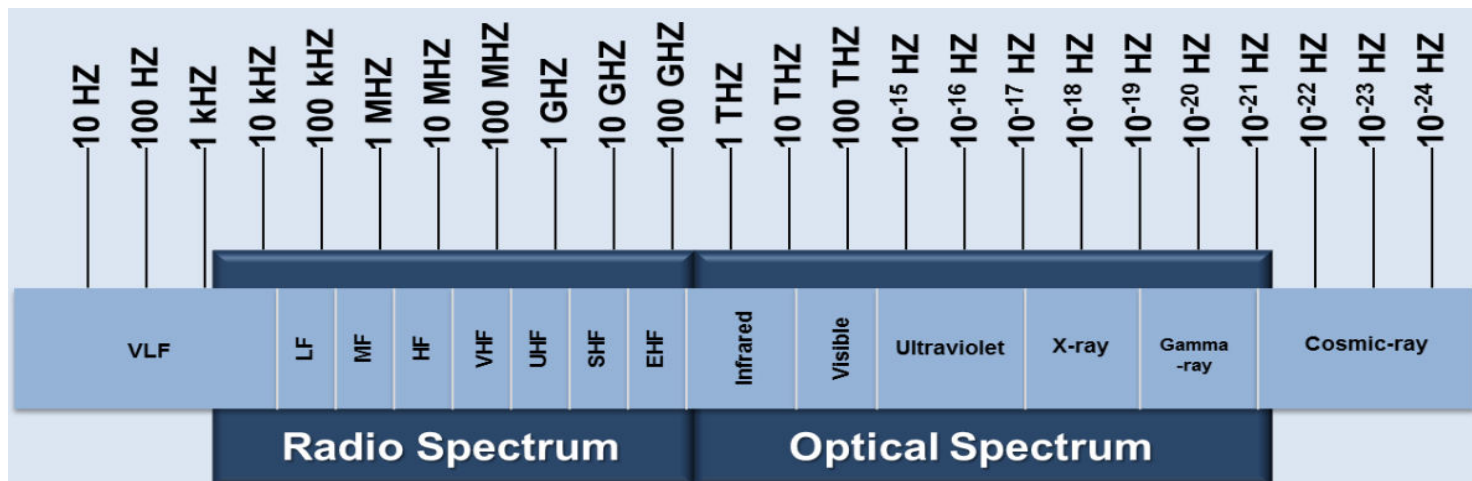
If not tuned to that frequency, the radio waves pass by without being received.



Different frequency ranges are used for different types of communication e.g. 88MHz → 108 MHz is FM radio stations



In wireless networks, each device (router or wireless adapter on a device) functions as both a transmitter and receiver



Band	Frequency range	Wavelength range
Extremely low frequency (ELF)	< 3 kHz	> 100 km
Very low frequency (VLF)	3 - 30 Hz	10 - 100 krn
Low frequency(LF)	30 - 300 kHz	1 - 10 km
Medium frequency (MF)	300 kHz - 3 MHz	100m - 1km
High frequency (HF)	3 - 30 MHz	10 - 100m
Very high frequency (VHF)	30 - 300 MHz	1 - 10m
Ultra high frequency (UHF)	300 MHz - 3 GHz	10cm - 1m
Super high frequency (SHF)	3 - 30 GHz	1 - 10cm
Extremely high frequency (EHF)	30 - 300 GHz	1mm - 1cm

## Current wireless networks use 2 distinct RF frequencies

Earlier equipment works in the 2.4 GHz band (frequencies between 2.4 GHz and 2.48 GHz)

Newer equipment can also use 5 GHz band (frequencies between 5.15 GHz and 5.85 GHz)

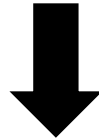


## **2.4 GHz band**

Free for anyone to use and for any purpose

No licensing fees

Space within the band is finite



## **Used by**

Wireless networks

Bluetooth wireless networks

Baby monitors (newer versions)

Garage door openers (newer versions)

Emergency radios

Microwave ovens

## **5 GHz band**

Relatively unused

Lot wider with more frequencies that can be used (5.15 GHz → 5.85 GHz)

Like 2.4, its unregulated which means its free for any device to use



No inherent benefit to operating at 2.4 GHz or 5 GHz except that 5 GHz is less crowded and thus less interference

Choose equipment that operates on less cluttered 5 GHz as less chance of interference

Wi-Fi is the wireless version of a wired Ethernet network, and it is commonly deployed alongside Ethernet

"Wi-Fi": type of wireless networking protocol that allows devices to communicate without cords or cables

De facto standard for home networks and public hotspot networks

Wi-Fi technology is now regulated by the Wi-Fi alliance (subgroup of IEEE)



Wi-Fi is the consumer friendly name for IEEE 802.11 wireless networking protocol.

802.11 standard defines how wireless devices communicate and how to secure that information

### Multiple Wi-Fi Protocols

(each operating at different frequencies, speeds and distances)

Wi-Fi Protocol	Release Date	Frequency Range	No of Data Streams	Maximum Bandwidth	Data Transfer Rate (max)	Transmission Range
802.11	1997	2.4 GHz	1	20 MHz	2 Mbps	66 Feet
802.11b	1999	2.4 GHz	1	20 MHz	11 Mbps	115 Feet
802.11a	1999	5.0 GHz	1	20 MHz	54 Mbps	115 Feet
802.11g	2003	2.4 GHz	1	20 MHz	54 Mbps	125 Feet
802.11n	2009	2.4/5.0 GHz	4	40 MHz	600 Mbps	230 Feet
802.11ac (draft)	2012	5 GHz	8	160 MHz	1.3 Gbps	230 Feet
802.11ad (proposed)	2014	60 GHz	4	2.16 GHz	7 Gbps	N/A

Home and business networkers looking to buy WLAN gear face an array of choices

Newer version are fully compatible with older ones  
e.g. you buy a 802.11n router and it will work with older 802.11b and 802.11g adapters

Wi-Fi Protocol	Release Date	Frequency Range	No of Data Streams	Maximum Bandwidth	Data Transfer Rate (max)	Transmission Range
802.11	1997	2.4 GHz	1	20 MHz	2 Mbps	66 Feet
802.11b	1999	2.4 GHz	1	20 MHz	11 Mbps	115 Feet
802.11a	1999	5.0 GHz	1	20 MHz	54 Mbps	115 Feet
802.11g	2003	2.4 GHz	1	20 MHz	54 Mbps	125 Feet
802.11n	2009	2.4/5.0 GHz	4	40 MHz	600 Mbps	230 Feet
802.11ac (draft)	2012	5 GHz	8	160 MHz	1.3 Gbps	230 Feet
802.11ad (proposed)	2014	60 GHz	4	2.16 GHz	7 Gbps	N/A

Wireless connections are a lot slower than the specified maximum due to distance, interference etc.

Radio signals don't suddenly stop when they get out of range, they weaken as you get father away from the transmitter.

To maximize data speeds, keep equipment close to the wireless router.

### 802.11 (legacy)

- Original Wi-Fi protocol
- Did not impact customer market
- Set benchmark for all future versions of protocols

### 802.11b

- First for general consumers
- Transferred data at 11 Mbps and well slower than 100 Mbps Ethernet
- Good enough for most homes/offices
- Suffered interference from other devices (baby monitors) using same 2.4GHz RF band

### 802.11a

- Used less crowded 5.0GHz RF band thus less interference from other wireless devices

### 802.11g

- Faster at 54 Mbps
- 'Extreme' g equipment which achieved data transfer rates at 105 Mbps

### 802.11n

- Standard used by most wireless equipment sold today

### 802.11ac (Gigabit Wi-Fi)

- Equipment already on the market
- 802.11ac equipment implement beam forming (a direct signal path between router and adapter as opposed to omnidirectional)

### 802.11ad

- Operates in higher 60 GHz frequency
- Not designed for traditional router based wireless networks
- Protocol for short range peer-to-peer connectivity e.g. stream HD video from one device to another (replace HDMI cable between Blue-Ray player and TV)

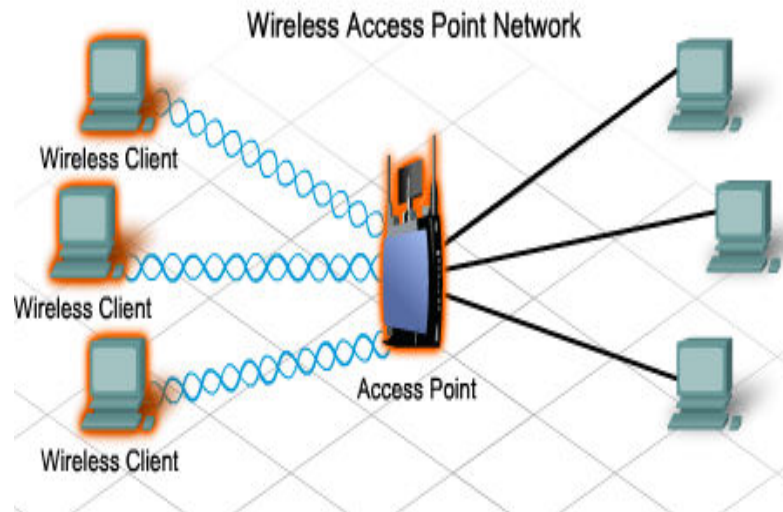
Wi-Fi Protocol	Release Date	Frequency Range
802.11	1997	2.4 GHz
802.11b	1999	2.4 GHz
802.11a	1999	5.0 GHz
802.11g	2003	2.4 GHz
802.11n	2009	2.4/5.0 GHz
802.11ac (draft)	2012	5 GHz
802.11ad (proposed)	2014	60 GHz



## Wireless LAN Components

Once a standard is adopted

Important that all components within the WLAN adhere to the standard or are at least compatible with the standard



## **Wireless Client (or 'STA' station)**

Any host (with a wireless NIC/adapter) that can participate in a wireless network.

e.g. laptops, PDA's, printers, projectors, Wi-Fi phones. and storage devices



**Wireless PCI NIC**



**External USB wireless NIC**

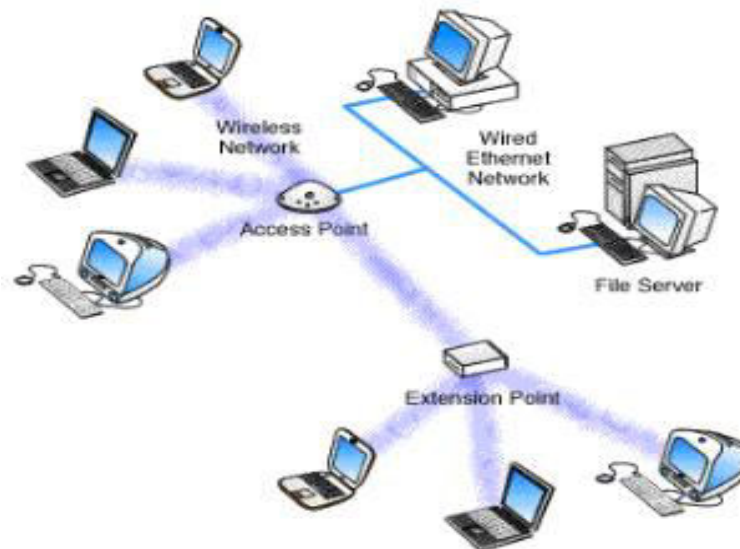
## Wireless Access Point (WAP)

Connects wireless nodes to wireless or wired networks.

Provides the bridge between the wireless LAN and the wired network i.e.

Operates at Layer 1

If a single area is too large to be covered by a single access point, then use multiple access points



In order for a STA to connect to the WLAN, the client configuration must match that of the AP

e.g. SSID, encryption, authentication

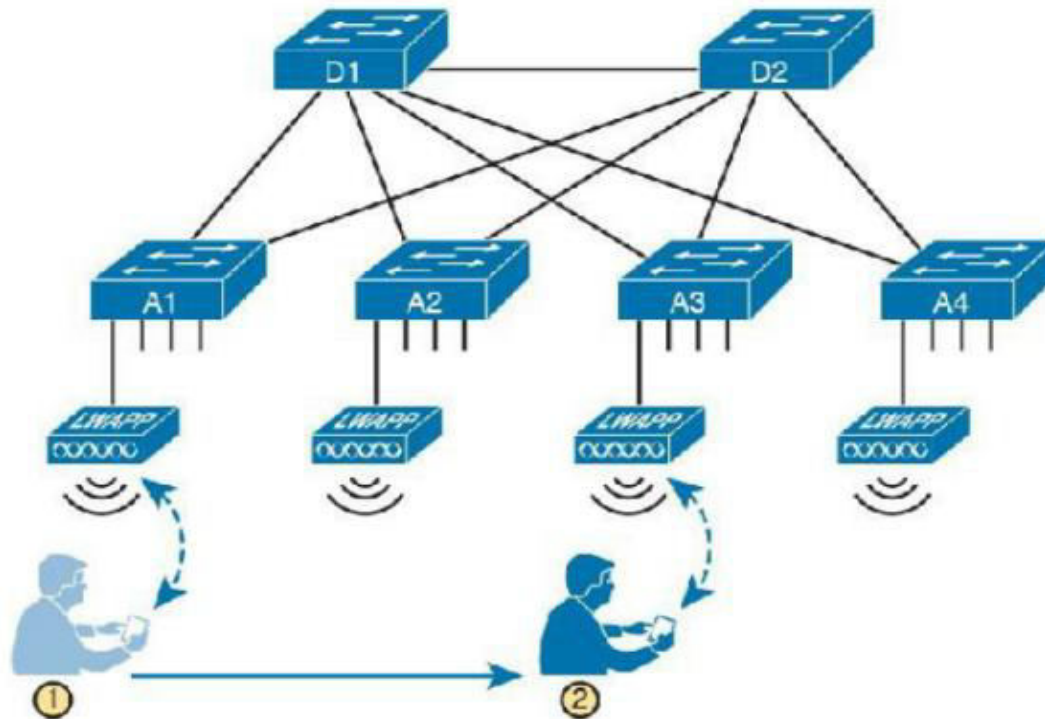
## Access Point (AP)

Communicates with the various wireless devices using 802.11 protocols and radio waves

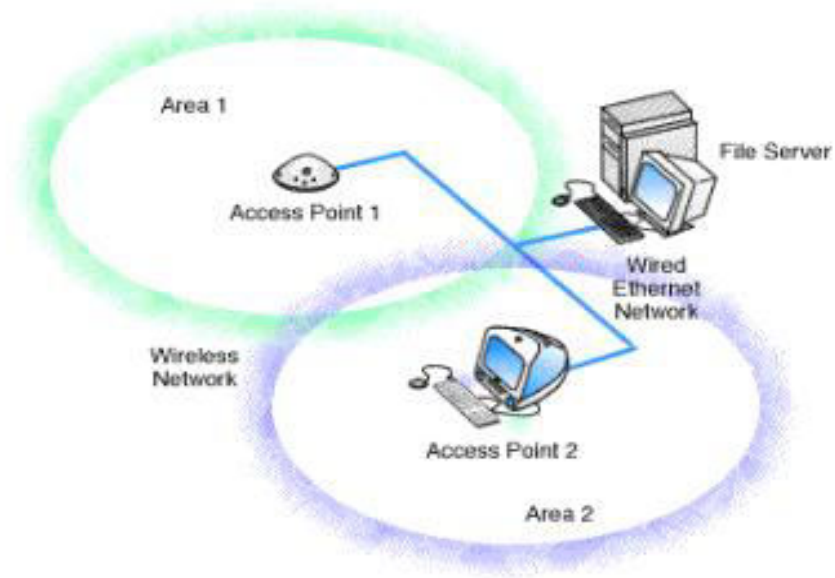
Uses Ethernet protocols on the wired side (most of the destinations that wireless users need to communicate with sit in the wired part of the network)

Converts between the differences in header formats between 802.11 and 802.3 frames

Before forwarding to/from 802.3 Ethernet and 802.11 wireless frames



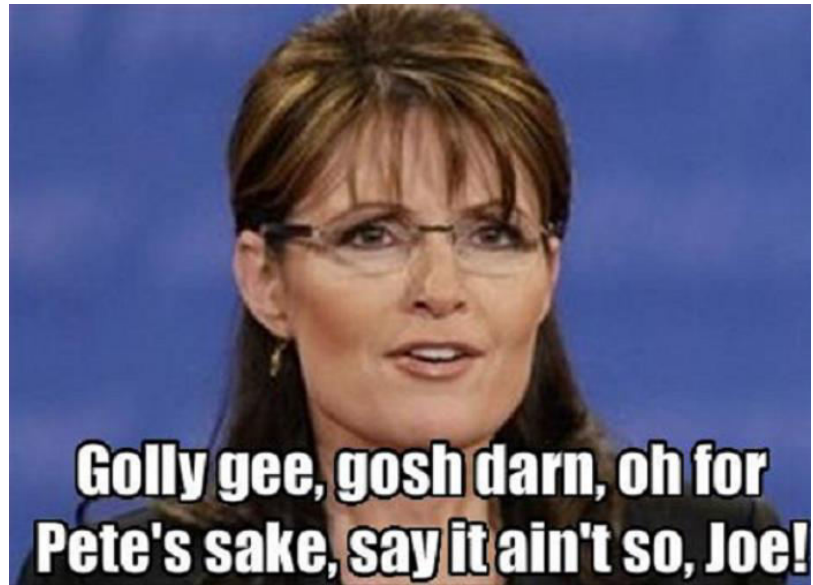
Each access point wireless area should overlap its neighbors.  
Provides a seamless area for users to move around i.e. **"roaming"**  
A wireless computer can "roam" from one access point to another



Much of the time spent designing WLANs revolves around deciding how many APs to place in each space



Imagine that if you had a dozen APs per floor, you might have hundreds of APs in a campus



Remove all the control and management features from the Aps

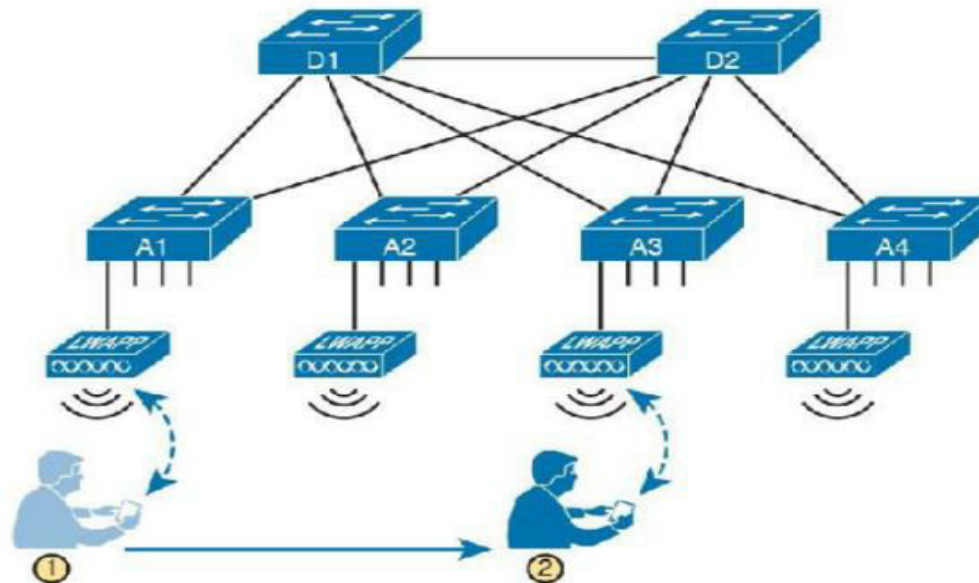
Put them in one centralized place → **Wireless Controller, or Wireless LAN Controller (WLC)**

APs no longer act autonomously, but instead act as lightweight APs (LWAPs)

Now just forwarding data between the wireless LAN and the WLC.

All the logic to deal with roaming, defining WLANs (SSIDs), authentication  
NOW

Happens in the centralized WLC rather than on each AP

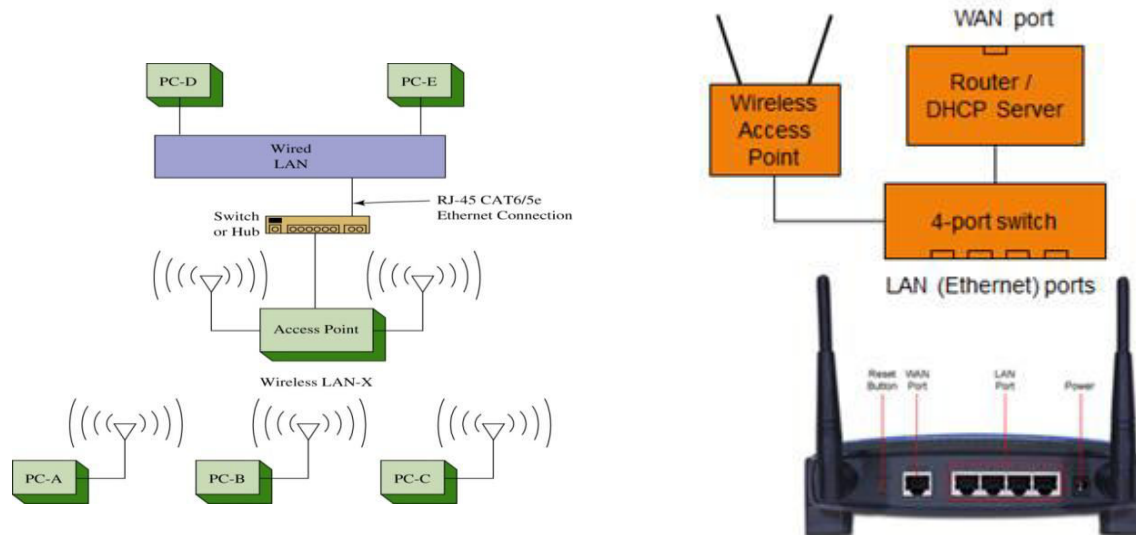




## Integrated Routers (Access Point)

Offers both wired and wireless connectivity

Serves as the AP in the wireless network



# Antennas

Increases the output signal strength ('gain') from a wireless device & measured in decibels (dB)

## Classified by the way they radiate the signal

1. Directional antennas concentrate the signal strength into one direction e.g. parabolic, dish
2. Omni-directional antennas radiates the signal equally in all directions.



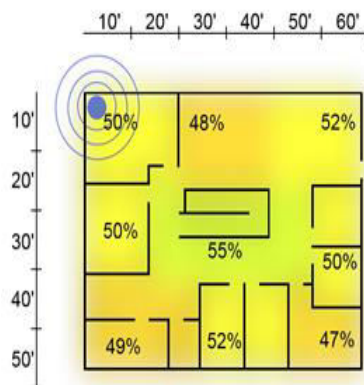
Omni-directional antenna



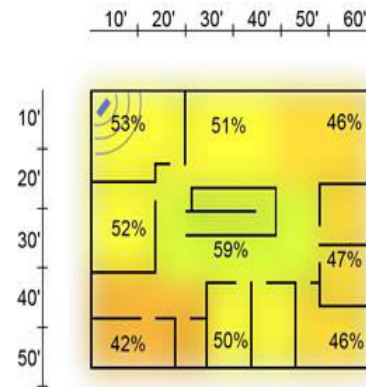
Semi-directional antenna



Replacement antenna on WAP



Omni-directional antenna



Semi-directional antenna

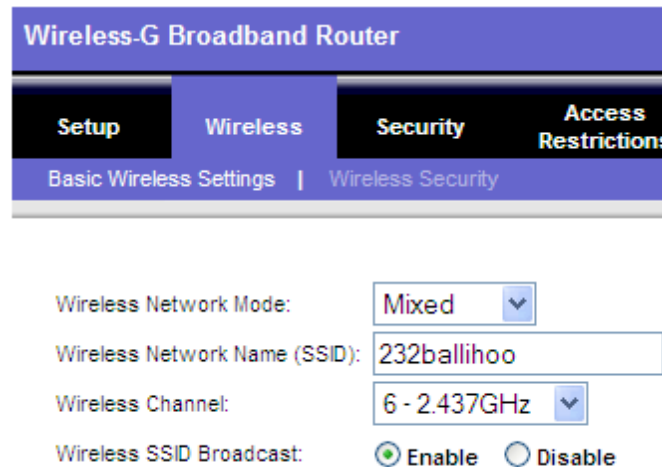
## Service Set Identifier (SSID)

Network name that identifies the network

Up to 32 alphanumeric (letters or numbers), case-sensitive characters

“Password” that enables a client to join the wireless network (not a security tool)

Change the SSID regularly so hackers (your neighbors) can not use it to access your home network



The image shows a screenshot of a web-based configuration interface for a 'Wireless-G Broadband Router'. The interface has a purple header bar with the title 'Wireless-G Broadband Router'. Below the header is a navigation bar with four tabs: 'Setup', 'Wireless', 'Security', and 'Access Restrictions'. The 'Wireless' tab is currently selected. Under the 'Wireless' tab, there are two sub-sections: 'Basic Wireless Settings' and 'Wireless Security'. The 'Basic Wireless Settings' section is active and displays the following configuration options:

- Wireless Network Mode:** A dropdown menu set to 'Mixed'.
- Wireless Network Name (SSID):** A text input field containing '232ballihoo'.
- Wireless Channel:** A dropdown menu set to '6 - 2.437GHz'.
- Wireless SSID Broadcast:** Two radio buttons, 'Enable' (which is selected) and 'Disable'.

Some routing companies used their company name as a default SSID e.g. Linksys router would have SSID labeled 'LINKSYS'

## Disable SSID broadcasting

When you disable, your own wireless devices won't be able to see your network in the list of available networks.

So enter the SSID manually when you initially go to connect

Wireless Network Mode:	Mixed ▼
Wireless Network Name (SSID):	232ballihoo
Wireless Channel:	6 - 2.437GHz ▼
Wireless SSID Broadcast:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

War Drivers or War Walking scan for the SSIDs being broadcast by wireless LANs



Still possible for the SSID to be obtained by packet sniffing.

Attacker uses packet sniffing to extract the SSID from data packets

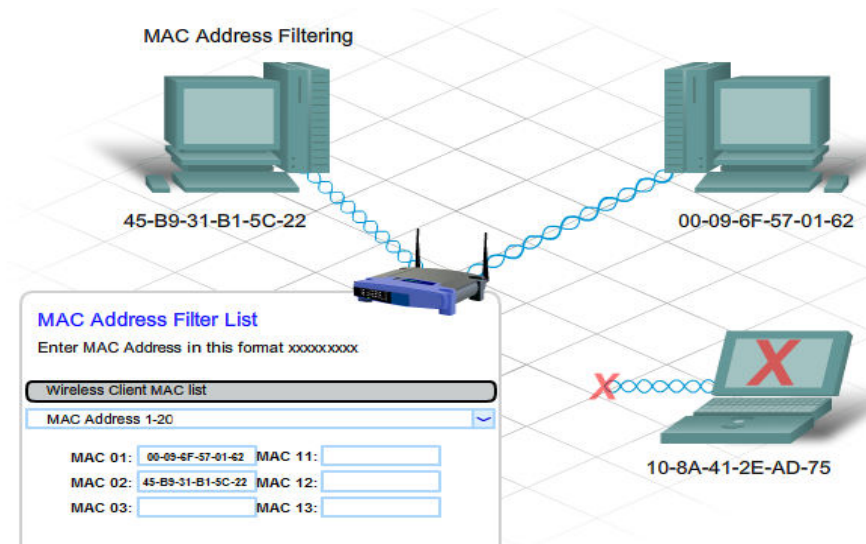


## MAC Address Filtering

When a wireless client attempts to associate with an AP it will send MAC address information

If MAC filtering is enabled, AP will look up its MAC address a preconfigured list.

Only devices whose MAC addresses have been listed will be allowed to connect.



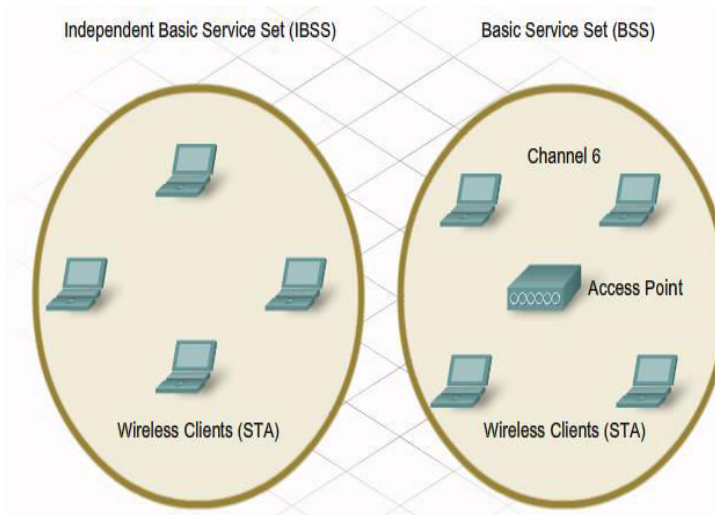
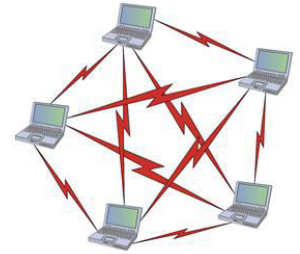
## Ad-hoc

Created by connecting two or more wireless clients together in a peer-to-peer network

Does not include an AP (Access Point).

Uses mesh topology

Area covered by this network → Independent Basic Service Set (IBSS)



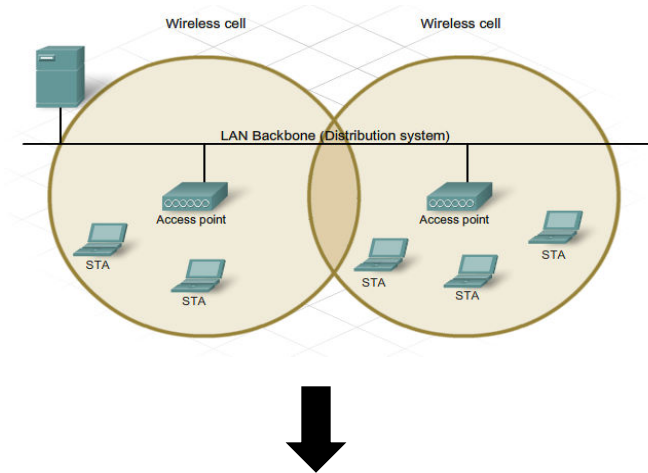
## Infrastructure Mode

Individual STAs can not communicate directly with each other.

AP controls who can talk and when (gives permission to devices & ensures that all STAs have equal access to the medium)

AP controls all communications and Area covered by a single AP is known as a **Basic Service Set (BSS) or Cell**

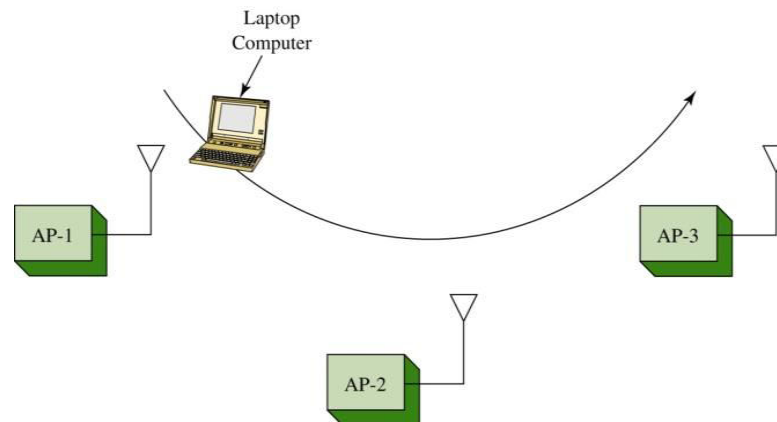
To expand the coverage area, it is possible to connect multiple BSSs → **Extended Service Set (ESS)**



In order to allow movement between the cells without the loss of signal, BSSs must overlap by approximately 10%

Allows the client to connect to the second AP before disconnecting from the first AP

**Hand-off** (when a users computer establishes an association with another access point with strongest signal level ).

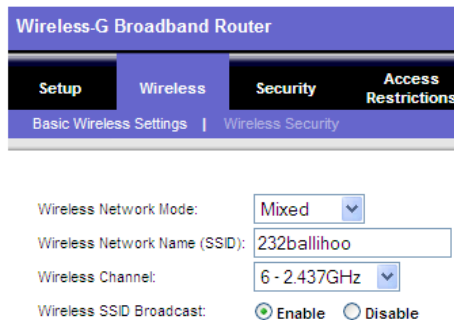




To keep outsiders from tapping into your wireless hardware, assign the network a **network code (key)**

Password which allows computers to access the network wirelessly.

You can specify that a network key be used for authentication to the network



Wireless-G Broadband Router

Setup | **Wireless** | Security | Access Restrictions

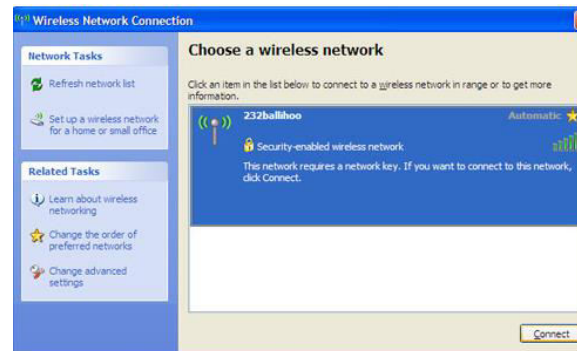
Basic Wireless Settings | Wireless Security

Wireless Network Mode: Mixed

Wireless Network Name (SSID): 232ballihoo

Wireless Channel: 6 - 2.437GHz

Wireless SSID Broadcast: ☒ Enable ☐ Disable



Wireless Network Connection

Network Tasks

- Refresh network list
- Set up a wireless network for a home or small office

Related Tasks

- Learn about wireless networking
- Change the order of preferred networks
- Change advanced settings

Choose a wireless network

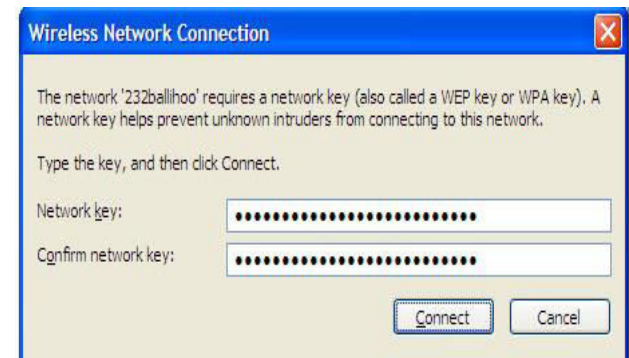
Click an item in the list below to connect to a wireless network in range or to get more information.

232ballihoo Automatic

Security-enabled wireless network

This network requires a network key. If you want to connect to this network, click Connect.

Connect



Wireless Network Connection

The network '232ballihoo' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key:

Confirm network key:

Connect Cancel

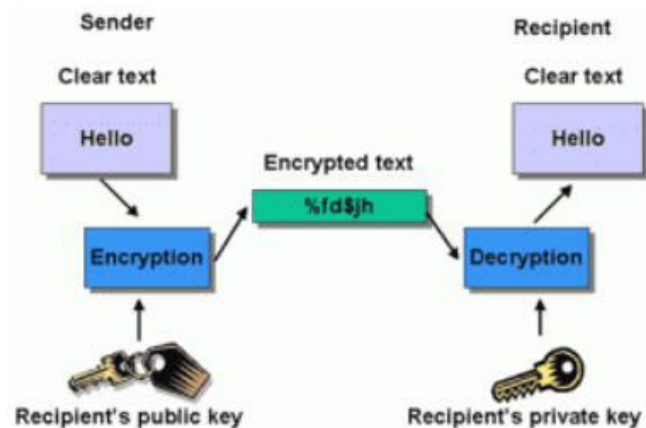
You can also specify that a network key be used to encrypt your data as it is transmitted over the network.

4 types of wireless security in use today & all require the use of a network key

Network key generated automatically by wireless router or manually specify it

### **WPA, WPA2, WEP 64-bit and WEP 128-bit**

**Data Encryption:** process of transforming data so that even if it is intercepted it is unusable.



## Wired Equivalency Protocol (WEP)

You setup the network key.

This key encrypts the information that one computer sends to another computer across your network

Not that great as can be hacked in < 1 minute as use of a static key on all WEP enabled devices

AP and every wireless device allowed to access the network must have the same shared WEP key



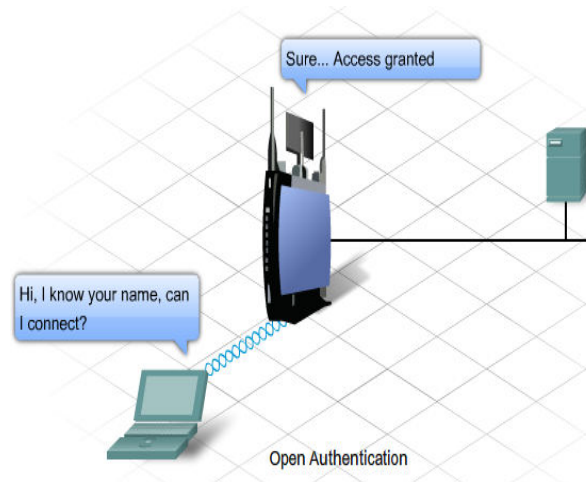
Two kinds of WEP: open system authentication and shared key authentication

## Open System Authentication or 'No Authentication'

Provides no security because of the "open" nature of this protocol.

Default is to trust all STA's that ask to be connected (requires no authentication).

Only security aspect is that the STAs should know the Service Set Identifier (SSID) or 'Network Name' of the AP



## Shared Key Authentication

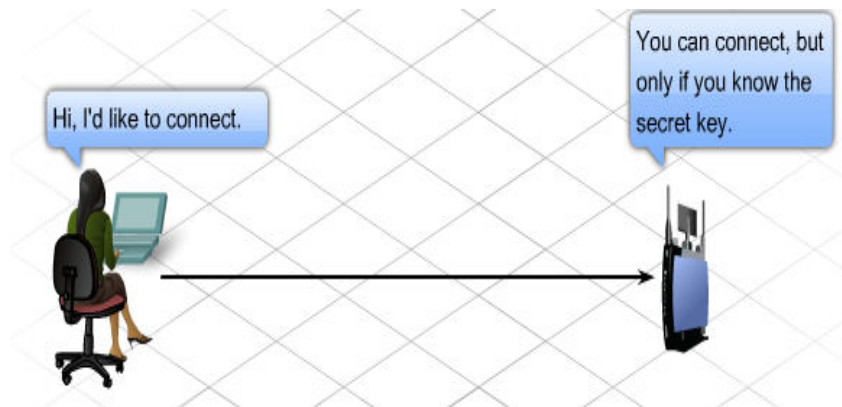
Relies on a secret key that is shared between a station and an access point to authenticate

Secret key is used to encrypt packets before they are transmitted

Integrity check is used to ensure that packages are not modified during the transition.

Key must be enabled and configured the same on the AP and client

Clients cannot associate with the AP until they use the correct key



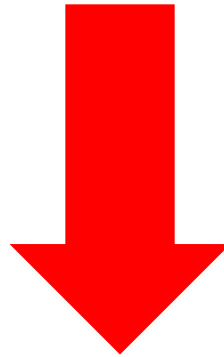
1. Station sends an authentication request to the access point.
2. Access point sends challenge text to the station.
3. Station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and it sends the encrypted text to the access point.
4. Access point decrypts the encrypted text using its configured WEP key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP key, and the access point authenticates the station.
5. Station connects to the network.

WEP's major weakness is its use of static encryption keys.

When you set up a router with a WEP encryption key, that one key is used by every network device to encrypt every packet

One way to overcome this vulnerability is to change the key frequently

Another way is to use a more advanced and secure form of encryption

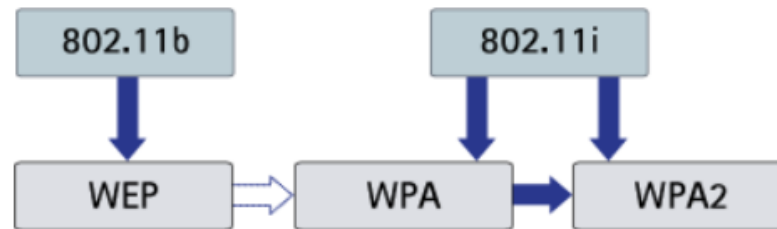


**Wi-Fi Protected Access (WPA)**

## Wi-Fi Protected Access (WPA)

Unlike WEP, generates new, dynamic keys each time a client establishes a connection with the AP

WPA2 offers strongest level of security available today & more secure than WPA



*Relationship between WEP, WPA and WPA2*

Choose the highest level of protection supported by all equipment on your network.

Order: WPA2 → WPA → WEP128 → WEP64

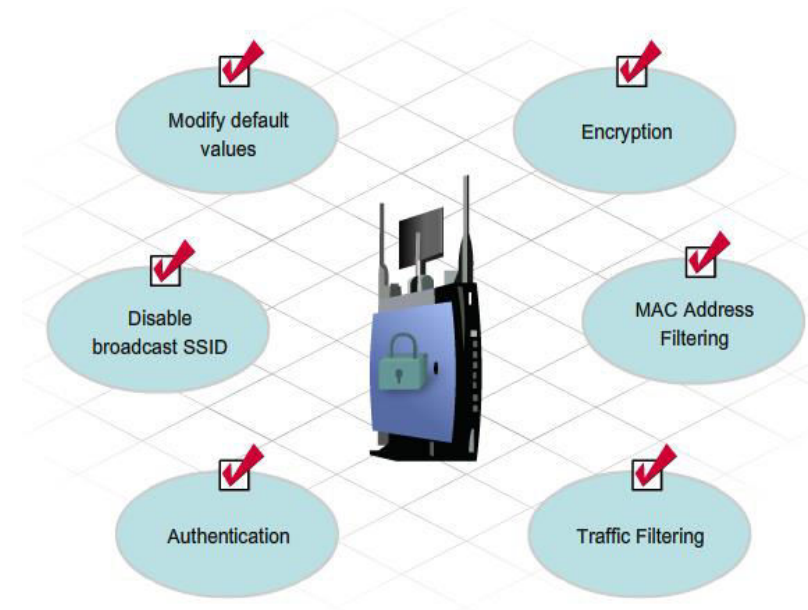
Security measures should be planned and configured  
**before**  
Connecting the AP to the network or ISP

### Basic Security Measures

- Change default values for the SSID, usernames and passwords
- Disable broadcast SSID
- Configure MAC Address Filtering

### Advanced Security Measures

- Configure encryption using WEP or WPA
- Configure authentication
- Configure traffic filtering







## **Protect against unauthorized access to your wireless network**

Activate wireless security technology built into Wi-Fi router

Change default password for wireless router

Change default network name (SSID)

Disable broadcast SSID function on the wireless router

Locate router towards center of a home not near the windows where it can extend the range of network

Install firewall, anti-virus s/w, anti-spyware on each PC

Deactivate file sharing on PC's so attackers can not access personal files

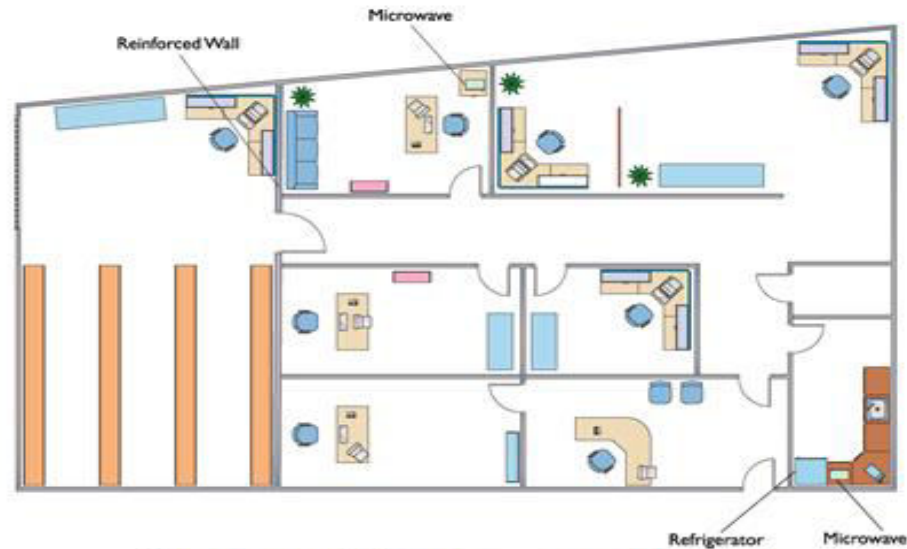
Backup data

## Site Survey

Process of evaluating a network solution to deliver the required coverage, data rates, network capacity, roaming capability

Person responsible for the site survey must be knowledgeable in WLAN design

Person responsible for the site survey **MUST BE** equipped with sophisticated equipment for measuring signal strengths and interference



**Site survey with interference sources noted**

♪ IT'S ♪  
OVER!

