



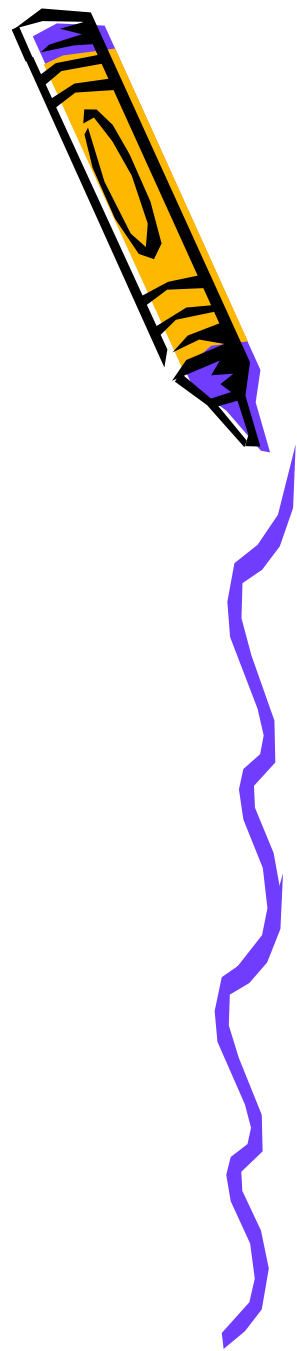
Presentation

Topic:

Wi - fi



WI-FI



wi-fi stands for:

wireless fidelity

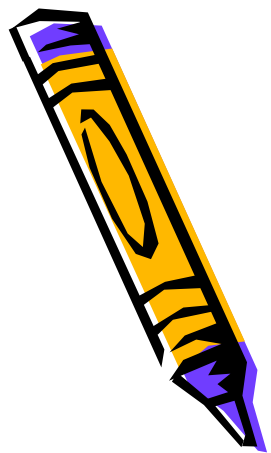
Wi-fi is a commercial name .It is not
a standard name

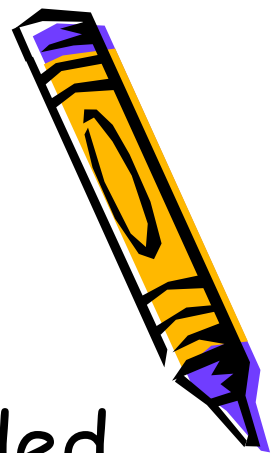


What is Wi-Fi?

The term Wireless fidelity is used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, 802.11g, dual-band, etc

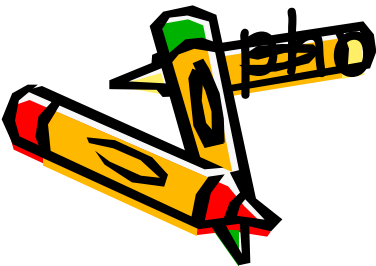
Wi-fi is a wireless technology that uses radio frequency to transmit data through the air





This technology was originally intended to allow mobile devices, such as laptops and PDAs to connect to local area networks.

." Today, it is often used for cheaper Internet access and by wireless phones.



Brief History



IEEE (Institute of Electrical and
Electronics

Engineers) established the 802.11 Group in
1990. Specifications for standard ratified
in 1997.

Initial speeds were 1 and 2 Mbps

IEEE modified the standard in 1999 to include
802.11 a and b



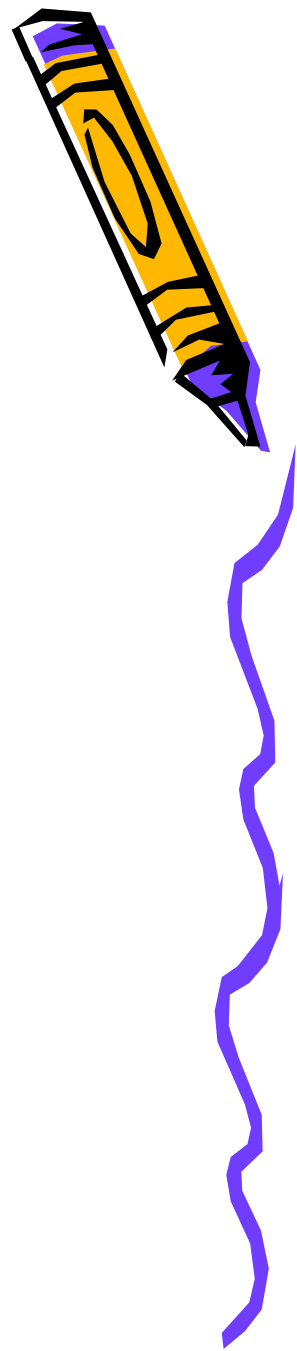
BRIEF HISTORY(cont)

802.11g was added in 2003 802.11b equipment first available, then a, followed by g

IEEE create standard but Wireless Ethernet Compatibility Alliance certifies products.



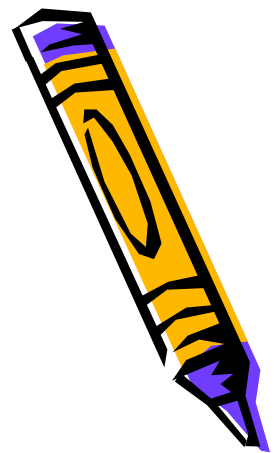
Why Wi-Fi?



- Setup Cost - Reduced cabling required
- Flexibility - Quick and easy to setup in
 - temp or permanent space
 - Scalable - Can be expanded with growth
 - Freedom - You can work from any location that you can get a signal
- Lower total cost of ownership - Because of
 - affordability and low install cost
 - Additionally Mobile Users - Can access the Corporate network from any public hotspot using VPN



What a wireless network is made up of:



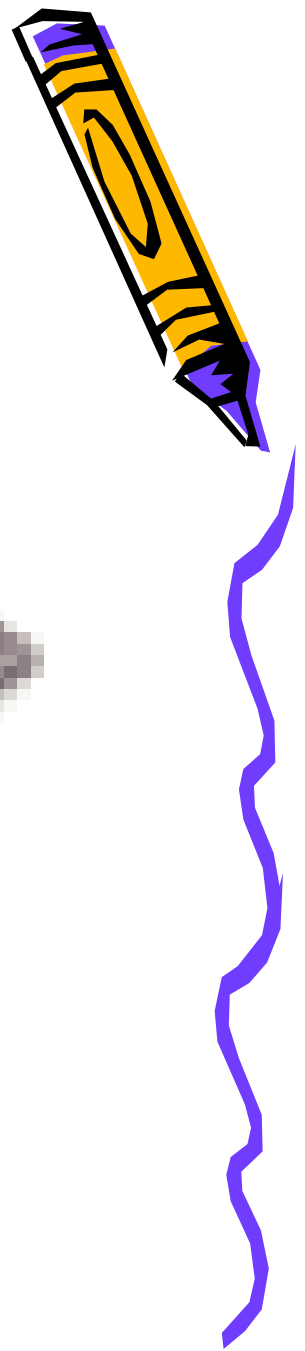
Wireless Network cards

Radios which send and receive signals from other radios or access points, usually PCMCIA* cards which fit into Laptop expansion slots, or PCI Bus in case of Desktop computers. (There are other, simpler options using USB).

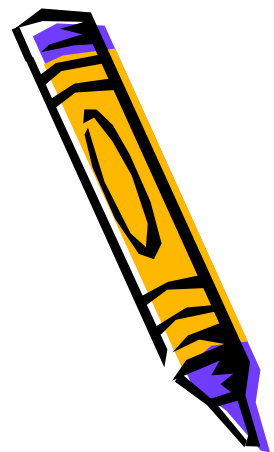
PDAs like PALM, and Pocket PC having a compact flash slot can also connect.




Wireless network card



Network system devices




 SIMMONS | Libraries

Wireless Installation: Relatively Simple

Access Points



Wireless card



The slide features a blue header with the Simmons College logo and the text 'SIMMONS | Libraries'. Below the header, the title 'Wireless Installation: Relatively Simple' is displayed. Underneath, the text 'Access Points' is followed by an image of a silver and blue wireless access point. To the right, the text 'Wireless card' is followed by an image of a Netgear wireless PC card and a laptop with a wireless card inserted.

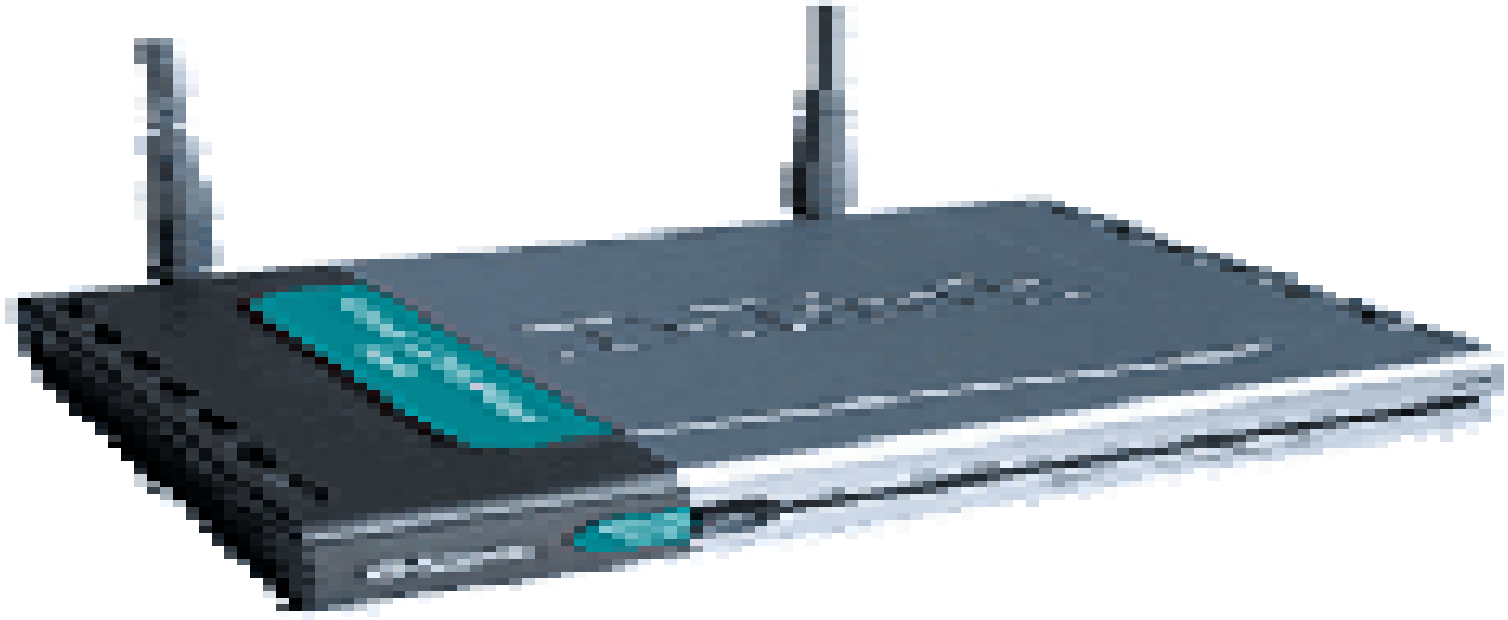


Base stations, Access points, or Gateways

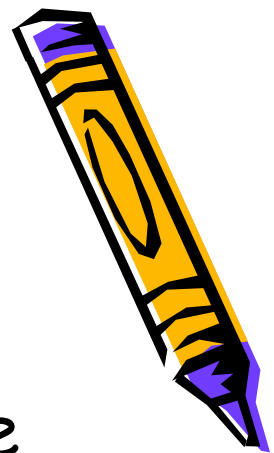
-The base station sends and receives radio signals to and from the Wi-Fi radio in your laptop or PC, enabling you to share your Internet connection with other users on the network. Access points and gateways have a wide range of features and performance capabilities, but they all provide this basic network connection service.



Access point



HARDWARE DEVICES USE IN WI-FI



- Wireless adapters or network interface controllers (NICs for short) are network cards with the 802.11 standard which let a machine connect to a wireless network.
- WiFi adapters are available in numerous formats, such as PCI cards, PCMCIA cards, USB adapters, and Compact Flash cards.



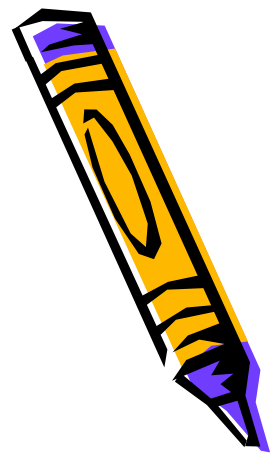
STATION & ACCESS POINT



- A **station** is any device that has such a card.
- **Access points** (**AP** for short; sometimes called *hotspots*) can let nearby wifi-equipped stations access a wired network to which the access point is directly connected.



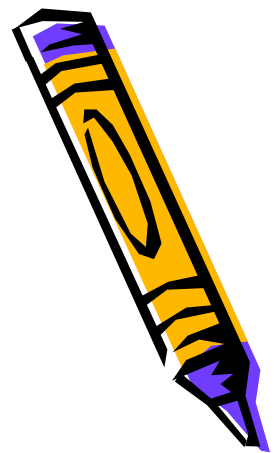
WiFi modes of operation (802.11 or Wi-Fi)



- Infrastructure mode, in which wireless clients are connected to an access point. This is generally the default mode for 802.11b cards.
- Ad hoc mode, in which clients are connected to one another without any access point.



INFRASTRUCTURE MODE



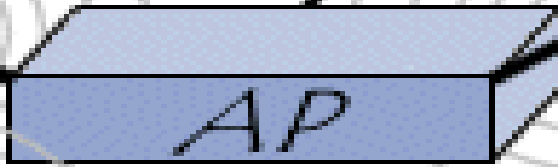
- In **mode infrastructure**, each station computer (**STA** for short) connects to an access point via a wireless link.
- The set-up formed by the access point and the stations located within its coverage area are called the *basic service set*, or **BSS** for short. They form one cell.
- Each BSS is identified by a BSSID, a 6-byte (48-bite) identifier.



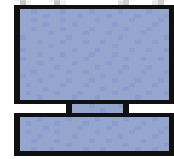
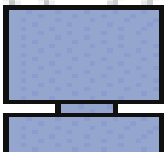
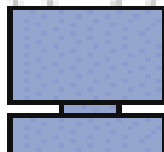
Infrastructure mode



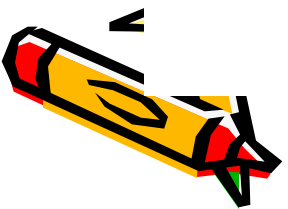
Network



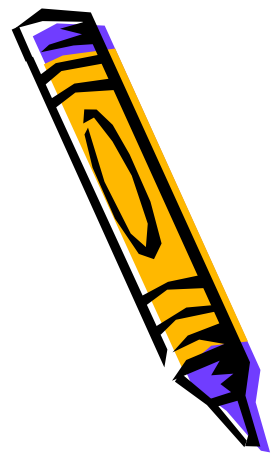
Access point



WiFi clients



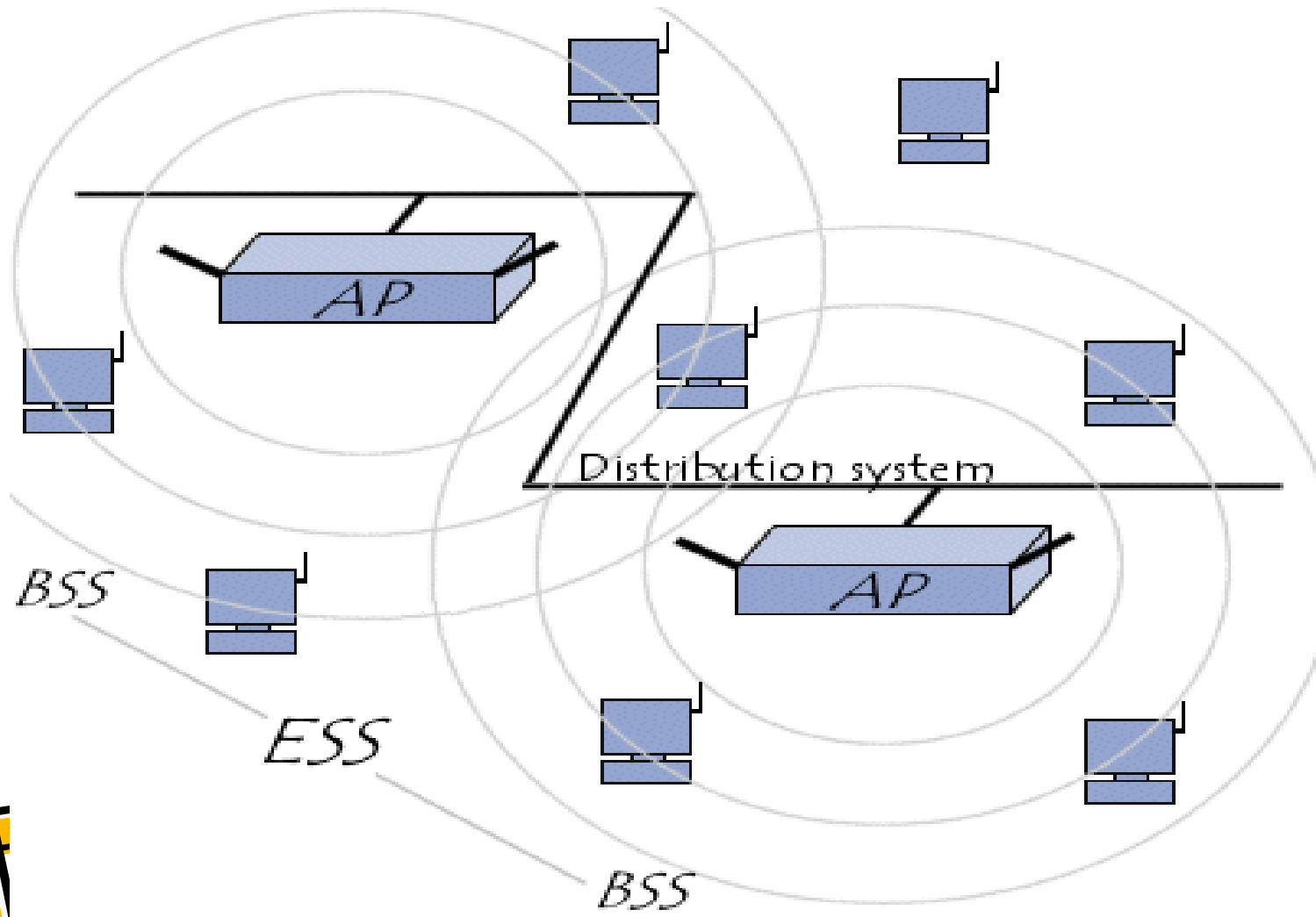
ESS



- It is possible to link several access points together (or more precisely several BSS's) using a connection called a *distribution system* (DS for short) in order to form an *extended service set* or *ESS*.
- The distribution system can also be a wired network, a cable between two access points or even a wireless network.

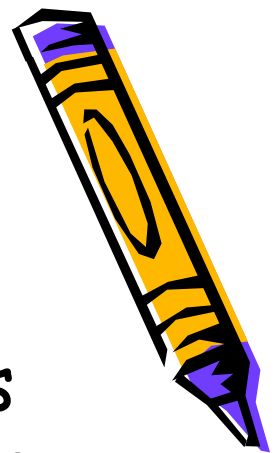


ESS

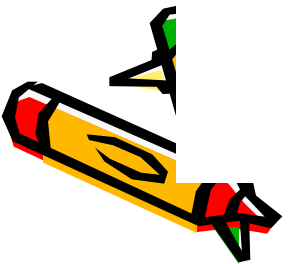
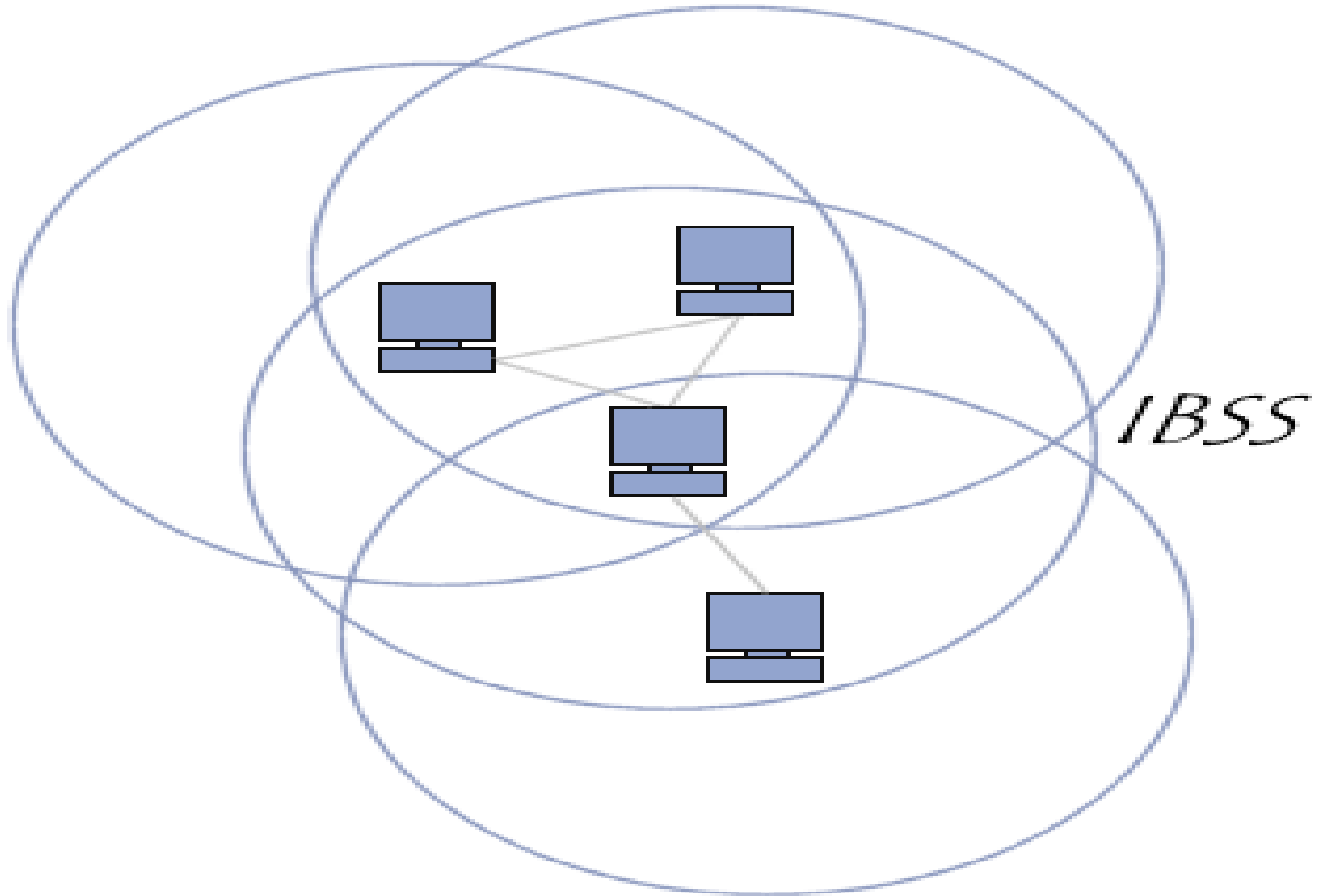


AD HOC MODE

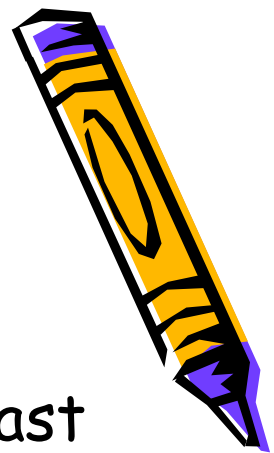
- In **ad hoc mode**, wireless client machines connect to one another in order to form a peer-to-peer network, i.e. a network in which every machine acts as both a client and an access point at the same time.
- The set-up formed by the stations is called the **independent basic service set**, or **IBSS** for short.



AD HOC MODE



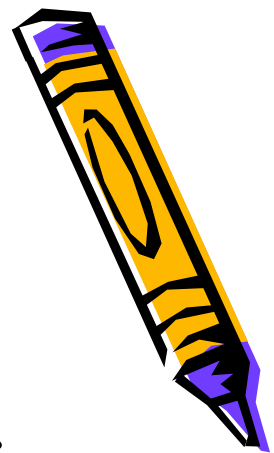
IBSS



- An IBSS is a wireless network which has at least two stations and uses no access point.
- In an ad hoc network, the range of the *independent BSS* is determined by each station's range.
- Unlike infrastructure mode, ad hoc mode has no distribution system that can send data frames from one station to another.



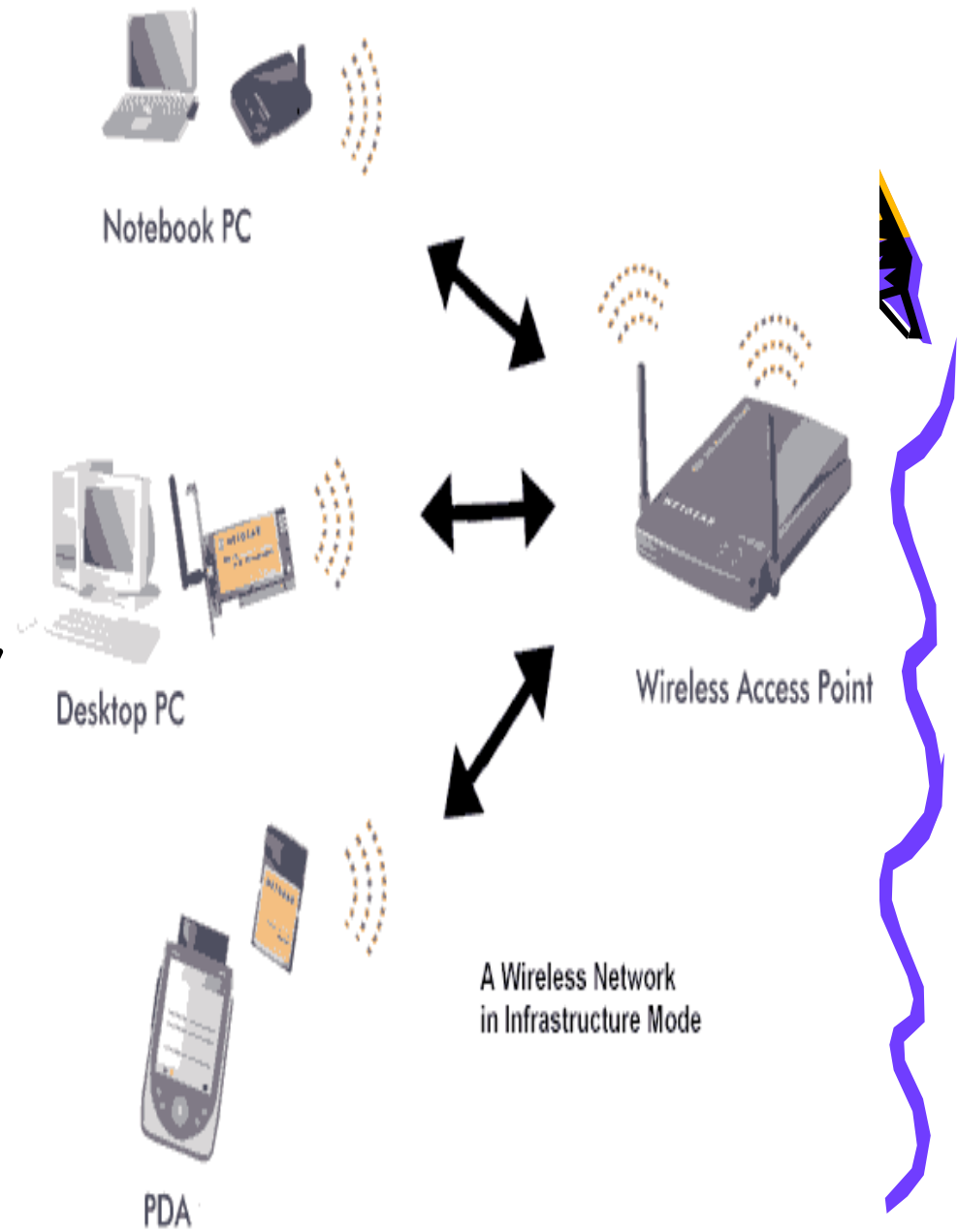
SELECTING b/w INFRASTRUCTURE AND ADHOC WIRELESS MODES



- 1) Because Ad Hoc Mode does not require an access point, it's easier to set up, especially in a small or temporary network.
- 2) Infrastructure takes advantage of the high power of an access point to cover wide areas. Ad Hoc Mode connections are limited, for example between two laptops, to the power available in the laptops.



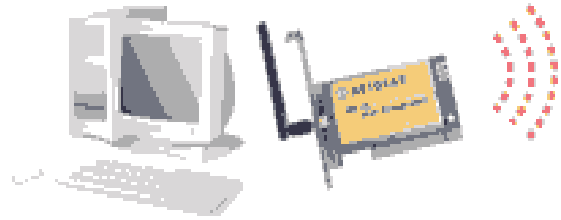
3) Because the network layout (the *network topology*) in Ad Hoc Mode changes regularly, system resources are taken just to maintain connectivity



4) In Ad Hoc Mode, chains of computers will connect to pass your data, if your computer is not directly in range. On the other hand, you do not have control over the path your data takes.



Notebook PC



Desktop PC



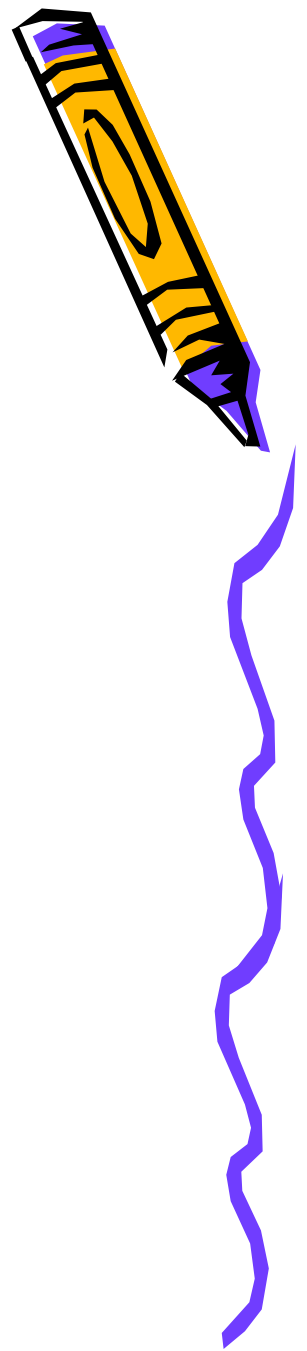
PDA

A Wireless Network in Ad Hoc Mode

5) In an Ad Hoc network with many computers the amount of interference for all computers will go up, since each is trying to use the same frequency channel.



High gain Parabolic grid antennas



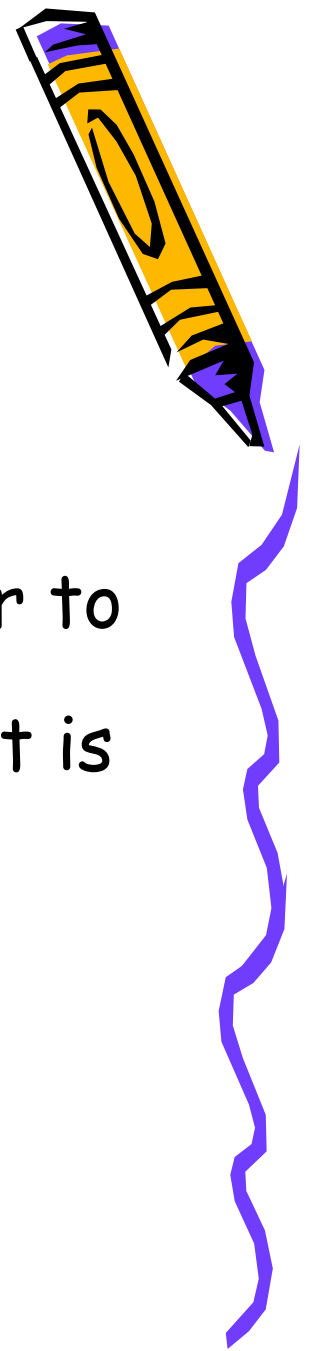
High gain Parabolic grid antennas to beam the signal to over 30km from tower to tower..

Typically 5.7-5.8 GHz, 2' Diameter Parabolic

Grid Antenna, 26 dBi gain, 6 degree

beam
width, N-Female connector

Risks related to wireless WiFi networks (802.11 or Wi-Fi)



- Lack of security
- Radio waves intrinsically have the power to propagate in all directions, with a relatively wide range. Because of this, it is very difficult to keep radio broadcasts confined to a limited area. Radio propagation also occurs three-dimensionally. The waves can therefore travel from one floor of a building to another (albeit with a high degree of attenuation.)

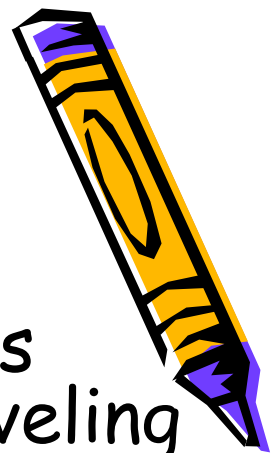


- The main consequence of this "wild propagation" of radio waves is that a non-authorized person may be able to listen to the network, possibly beyond the enclosure of the building where the wireless network is set up.
- The critical issue is that a wireless network can very easily be installed in a business without the IT department even knowing! An employee only has to plug an access point into a data port for all communication on the network to become "public" throughout the access point's broadcast range.



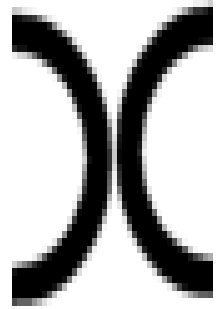
- **War-driving**

- Given how easy it is to "listen" to wireless networks, some people have taken to traveling around a city with a wireless-compatible laptop computer (or PDA) looking for wireless networks. This practice is called **war driving** (sometimes written *wardriving* or *war-Xing* for "war crossing"). Specialized war-driving software allows the locations of these open access points to be mapped accurately with the help of a Global Positioning System (GPS).

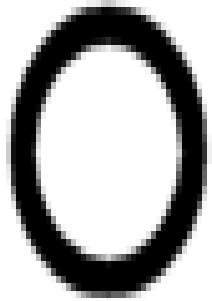


- These maps can show available unsecured wireless networks, sometimes allowing people to access the Internet. Many websites have been started to share this information; in fact, in 2002, students in London invented a sort of "sign language" to indicate the presence of wireless networks in an area by drawing symbols on the sidewalk in chalk. This is called "warchalking". Two opposing semicircles mean that the area is covered by an open network that provides Internet access, a circle indicates the presence of an open wireless network without access to a wired network, and a W inside a circle shows that there is a properly secured wireless network.

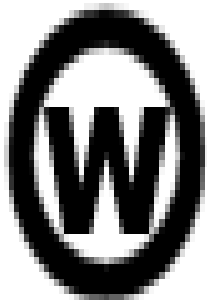




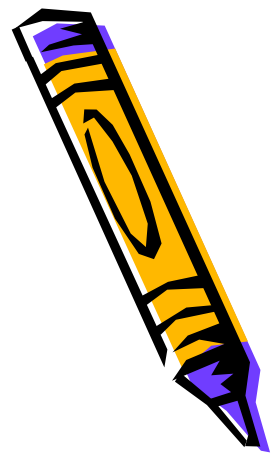
Open connected network



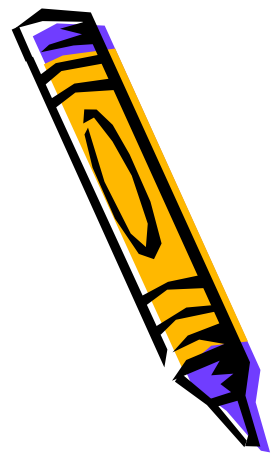
Open network



Secure network



Security risks

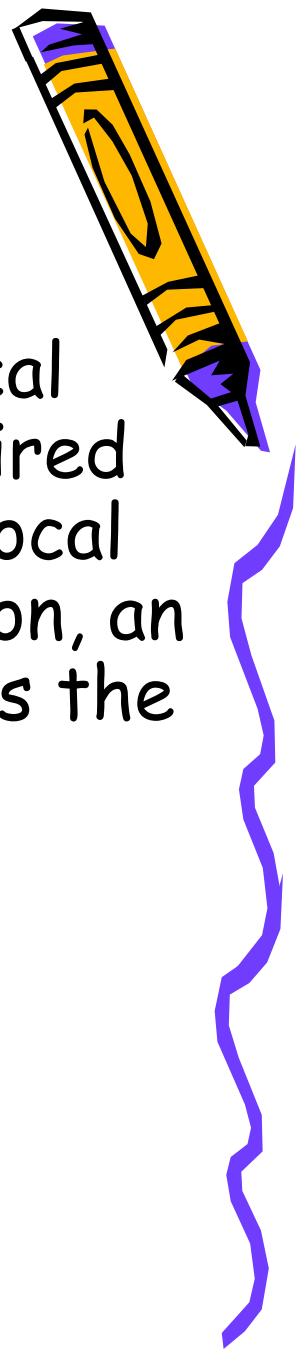


- **Data interception**
- By default, a wireless network is unsecured. This means that it is open to everyone, and anyone within the coverage area of an access point may potentially listen to communications being sent on the network. For an individual, there is little threat, as data is rarely confidential, unless the data is of a personal nature. For a business, however, this may pose a serious problem.



- **Network intrusion**

- When an access point is installed on a local network, it lets any station access the wired network, as well as the Internet, if the local network is connected to it. For this reason, an unsecured wireless network gives hackers the perfect gateway to an business or organization's internal network.

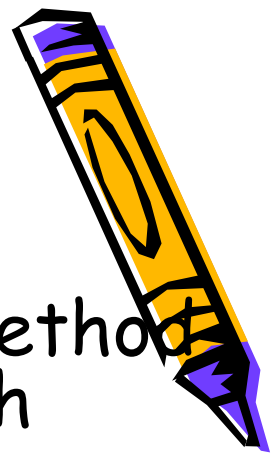


- **Radio jamming**
- Radio waves are very sensitive to interference. This is why a signal can easily be jammed by a radio transmission with a frequency close to that used by the wireless network. Even a simple microwave oven can make a wireless network completely inoperable if it is being used within an access point's range.



- Denial of service

- The 802.11 standard's network access method is based on the CSMA/CA protocol, which involves waiting until the network is free before transmitting data frames. Once the connection is established, a station must be linked to an access point in order to send its packets. Because the methods for accessing a network and associating with it are known, it is easy for a hacker to send packets requesting for a station to become disassociated from the network. Sending out information intended to disrupt a wireless network is called a denial of service attack.



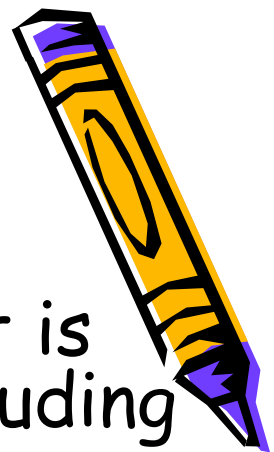
Wi-Fi wireless network security (802.11 or WiFi)



- Adapted infrastructure
- The first thing to do when a wireless network is installed is to place the access points in reasonable locations depending on the desired area of coverage. However, it is not uncommon to find that the covered area ends up being larger than desired, in which case it is possible to reduce the access terminal's strength so that its broadcast range matches the coverage area



- **Avoid using default values**
- When an access point is first installed, it is configured to certain default values, including the administrator's password. Many novice administrators think that once the network is operational, there is no point in changing the access point's configuration. However, the default settings offer only a minimal level of security. For this reason, it is vital to log in to the administration interface (generally via a web interface or by using a particular port on the access terminal), especially to set an administrative password.



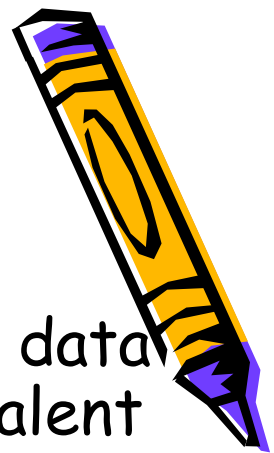
- Filtering **MAC** addresses

- Every *network adapter* (the generic term for a network card) has its own physical address (called a MAC address). This address is represented by 12 digits in hexadecimal format, split up into two-digit groups separated by dashes.

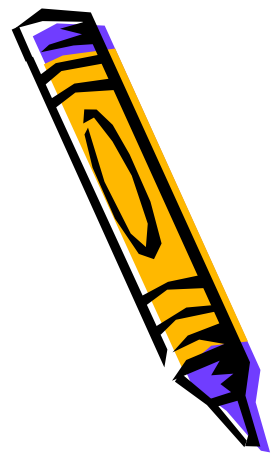
- The configuration interfaces of access points generally allow them to keep a list of access permissions (called the ACL, for Access Control List) based on the MAC addresses of the devices authorized to connect to the wireless network.



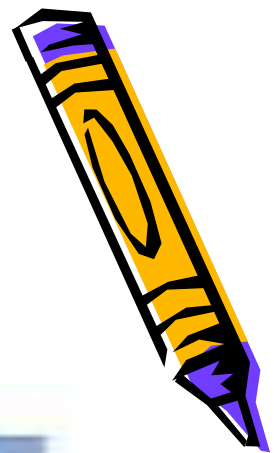
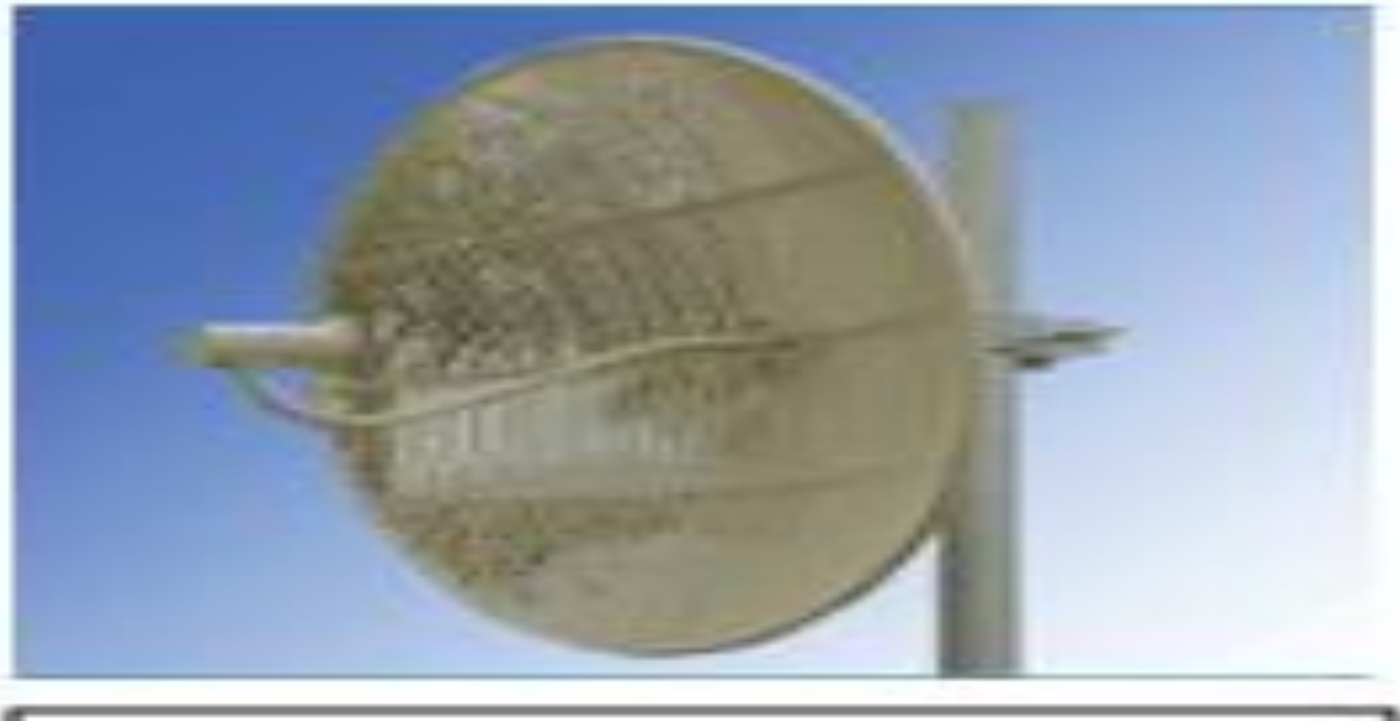
- **WEP - Wired Equivalent Privacy**
- To solve transfer security issues on wireless networks, the 802.11 standard includes a simple data encryption mechanism called **WEP** (Wired equivalent privacy).
- **Improve authentication**
- In order to more effectively manage authentication, authorization, and accounting (**AAA** for short), a **RADIUS** server (*Remote Authentication Dial-In User Service*) may be used. The **RADIUS** protocol lets user accounts and related access permissions be centrally managed.



- Setting up a VPN
- For all communications which require a high level of security, it is better to use strong encryption of data by installing a virtual private network (VPN).



Parabolic antenna



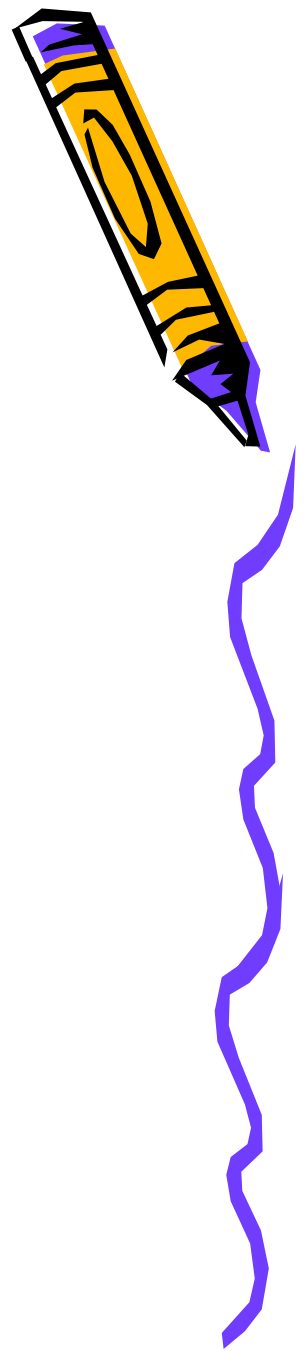
Sector antennas

Sector antennas to beam the signal
from the towers

to the community users

Typically 2.4-2.5 GHz, 90 degree
sector antenna, 17

dBi gain



Sector antenna





Customer Premises equipment (CPE) to
access the
signal from the towers..

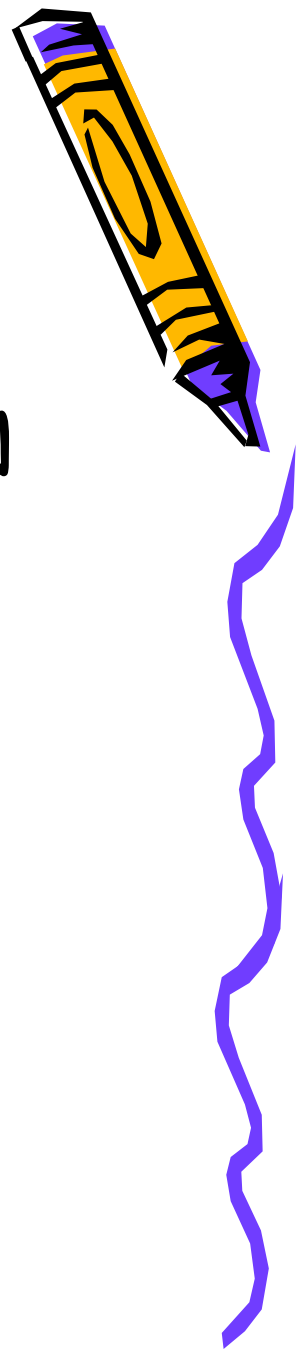
Typically 23dBm Radio + 15dBi Antenna =
 38dBm

Other components that need to be installed
in order to put
the above systems together



Basic Technology Concepts

WiFi b-a-g

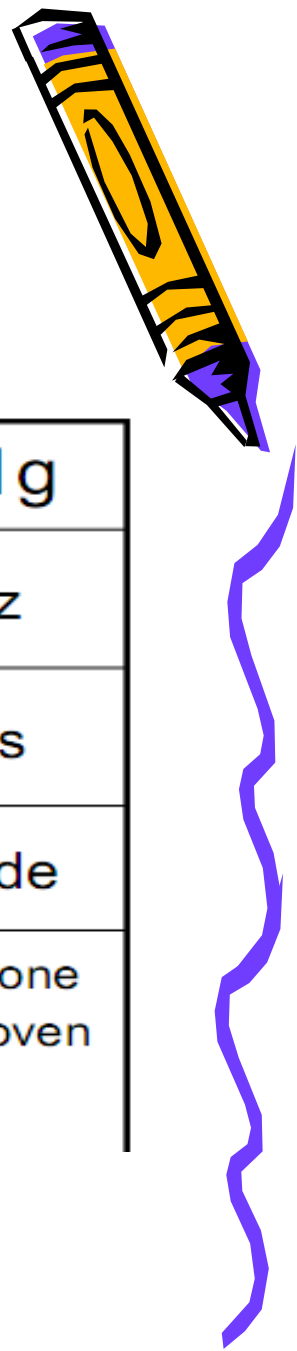


- IEEE Standards for Wireless LAN Spread Spectrum.
- Radio Technology (802.11).
- 802.11b- 2.4GHz @11mbps.
- 802.11a- 5GHz @54mbps.
- 802.11g- 2.4GHz @54mpbs.



Basic Technology Concepts

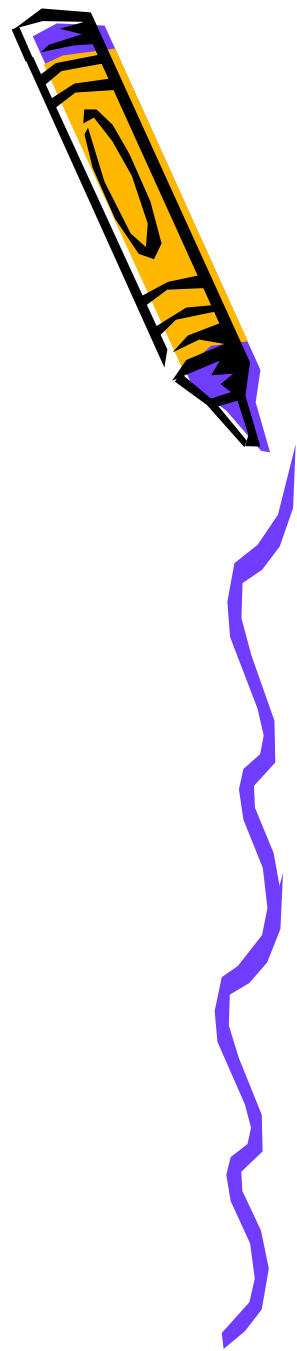
WiFi b-a-g



	802.11b	802.11a	802.11g
Frequency band	2.4GHz	5GHz	2.4GHz
Max data rate	11Mbps	54Mbps	54Mbps
availability	Worldwide	US	Worldwide
Interference sources	Cordless phone Microwave oven Bluetooth	Hiperlan devices	Cordless phone Microwave oven Bluetooth



802.11a



802.11a specification operates at radio frequencies between 5.15 and 5.825 GHz, i.e.

802.11a utilizes 300 MHz bandwidth

The FCC has divided total 300 MHz in this band into three distinct 100 MHz bands: low, middle, and high, each with different legal maximum power.

Band Channel Max Power

High band 5.725-5.825 GHz 9-12 1000 mW

Middle band 5.25-5.35 GHz 5-8 250 mW

Low band 5.15-5.25 GHz 1-4 50 mW



802.11a



- Completely different from 11b and 11g.
- Flexible because multiple channels can be combined for faster throughput and more access points can be co-located.
- Shorter range than 11b and 11g.
- Runs in the 5 GHz range, so less interference from other devices.
- It has 12 channels, 8 non-overlapping, and supports rates from 6 to 54 Mbps, but realistically about 27 Mbps max.
- Uses frequency division multiplexing technology.



802.11b



- Been around the longest, well-supported, stable, and cost effective, but runs in the 2.4 GHz range that makes
- it prone to interference from other devices (microwave ovens, cordless phones, etc) and also has security disadvantages
- Limits to the number of access points in range of each other, three
- Has 11 channels, with 3 non-overlapping, and supports rates from 1 to 11 Mbps, but realistically about 4-5 Mbps max
- Uses direct-sequence spread-spectrum technology



802.11b+

- Non-standard, runs in the 2.4 GHz range.
- Is backwards compatible with 802.11b.
- Supports rates from 1 to 22 Mbps, but realistically about 6 Mbps max.
- Uses a totally different type of modulating technology.



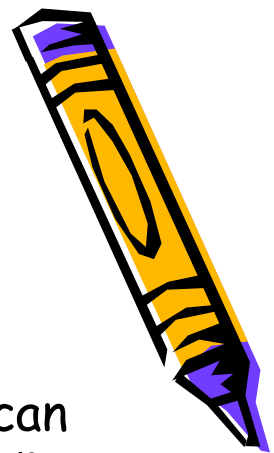
802.11g



- Extension of 802.11b, with the same disadvantages (security and interference).
- Has a shorter range than 802.11b.
- Is backwards compatible with 802.11b so it allows for a smooth transition from 11b to 11g.
- Flexible because multiple channels can be combined for faster throughput, but limited to one access point.
- Runs at 54 Mbps, but realistically about 20-25 Mbps and about 14 Mbps when b associated.
- Uses frequency division multiplexing technology.



How Wi-Fi works



Many computers today have Wi-Fi built in, however a person can add a Wi-Fi network card to connect to a LAN when near one of the network's access points.

The connection is made through unlicensed radio signals.

It is completely wireless, so homes and businesses can be networked without expensive wiring.

The geographical region covered by one or several access points is called a hot spot.

The average range of a Wi-Fi network varies, but on average it is 150ft indoors and 300ft outdoors.

It uses the IEEE 802.11 specification with variances of 802.11a, 802.11b, 802.11g, 802.11n.



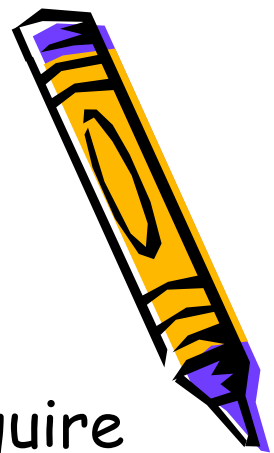
Advantages of wi-fi



- WiFi uses unlicensed spectrum
- Bypassing the need of costly & poor telephone line, it is more cost effective and
- much easier to deploy
- It requires much lower cost in the long runs, rather than rely on Telco's infrastructure
- WiFi belongs to open International standards, equipments can be obtained easily in the market at very competitive price
- WiFi offer the freedom to move and supports roaming
- WiFi support various degree of security & encryption
- LAN speed performance and obviously broadband Low cost infrastructure



Advantages of Wi-Fi



Uses unlicensed radio spectrum and does not require regulatory approval for individual organization.

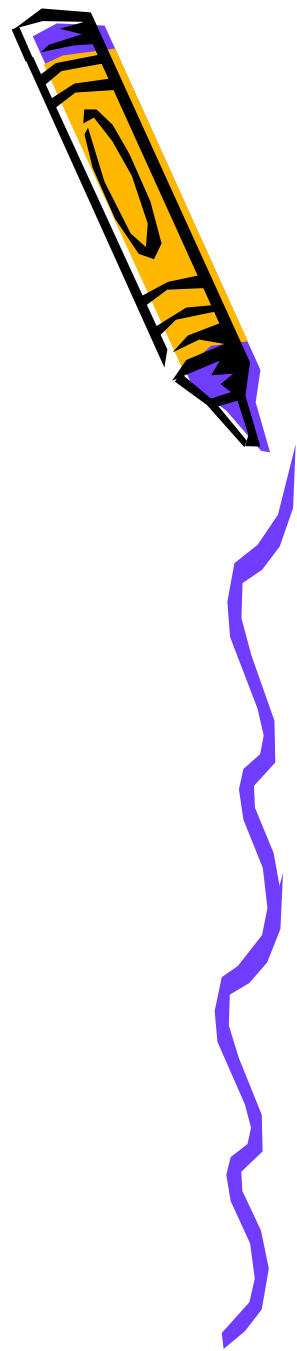
Allows LANs without cabling, potentially reducing the costs of networking a home or business, and allowing Internet access where cable cannot be run, such as outdoors.

Competition between vendors has lowered prices considerably since their inception.

It is a global set of standards where, unlike cell phones, it works in different countries around



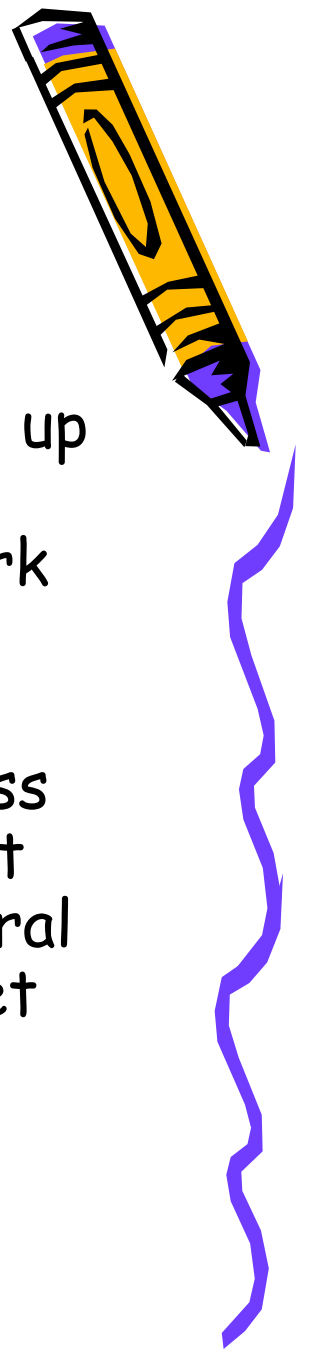
Range and Performance



- Performance decreases as distance increase
- 802.11a
 - Indoor 40-300 feet
 - Outdoor - 100 to 1000 feet
- 802.11b
 - Indoor 100-300 feet
 - Outdoor 400 - 1500 feet
- Interference - doors, walls, furniture, ceiling
- 253 maximum number of client per AP, but
- 15-20 recommended



Free Wi-Fi

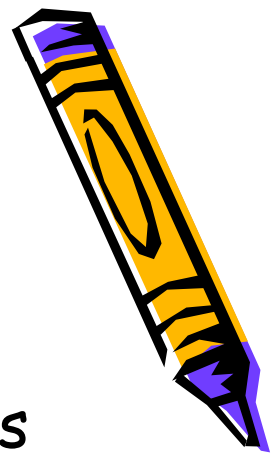


Many groups, communities, and cities are setting up their own free Wi-Fi networks, adopting a common peering agreement so that the network may be openly shared with one another.

Municipalities are working together with local communities to help expand these free wireless connections for many reasons, such as internet access for underprivileged areas and small, rural communities looked over by corporate Internet companies.



Disadvantages of Wi-Fi



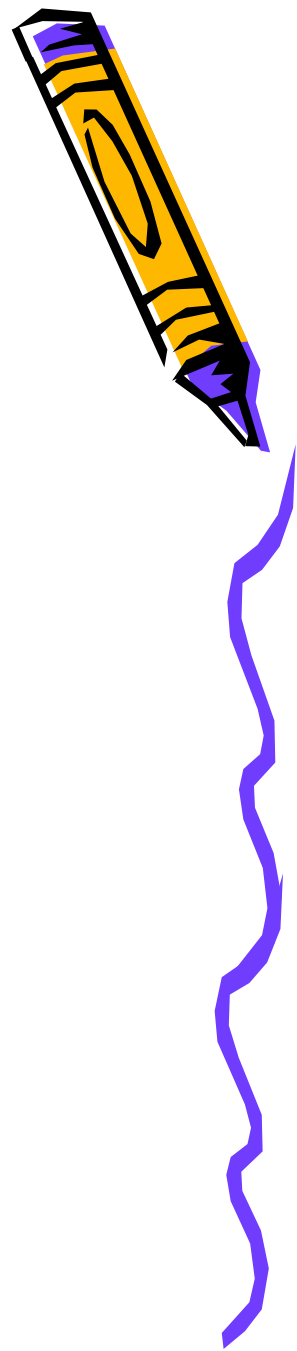
The spectrum is crowded with other technologies such as Bluetooth, microwave ovens and cordless phones, causing potential degradation of performance.

Closed access points on the same frequency as open access points can prevent access to those open access points.

Power consumption is fairly high compared to other standards, making battery life and heat a concern.



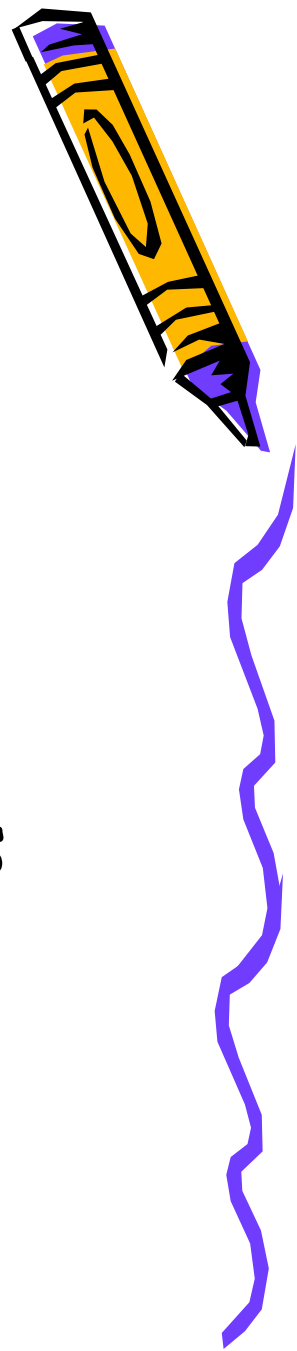
Disadvantages



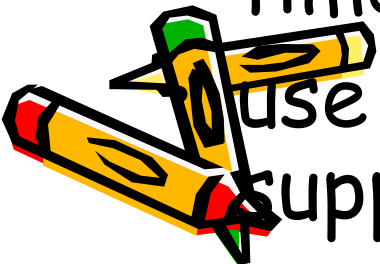
- Planning - Depending on the goal
- Security - Greater exposure to risks
- Access
- Compromising Data
- Denial of Service
- Speed - Slower than cable
- Range - Affected by various medium
- Travels best through open space
- Reduced by walls, glass, water, etc



How are Multiple Transmitters Supported?

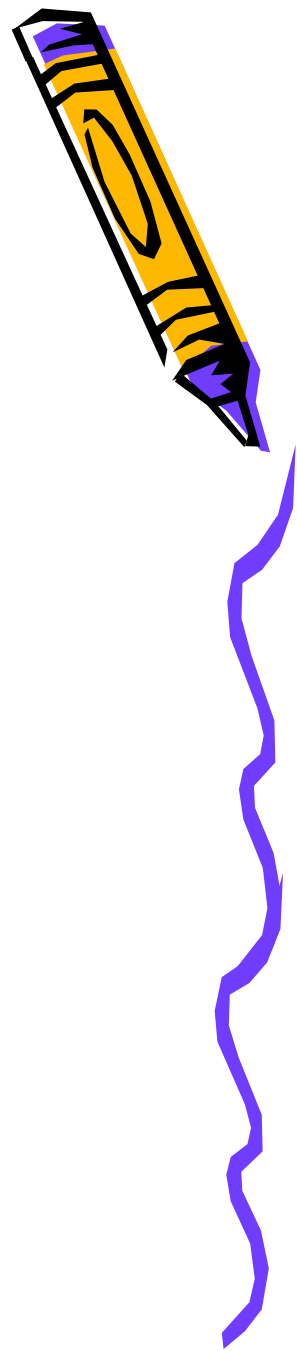


- Recall the method for supporting multiple
- transmitter is called the multiple access method.
- In 802.11 systems, only one user is allowed to
- communicate with a receiver at a time (cannot
- use another frequency channel
- support a

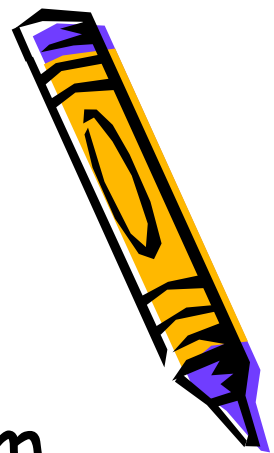


How wireless media is accessed by the users

- FOLLOWING TECHNIQUES ARE USED
- FHSS
- DSSS
- OFDM



Frequency-hopping spread spectrum

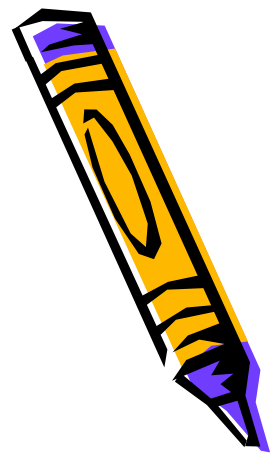


- Frequency-hopping spread spectrum (FHSS) is a method of transmitting radio

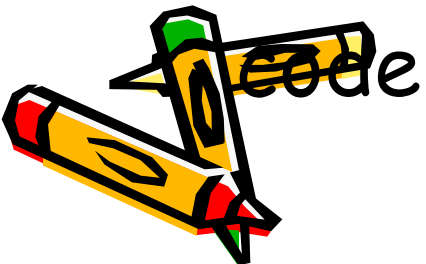
signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver.



DSSS



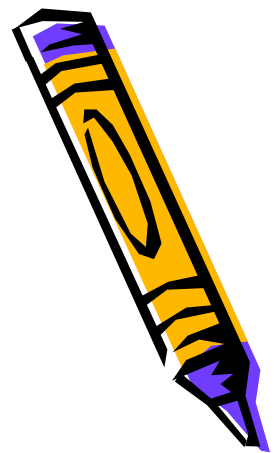
- DSSS stands for direct sequence spreads spectrum.
- This method extends the bandwidth of the original signal
- Each bit is assigned a code of n bits called chips
- Bits are assigned by using spreading



code



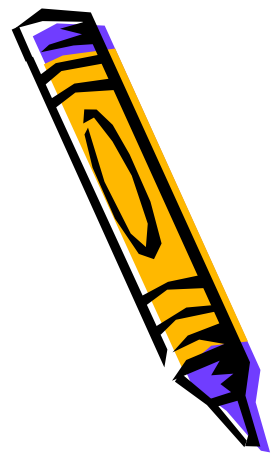
OFDM



- OFDM stands for orthogonal frequency division multiplexing.
- In this method all the bands are used by one user at a time
- Dividing the band into sub bands diminishes the effect of interference



How user gets access



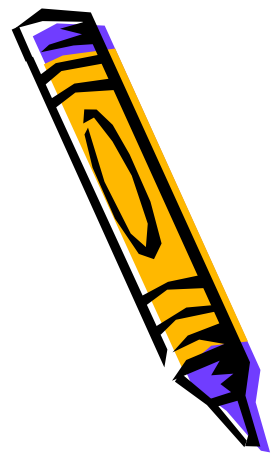
The way the one user is selected depends on

the carrier sense multiple access with collision

avoidance (CSMA/CA) random access method.



CSMA



- To help illustrate the operation of CSMA, we will use an analogy of a dinner table conversation.
- Let's represent our wireless medium as a dinner table, and let several people engaged in polite conversation at the table represent the wireless nodes.

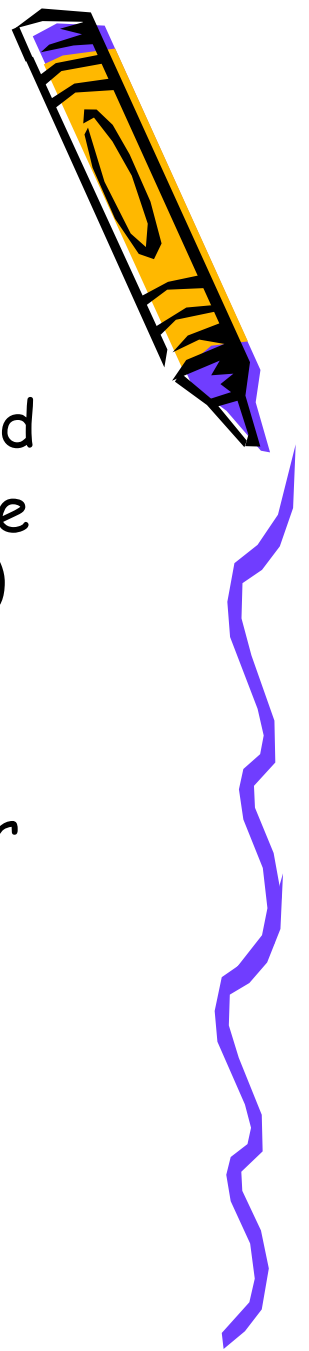


CSMA/CA



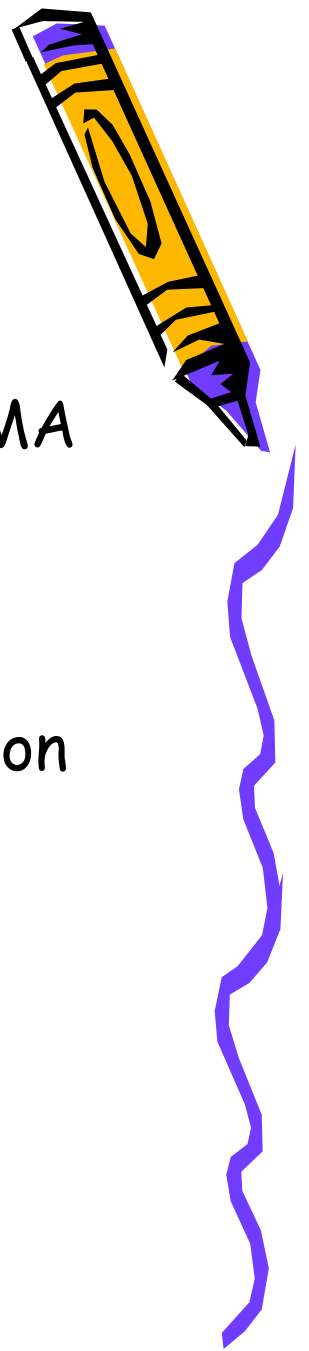
- o Carrier-sense multiple access gives us a good start in regulating our conversation, but there is one scenario we still need to address.
- o Let's go back to our dinner table analogy and imagine that there is a momentary silence in the conversation.





- o Now let's imagine that you are at the table and you have something you would like to say. At the moment, however, I am talking. CSMA (Cont'd)
Since this is a polite conversation, rather than immediately speak up and interrupt, you would wait until I finished talking before making your statement.





- o This is the same concept described in the CSMA protocol as carrier sense.
- o Before a station transmits, it "listens" to the medium to determine if another station is transmitting. If the medium is quiet, the station recognizes that this is an appropriate time to transmit.

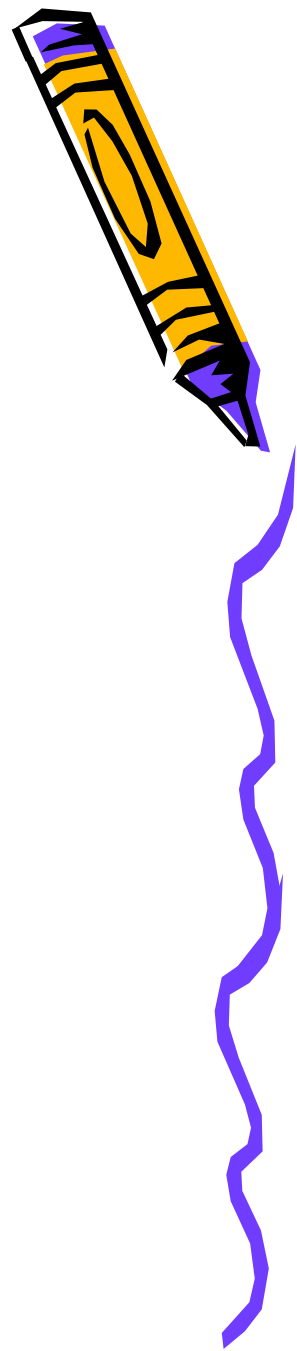


The collision will result in an unexplained message to the intended receivers (listeners). What we need is a polite contention method to get access to the medium; this is the collision avoidance part of CSMA/CA.

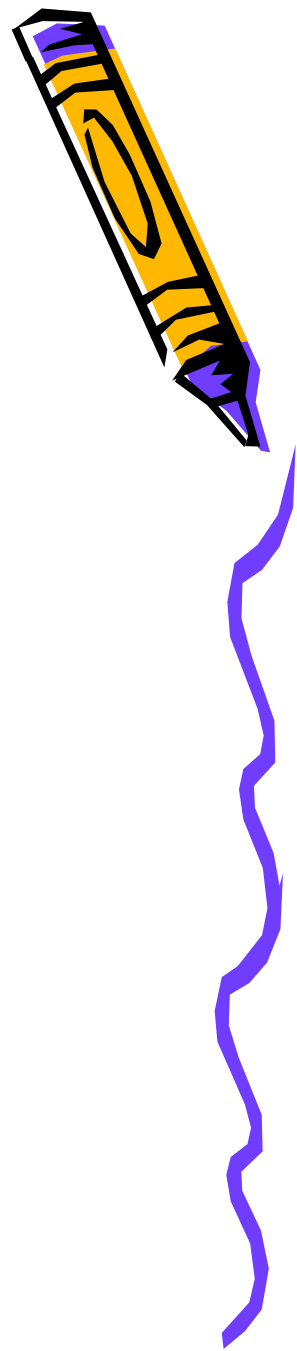
802.11 has come up with two ways to deal with this kind of collision.

One uses a two-way handshake when initiating a transmission.

The other uses a four-way handshake.



2 Way Handshake



Node with packet to send monitors channel.

If channel idle for specified time interval called DIFS, then node transmits.

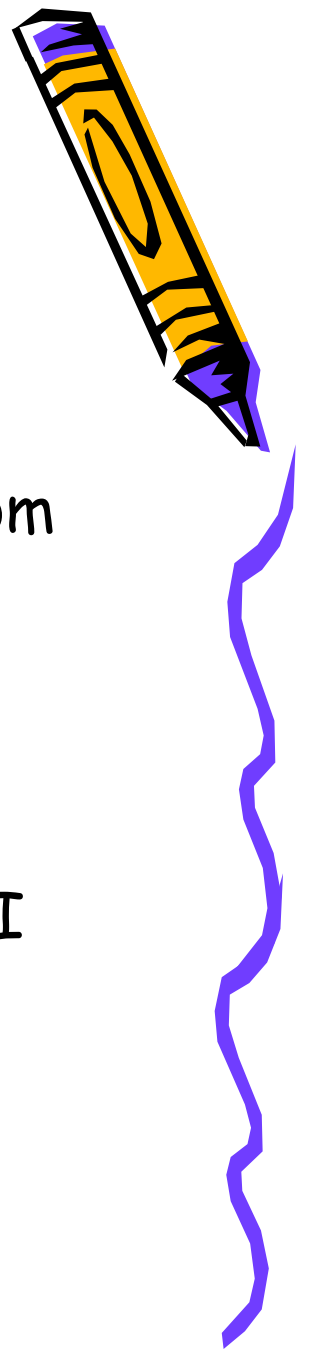
If channel busy, then

- node continues to monitor until channel idle for DIFS.

- At this point, terminal backs-off for random time (collision avoidance) and attempts transmitting after waiting this random amount of time.



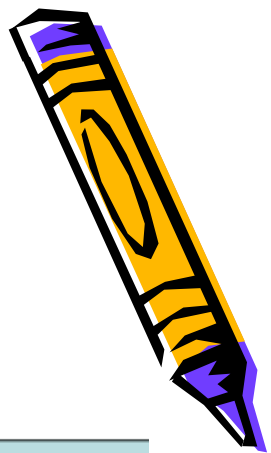
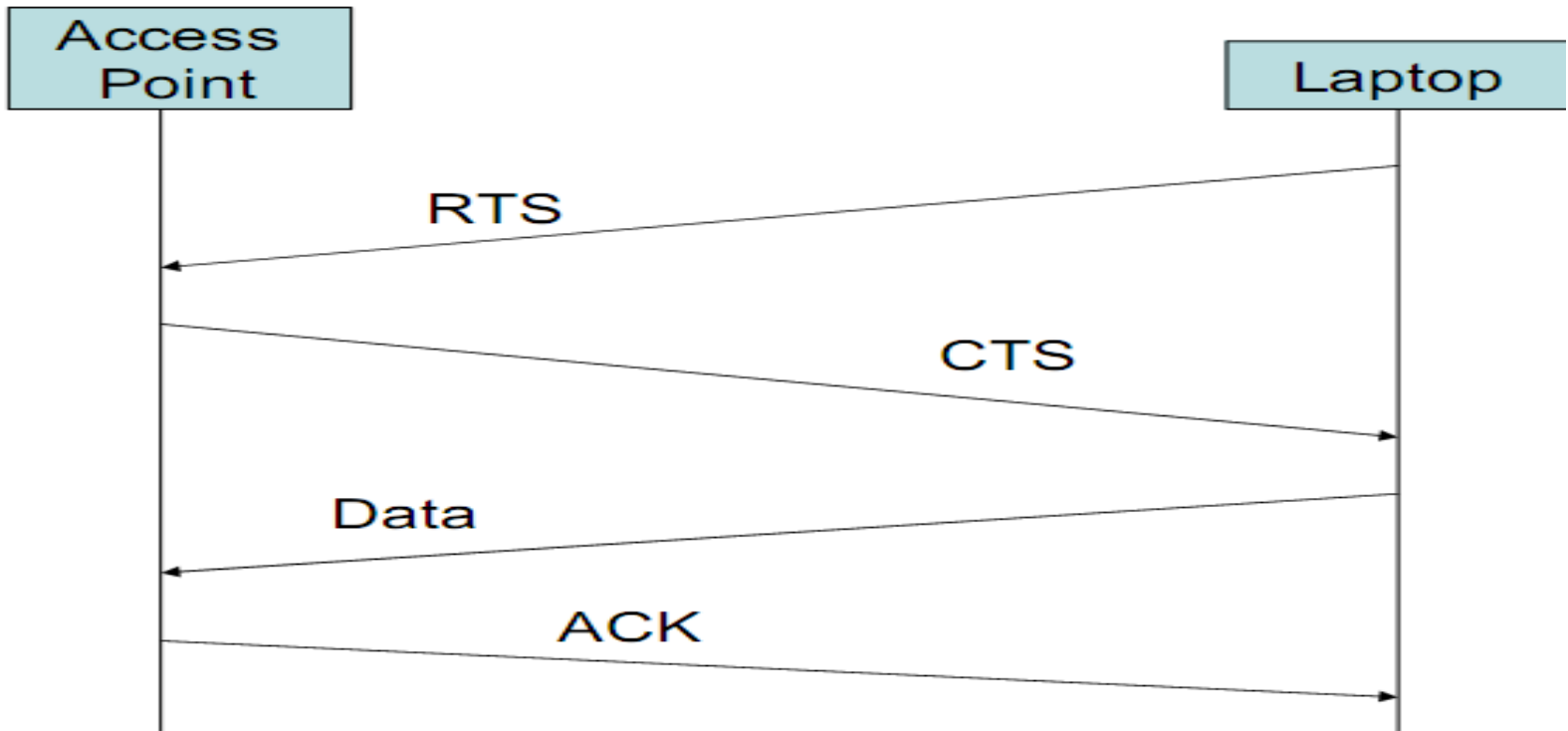
4 Way Handshake



- "Listen before you talk"
- If medium is busy, node backs-off for a random amount of time after waiting DIFS, just as before.
- But now, instead of packet, sends a short message: Ready to Send (RTS). This message is basically attempting to inform others that "I have something to send."



Access procedure

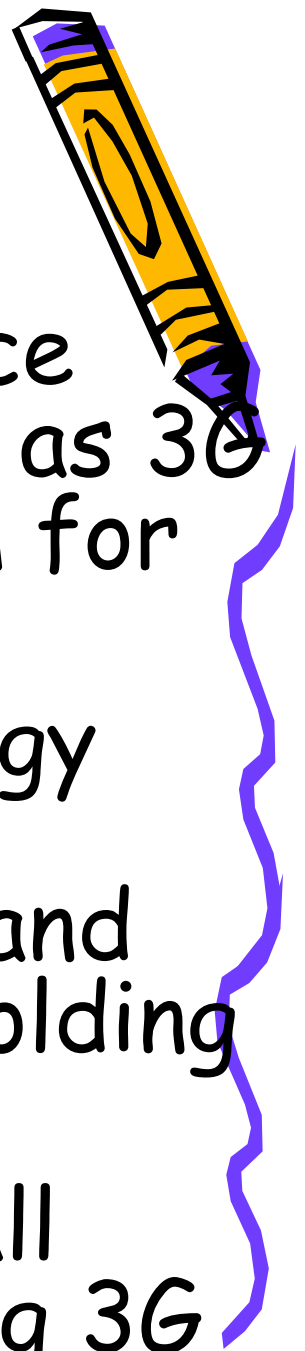


Wi-Fi vs. Cellular

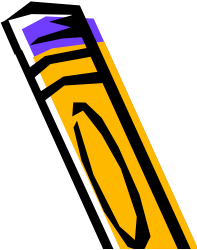
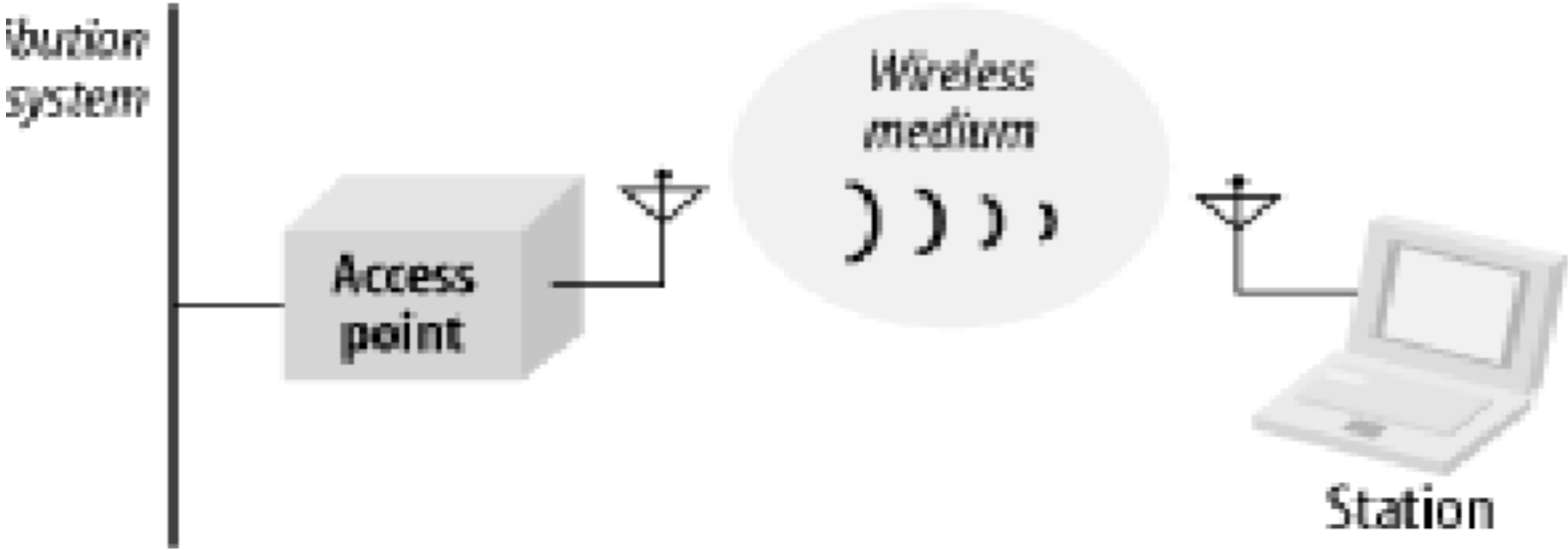
Some expect that Wi-Fi will replace cellular telephone networks such as 3G and GSM, leading to the 4G term for Wi-Fi

Today, the current Wi-Fi technology lacks roaming and authentication features, plus the limited range and the narrow spectrum it uses is holding back this replacement.

However, the bandwidth and overall capabilities are already exceeding 3G telephone standards.



Wireless LAN Networks



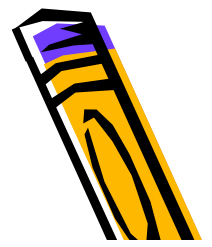
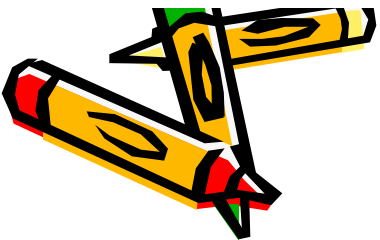


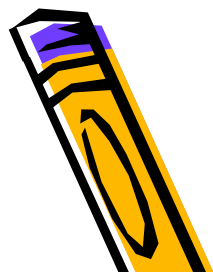
APPLICATIONS OF
WI-FI



Point-to-Point or Point-to-Multi Point

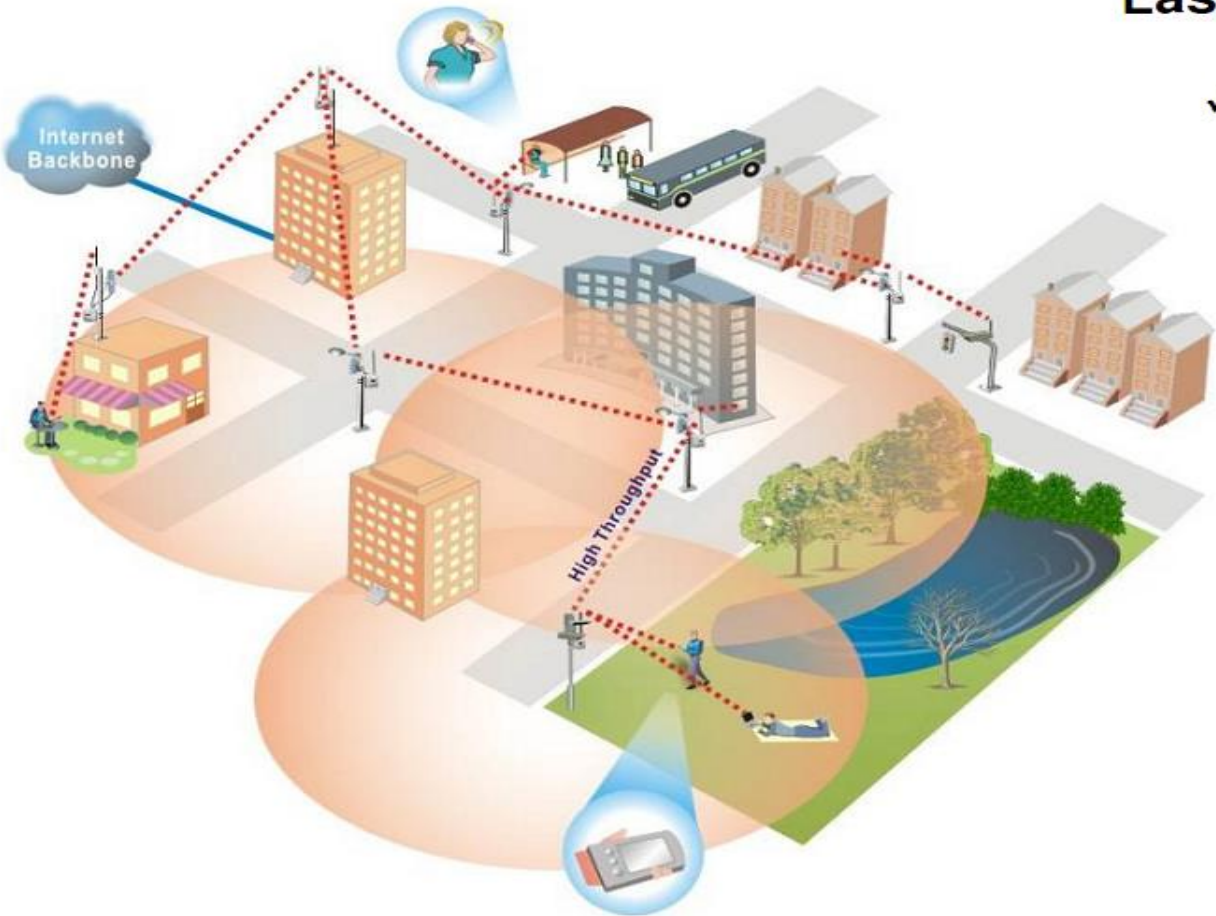
- ✓ Long distance link
- ✓ Headquarter and Branches

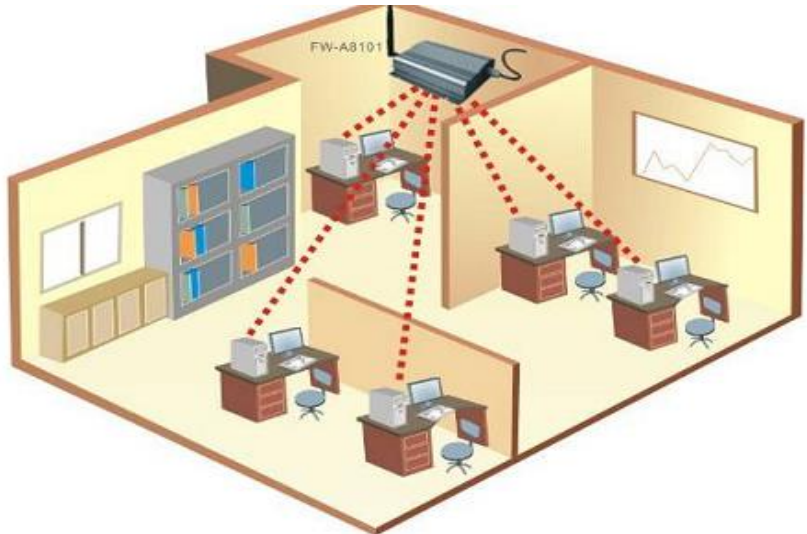
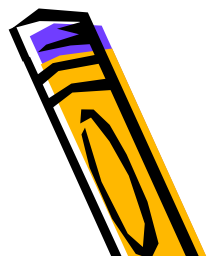




Last-mile

✓ Residential area





Indoor Wi-Fi Extension



WiFi Hut Wireless 5.8 GHz Point to Multi Point Configuration

RS-5800 AP-60



Panel Antenna

15 Mile Range

15 Mile Range

RS-5800 SU-60

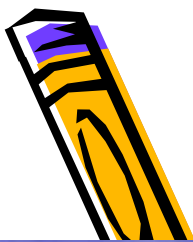


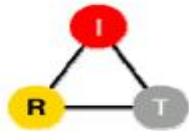
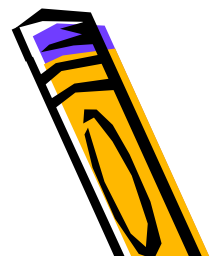
18 Inch Parabolic Antenna

RS-5800 SU-60

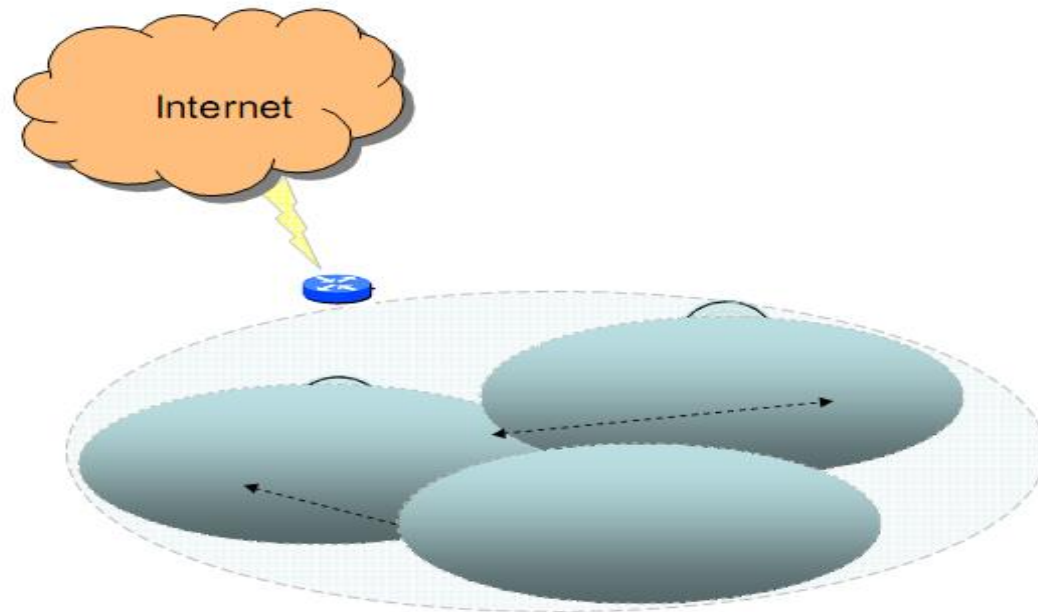


18 Inch Parabolic Antenna

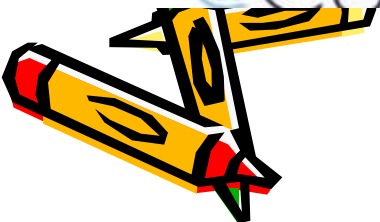


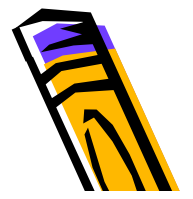


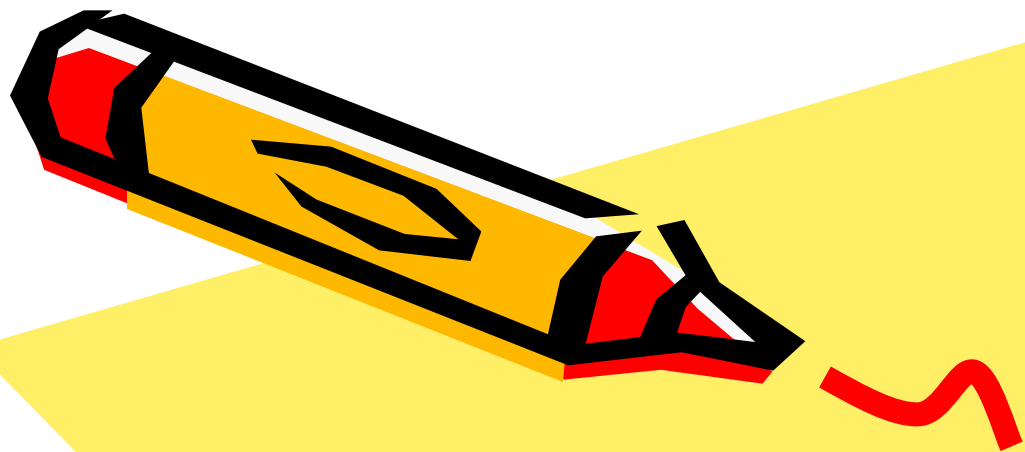
Cooperation Between Stations in Wireless Networks



CS 
@CU







END

Hope for the best

