DIGI WIFI GUIDE

WiFi: a comprehensive approach from a Digi perspective

May 21, 2008

Version 0.3

TABLE OF CONTENTS

PURPOSE

This document is intended to help a persons understanding of wireless (WiFi) technology (802.11) and how it relates to Digi products. It is also intended to assist in setup, optimization, troubleshooting issues, as well as to help avoiding common problems that come up with using wireless technology and Digi products.

This document is not intended to cover every aspect of wireless networks, nor does it discuss other wireless technologies such as, Bluetooth or Cellular for example.

WiFi BASICS

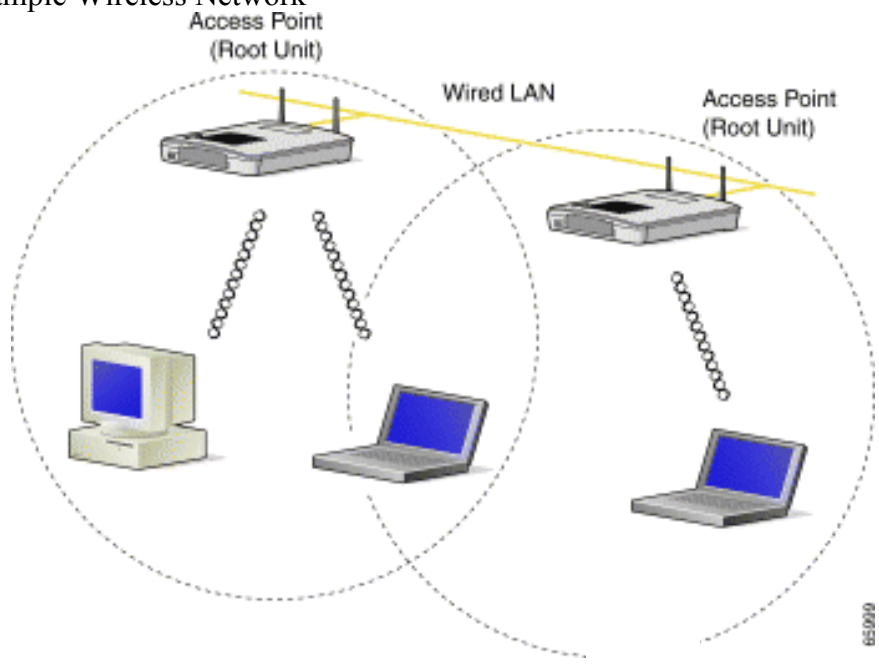
Wireless networks use radio waves to link wireless devices together forming a 'wireless network', instead of using more traditional methods of cabling.

Some of the advantages to wireless networks are portability of networked devices and removal of unnecessary wires. Some of the disadvantages include wireless interference leading to range limitation and lower data rates, as well as potential security issues.

Wireless is also known as WiFI, or it's more proper name: the IEEE 802.11 standard. These terms will be used interchangeably throughout this paper.

The main type of wireless network will involve a number of wireless devices (called clients) talking through a master wireless device known as an **Access Point** (AP for short). This type of setup is called an **Infrastructure** network. Most wireless networks are of this type.

Infrastructure Example Wireless Network



Alternatively, wireless devices can get on a wireless network without an access point. This is called an **Ad Hoc** network.

Ad Hoc wireless network

Clients will need to join the wireless network before they can talk across it. This is called **Association**. In order for a device to associate it must know the following items about the desired wireless network:
SSID: the name of the wireless network.
Encryption: if and how the network encrypts or "scrambles" its data.
Authentication: how and if the network requires its members to "prove" their identity.
Channel: what channel (frequency range) the wireless network uses.
* these items will be talked about in detail later.

Once a device is associated it can then send and receive data from other associated devices on the same network. When the client is done or needs to leave, it then can **Disassociate** and be removed from the wireless network.

That's how WiFi devices operate, on a basic level. Now let's discuss in more detail the aspects of **WiFi Types**, **Encryption**, **Authentication**, and **Channels**.

TYPES OF WIFI

There are different versions of the 802.11 wireless standard. For the sake of our discussion we will be mostly talking about 802.11b and 802.11g. Here's a listing below with some basic characteristics of each:

WIRELESS STANDARD NAME[1]	MAX DATA RATE[2]	FREQUENCY	RANGE[3]	YEAR INTRODUCED
802.11 (original)	2 Mbps	2.4 GHz	40-300 ft.	1997
802.11a	54 Mbps	5 GHz	10-40 ft.	1999
802.11b	11 Mbps	2.4 GHz	40-300 ft.	1999
802.11g	54 Mbps	2.4 GHz	40-300 ft.	2004
802.11n [4]	600 Mbps	2.4 or 5.0 GHz	80-600 ft.	2010 (TBD)

1) There are also other versions (802.11d, 802.11f, etc.), but for the sake of this discussion we won't cover them.

2) Max Data Rate is theoretical. As a guideline you will get 50-60% of the maximum rate.

3) This is assuming an indoors environment. Outdoors, ranges are generally better. Keep in mind, **range is highly dependent on environmental factors.**

4) 802.11n has not yet been finished.

The first wireless LAN standard, 802.11, was introduced in 1997. It utilizes the 2.4 frequency band with Frequency and is capable of delivering data rates of 1 Mbps and 2 Mbps. The 802.11 standard is now obsolete, and no longer used in new setups.

The 802.11b standard was approved in July 1999 and can be considered the second generation. Like 802.11, 802.11b also operates in the 2.4 GHz frequency. The data rate was improved and is up to 11 Mbps. Range was also extended by a large margin as well. At this point, 802.11b is by far the most cost-effective and widely used wireless LAN technology in both small office / home office and enterprise environments.

At the same time the 802.11b standard was setup, the 802.11a specification was approved as well. This standard operates in the 5 GHz frequency and provides data rates up to 54 Mbps.

The 802.11g standard was approved in 2003. It provides a maximum data rate of 54 Mbps. In addition, the standard is also fully backwards-compatible with existing 802.11b wireless networks.

The 802.11n standard is not yet approved. It is expected to have four times the data rate of 802.11g (216 Mbps?) and twice the range.

ENCRYPTION

Encryption is a method of scrambling a message that makes it unreadable to unwanted parties. There are different methods of encryption. They are: **None**, **WEP**, **WPA**, and **WPA2**.

When talking about encryption there is generally a trade off that occurs between the security of the data and the "convenience" of the wireless network (time and costs of setting it up, getting good speed, etc.). Each encryption method has its benefits and drawbacks. They are discussed below:

None

No encryption is used. Data is sent without scrambling it and can be read by anyone. The advantages for networks using no encryption are that they are easier to setup and generally have faster throughput (speed). The drawback is that it is not secure and can be read by everybody.

WEP

WEP is the oldest form of encryption in the WiFi world. It was introduced in 1997. At the time it was thought to have been secure. As time went on however major flaws were found in it. Today, it should not be considered truly secure. It is however better than nothing. It is also the default security that comes with many wireless products. As such, it's pretty easy to setup.

WEP can come in 2 different forms:
WEP 64-bit - which uses a 40-bit key
WEP 128-bit - which uses a 104-bit key

WPA (TKIP)

WPA was created after the flaws in WEP were found to make it not secure. WPA for the most part fixes the flaws that were in WEP. WPA uses a cipher called TKIP to encrypt and unencrypt data. WPA is for the most part "secure". For home or small business wireless networks, it should be adequate for almost anything. For enterprise class networks it still ok in some cases; depending on how sensitive the data moving across the wireless network is. Although WPA is newer than WEP, most products support it.

WPA2 (AES/CCMP)

Although WPA addressed the flaws of WEP, it was still found to have theoretical weaknesses that someday will be exploited. WPA2 was released a few years ago to deal with this. It uses the AES/CCMP cipher to encrypt and decrypt data. WPA2 is a great

choice for almost any kind of wireless network requiring robust security. It has a few drawbacks however. Because it's still somewhat new, older products can't support it. It is also computationally expensive. As a result speed of the wireless network can suffer.

AUTHENTICATION

As mentioned before, authentication deals with proving the identity of the wireless device attempting to associate with the network. There are different methods of doing this. They are: **Open**, **Shared Key**, and **802.1 x authentication**.

Open

Open Authentication is when the access point simply accepts the wireless devices identify without verifying or proving it. The benefits to this is simplicity and compatibility (all devices can do it).

Shared Key

Shared Key is when the wireless devices must present the proper key to get on the network. This is used with WEP encryption. Although Shared Key has more security than Open Authentication it should not be considered "secure". One of the benefits of Shared Key Authentication is simplicity.

802.1x Authentication

802.1x is not one single method of authentication but rather a framework that encompasses many different methods of authenticating wireless devices. This is typically used in Enterprise grade wireless Environments. Some common methods are listed below:

EAP-TLS – uses certificates to verify the identity of the wireless device AND the network.

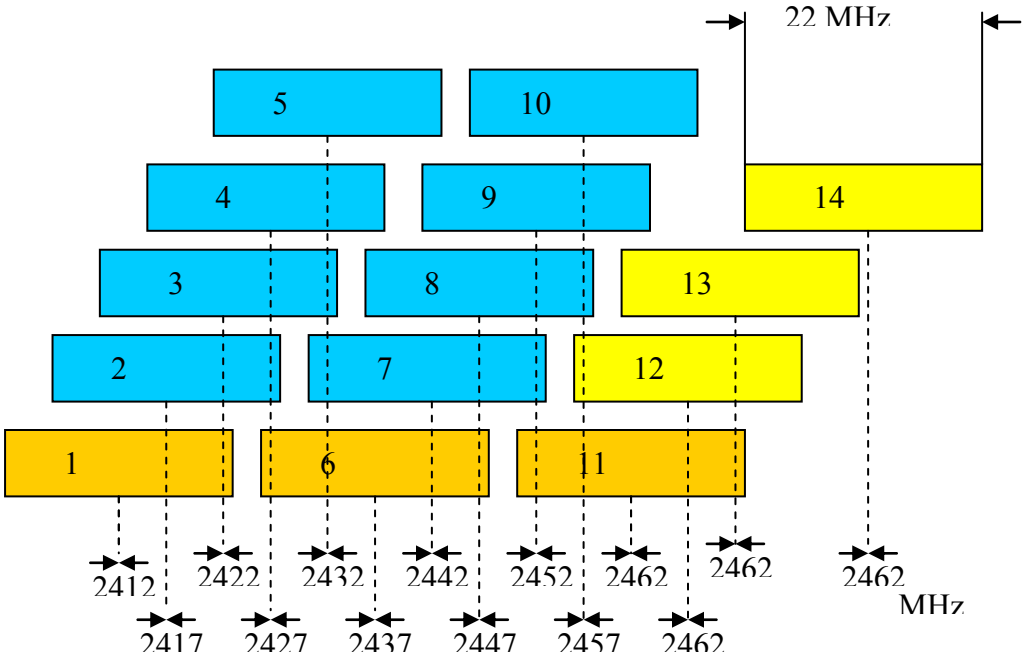
EAP-TTLS – which uses one way certificate to verify the networks identify

MSCHAPv2 – uses username password combinations for windows machines

CHANNELS

Wireless networks operate on particular frequencies. 802.11b and 802.11g operate in the 2.412-2.484 Mhz range. These are broken down into 14 channels . Data is transmitted on a channel by radio frequencies over a certain frequency range. In order to avoid bad performance caused by the overlapping ("collision") of channel frequencies in a wireless LAN environment, it is very important that the channels of neighboring access points are selected accordingly. See also section "**Deploying a Wireless LAN**" for more information and general guidelines on how to lay out a wireless network.

In case of the 802.11b and 802.11g standards, the center frequencies of the 14 possible channels range from 2,412 GHz to 2,484 GHz, with each 11 Mbps channel being 22 MHz wide and centered in 5 MHz intervals. **This means that only 3 channels (1, 6, and 11)** in North America are not subject to overlapping.



COMMON PROBLEMS

Environmental factors

The wireless medium is notorious for this very reason. Various factors can slow down the data rate, lose data, or even ruin the connection.

Materials can interfere with communications. Metal, silvering (mirrors), thick glass, concrete, ceramic, walls, and even large groups of people can absorb or reflect wireless signals. Both of which behaviors are not desired.

Signals also interfere with communications. These include microwaves, fluorescent lights, motors, 2.4Ghz phones, other WiFi devices, and some military equipment (radars).

It's generally a good idea to test the wireless network in the general area first. Walking around and checking signal strength should help you identify problem areas in advance. When problem areas are found it might be a good idea to manually turn down the transmit rate on the devices. Although this will reduce the speed of the network, it will help minimize interference.

Range

As the distance between two devices increases the received signal between them is reduced. This also affects the speed of the connection (throughput). If the devices have a strong signal between them, then their transmit speeds will be highest. As distance increases and signals get weaker the devices will lower their speed. This will have the effect of extending their range. At some point, when the range is too great, the connection won't work well or will be lost entirely.

Enabling security

This is difficult because there are more things that can go wrong. It's easy to make mistakes when entering security features (like the Pre-Shared Key for example). This causes the module to not associate with anything and just "hang" in limbo. The customer then has to reset to factory defaults and start all over.

Confirm security settings before setting up the access point and wireless devices. This includes the type of encryption (WEP, WPA-TKIP, WPA-AES, etc.) as well as any related information (Pre Shared Keys, certificates, WEP key, etc). One good practice is to have an access point setup with no encryption, just to see that the wireless devices joins the access point first.

Misconceptions

WiFi is something that is not well known. For example, it's a common misunderstanding that if two wireless devices have an unobstructed line of sight between them they shouldn't have problems.

There are several good books and resources online that will help ones understanding of WiFi. Also, there are some good white papers at the end of this document that explain some of more technical details.

SPECIFIC PROBLEMS

SSID Conflict
When two networks have the same SSID, wireless devices on one network may try to connect to the other network (because they look like the same network), which can cause problems. This can easily happen when two different networks use hardware from the same vendor with the same default SSID. To avoid such problems, configure a unique SSID for your network that won't conflict with other networks.

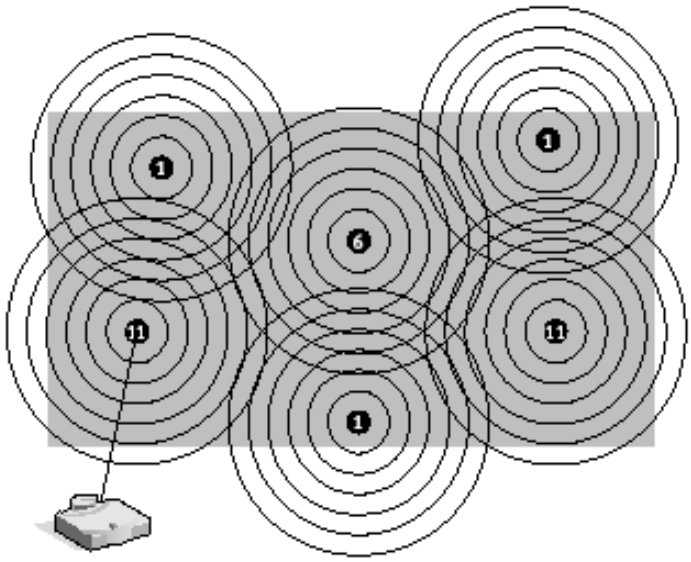
Device won't associate
Check wireless settings (SSID, channel, range, and sources of interference).

Device won't associate (using encryption)
The security settings possibly are not correct. In order to connect to an encrypted network you must have the correct encryption specified as well as the proper key.

Channel Conflict
When deploying multiple access points to cover a greater area you will want them to use differing channels so that they don't interfere with each other. It is usually best to use channels 1, 6, and 11 (in the case of 802.11b or g), as they are completely free from overlapping.

Below is a typical "honeycomb" configuration that demonstrates how to position channels. In this example no channel (cell) is next to another of same channel (example, channel 1 is never next to channel 1).

However, as wireless technology continues to become more and more pervasive, many people are using channels 1, 6, and 11 already. In some cases it actually makes more sense to use other channels (3,4, 8,9).



SETTING UP DIGI WIFI DEVICES

This is an example of how to setup a digi device (i.e. Digi Connect® Wi-ME, Digi Connect® WiEM, or Digi Connect® WiSP, ConnectPort™ TS W) out of the box to associate with a Wireless Access Point. The instructions are intended to be general only. Specific directions on a particular product can be found in the Quick Start Guide that it comes with. Further documentation can be found on Digi's Support site (support.digi.com).

Configure the Access Point
Use the following settings:
SSID: Connect
Encryption: none
Authentication: none
DHCP Server: yes

2) Power up Digi device:
Take the Digi branded device out of the box and power it on. With the above configuration it will associate with the Wireless Access Point. You can confirm this has happened by seeing that the devices Link LED (amber colored for ConnectPort™ WiME or green colored for ConnectPort™ WiEM and ConnectPort™ WiSP) is on solid.

3) "Discover" the Digi device:
At this point you should be able to "discover" the device using the appropriate discovery utility. This will be run from a system that has also joined the same access point as the Digi device. You can download this tool from Digi's website (http://www.digi.com/support).

TROUBLESHOOTING TIPS

These tips deal with getting a Digi device connected or keeping it connected. Depending on the nature of the problem encountered, some of these suggestions may not apply.

- Confirm that the wireless settings on the Digi are equivalent with the intended wireless network (SSID, encryption, authentication, channel, mode, DHCP, etc.)

- Check the Digi devices Link LED (amber colored for Digi Connect™ WiME or green colored for Digi Connect™ WiEM and Digi Connect™ WiSP) . If it's solid then that means it is associated with a wireless access point (although not necessarily the intended one). If it's blinking quickly (once every second), then it's not associated but searching for a wireless network to join. If it's blinking slowly (once every 5 seconds), then it's associated with an ad hoc network.

- Make sure the wireless access point is not running in "G only" mode (802.11g). If it is, the Digi device won't be able to associate with it (most Digi devices use 802.11b only).

- If possible or applicable, make sure the Digi wireless device has the newest firmware loaded onto it. You can obtain the latest firmware from Digi's support site (http://www.digi.com/support).

- Optimize the Digi device to the desired wireless access point. On the Digi device, manually set the SSID, channel, and mode (associate with access point). Then lower the transmit speed to it's minimum (1mb).

- To force the Digi wireless device to associate with the desired wireless access point you can remove its antenna and move it within a foot of the desired wireless access point. This is useful for initial configuration of the Digi branded wireless device. Check the settings on the Wireless Access Point. If you have any other wireless access points in the area you might want to power them off as well

- If the Digi branded wireless device is still not associating then try resetting the unit back to factory defaults and reconfigure (see the Users Guide for details).

- If the Digi branded wireless device Link LED indicates that the unit is associated (solid instead of blinking), but you still can't discover it; turn off the wireless access point or ad hoc network. Does the link LED start blinking rapidly? If it does, then that means that the Digi wireless device was associated with it. If not, then you know that the Digi wireless device has associated with some other wireless network. Also, when attempting to discover the device, make sure your PC has disabled all firewalls and anti-virus ware that may be blocking the discovery message responses.

- Make sure the wireless access point being used is running the most current firmware. In rare circumstances bugs in the Wireless Access Points firmware can prevent communication.

- Run the module in "serial debug" mode (Digi Connect™ WiSP). Flip the unit over and set all red and white jumper pins in position so that they are the farthest from the serial port (on). Then attach a null modem serial cable and open a terminal program from the PC or laptop with the following settings: 9600 baud, 8 data bits, 1 stop bit, no parity, no flow control. You can then type the following command to enable a wireless trace:

set trace state=on mode=concurrent mask=wlan:+cdiw

Let the Digi Connect™ Wi-SP run for a while. You should shortly start to see debug information coming from the serial port. It will tell you if the device is associating and with what. The trace should provide some clues as to the problem.

- Perform a beacon trace of the wireless network. This involves “sniffing” the wireless traffic with a special tool. See BEACON TRACING INFORMATION section in the Table of Contents.

FAQ's

Q: What kind of range can I expect to get using wireless devices?

A: Range depends on a number of factors: local interference, indoors vs. outdoors, transmission speeds, and Wireless Access Point settings. All of the above can reduce effective range. See section <<ABC>> of this document describing what levels of attenuation different materials cause as well as an estimated range guide.

Q: Are wireless connections secure?

A: Because of the very nature of wireless technology it is easier to listen to a wireless transmission than a transmission over a wired connection. However, there are some very good ways to protect data.

Q: Will wireless networks work the same as a wired network?

A: Wireless networks have a lot of things in common with wired networks but there are some important differences such as: data rates are typically lower and the latency between network responses is greater.

Q: Should I use a wireless network instead of a wired network?

A: When deciding whether or not to use a wireless networks several things must be taken into consideration. As we mention above, wireless brings the advantages of ease of deployment and portability but can introduce speed, latency, and security issues.

Q: How do I get my wireless Digi branded product associated to my Wireless Access Point using encryption?

A: You will want to review our User's and Command Reference Guides for further details. These guides and additional documentation can be found on our support site: http://www.digi.com/support/

Q: My Digi branded wireless device keeps losing it's wireless connection. Why is it doing this and how can I prevent this from happening again?

A: Typically environmental factors such as range from the Wireless Access Point, wireless interference, etc, effect a wireless connection.

Q: What's the maximum number of wireless devices in an area?

A: The maximum theoretical number of devices on an WiFi wireless network is 2,096. In reality however, other factors greatly reduce this number. It's not uncommon to see numbers in the 32-128 device range (from the access point vendors). As more and more devices associate with the network, the slower the network becomes overall. The reason for this is because they all have to share the same throughput speed.

WHITE PAPERS (WPs)

The following section is various white papers that have been collected. Although they are not Digi device centric, they help explain some aspects of WiFi technology and how to best use it.

1) Wireless Primer, Mike Rohmhoser, Digi International, Jan 2005.
ftp://ftp1.digi.com/support/images/wifi_primer.doc

2) Securing Your Wireless Network:
http://www.practicallynetworked.com/support/wireless_secure.htm

3) WPA verses 802.11i (WPA2):
http://www.openxtra.co.uk/articles/wpa-vs-80211i

4) Range vs. Rate Dilemma of WLANs:
http://www.commsdesign.com/design_corner/showArticle.jhtml?articleID=17301701

5) Cisco White Paper
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6973/ps8382/prod_white_paper0900aecd806b8ce7_ns767_Networking_Solutions_White_Paper.html

GLOSSARY

802.11
The original WiFi standard introduced back in 1997. It is now obsolete.

802.11a
A second generation standard that was introduced in 1999. It has short range, but is good for many wireless devices in a small area. As such, it is still used today.

802.11b
A second generation standard that was introduced in 1999. It is gradually being replaced with 802.11g.

802.11g
A third generation standard that was introduced in 2001. It is gradually replacing 802.11b because it is much faster (54 Mbps).

802.11n
Forth generation WiFi standard that is not yet completed. It is expected to have a high data rate (around 600 Mbps) and doubled range.

802.1X
Wireless Authentication framework. It uses EAP which has many different methods of authenticating wireless devices and even access points themselves (examples: TLS, TTLS, MSCHAPv1-2).

Access Point
See *AP*

Ad Hoc (network)
A wireless network that does not have an access point.

AES
Advanced Encryption Standard – a form of wireless data encryption. This is used with CCMP to form the 802.11i security standard. It is also known as WPA2.

AP
Access Point. Bridge-like device that attaches wireless stations to a wired network.

Association
When a wireless devices joins a wireless network.

Authentication
The process in which a wireless device attempts to prove it's identity to the wireless network so that it can join it.

"B-Mode"
Slang for 802.11b. Typically, this is used to mean that a device is 802.11b capable.

Beacon
A type of message that the access point regularly sends out into the area announcing the presence of the wireless network. Think of it as a lighthouse sending out a beam of light.

Beacon Trace
The act of monitoring wireless data at the beacon level. Normally, this is not possible with normal methods in windows (i.e. the Wireshark/Ethereal application running with a standard wireless network adapter in the Windows operating system)

Bridge
A network device that connects two different networks together. Example, an access point is a bridge between a wired and wireless networks.

BSSID
Basic Service Set Identifier. It's a 48 bit ID used by all stations.

CCK
Complementary Code Keying – a modulation scheme.

CCMP
Counter Mode with CBC MAC Protocol. This is used with AES to meet the 802.11i encryption standard. This is also known as WPA2.

Channel
The frequency that WiFi uses. 2.4GHz is used for the 802.11, 802.11b, and 802.11g standards. 5 GHz is used for the 802.11a standard.

Collision
When two or more wireless devices try to talk at the same time. This results in non of the devices being able to send messages at that particular time.

CTS
Clear to Send. When a wireless station announces that it's ready to receive the next part of a wireless transmission. This is used for large data transfers.

Data Rate
See Throughput.

DHCP

Dynamic Host Configuration Protocol. A method of giving out pre determined IP addresses on a network to network devices. This is as opposed to the device setting it's own IP address (called static IP).

Disassociate
Un-associate. The act of removing a wireless device from the wireless network.

Deauthenticate
Un-authenticate. The act of removing a wireless devices proven identity to the wireless network.

DSSS
Direct-Sequcne Spread Spectrum. Transmission technique where the signal is spread across a wide frequency band for transmission.

EAP
Extensible Authentication Protocol. Used with 802.1X Authentication. An encompassing protocol with many methods used for authenticating wireless devices to the wireless network.

Encryption
Scrambling wireless traffic so that it can not be easily read by unwanted parties.

Ethereal
An application used for collecting network data for analyzing and troubleshooting.

Fragment
When data is broken down into chunks so that it can be sent over the wireless network.

FCC
Federal Communications Commission.

FHSS
Frequency Hopping Spread Spectrum.

Firmware
Instruction code written for devices. This is commonly used to describe software that runs in anything other than a computer. (PDA, cell phone, etc.)

Frequency
The wavelength of a signal.

"G Mode"
Slang for 802.11g. Typically, this is used to mean that a device is 802.11b capable.

IBSS

Independent Basic Service Set. Also known as an *ad hoc* network.

IEEE
Institute of Electrical and Electronics Engineers. This is the professional body of engineers that created the 802.11 standard.

Infrastructure (mode)
A wireless network that uses an access point. This is opposed to an *ad hoc* network that does not use an access point.

Interference
Something that can cause a wireless devices transmission to fail. Examples of interference are: other wireless networks, microwave ovens, cordless phones

LED
Light Emitting Diode. A small low power light.

Modulation
Converting data to actual wireless signals. A signal will be sent on a particular frequency. In the case of WiFi this is also known as a channel.

ODFM
Orthogonal Frequency Division Muliplexting. A technique that splits a wide frequency band into a number of narrow frequency bands and inverse multiplexes data across the subchannels. 802.11a and 802.11g are based on ODFM.

PSK
Pre-Shared Key. An Authentication method where the stations must present the correct "key" to the network to join it.

Probe Response
The response the access point sends after it receives a *Probe Request*. This is to tell the wireless device the settings that the wireless network requires in order to join it.

Probe Request
An announcement sent from the wireless device to access points, telling them the settings of the wireless network that it wants to join.

RADIUS
Remote Access Dial In User Service. An authentication method. It involves the wireless device supplying a username and password to be allowed to authenticate with the network. This is used most in enterprise grade networks.

Range
The distance in which wireless transmissions must travel to get to their destination. As range increases, the data rate of the wireless connection decreases.

Roaming
Roaming is very subjective term and is not defined in the WiFi standard. Generally, is used to describe the act of moving a wireless device around and have it seamlessly communicate with the wireless network as it moves from access point to access point.

RTS
Ready to Send. When a wireless device announces that it's ready to send the next part of a wireless transmission. This is used for large data transfers that must be broken down into fragments.

SSID
Service Set Identifier. The name of the wireless network. This is a critical piece of information to join a wireless network.

Security
Using wireless *Authentication* and wireless *Encryption* to keep data secure as it crosses the wireless network.

Throughput
The amount of data that can be sent in a given time. Common throughput values for wireless (802.11b) are 1, 2, 5.5, and 11Mbps. Mbps is Mega bits per second.

TKIP
Temporary Key Integrity Protocol. An encryption method that was invented to replace the WEP encryption method.

WEP
Wired Equivalent Privacy. An old encryption method. It has since been found to have major flaws; although it is better than nothing. As such, it has been largely replaced by WPA (TKIP) and WPA2 (AES/CCMP).

WiFi
Wireless Fidelity. An easy to remember name for the 802.11 wireless standards.

Wireshark
An application used for collecting network data for analyzing and troubleshooting.

WPA
WPA encryption that uses the TKIP cipher. Also see *TKIP*.

WPA2
WPA encryption that uses the AES/CCMP cipher. Also see *AES* or *CCMP*