i341 – Networks and Distributed Applications

Wireless LANs (WLANs) & IEEE 802.11

Rev: 2016

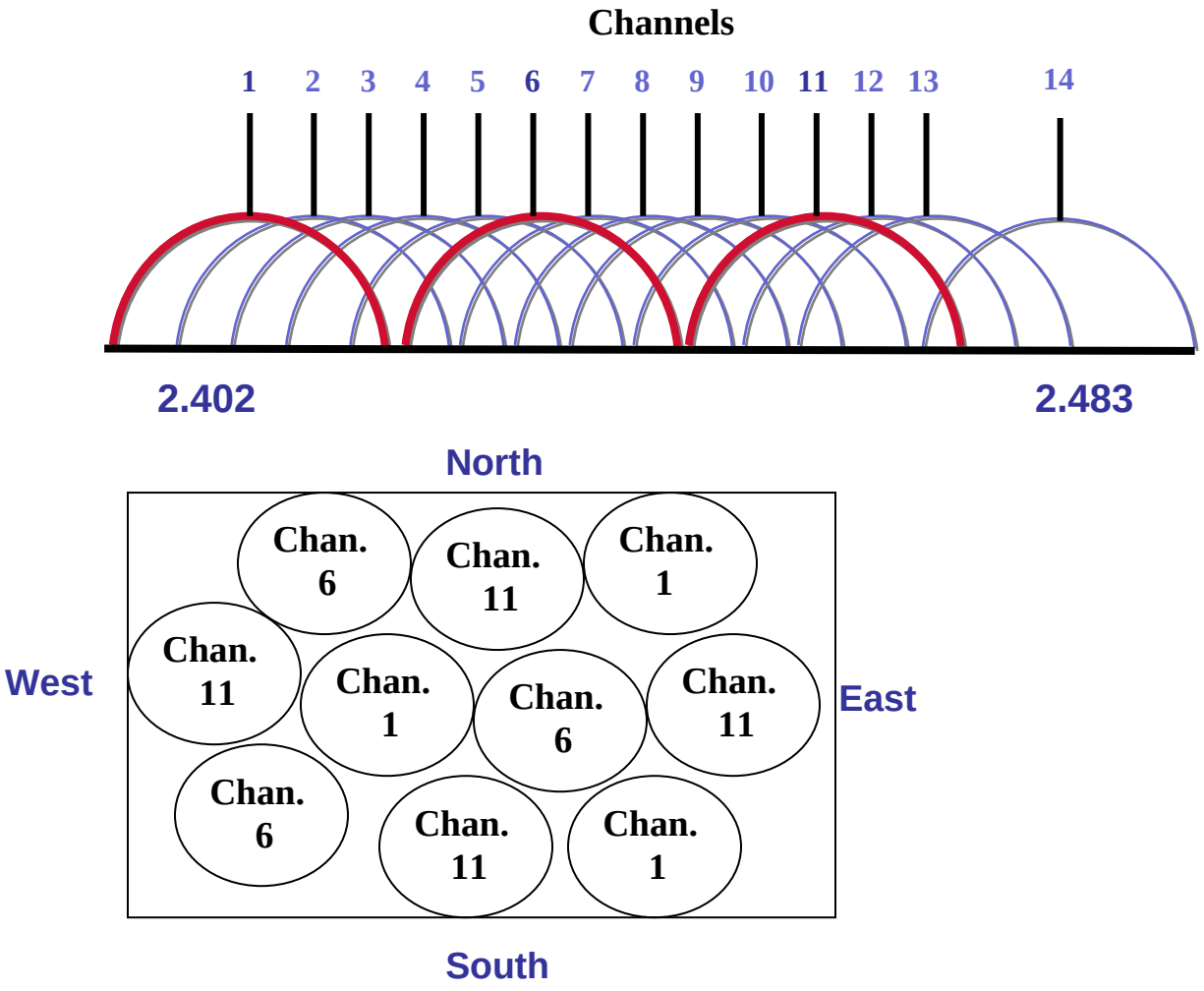
802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

There are several **specifications in the 802.11 family**:

- **802.11** -- applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
- **802.11a** -- an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- **802.11b** (also referred to as *802.11 High Rate* or *Wi-Fi*) -- an extension to 802.11 that applies to wireless LANS and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- **802.11g** -- applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.
- **802.11n** – high speed WLAN (up to 200 Mb) runs on both 2.4 and 5 GHz
- **802.11ac** - This specification has expected multi-station WLAN throughput of at least 1 Gbps and a single link throughput of at > (500 Mbit/s), accomplished by extending the air interface concepts embraced by 802.11n: wider RF bandwidth (up to 160 MHz), more MIMO spatial streams (up to 8), multi-user MIMO

802.11 RF Channel Allocation

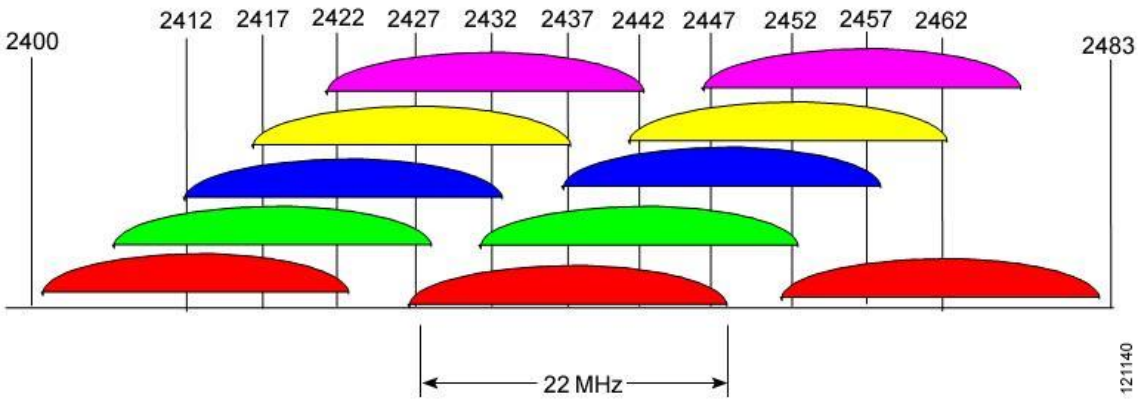
IEEE 802.11b/g - Direct Sequence @ 2.4 GHz



802.11 RF Channel Specification (source: Cisco CCO)

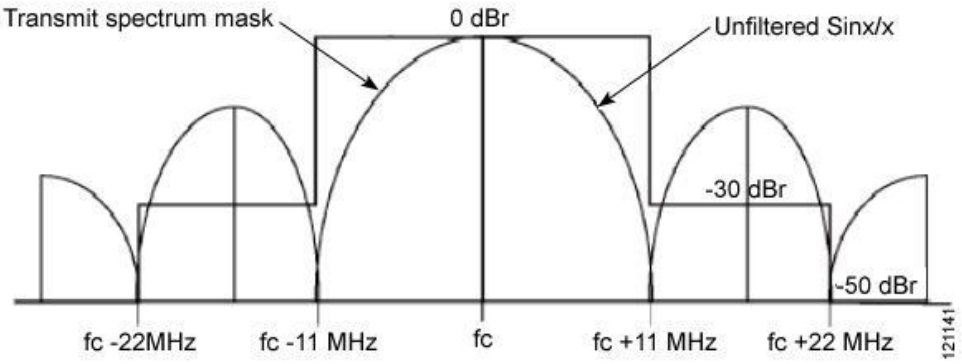
The IEEE 802.11 standard establishes several requirements for the RF transmission characteristics of an 802.11 radio. Included in these are the channelization scheme as well as the spectrum radiation of the signal (that is, how the RF energy spreads across the channel frequencies). The 2.4-GHz band is broken down into 11 channels for the FCC or North American domain and 13 channels for the European or ETSI domain. These channels have a center frequency separation of only 5 MHz and an overall channel bandwidth (or frequency occupation) of 22 MHz. This is true for 802.11b products running 1, 2, 5.5, or 11 Mbps as well as the newer 802.11g products running up to 54 Mbps. The differences lie in the modulation scheme (that is, the methods used to place data on the RF signal), but the channels are identical across all of these products.

North American Channelization Scheme



The level of RF energy that crosses between these channels determines interference. Radios do not have an exact edge to their channel, and energy spreads beyond the edges of the channel boundaries. However, the overall energy level drops as the signal spreads farther from the center of the channel. The 802.11b standard defines the required limits for the energy outside the channel boundaries (+/- 11 MHz), also known as the spectral mask.

802.11b Spectral Mask which defines the maximum permitted energy in the frequencies surrounding the channel's center frequency (or fc).



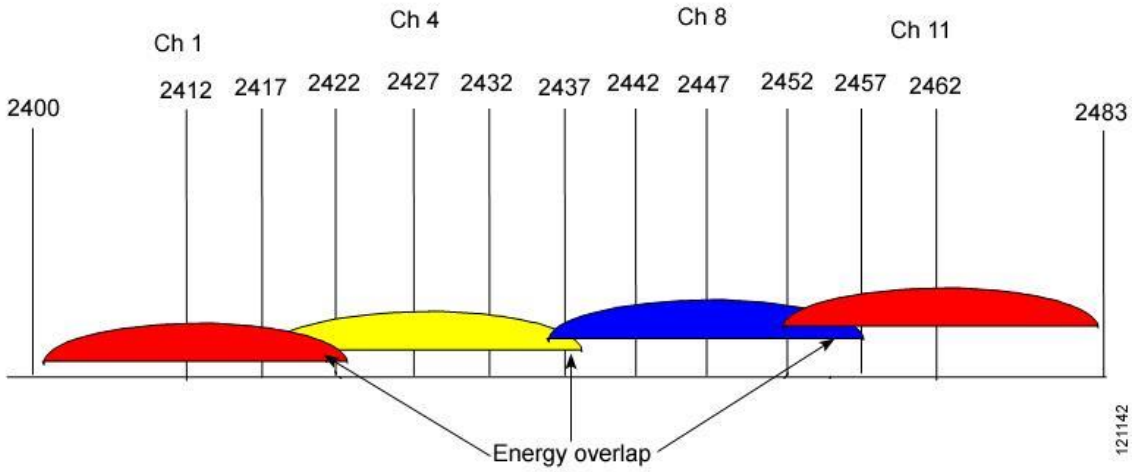
The energy radiated by the transmitter extends well beyond the 22-MHz bandwidth of the channel (+/- 11 MHz from fc). At 11 MHz from the center of the channel, the energy must be 30 dB lower than the maximum signal level, and at 22 MHz away, the energy must be 50 dB below the maximum level. As you move farther from the center of the channel, the energy continues to decrease but is still present, providing some interference on several more channels.

The worst-case scenario is a 100-mW transmitter and a good receiver. For example, the Cisco Aironet 350 radio transmits at 100 mW, or +20 dBm. The 350 receiver can receive signals as low as -85 dBm (and even down to -93 dBm at 1 Mb).

Note The more negative the receiver sensitivity number, the lower the signal level necessary to properly decode the signal.

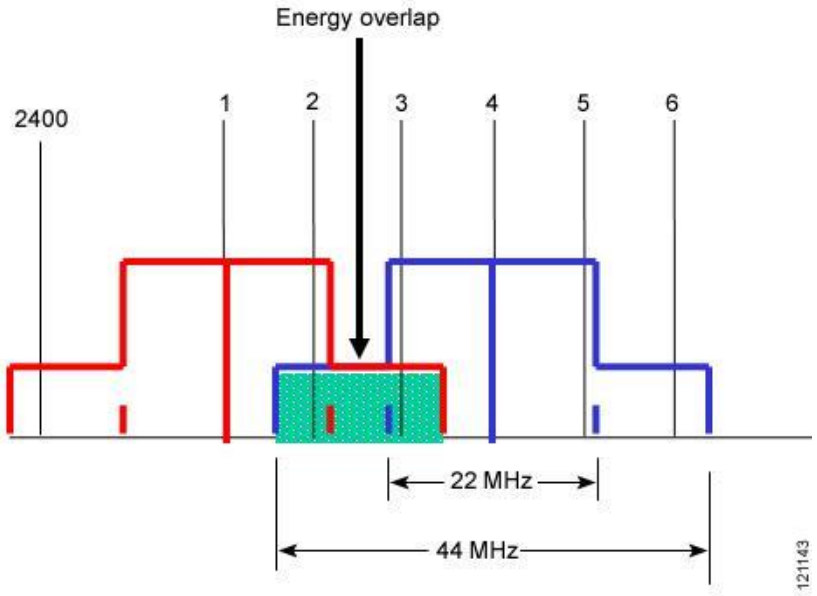
Therefore, at 11 MHz away, the energy from the transmitter is 35 dB below the maximum (100 mW/20 dBm), putting it at a possible -15 dBm. Move another 11 MHz away, and the signal level is 50 dB below the maximum (100 mW/20 dBm or -30 dBm), which is still over 50 dB higher than the receiver needs to receive properly. In short, the receiver still hears the signal, even at 22 MHz away.

Four-Channel RF System



The energy overlap between the channels does not appear to be significant. However, as discussed earlier, this overlap is at the +/- 11-MHz and 22-MHz points, where the energy is still quite strong. If we use the transmitter mask to show the possible energy that could be available, we see that there is significant energy from channel 1 in the area for the receiver of channel 4 to hear (see Figure 4).

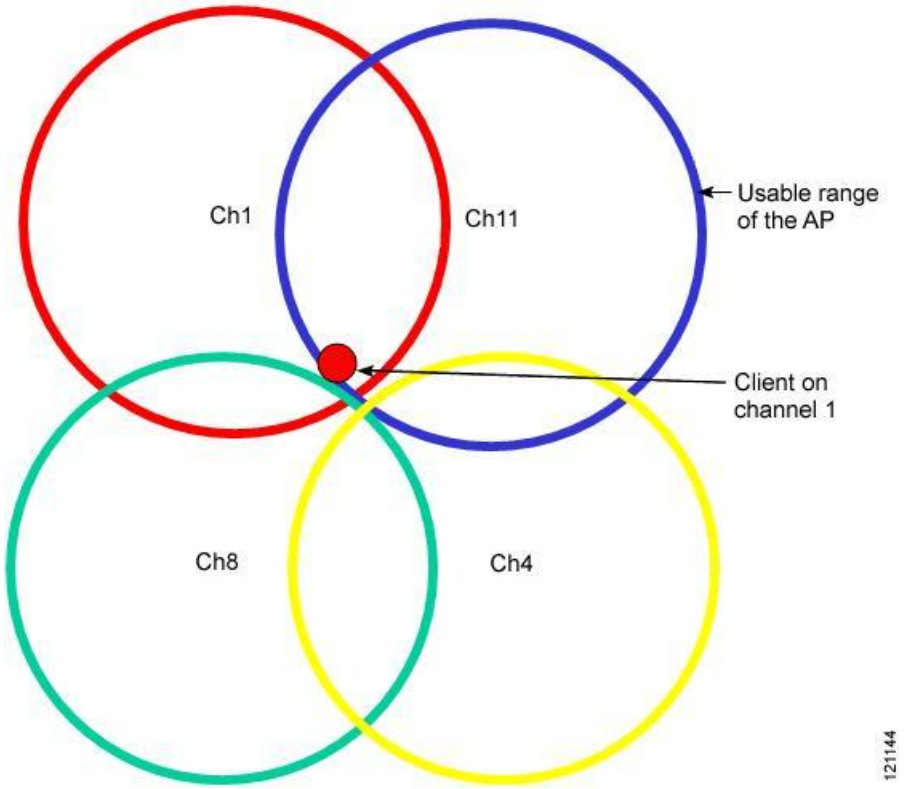
Figure 4 Transmitter Mask Showing Available Energy



Deploying Access Points

The counter-argument to the position that a device on channel 4 will hear a device on channel 1 involves the concept of physical separation. It is possible that proper placement of the access points provides enough physical separation between the cells so that the energy level at the edge of each cell is low enough so as not to generate interference.

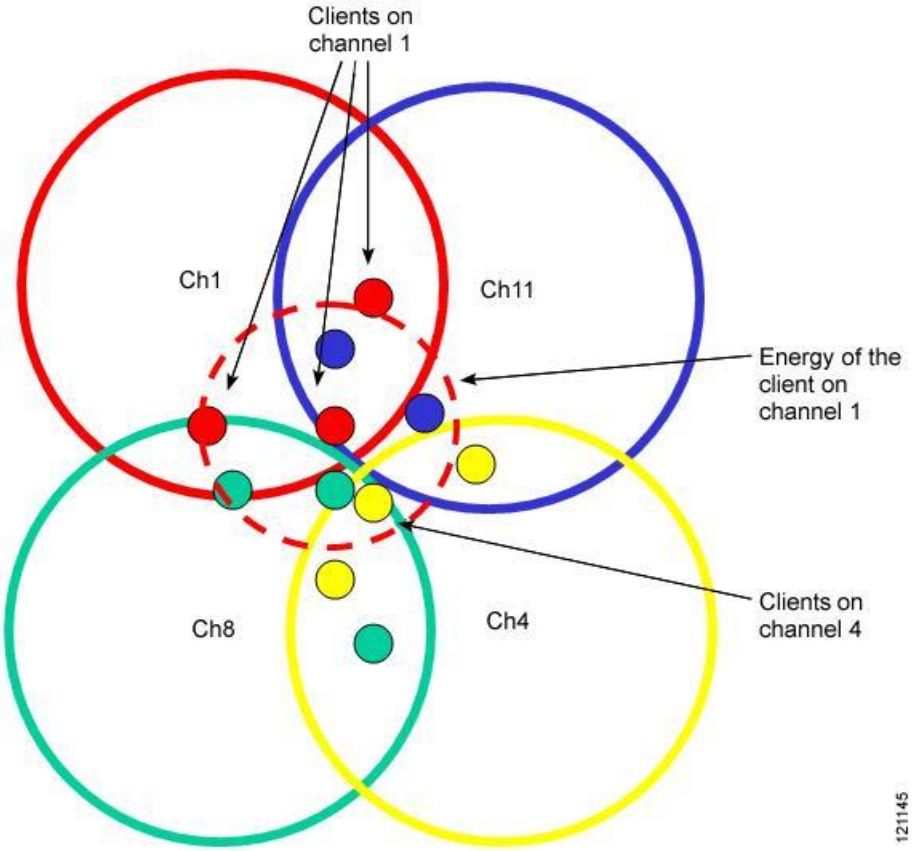
Example - Positioning Access Points to Avoid Interference



For an environment with a very low user density, this assumption could be true. In a site survey, interference between the access point on channel 4 and the client on channel 1 would not likely be noticed. But this is not the case in a high user density system in which the four-channel argument is intended to be used. Typically, access point coverage cells are not overly large in a high user density environment, permitting fewer users per access point (resulting in higher bandwidth per user). As a result, the range of the client transmitter is only slightly less than that of an access point in this deployment scheme. For this case, however, we can assume that the client has 50 percent of the access point transmitter range (keeping in mind that the larger antenna on the access point improves the receive signal, enabling it to still hear the client).

The previous figure shows that the energy of the channel 1 client transmitter is physically located very close to the channel 4 client receiver and will very likely cause interference.

Interference between Clients



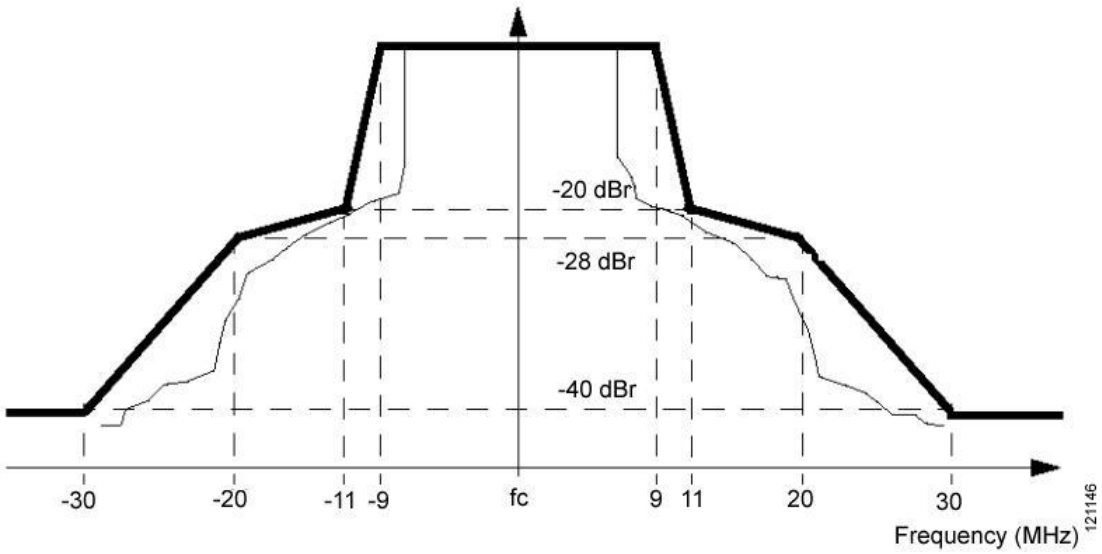
This proximity is important because 802.11 specifies the protocol using carrier sense multiple access (CSMA), meaning listen before transmitting. In this case, channel 4 clients refrain from transmitting until the client that is transmitting on channel 1 is finished. In a system with few users, this is probably not a problem. However, as the number of clients increases, so does the possibility of holdoffs.

This scenario also increases the likelihood of collisions, resulting in retries for both clients and decreasing the efficiency of the WLAN. If the cross-channel signal is low enough not to be decoded as a valid 802.11 signal, it is considered noise. This is when collisions start to occur. The noise is strong enough that the desired signal gets corrupted, and the packet needs to be retransmitted. Overall, this is much worse than a holdoff because the device transmits the packet twice (or more) rather than waiting for a clear time and sending it once.

Moving to 802.11g

The spectral efficiency (that is, the way in which the frequencies surrounding the center of the channel are used) for the orthogonal frequency division multiplexing (OFDM) modulation used in 802.11g devices is much worse than that for the complementary code keying (CCK) modulation used in 802.11b devices. Figure 7 shows the transmitter specification for 802.11g.

Figure 7 802.11g Transmitter Specification



At 11 MHz from the center, the transmitter energy level is only 20 dB below the maximum (as opposed to 35 dB for 802.11b), and at 22 MHz away, the energy is only about 30 dB below (as opposed to 50 db for 802.11b). Even as far out as 40 MHz, the energy is still only 40 dB below the maximum. Using the four-channel scheme here results in an overlap as shown above. Notice how much greater the energy overlap is when using 802.11g.

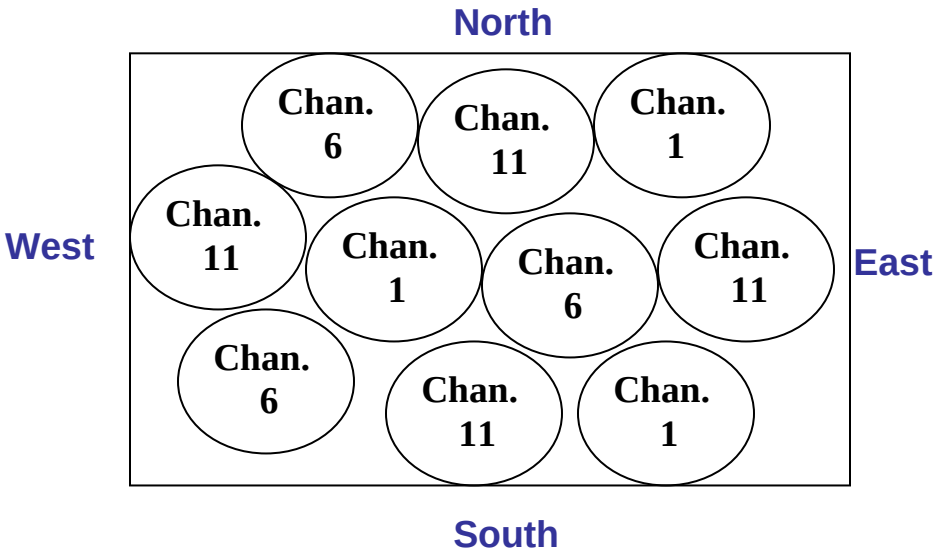
Table 1 Result Summary Showing Average Throughput per Client

Channels	Throughput (KB)
1, 1, 6, and 11	601.1
1, 4, 8, and 11	348.9

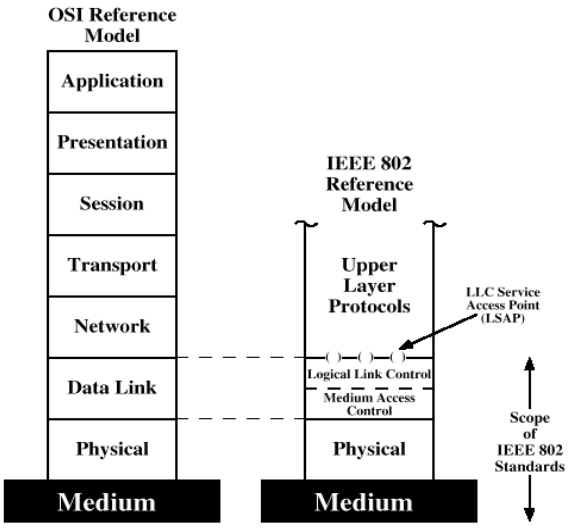
Many have long recommended a three-channel approach to provide nonoverlapping channels. A four-channel scheme can cause severe issues when the system is brought online and the number of users starts to increase.

In a four-channel design, the signal of one device is noise to another device. Even in a design where a channel 1 cell would never overlap a channel 4 cell, for example, you must still account for clients transmitting that are not in the same location as the access point. By looking at only the access points, one is ignoring the majority of radios in the network. Virtually all new radio deployments support 802.11g and/or 802.11a and thus OFDM, which has much more sideband energy than 802.11b.

If designing a system with four channels, the risk of interference between cells greatly increases, resulting in poor performance and lower throughput. As the volume of users and bandwidth needs increase, problems will slowly arise, making it necessary to resolve the issue at a later date. It it is generally a de-facto standard by professionals in the wireless LAN industry to start by using three non-overlapping, non-interfering channels.



Example - Three nonoverlapping, noninterfering channels 802.11 b/g



OSI Model and IEEE 802 Protocol Layers

Wireless LAN Standards

Use this chart to get some quick information to help you differentiate between the available wireless networking standards and choose which standard might be the right fit for your business. See the links below the chart for further information on wireless networking standards.

Standard	Data Rate	Modulation Scheme	Security	Pros/Cons
IEEE 802.11	Up to 2Mbps in the 2.4GHz band	FHSS or DSSS	WEP & WPA	This specification has been extended into 802.11b.
IEEE 802.11a (Wi-Fi)	Up to 54Mbps in the 5GHz band	OFDM	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b.
IEEE 802.11b (Wi-Fi)	Up to 11Mbps in the 2.4GHz band	DSSS with CCK	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-

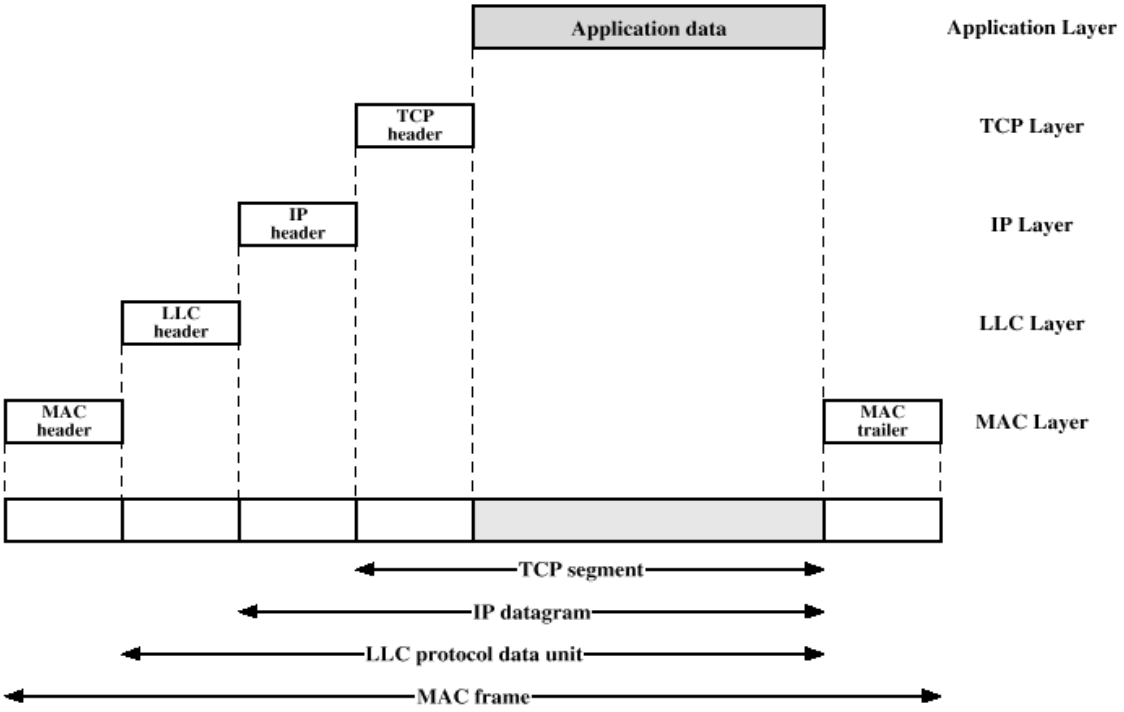
				speed access to data at up to 300 feet from base station. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
IEEE 802.11g (Wi-Fi)	Up to 54Mbps in the 2.4GHz band	OFDM above 20Mbps, DSSS with CCK below 20Mbps	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
Bluetooth	Up to 2Mbps in the 2.45GHz band	FHSS	PPTP, SSL or VPN	No native support for IP, so it does not support TCP/IP and wireless LAN applications well. Not originally created to support wireless LANs. Best suited for connecting PDAs, cell phones and PCs in short intervals.
HomeRF	Up to 10Mbps in the 2.4GHZ band	FHSS	Independent network IP addresses for each network. Data is sent with a 56-bit encryption algorithm.	**Note:** HomeRF is no longer being supported by any vendors or working groups. Intended for use in homes, not enterprises. Range is only 150 feet from base station. Relatively inexpensive to set up and maintain. Voice quality is always good because it continuously reserves a chunk of bandwidth for voice services. Responds well to interference because of frequency-hopping modulation.
HiperLAN/1 (Europe)	Up to 20Mbps in the 5GHz band	CSMA/CA	Per-session encryption and individual authentication.	Only in Europe. HiperLAN is totally ad-hoc, requiring no configuration and no central controller. Doesn't provide real isochronous services. Relatively expensive to operate and maintain. No guarantee of bandwidth.
HiperLAN/2 (Europe)	Up to 54Mbps in the 5GHz band	OFDM	Strong security features with support for individual authentication and per-session encryption keys.	Only in Europe. Designed to carry ATM cells, IP packets, Firewire packets (IEEE 1394) and digital voice (from cellular phones). Better quality of service than HiperLAN/1 and guarantees bandwidth.

Last updated: June 26, 2003

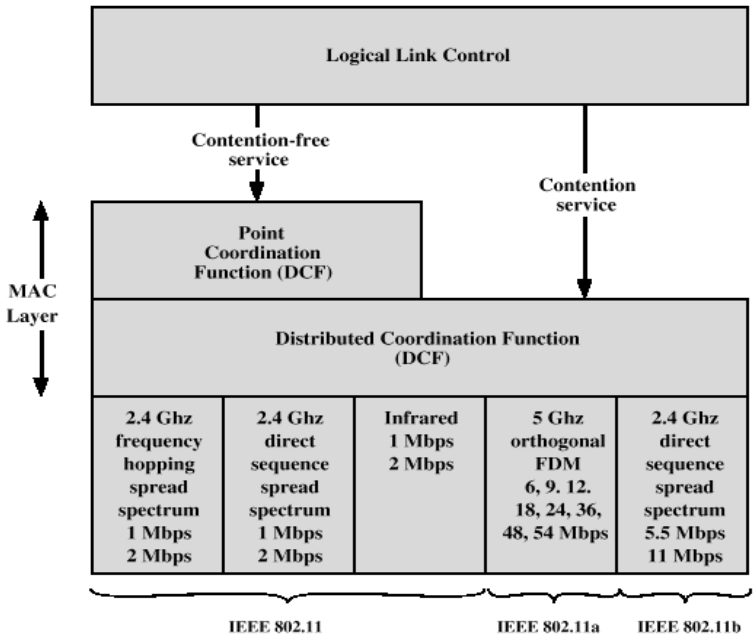
IEEE 802.11 Architecture

The 802.11 architecture is comprised primarily of four elements:

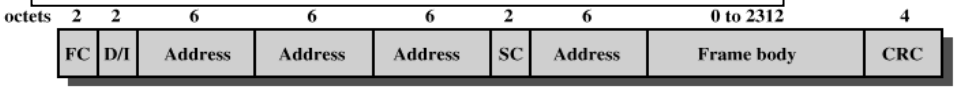
1. **Distribution system (DS)**
2. **Access point (AP)**
3. **Basic service set (BSS)**
    a. **Stations competing for access to shared wireless medium**
    b. **Isolated or connected to backbone DS through AP**
4. **Extended service set (ESS)**
    a. **Two or more basic service sets interconnected by DS**



IEEE 802 Protocols

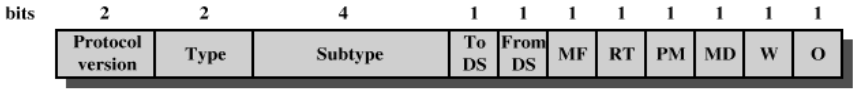


IEEE 802.11 Protocol Architecture



FC = Frame control
D/I = Duration/Connection ID
SC = Sequence control

(a) MAC frame



DS = Distribution system
MF = More fragments
RT = Retry
PM = Power management
MD = More data
W = Wired equivalent privacy bit
O = Order

(b) Frame control field

IEEE 802.11 MAC Frame Format

MAC Frame Fields

- Frame Control – frame type, control information
- Duration/connection ID – channel allocation time
- Addresses – context dependant, types include source and destination
- Sequence control – numbering and reassembly
- Frame body – MSDU or fragment of MSDU
- Frame check sequence – 32-bit CRC

Frame Control Fields

- Protocol version – 802.11 version
- Type – control, management, or data
- Subtype – identifies function of frame
- To DS – 1 if destined for DS
- From DS – 1 if leaving DS
- More fragments – 1 if fragments follow
- Retry – 1 if retransmission of previous frame

Control Frame Subtypes

- Power save – poll (PS-Poll)
- Request to send (RTS)
- Clear to send (CTS)
- Acknowledgment
- Contention-free (CF)-end
- CF-end + CF-ack

Management Frame Subtypes

- Association request
- Association response
- Reassociation request
- Reassociation response
- Probe request
- Probe response
- BeaconAnnouncement traffic indication message
- Dissociation
- Authentication
- Deauthentication

General 802.11 frame concepts

The 802.11 standard defines various frame types that stations (NICs and access points) use for communications, as well as managing and controlling the wireless link. Every frame has a control field that depicts the 802.11 protocol version, frame type, and various indicators, such as whether WEP is on, power management is active, and so on. In addition all frames contain MAC addresses of the source and destination station (and access point), a frame sequence number, frame body and frame check sequence (for error detection).

802.11 data frames carry protocols and data from higher layers within the frame body. A data frame, for example, could be carrying the HTML code from a Web page (complete with TCP/IP headers) that the user is viewing. Other frames that stations use for management and control carry specific information regarding the wireless link in the frame body. For example, a beacon's frame body contains the service set identifier (SSID), timestamp, and other pertinent information regarding the access point.

Note: For more details regarding 802.11 frame structure and usage, refer to the 802.11 standard, which is free for download from the 802.11 Working Group Web site.

Management Frames

802.11 management frames enable stations to establish and maintain communications. The following are common 802.11 management frame subtypes:

Authentication frame: 802.11 authentication is a process whereby the access point either accepts or rejects the identity of a radio NIC. The NIC begins the process by sending an authentication frame containing its identity to the access point. With open system authentication (the default), the radio NIC sends only one authentication frame, and the access point responds with an authentication frame as a response indicating acceptance (or rejection). With the optional shared key authentication, the radio NIC sends an initial authentication frame, and the access point responds with an authentication frame containing challenge text. The radio NIC must send an encrypted version of the challenge text (using its WEP key) in an authentication frame back to the access point. The access point ensures that the radio NIC has the correct WEP key (which is the basis for authentication) by seeing whether the challenge text recovered after decryption is the same that was sent previously. Based on the results of this comparison, the access point replies to the radio NIC with an authentication frame signifying the result of authentication.

Deauthentication frame: A station sends a deauthentication frame to another station if it wishes to terminate secure communications.

Association request frame: 802.11 association enables the access point to allocate resources for and synchronize with a radio NIC. A NIC begins the association process by sending an association request to an access point. This frame carries information about the NIC (e.g., supported data rates) and the SSID of the network it wishes to associate with. After receiving the association request, the access point considers associating with the NIC, and (if accepted) reserves memory space and establishes an association ID for the NIC.

Association response frame: An access point sends an association response frame containing an acceptance or rejection notice to the radio NIC requesting association. If the access point accepts the radio NIC, the frame includes information regarding the association, such as association ID and supported data rates. If the outcome of the association is positive, the radio NIC can utilize the access point to communicate with other NICs on the network and systems on the distribution (i.e., Ethernet) side of the access point.

Reassociation request frame: If a radio NIC roams away from the currently associated access point and finds another access point having a stronger beacon signal, the radio NIC will send a reassociation frame to the new access point. The new access point then coordinates the forwarding of data frames that may still be in the buffer of the previous access point waiting for transmission to the radio NIC.

Reassociation response frame: An access point sends a reassociation response frame containing an acceptance or rejection notice to the radio NIC requesting reassociation. Similar to the association process, the frame includes information regarding the association, such as association ID and supported data rates.

Disassociation frame: A station sends a disassociation frame to another station if it wishes to terminate the association. For example, a radio NIC that is shut down gracefully can send a disassociation frame to alert the access point that the NIC is powering off. The access point can then relinquish memory allocations and remove the radio NIC from the association table.

Beacon frame: The access point periodically sends a beacon frame to announce its presence and relay information, such as timestamp, SSID, and other parameters regarding the access point to radio NICs that are within range. Radio NICs continually scan all 802.11 radio channels and listen to beacons as the basis for choosing which access point is best to associate with.

Probe request frame: A station sends a probe request frame when it needs to obtain information from another station. For example, a radio NIC would send a probe request to determine which access points are within range.

P**robe response frame**: A station will respond with a probe response frame, containing capability information, supported data rates, etc., when after it receives a probe request frame.

Control Frames

802.11 control frames assist in the delivery of data frames between stations. The following are common 802.11 control frame subtypes:

Request to Send (RTS) frame: The RTS/CTS function is optional and reduces frame collisions present when hidden stations have associations with the same access point. A station sends a RTS frame to another station as the first phase of a two-way handshake necessary before sending a data frame.

Clear to Send (CTS) frame: A station responds to a RTS with a CTS frame, providing clearance for the requesting station to send a data frame. The CTS includes a time value that causes all other stations (including hidden stations) to hold off transmission of frames for a time period necessary for the requesting station to send its frame. This minimizes collisions among hidden stations, which can result in higher throughput if you implement it properly.

Acknowledgement (ACK) frame: After receiving a data frame, the receiving station will utilize an error checking processes to detect the presence of errors. The receiving station will send an ACK frame to the sending station if no errors are found. If the sending station doesn't receive an ACK after a period of time, the sending station will retransmit the frame.

Data Frames

Of course the main purpose of having a wireless LAN is to transport data. 802.11 defines a data frame type that carries packets from higher layers, such as web pages, printer control data, etc., within the body of the frame. When viewing 802.11 data frames with a packet analyzer, you can generally observe the contents of the frame body to see what packets that the 802.11 data frames are transporting.

Physical Media Defined by Original 802.11 Standard

- Direct-sequence spread spectrum
  - Operating in 2.4 GHz ISM band
  - Data rates of 1 and 2 Mbps
- Frequency-hopping spread spectrum
  - Operating in 2.4 GHz ISM band
  - Data rates of 1 and 2 Mbps
- Infrared
  - 1 and 2 Mbps
  - Wavelength between 850 and 950 nm

IEEE 802.11a and IEEE 802.11b

- IEEE 802.11a
  - Makes use of 5-GHz band
  - Provides rates of 6, 9 , 12, 18, 24, 36, 48, 54 Mbps
  - Uses orthogonal frequency division multiplexing (OFDM)
  - Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM
- IEEE 802.11b
  - Provides data rates of 5.5 and 11 Mbps
  - Complementary code keying (CCK) modulation scheme

BlueTooth A short-range radio technology aimed at simplifying communications among Internet devices and between devices and the Internet. It also aims to simplify data synchronization between Internet devices and other computers. Products with Bluetooth technology must be qualified and pass interoperability testing by the Bluetooth Special Interest Group prior to release. Bluetooth's founding members include Ericsson, IBM, Intel, Nokia and Toshiba.

Wireless Home Networking - *Wi-Fi Standards* (***Source***: Joseph Moran 11-7-02)

Before you do anything, including buy a single piece of equipment, the first order of business for your wireless local area network (WLAN) is to determine the type of wireless technology that is most appropriate for your environment. Because each has its own characteristics, strengths, and weaknesses, you'll find some are better suited than others to your particular situation.

In the world of WLAN standards there are several you can choose from today, and more on the horizon. While many are similar in the way they operate or the type of equipment they use, there are also key differences that you must be aware of.

When comparing the different standards, it's easy to get caught up in a lot of the technical minutiae that differentiate them. When all is said and done though, you'll find three major factors that you need to concern yourself with--cost, speed, and range.

802.11b/2.4GHz vs. 802.11a/5GHz
There are currently two major WLAN standards, and both operate using radio frequency (RF) technology. The two standards have heretofore been colloquially referred to as 802.11b and 802.11a - together they're collectively called Wi-Fi. To reduce confusion, however, the wireless standard group called the Wi-Fi Alliance will refer to the two technologies as 2.4GHz and 5GHz, respectively, as least on product packaging. These monikers refer to the frequency band that each technology utilizes.

In the alphabet, "a" comes before "b." In the world of wireless networking though, "b" definitely came before "a." The 802.11b specification was the first to be finalized and reach the marketplace.

Performance

802.11b/2.4GHz devices operate in an unlicensed radio band and transmit data on the same frequency as some household appliances, including some cordless phones and even microwave ovens. The 802.11b specification provides for a bandwidth rating of 11 Megabits per second (Mbps) (define). This is just a theoretical maximum, however. Wireless networks, as well as wired LANs, never let you obtain that level of performance, or even close to it. The actual throughput you can expect to obtain from an 802.11b network will typically be between 4 and 5Mbps.

This level of performance is more than sufficient for most rudimentary computing tasks. When you consider that a typical broadband DSL or cable modem connection might provide you with from 600kbps to 1.6Mbps of downstream bandwidth (define), you can see that the speed of 802.11b is not be an impediment to activities like Web browsing, e-mail, file transfer, running applications, and even streaming Internet-based audio and video.

It is not difficult to envision scenarios where your bandwidth needs might be greatly increase, for example when you want to quickly transfer very large files like graphics, audio, or video or stream those same audio and video files, like your collection of MP3s or home movies on your hard disk.

If you often see the need for more speed, consider 802.11a. Products based on this 5GHz specification offer higher performance. 802.11a has a maximum bandwidth of 54Mbps, almost five times that of 802.11b. Like its predecessor though, you won't see anything near that in the real world. Instead, expect a maximum throughput of between 20 and 25Mbps - still five times what you get from 802.11b.

WLAN Range

The performance of both 802.11b and 802.11a decreases as your distance from the antenna increases. This degradation is neither linear nor granular; in other words, you don't lose half the performance when your distance doubles, and the performance doesn't decline in small increments as you move farther away.

Instead, each wireless specification has a handful of pre-defined bandwidth levels at which it can operate (802.11b has four, while 802.11a has seven). The bandwidth levels drop markedly as you move further away, and by the time you are at the extreme ranges, the bandwidth available is only a small fraction of the maximum.

When indoors, 802.11b signals can travel as far as 150 meters (492 feet). Outdoors, 11b range is over three times greater- 500 meters (1640 feet, or nearly 1/3 of a mile). The outdoor ranges are higher because there are fewer obstacles, like walls, to absorb or block

the radio signal. At either of these extreme ranges, the bandwidth available is a mere 1Mbps, which would yield throughput (define) closer to that of your broadband connection. That low level of throughput could hamstring your networking activities.

On the other hand, for 802.11b to operate in its maximum bandwidth mode of 11Mbps, the distance indoors can be no more than 50 meters (164 feet); outdoors it should be 250 meters (820 feet).

When it comes to the relationship between performance and range, 802.11a behaves in much the same way as 802.11b. That is to say, there is an inverse relationship, so performance goes down as distance goes up.

The trade-off is that 802.11a offers lower range. Indoors, 802.11a allows for a maximum range of only about 100 meters (about 300 feet). Outdoors, the range jumps to over 350 meters (1200 feet). Like 802.11b, when you are using 802.11a equipment at extreme range, you can only communicate at the lowest speed supported, which in this case is 6Mbps.If you want the full 54Mbps bandwidth, your range indoors is limited to a mere 18 meters (60 feet), and outside to approximately 30 meters (100 feet).

With either technology you lose 50% or more of your range in order to enjoy wireless data transfer at the fastest rate possible. The bottom line is that figures for maximum range, like those for maximum bandwidth, should be taken with a healthy dose of sodium chloride. When evaluating the performance and range ratings of wireless networking products, treat them as you would the gas mileage rating on a car. Remember that your mileage will vary.

Penetration

In addition to the obvious differences in range, another differentiating factor between 802.11b and 802.11a is the quality, or let's call it robustness, of their signals.

Because of the higher frequency (and thus shorter wavelength) that they use, 802.11a signals have a much tougher time penetrating solid objects like walls, floors, and ceilings. As a result, the price for 802.11a's higher speed is not only shorter range but a weaker and less consistent signal.

In much of our testing of 802.11a products, we have often seen the signal strength fluctuate wildly, and in some cases disappear altogether, even though we were not that far from the access point, and certainly within the published range of the device.

By contrast, although 802.11b signal strength can also vary, it is much less common, and we've never completely lost a signal unless we were at the extreme edge of the device s range.

Enhanced Modes
Each of the wireless LAN standards has an extra or enhanced mode that provides an increase in performance. These modes are not official standards, and they require that the network be operated under certain conditions or with particular equipment.

802.11b+ 22Mbps mode
Some of the latest 802.11b/2.4GHz products utilize a particular Texas Instruments chipset, the ACX1000, that uses an enhanced form of modulation, which doubles the maximum bandwidth from 11 to 22Mbps. Testing has indicated that this doubling of bandwidth yields only a 50% throughput increase, however, from about 4Mbps up to 6Mbps.

802.11a/5GHz "Turbo" mode
Most 802.11a/5GHz devices using chipsets from Atheros support a "Turbo" mode that can raise the data rate from 54 to 72Mbps - 108Mbps in some newer products. In order to utilize this enhanced mode, you need to be using hardware from the same vendor on both sides of the connection.

Use of the turbo mode renders only a small increase in real-world speed over the 54Mbps mode, and this increase comes at the expense of range, which is further diminished when the wireless network is operating in Turbo mode.

802.11g
802.11g is a wireless LAN specification that has been the subject of discussion and debate since before the 802.11a spec was released earlier this year - companies like Texas Instruments wanted their technology to be the cornerstone of "g" for example. 802.11g has been under development for some time, and while not yet finalized, it is nearing completion. The first products based on the draft of the specification are expected to emerge at the end of 2002. Many 802.11b-based products out today will be upgradeable to 11g with firmware changes.

It's impossible to say for sure what kind of performance or range 802.11g products will have. However, the goal of 802.11g is to provide performance comparable to the 54Mbps of 802.11a, while maintaining compatibility with 802.11b (and similar range as well). This compatibility is maintained because 802.11g operates in the same 2.4GHz frequency as 802.11b. So, 802.11b and 802.11g devices will be able to communicate with each other, but when they do the 802.11g will be no faster than the 802.11b product it is working with - they'll both be at the slowest speed common to each.

Therefore, if you've already got an 802.11b network in place, 802.11g's backward compatibility will preserve your investment in existing hardware. This is in contrast to the situation when 802.11a emerged. Because it uses a completely different frequency and type of modulation than 802.11b, users wanting to upgrade to 802.11a needed to buy entirely new hardware.

Just recently, dual-mode access points and NICs have started to appear that simultaneously support both 802.11a/5GHz and 802.11b/2.4GHz. It's very likely that many of the first 802.11g products will also be multimode products able to operate as either 802.11g (and by extension, 802.11b) or 802.11a devices. **Seamless failover ??**

How to choose (802.11 a vs b/g) ?
As you can see, despite the superficial similarities between 802.11a and 802.11b WLAN standards, there are still significant differences between the two concerning the issues of speed, range, quality of signal, cost, and upgradeability.

So which of the two should you choose?

In the majority of cases, for a typical small (home) office network 2.4GHz will be the way to go, given its combination of good speed, range, reasonable cost, and upgrade potential. If you absolutely need higher speeds than even 22Mbps 802.11b can offer you, a 5GHz WLAN will do the job, but you'll need to factor in not only the significantly reduced range, but the fact that the signal may be excessively absorbed or reflected in the interior of your office.

Beating Signal Loss in WLANs

By Jim Geier

July 23, 2002

Wireless signals propagating through the air lose strength while encountering natural and manmade obstacles. It would be nice if RF signals would propagate without an bounds, but that simply doesn't occur on Earth.

In order to deploy an effective wireless LAN solution, installers must have a good understanding of the causes of signal loss (attenuation) and how to implement applicable countermeasures. This knowledge becomes extremely important when performing an RF site survey, which technicians use to determine the optimum location of access points to provide necessary range. With familiarity of RF attenuation, you'll accomplish RF site surveys more efficiently and get higher performing wireless network installations as a result.

Attenuation basics

Attenuation is simply a reduction of signal strength during transmission. You represent attenuation in decibels (dB), which is ten times the logarithm of the signal power at a particular input divided by the signal power at an output of a specified medium. For example, an office wall (i.e., medium) that changes the propagation of an RF signal from a power level of 200 milliwatts (the input) to 100 milliwatts (the output) represents 3 dB

of attenuation. Consequently, positive attenuation causes signals to become weaker when traveling through the medium.

When signal power decreases to relatively low values, the receiving 802.11 radio will likely encounter bit errors when decoding the signal. This problem worsens when significant RF interference is present. The occurrence of bits errors causes the receiving 802.11 station to refrain from sending an acknowledgement to the source station. After a short period of time, the sending station will retransmit the frame, possibly at a lower data rate with hopes of extending the range of the transmission.

Excessive attenuation causes the network's throughput to decrease because of operation at a lower data rate and the additional overhead necessary to retransmit the frames. Generally, this means that the user is operating within the outer bounds of an access point's range. There's enough attenuation present to decrease signal power below acceptable values. At worst case, signal power loss due to attenuation becomes so low that affected users will lose connectivity to the network.

Causes of attenuation

Both signal frequency and range between the end points of the medium affect the amount of attenuation. As either frequency or range increases, attenuation increases. Unlike open outdoor applications based on straightforward free space loss formulas, attenuation for indoor systems is very complex to calculate. The main reason for this difficulty is that the indoor signals bounce off obstacles and penetrate a variety of materials that offer varying effects on attenuation.

Discussion of the various algorithms to estimate indoor path loss is beyond the scope of this article. As a general rule of thumb, however, expect to encounter approximately 100dB of attenuation over distances of 200 feet when using 802.11b radios operating at 11Mbps. Keep in mind also that attenuation is not linear--it grows exponentially as range increases.

Typical office obstacles such as doors, windows and walls offer fairly known levels of attenuation. These values of attenuation are in addition to the path loss mentioned earlier. The following provides some examples of the attenuation values of common office construction:

Plasterboard wall	3dB
Glass wall with metal frame	6dB
Cinder block wall	4dB
Office window	3dB
Metal door	6dB
Metal door in brick wall	12.4dB

As a result, a typical small office could have several plasterboard walls equating to an additional 9 to 12dB of attenuation. Metal doors and glass walls could sometimes be in the way of the propagation of the signal, causing even larger amounts of attenuation. Of course this decreases the operating range of the access points.

Counteracting attenuation

The main goal of combating attenuation is to avoid having signal power within the area where users operate to fall below the sensitivity of the 802.11 radio receivers. You need to ensure that the receiver is always able to hear the transmissions. Bear in mind also that higher levels of RF interference, such as that caused by 2.4GHz cordless phones or Bluetooth devices, will negatively impact the ability for the receiver to decode the signal. As RF interference signal levels become higher than 802.11 signals, an 802.11 receiver will encounter considerable bit errors when trying to demodulate the 802.11 signals.

How much attenuation is acceptable? The mathematical method for determining this is to take into account EIRP (equivalent isotropically radiated power) and receiver sensitivity. Receiver sensitivity is different depending on whether you're using 802.11a or 802.11b and the data rate that users are operating. The higher the data rate, the lower the receiver sensitivity requirements. In other words, a receiver must be more sensitive to detect higher data rate signals.

For example, the EIRP of the source station could be 200 milliwatts (23dBm) and the receiver sensitivity would be -76dBm for 802.11b at 11Mbps. Thus, you can only afford to have 99dB of attenuation [23dBm -- (-76dBm)] before the signal drops below the receiver's ability to hear the signal. Thus at 200 feet from the access point, the user's 802.11b receiver will probably barely notice signals from the access point. If obstructions such as walls are present, then operating range will be less.

You can use these concepts to help with planning the location of access points. When setting up access points to operate near their maximum range, be aware that obstacles such as walls will offer additional amounts of attenuation that could cause loss of connectivity. For example if you're planning the range of a particular access point to be 200 feet, then having a few walls in between the access point and users will cause an additional 9dB or more of attenuation, which could likely be enough to push the signal power down below the receiver's sensitivity. As a result, place your access points closer together to ensure adequate coverage.

It's nearly impossible to accurately determine the range of wireless signals through indoor facilities without performing some live testing. As a result, be sure to accomplish an RF site survey to verify location estimates. The use of an 802.11 radio along with site survey software with successful test results proves that signal levels are above minimum requirements. Also consider using a wireless LAN analyzer, such as AirMagnet or AiroPeek to measure signal power at various points throughout the facility to ensure signal power levels are well above the receiver sensitivity.

EIRP Limitations for 802.11 WLANs

By Jim Geier

July 18, 2002

The spectrum regulatory body of each country restricts signal power levels of various frequencies to accommodate needs of users and avoid RF interference. Most countries deem 802.11 wireless LANs as license free. In order to qualify for license free operation, however, the radio devices must limit power levels to relatively low values.

In many cases, installers would prefer to use comparatively high transmit power to increase the range of access points. The problem, however, is that RF interference with other nearby equipment would occur more often. The RF spectrum is limited, so we must control the amount of power must we use.

The FCC makes the rules

In the U.S., the FCC (Federal Communications Commission) defines power limitations for wireless LANs in FCC Part 15.247. Manufacturers of 802.11 products must comply with Part 15 to qualify for selling their products within the U.S. Regulatory bodies in other countries have similar rules.

Part 15.247 provides details on limitations of EIRP (equivalent isotropically radiated power). EIRP represents the total effective transmit power of the radio, including gains that the antenna provides and losses from the antenna cable. You must take all of these into account when calculating the EIRP for a specific radio.

The gain of an antenna represents how well it increases effective signal power in a particular direction, with dBi (decibels relative to an isotropic radiator) as the unit of measure. dBi represents the gain of an antenna as compared to an isotropic radiator, which transmits RF signals in all directions equally. More precisely, dBi equals 10 times the logarithm (base 10) of the electromagnet field intensity of the antennas favored direction divided by the electromagnetic field intensity of an isotropic antenna (with measurements taken at the same distance).

Manufacturers determine the antenna's dBi value, so it's a relief we don't have to calculate it. What we do need to know, however, is that every three dBi doubles the power of an RF signal. As a result, higher values of dBi extend the range of a wireless LAN.

FCC tighter on mobile WLANs

A typical indoor WLAN consists of enough access points to cover the facility to enable wireless mobility for users. Radio NICs in user devices and access points generally have omni-directional antennas that propagate RF energy in most directions, which maximizes connectivity for mobile applications. When using omni-directional antennas having less

than 6 dB gain in this scenario, the FCC rules require EIRP to be 1 watt (1,000 milliwatts) or less.

In most cases, you'll be within regulations using omni-directional antennas supplied by the vendor of your radio NICs and access points. For example, you can set the transmit power in an 802.11b access point or client to its highest level (generally 100 milliwatts) and use a typical 3 dB omni-directional antenna. This combination results in only 200 milliwatts EIRP, which is well within FCC regulations.

FCC loosens up

The FCC eases EIRP limitations for fixed, point-to-point systems that use higher gain directive antennas. If the antenna gain is at least 6 dBi, the FCC allows operation up to 4 watts EIRP. This is 1 watt (the earlier limitation) plus 6 dB of gain.

The higher gain antennas have greater directivity, which propagate RF energy more in one direction than others. This reduces the possibility of causing RF interference with other nearby systems. Thus, the use of higher gain antennas, even if they result in higher EIRP, is acceptable. The users benefit by having greater range, and neighboring systems are much less likely to encounter RF interference.

For antennas having gain greater than 6 dBi, the FCC requires you to reduce the transmitter output power if the transmitter is already at the maximum of 1 watt. The reduction, however, is only 1 dB for every 3 dB of additional antenna gain beyond the 6 dBi mentioned above. This means that as antenna gain goes up, you decrease the transmitter power by a smaller amount. As a result, the FCC allows EIRP greater than 4 watts for antennas having gains higher than 6 dBi.

As you can see, the deployment of a wireless LAN for typical mobile applications using omni-directional antennas is fairly straightforward in terms of EIRP limitations. The problems come into play when installing systems to connect buildings within a metropolitan area. In this case, pay close attention to the FCC rules. You could find yourself violating the rules if you don't calculate the EIRP and see if you're within limitations.

Setting Up a Secure Wireless Network

Source: Intranet Journal Staff

Understanding the Basics

If you're thinking about building a wireless network for your home or office, it pays to do a little planning to ensuree you implement it as securely as possible. Remember how you listened to your next-door neighbor's conversation with her mother-in-law about what happened at last year's 4th of July party on your baby monitor? Like all radio frequencies, anyone with a receiver can tune into a wireless channel, so you need to take extra precautions to prevent to your big-eared neighbor and cybercriminals from listening in.

The primary reason for building a wireless LAN (WLAN) is for increased mobility — so you can move around from room to room without being tethered to a network jack. Another reason people like wireless LANs is because they can network their computers together without having to snake wires through their walls. Since you don't have to deal with the wires, in some regards building a wireless LAN is actually easier than you might think.

There are all different kinds of wireless protocols used for different types of wireless networks, but if you want to build a WLAN for your home or office the type of protocol you'll want to use is called 802.11b. When you build a wireless network, you are basically setting up a transmitter called an access point that has an antenna on one side and a wire on the other. The wire plugs into a typical wired connection — an Ethernet, a DSL line, cable connection, or dial-up modem. The antenna talks to the wireless network interface card on your computer, sending network traffic from your laptop to an access point. If it sounds confusing, think of your cordless phone. On one end your cordless phone plugs into a wire, while at the same time the antenna on the hand-held receiver transmits to the base station where the wire is plugged in.

Set Up Your Access Point

One of the first things you'll need to do is setup a wireless access point (AP). If you're setting up your wireless network for a business, you'll want to use a more fully featured high-end AP like a Cisco Aironet 350 Series access point. If you're setting up an access point for a home network, a low-end access point such as a Linksys WAP 11 or an Apple AirPort will suffice. Any access point worth its salt has a TCP/IP interface whether you are setting it up for your home or office, which is something to keep in mind when making your purchasing decisions.

When setting up your access point, you'll want to first connect it to the wired hub, then configure the wireless interface, then the wired interface, and last but not least, configure the security. Configuration of the various network interfaces and access point features is different for every vendor. However, if you can read and follow directions, it's possible to

do the installation yourself, even if you don't have prior experience. Just open the access point installation and configuration guide and follow along. If you run into snags call the vendor support line list in your access point manual and ask for help. The types of things you'll need to setup include the radio frequency, the distance between access points, and the access point IP address.

Some of the features you can expect to find in either home or enterprise class access points are listed in this table:

Feature	Small Office/Home Office	Large Office
IEEE 802.11b compliance	✓	✓
DHCP Server	✓	✓
Network Address Translation	✓	✓
IPSec Pass Through	✓	✓
IAPP		✓
Site Management Tools		✓
WEP (Security)	✓	✓
TKIP (Security)		✓

You can also use what is known as a wireless station instead of an access point. However, wireless stations may take a bit more work to setup, and I won't be talking about them further in this article. For more information on wireless stations can you check out http://www.live.com/wireless/unix-base-station.html.

Your access point is the link between the wireless world and the wire. So after you setup the wireless interface, you need to setup up the wired end of the connection — the Ethernet interface. When you configure the Ethernet interface, you will select the speed and duplex particulars. For many access points, however, the speed and duplex settings are self-setting.

Set Up Your Laptop

Since the purpose of a wireless network is mobility, it makes more sense to use a laptop (rather than a desktop) to connect to the WLAN. If the purpose of your WLAN is to avoid shoving wires through walls, it's possible that you may want to connect a desktop system or server to the WLAN. For the purpose of this article, we'll use a laptop to get you up and running. Your laptop will need a wireless network interface PCMCIA card. A wireless network interface card made by any reputable company should suffice. Some of the popular ones of the market today that you might want to consider include:

- Agere Wireless LAN PC Card
- Proxim/ORiNOCO Wireless Proxim ORiNOCO 11b Client
- Cisco Aironet 5GHz 54Mbps Wireless LAN Client

Wireless network interface cards have a 48-bit MAC address associated with them that is completely unique to each card. Installing the wireless PCMCIA card is really no more difficult than installing a regular PCMCIA card. In fact, all the new laptops running Windows operating systems should recognize the card and launch a Setup Wizard that will actually guide you through the installation process by prompting you to make certain decisions along the way. You'll need to install the device driver and enter the SSID associated with your access point.

Setting Up Security

If you have a low-end access point, your security will be limited to Wired Equivalent Privacy (WEP) and MAC address filters. With a higher end access point, you'll be able to turn on Temporal Key Integrity Protocol (TKIP). WEP is a system for encrypting your data to keep it private from unauthorized users. It was designed to provide privacy equal to what you get on a wired network. TKIP works on top of WEP, offering stronger security than WEP, and increased assurance that your data will not be compromised.

While it has been found that WEP does not offer strong security, it does offer some security, and any security is better than none. Therefore, you should turn WEP on no matter what. You can also layer more security, such as TKIP, on top of it. WEP uses secret keys that get combined with a keystream that then encrypts your data into ciphertext. At the receiving end, a corresponding keystream is used to decrypt the data.

WEP is used to authenticate you to the network and a component of it needs to setup on both the PCMCIA card and on the access point. WEP can be implemented in 40-bit mode or 128-bit mode. As you may suspect, using the 128-bit mode offers more security than the 40-bit mode.

TKIP evolved to solve some of the security problems that WEP does not solve. However, TKIP is relatively new, and many access points and wireless client cards do not support it. If you want to use TKIP, you'll need to be sure you purchase wireless access points and client cards that support it. With WEP, wireless hackers who have the will and time to do so, can obtain the encryption key need to unlock access to the data. In response to the vulnerabilities of WEP, a task group of the IEEE designed TKIP to add stronger security on top of WEP.

TKIP offers new encryption algorithms, and constantly changes the encryption keys making them harder for wireless hackers to capture them. Because the keys are constantly changing, if one of them gets captured, it won't do a hacker much good because by the time they try to use it, the wireless LAN will be using different encryption keys. With TKIP, the encryption keys are also encrypted themselves so you would first need to decrypt the key, before you can use the key to decrypt the network traffic.

MAC address filtering is used to limit what pieces of hardware can access the wireless network. On a large network, filtering the MAC address can be quite an administrative chore and it's worth using cards with sequential MAC addresses to make the job easier. If you want to use sequential MAC addresses, this is something you will need to specify when you make your purchasing decisions. On some wireless PCMCIA cards you can change the MAC address, but on many wireless PCMCIA cards the MAC address is fixed.

For even more security, you can also install a Virtual Private Network (VPN) on your wireless network. Unless you have truly sensitive information, it's probably not worth the time and effort to do this. By using a VPN, you tunnel your wireless data through an IPSec gateway. Using WEP, TKIP, and a VPN together will create a very strong security barrier on your wireless network. Using a VPN can create performance bottlenecks, so don't use one if you don't need one.

Summing It Up

Setting up a secure wireless network is not as hard as it may seem. Anyone with the ability to research wireless product capabilities, and follow the installation instructions can do it. The advantages of not using wires is tremendous, and while some organizations may be reluctant to use wireless networks today, in time they will become ubiquitous and wires will become history.

Maximizing Wireless LAN Performance

Source: (article by Jim Geier)

When wireless LANs first became available in the early 1990s, primary applications were wireless bar code solutions for needs like inventory control and retail price marking. Data transfers for these types of applications don't demand very high performance. In fact, 1Mbps data rates are generally sufficient to handle the transfer of relatively small bar codes for a limited number of users.

Today, enterprises are deploying wireless LANs for larger numbers of users with needs for corporate applications that involve e-mail, Web browsing, and access to various server-based databases. The need for higher data rates and techniques to improve performance of wireless LANs is becoming crucial to support these types of applications. To get that extra performance, you have a lot to consider.

Choose the Right 802.11 Physical Layer. An important element that impacts the performance of a wireless LAN is the selection of the appropriate Physical (PHY) Layer (i.e., 802.11a, 802.11b, or 802.11g). 802.11a offers the highest capacity at 54Mbps for each of twelve (maximum) non-overlapping channels and freedom from most potential RF interference. 802.11b provides 11Mbps data rates, with only three non-overlapping channels. 802.11g will eventually extend 802.11b networks to have 54Mbps operation,

but the three non-overlapping channels limitation will still exist. Of course requirements dictate needs for performance, which will point you toward a particular PHY. If you need maximum performance, then 802.11a is the way to go, but you may need more access points because of the weaker range it has compared to 802.11b.

Properly Set Access Point Channels. The 802.11b standard defines 14 channels (11 in the U.S.) that overlap considerably, leaving only three channels that don't overlap with each other. For access points that are within range of each other, set them to different channels (e.g., 1, 6, and 11) in order to avoid inter-access point interference. You can also take advantage of the automatic channel selection features that some access points offer. I often see companies setting their access points all to the same channel. The problem with this is that sometimes roaming will not work as users move about the facility, and the transmission of a single access point blocks all others that are within range. As a result, performance degrades significantly. With 802.11a, this is not an issue because the 802.11a standard defines separate, non-overlapping channels.

Provide adequate RF coverage. If access points are too far apart, then some users will be associating with the wireless LAN at something less than the maximum data rate. For example, users close to an 802.11b access point may be operating at 11Mbps; whereas, a user at a greater distance may only have 2Mbps capability. In order to maximize performance, ensure that RF coverage is as spread out as possible in all user areas, especially the locations where the bulk of users reside. The completion of an effective RF site survey will aid tremendously with this exercise. The proper setting of transmit power and selection of antennas will also aid in positioning access points for optimum performance.

Avoid RF interference. Cordless phones and other nearby wireless LANs can offer significant interfering signals that degrade the operation of an 802.11b wireless LAN. These external sources of RF energy in the 2.4GHz band periodically block users and access points from accessing the shared air medium. As a result, the performance of your wireless LAN will suffer when RF interference is present. So obviously you should strive to minimize sources of RF interference and possibly set the access point channels to avoid the interfering signals. Again, an RF site survey will help you discover interference problems before designing and installing the wireless LAN. If it's not possible to reduce potential interference to an acceptable level, then consider deploying 5GHz, 802.11a networks.

Consider RTS / CTS. The optional request to send / clear to send (RTS / CTS) protocol of the 802.11 standard requires a particular station to refrain from sending a data frame until the station completes a RTS / CTS handshake with another station, such as an access point. RTS / CTS reduces collisions associated with hidden nodes and may improve performance. Collisions can occur when hidden nodes blindly transmit when another station (blocked by some obstruction or significant range) is already transmitting. This causes a collision and results in each station needing to retransmit their frames, doomed again by a possible collision due to the hidden node scenario. The outcome is lower throughput. If you suspect hidden nodes are causing collisions / retransmissions, then try

setting the RTS / CTS threshold lower through a trial and error process while checking the impacts on throughput.

Fragmentation. An 802.11 station can use the optional fragmentation protocol to divide 802.11 data frames into smaller pieces (fragments) that are sent separately to the destination. Each fragment consists of a MAC Layer header, FCS (frame check sequence), and a fragment number indicating its ordered position within the frame. With thresholds properly set, fragmentation can reduce the amount of data that needs retransmission. RF interference often causes only a small number of bit errors to occur. Instead of resending the entire data frame, the station implementing fragmentation only needs to retransmit the fragment containing the bit errors. The key to making fragmentation improve throughput is to set the thresholds properly. A threshold too low will result in smaller fragments (making retransmissions efficient), but the greater number of fragments requires substantial overhead because of the additional headers and checksums. As with RTS / CTS, use a trial and error process to set the threshold while keeping an eye on consequential throughput. If there is no appreciable RF interference, then it's best to deactivate fragmentation.

Overcoming Wireless Network Configuration Obstacles

Source: article by Ronald Pacchiano

I just purchased a new laptop computer to replace my outdated desktop. Instead of throwing out the old PC I decided I would clean it up and give it to my kids to use. I have a high-speed cable modem in a home office that I use for Internet access, which was previously connected directly to my PC. Now that we have two computers in the house, I would like to find a way to share the cable modem.

So on a recent trip to Costco I purchased a D-Link wireless router and PC card combo pack. The nice thing about this router is that it works with both wired and wireless networks. I connected the desktop directly to the router via an Ethernet cable and installed the wireless PC Card on my laptop. The desktop is now working perfectly with the wireless router, but I can't seem to get my laptop online.

After examining the transmission control protocol/Internet protocol (TCP/IP) settings of both PCs, I think I might have discovered the problem. It appears that my laptop is using an IP address of 169.254.255.2, while my desktop is using an address of 192.168.0.2. I double-checked my router settings, and the dynamic host configuration protocol (DHCP) server is supposed to be assigning IP addresses beginning with 192. I am at a loss to explain how the laptop is getting the 169.x.x.x IP address.

I'm concerned that I might be connecting to someone else's wireless network, because if I connect my laptop to the router using an Ethernet cable, everything works fine. What do you think the problem is, and how do I find out where this 169.x.x.x address is coming from?

A.

The cause of your problem isn't as ominous as you might think. Most importantly, the problem has nothing to do with you connecting to someone else's wireless network; rather, it has to do with the fact that your wireless network interface card (NIC) is not communicating properly with your router. This is a very common problem. In all of the times I've answered this question in the past, I've never really explained what mechanism is responsible for generating the 169.x.x.x IP address. This is actually the result of a feature built into most Windows-based operating systems called automatic private IP addressing (APIPA).

APIPA enables a computer to automatically assign itself an IP address when there is no DHCP server available to perform that function. You see, when a DHCP client boots up, it first looks for a DHCP server in order to obtain an IP address and subnet mask. If the client is unable to find the information, it uses APIPA to automatically configure itself with an IP address from a specific range that has been reserved especially for Microsoft by the Internet Assigned Numbers Authority (IANA). That IP address range is 169.254.0.1 through 169.254.255.254.

The client also configures itself with a default class B subnet mask of 255.255.0.0. The APIPA service will also continuously check for the presence of a DHCP server (every five minutes, according to Microsoft). If it detects a DHCP server on the network, APIPA stops and the DHCP server replaces the APIPA networking addresses with a dynamically assigned address.

Diagnosing Wireless Configuration Issues

Now that you understand where the 169.254.x.x IP address is coming from and why it has been issued, you also know that your wireless network adapter is not communicating properly with your wireless router (since it's not receiving a DHCP-assigned IP address). Your PC is working when used with the Ethernet cable, so I think it's safe to assume that your TCP/IP protocol has been installed and configured correctly. Therefore it must be a problem with the way you configured your wireless network. Any number of variables could be causing this situation. Let's take a look at few of the more common ones.

One of the biggest hurdles to getting a wireless local area network (WLAN) configured properly is wired equivalent privacy (WEP) and Wi-Fi protected access (WPA) encryption. I know you want your network to be secure, and I would never tell you to run your network without encryption, but during the configuration process it is significantly easier to get things up and running with encryption disabled. So the first thing I would recommend doing is disabling WEP/WPA.

Next, you should verify that both the router and the PC card are using the same service set identifier (SSID). The SSID is a unique 32-character identifier that differentiates one WLAN from another. All devices attempting to connect to a specific WLAN must use the same SSID. The SSID's function is similar to that of a wired network's Workgroup or Domain name, and a workstation will not be permitted to wirelessly connect to the network unless it can provide this unique identifier.

After that, you should confirm that both devices are set to broadcast on the same channel. There are 11 channels available, and I believe 6 is the default channel for most 802.11b products. It doesn't really matter which one you use, as long as they match.

Wireless networks also operate in one of two modes: Infrastructure or AdHoc. Your wireless adapter should be running in Infrastructure mode.

In AdHoc mode, a wireless client can communicate directly with other wireless clients without the need for an access point or router. In Infrastructure mode, an access point or router is needed for a wireless client to gain access to the WLAN. As a result, whenever there's a need for wirelessly sharing a cable modem or DSL connection, Infrastructure mode needs to be used.

Additionally, you might want to keep the laptop in the same room as the router, at least during the initial configuration, to minimize potential interference from concrete walls or steel beams.

Once your wireless adapter and the wireless router are configured correctly, the DHCP service will automatically assign it a suitable IP addresses. With the wireless network successfully configured, we can now enable WEP.

It is very important to remember that there are many different levels of encryption available, with the most common being 64- and 128-bit. Some products, like those from D-Link, can even support 256-bit encryption. I would recommend that you use the highest level of encryption that your hardware can support — in this case, 256-bit.

In order for encrypted devices to communicate with each other, they need to share a common key. Key types are typically made up of either HEX (Hexadecimal) or ASCII (American Standard Code for Information Interchange) characters. Both the wireless adapter and the router must be using the same encryption level and the same key type.

While this may sound simple enough, it is very easy to mistype a key or change an encryption level, which would completely disable your wireless network, so double-check everything during the configuration process. Remember, don't assume anything; verify for yourself that all of the required settings are correct.

This should be enough information to get you started. Follow these general guidelines, and you should find yourself online in no time.

WLAN Management Considerations

Source: (article by Jim Geier)

Wireless LANs are certainly the wave of the future for business networking. Everywhere you look, there is a company deploying a wireless local area network (WLAN) into their daily operations. And as they do so, many companies are finding out that they must now manage it.

If an organization can not effectively manage their WLAN, benefits quickly diminish and it becomes more of a cost burden than savings. This is where network management software comes into play. Wireless network management software gives a company the ability to get the best possible performance and tightest security from their WLAN.

WLANs have Different Needs

WLANs are built on technology that is fundamentally different than that of wired networks. As a result, you can not manage WLANs in the same way. Plus, the ever evolving security challenges and technological innovations of WLANs make wireless management software even more of a necessity.

Wireless network management software will let you get the maximum performance from your WLAN, while making it as secure as possible. For example, management software will constantly monitor every access point in a WLAN, giving instant feedback so a network administrator can constantly tweak the wireless network, keeping it as fast and secure as possible.

Identifying Rogue Access Points

Analysts estimate that 30 percent or more of access points in business settings are unsecured, rogue access points. Employees deploy most of these access points for personal benefit, but the access points can unintentionally make the network vulnerable to attacks by hackers. Manual detection of rogue access points can be very expensive and time-consuming, as well as not very thorough.

Wireless network management software, on the other hand, can automatically detect every rogue access point and pin-point its location, saving money and dramatically improving security. The software locates the rogue access points by examining all of the routers and switches in the network and applies a series of tests and filters to determine which access points are supposed to be on the network and which are rogue.

Monitoring Authorized Access Points

It is necessary to constantly monitor access point settings to ensure that they remain in compliance with current security policies and are performing well. Wireless network management software continuously monitors all of the access points in the network and alerts the IT staff if anything strange is going on. The IT staff can set the performance and security thresholds at any value they wish and change them at any time.

The management software can produce detailed WLAN performance reports, giving the IT staff a way to review and fine-tune the network. Some software packages also have auto-repair features, which automatically return the access points to their proper settings.

Attributes to Consider

Many companies are now offering WLAN management tools, such as AirWave, Computer Associates, Cisco, Symbol, and Wavelink, among others. When evaluating WLAN management software, there are certain attributes that distinguish a superior management solution. Consider the following features when shopping for WLAN management software:

- **Centralization**. The software should allow you to control everything from a central location. A network administrator should be able to perform activities such as configuration and monitoring of infrastructure, changing access point settings, and firmware upgrades from one terminal.
- **Multiple Vendor Support**. The software should support access point hardware from a variety of vendors, allowing system design flexibility.
- **Flexibility**. Easy upgradeable software is a definite plus. Software that can not change with the times is a poor investment.
- **Easy Integration with Existing Network Infrastructure**. It is always good when a product can integrate with a legacy system, because the company does not lose its existing investment. The software must also be able to integrate seamlessly with other network management software, such as HP's OpenView.
- **Ease of Use**. The software must have a user friendly operating environment, be easy to navigate, and provide adequate help when needed.
- **Automation**. When configuration changes are needed, the software must be able to automatically implement the changes over large groups of access points. This will eliminate the chance for human error and ensure uniform implementation of the changes.

Don't stop short after installing a WLAN. Be sure to consider the management tools required to ensure your network delivers maximum performance and security.

Careers at Airespace – *now Cisco* *(sample of careers in wireless and skills required)*

Level 3 Tech Support Engineer

Location
San Jose

Primary Responsibility
You will be working in a small, fast paced organization that is bringing exciting new wireless systems to market. We are looking for dynamic, self-driven individuals to support customers while simultaneously helping to build a superior support organization. An individual in this position will be expected to work all levels of support while we work on building out the processes and tools needed to exceed customer expectations. In addition, this individual will work closely with Engineering on all aspects of product development including but not limited to doc review, user interface review, alpha and beta test. Periodic trips to the field will be needed to go onsite to support customers. On Call duty to support the 7/24 service level agreements will also be part of this individual's responsibilities.

The successful candidate must have at least all of the following:

- Bachelor degree or equivalent experience
- Technical certification in Networking (eg. CCIE/CCNP)
- 3+ years of formal tech support experience
- 5+ years of experience in working with IP networking products as either a tech support engineer, network administrator, network consultant and/or field support engineer
- Able to administer Linux and Windows systems
- A self-starter
- Strong analytical and troubleshooting skills
- Basic network troubleshooting skills
- Strong written and verbal communications skills
- Work well with all types of customers
- Capable of working in fast paced, startup environment
- Work well under pressure
- Work well in cross functional teams
- Willingness to travel locally/nationally/globally
- Detail oriented
- Stable job history

Ideal candidates will have one or more of the following:

- 802.11 experience highly desirable
- Familiarity with RADIUS and Extended Authentication Protocols
- IP Network administration experience in complex environments with multiple VLANs
- Experience in configuring and troubleshooting routers/switches
- Familiarity with IPSEC/VPN clients and servers
- Experience with a network management system (NMS) application
- Experience with commercial and/or public domain analyzer tools for troubleshooting networking and security