

Architecting Next-Generation Networks



Produced Exclusively for Broadcom by



Chapter 3: Extending Enterprise Networks with Wi-Fi®	36
A Brief History of Wireless Networking	37
802.11 Legacy	37
802.11b	37
802.11a	38
802.11g	38
802.11 Everything Else	39
How Wireless Networking Works	40
Basic Operations	40
802.11 Legacy Specifics	42
802.11b Specifics	42
802.11a Specifics	43
802.11g Specifics	43
Broadcom Xpress Frame Bursting Technology	43
Radios Matter	45
Mixed 802.11b and 802.11g Environments	46
Building Wireless LANs	47
802.11b Architecture	48
802.11a and 802.11g Architecture	48
Wireless Security Concepts	49
WEP	49
802.11i	50
WPA	50
AES	50
802.1X	50
Putting It All Together	51
The Wired Weak Point	52
Architecting Secure, Next-Generation Wireless LANs	52
Prerequisites	52
Client Software Support	52
Hardware Support	53
Management and Maintenance Concerns	53
Summary	54

Chapter 3: Extending Enterprise Networks with Wi-Fi®

Wireless networking is arguably the most important advance in networking technology since Ethernet. Today, wireless networking is enabling a whole new range of devices and functionality. With wirelessly networked notebook computers and handheld devices, for example, employees can stay connected whether they are attending a meeting across the building or catching a plane across the country. And cell phones with built-in wireless networking are emerging to help companies cut costs and improve productivity by using Voice over IP (VoIP).

The state of wireless networking has evolved rapidly over the past several years. The good news for those who are considering implementing a wireless network is that the technology has reached a state in which there are well-defined standards and a widely accepted seal of interoperability to ensure that competing products work together. IEEE 802.11g has now emerged as the mainstream wireless LAN standard and new advances in the physical layer of wireless networking aren't expected before 2005. Measures to secure wireless network communications are also now well defined.

In addition, today's wireless LAN products are smarter and more flexible; thus, they will be able to more easily adapt to emerging standards and features. The easiest decision you can make is to buy portable devices that provide built-in wireless networking. For pocket-sized mobile devices such as handhelds, choose 802.11b, because it is the most common wireless networking standard and it enables lower power adapters than the higher-performance alternatives. Laptops and other portable computers, however, will benefit from the higher raw data rates of 802.11g, 802.11a, or, better yet, a dual-mode adapter that supports both 802.11a and 802.11g. Most manufacturers already offer these technologies built-in to new laptops, and you can upgrade older units by using PC Cards or USB adapters.

Innovations in CMOS technology have helped drive Wi-Fi® performance up while driving costs down. CMOS is the most widely used manufacturing technology in the world and the digital portion of most wireless networking chip sets is built in CMOS. With radios now designed in CMOS technology, chip-set suppliers are able to combine the entire wireless LAN solution onto a single chip. This recent innovation squeezes all the functionality, including the analog radio, onto a single piece of silicon. These devices enable wireless network-enabled handheld devices that are smaller, use less power and are less expensive.


In this chapter, you'll learn how wireless networking operates, why the technology is important, and how to tell the difference between a stable, future-proof wireless network and proprietary offerings that likely will not support your enterprise in the years to come.

A Brief History of Wireless Networking

Before you can start selecting wireless networking technologies, it is useful to know a little bit about where those technologies came from. Seeing the progression of wireless LAN technologies makes it easier to predict where wireless networking is going in the future and to determine which of today's technologies will provide the most stable, long-lasting solution for your enterprise.

802.11 Legacy

802.11 is the family of Institute of Electrical and Electronics Engineers (IEEE) specifications that address wireless networking. The first implementations of these technologies were capable of achieving speeds of 1Mbps and 2Mbps. Popular primarily in vertical applications, these original technologies didn't provide enough bandwidth for enterprise use. However, they did act as a proof-of-concept for the viability and market interest of wireless networking in general, and set the stage for significant advances.

 It's doubtful that you will see much original 802.11 in use these days unless you're working in an industry that has implemented a vertical solution based on the technology. Although 802.11 saw early popularity in applications such as manufacturing and healthcare, it wasn't widely implemented in mainstream enterprise environments.

802.11b

The IEEE approved two enhancements to the original 802.11 standard in 1999, 802.11a and 802.11b. 802.11b occupies the same 2.4GHz radio frequency as the original 802.11 specification, extending raw data rates to 11Mbps. It was the first major commercial success for wireless networking, primarily because it provided similar maximum data rates to 10Base-T Ethernet, making it viable for corporate use. Many manufacturers quickly released commercial 802.11b products, including 3Com, Apple, Cisco, Dell, Gateway, Hewlett-Packard and others.

The Wi-Fi CERTIFIED™ Designation


Although the IEEE created the 802.11 family of specifications, the organization doesn't enforce the specification or ensure that manufacturers create products that precisely meet the specification. To ensure that manufacturers produce implementations that are interoperable with other 802.11 devices, the Wi-Fi Alliance provides interoperability testing and a seal of approval.

Currently comprised of more than 200 member companies, the Wi-Fi Alliance's Wi-Fi CERTIFIED™ designation ensures that products claiming to be 802.11b compatible are, in fact, fully interoperable with other 802.11b devices. The Wi-Fi Alliance conducts rigorous tests of hardware and software to ensure compatibility before issuing the designation, providing consumers with confidence that all Wi-Fi CERTIFIED products will work with one another. Today, Wi-Fi CERTIFIED has been expanded to include 802.11g and 802.11a, and more than 1000 products have been Wi-Fi CERTIFIED to date.

Wi-Fi CERTIFIED has become so popular and widely recognized that it's harder to find products that don't carry the designation. Still, don't bother purchasing products that aren't certified should you come across any—the benefit of compatibility and specification adherence is worth looking for the Wi-Fi logo. Wi-Fi CERTIFIED is your guarantee of interoperability between devices.

802.11a

With 802.11a, the IEEE took the standard up to 5GHz, offering raw data rates up to 54Mbps. As with 802.11b, 802.11a provides for lower data rates to compensate for coverage, offering speed fallbacks to 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 9Mbps and 6Mbps. 802.11a products began appearing in 2001. The higher speed allows greater capacity, but the higher frequency means shorter range. The biggest issue for 802.11a is that its different radio frequency makes it incompatible with 802.11b, which has seen wide deployment throughout the world. These limitations have hindered adoption of 802.11a. As the market continues to evolve, manufacturers are releasing network adapters and wireless access points (APs) that support *tri-mode* operation—which means they support 802.11a, 802.11b, and 802.11g—or *dual-band*—which means they cover both 2.4GHz and 5GHz frequencies—allowing client devices to connect with whichever form of wireless networking is best at the time.

 The Wi-Fi CERTIFIED program requires manufacturers to indicate whether their certified product operates at 2.4GHz or 5GHz, making it easier for consumers to buy the right equipment for their needs.

802.11g

802.11g is the new mainstream wireless networking technology. Ratified by the IEEE in June 2003, 802.11g works in the same 2.4GHz range as 802.11b. 802.11g provides speeds of 54Mbps, with fallback to speeds of 48Mbps, 36Mbps, 24Mbps, 18Mbps, 12Mbps, 11Mbps, 9Mbps, 6Mbps, 5.5Mbps, 2Mbps and 1Mbps, if necessary. Like 802.11a, 802.11g is nearly five times faster than 802.11b. Its advantage is that it is fully backward compatible with 802.11b, making it the logical successor to that protocol. In fact, to carry the Wi-Fi CERTIFIED designation, 802.11g products must provide full backward support for 802.11b, ensuring a smooth migration to the new protocol.

54g™

54g™ is Broadcom's implementation of the 802.11g standard, providing maximum performance in speed, reach, and security. 54g™ products are fully 802.11g compatible and provide the fastest possible speeds allowed by that specification. 54g™-branded products offer extended ranges thanks to SmartRadio™ and the standards-based Broadcom Xpress™ technology, built-in Wi-Fi Protected Access™ (WPA) and Advanced Encryption Standard (AES) security (which we'll discuss later in this chapter). 54g™ products were the first to achieve Wi-Fi certification, and were included in the 802.11g Wi-Fi test bed that all other products are tested against for interoperability.



The Wi-Fi Alliance recently announced a new brand, Wi-Fi ZONE™. This brand is used to designate public wireless LAN access that is built using Wi-Fi CERTIFIED hardware. If your client device contains Wi-Fi CERTIFIED hardware, a Wi-Fi ZONE provides a place where you're ensured interoperability. You can find a list of places offering Wi-Fi ZONE access at <http://www.wi-fizone.org>.

It is becoming more common to find APs that support a variety of standards, including 802.11a and 802.11g. These APs make it easy to get connected no matter which type of equipment you have in your client device.

Dual-Band 802.11a/b/g

For the enterprise, dual-band is a compelling option when architecting your network. Client devices such as laptops can automatically select 802.11g or 802.11a, depending on traffic and usage patterns. Near the end of this chapter, we'll explore sample network architectures that leverage these devices to provide the most robust, future-proofed wireless network possible.

802.11 Everything Else

The 802.11 specification includes the three physical layer extensions described earlier, 802.11a, b, and g. In addition, each new extension to the standard must first be designed and approved by an IEEE task group chartered with moving the standard forward. The IEEE task groups that are working toward final specification include:

- 802.11d—Used in country-specific domains
- 802.11e—Enhancements to the media access control (MAC) layer, including quality of service (QoS) and packet bursting
- 802.11f—The Inter-Access Point Protocol (IAPP), which establishes communications between access points in a network so that clients can roam between them
- 802.11h—A 5GHz networking enhancement using dynamic channel/frequency selection and transmit power control for European compatibility
- 802.11i—Security enhancements
- 802.11j—Enhancements for use in Japan
- 802.11n—Higher throughput improvements



IEEE specifications typically require years of work and research and, sometimes, the specifications' goals turn out to be unreachable given current technologies, or those goals evolve enough that a new specification is warranted. In addition, pieces of a specification are sometimes implemented in the marketplace ahead of the full specification ratification. WPA and Broadcom Xpress technology, both of which we'll cover later in this chapter, are examples of how the IEEE draft specifications can drive product development even before full ratification.

Of these additional specifications, 802.11e and 802.11i provide the most important benefits to wireless networking in general. 802.11i is of particular importance, as it deals with security in wireless networking—a topic that has been a concern since the limitations and vulnerabilities of Wired Equivalent Privacy (WEP) became clear.

How Wireless Networking Works

Wireless networking occupies the same layer of the network as Ethernet. Whereas Ethernet (spelled out in the 802.3 standard) specifies the physical characteristics of an electrical transmission over copper wires, 802.11 specifies the physical characteristics of a radio transmission through the air. The basic purpose of wireless networking is to translate digital signals into an analog radio signal, then to receive that signal and convert it back into digital. Like Ethernet, wireless networking doesn't care about upper-layer protocols carried over the network and can transmit TCP/IP and IPX/SPX.

Basic Operations

There are two types of networks specified in the standard—*ad-hoc* and *infrastructure* networks. Most wireless LAN adapters in client devices are capable of establishing an ad-hoc network—a point-to-point connection between two clients; however, most networks are set up in infrastructure mode. In an infrastructure wireless LAN, which Figure 3.1 shows, clients transmit information to an AP. The AP acts much like a hub in a wired network, connecting several wireless clients to one another. APs also connect the wireless clients to a wired network, providing access to servers, printers, the Internet, and so forth.

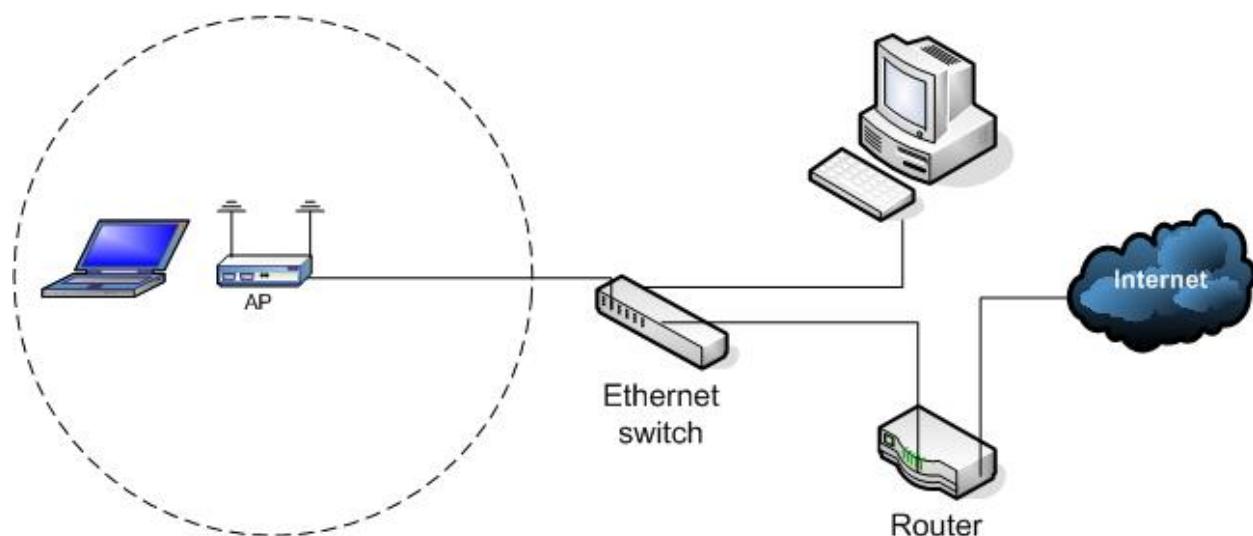


Figure 3.1: Simple WLAN configuration.

Engineering a wireless network requires careful placement of these APs to provide complete coverage. APs can—and should—have an overlapping signal area; clients will automatically select one AP, then select a new AP when moving out of range of the first. As Figure 3.2 shows, you might need to provide significant overlap for high-density areas, increasing the total amount of bandwidth available to the wired network.

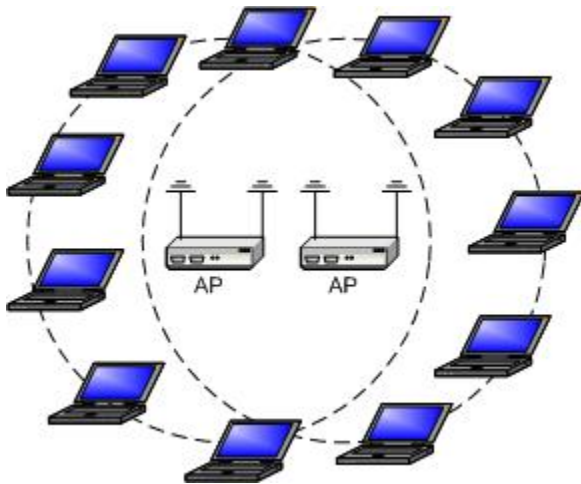


Figure 3.2: Overlapping APs provide more bandwidth for a larger number of clients.

Think of it this way: each 802.11g AP provides up to 54Mbps connectivity between wireless clients and the wired network. However, each 802.11g AP must share its available bandwidth with all the clients on the network. By adding a second AP in the same transmission area, some clients will be able to utilize that AP's connection to the wired network rather than the first AP's connection. A simple analogy is a highway: adding lanes won't increase the speed limit, but it will allow more cars to travel at that top speed.

Shared Bandwidth

An AP can only provide its maximum throughput to a single wireless client at a time. If there are two wireless clients within range, they will share that bandwidth, just as they would on a wired Ethernet segment. In fact, APs provide a function logically similar to Ethernet hubs, connecting wireless clients and allowing them to share the available bandwidth.

By contrast, Figure 3.3 shows what happens when APs don't provide sufficient coverage. Mobile clients may travel out of range of one AP before reaching another AP, resulting in a loss of connectivity. It's important to understand the transmission characteristics of your clients and APs and to thoroughly test AP placement when deploying a full-coverage wireless network.

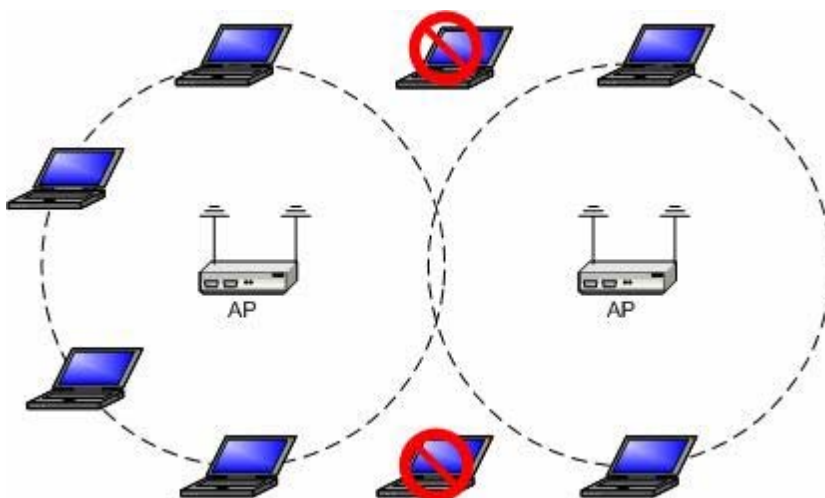



Figure 3.3: Insufficient coverage can cause a loss of connectivity.

 Hardware can make a big impact when it comes to coverage. Antenna design can be especially important, and add-on third-party antennas can be used to increase the range of a wireless network.

802.11 Legacy Specifics

The original 802.11 standard specified products in the 2.4 GHz frequency band and allowed both *frequency-hopping spread spectrum* (FHSS) and *direct-sequence spread spectrum* (DSSS) technologies. Products operate in the unlicensed Industrial, Scientific and Medical (ISM) band, which means that no license is required for operation, but they must accept interference from other ISM-band devices. DSSS basically provides a means for structuring the signal to be transmitted. The DSSS transmissions create a pseudo-random noise signal and add it to the signal being transmitted. The receiver—which knows the noise sequence—can filter out the noise to retrieve the original signal.


The basic DSSS standard includes a 1Mbps and 2 Mbps mode of operation. To double the raw data rates to 2Mbps, a technique called *differential quadrature phase shift keying* (DQPSK) is specified. With DQPSK, phase shifts represent two-bit combinations instead of a single bit at 1Mbps, thus doubling raw data rates. The single-bit technique is called *differential binary phase shift keying* (DBPSK).

The 2.4GHz radio frequency of 802.11 allows for a nominal range of about 350 feet. The band allows for as many as 14 channels, depending on geography. With each channel reaching about 20MHz in each direction, there is only room for three non-overlapping channels in the 2.4GHz band.

802.11b Specifics

The 802.11b specification sticks with DSSS and a refinement called HR-DSSS. To reach the higher data rates, a scheme called *complementary code keying* (CCK) is used. CCK is basically a set of algorithms that enables each bit to represent an even greater number of bits. At its maximum, the raw data rate for 802.11b reaches 11Mbps with fallback to 5Mbps and the 2Mbps and 1Mbps of the original 802.11 specification.

Coverage is a significant consideration for deploying wireless LANs. Radio signals are affected by wallboard, metal, and other everyday materials. If a network can't hold a connection reliably at 11Mbps, it will fall back to 5.5Mbps, 2Mbps and 1Mbps. As a result, it is important to properly distribute wireless APs throughout a location to provide the best signal coverage.

 All range measurements for wireless networking are theoretical ranges; actual operating range depends on a number of factors, including antenna type, antenna location and orientation, interference and environmental factors.

802.11a Specifics

802.11a also uses a different transmission structure than 802.11b—*orthogonal frequency division modulation* (OFDM), which is sometimes called *discrete multitone modulation* (DMT). The technique has seen widespread use in other high-speed networking applications, namely a form of asynchronous digital subscriber line (ADSL). OFDM is highly resistant to noise and jamming and can be combined with other techniques to resist signal dispersion, burst noise, fading, and other transmission problems. Because 802.11a uses 5GHz radio frequencies, it has a shorter operating range than 802.11b. However, 802.11a is well suited for high traffic locations because it can support as many as 12 non-overlapping channels, so there are more channels available to support client devices.

802.11g Specifics

802.11g uses the same DSSS, HR-DSSS as 802.11b and adds the same OFDM modulation method as 802.11a. Like the original 802.11 and 802.11b, 802.11g supports a range of about 350 feet and three non-overlapping channels because it resides on the same 2.4GHz radio frequency.

Broadcom Xpress Frame Bursting Technology

There is growing demand for more bandwidth, yet a wireless LAN standard for data rates beyond 54Mbps is at least a year away. In the meantime, there are technologies available to improve efficiency, thereby increasing the effective bandwidth of today's data rates.

One such technique is called frame bursting. Frame bursting, an extension of a feature in an original version of the 802.11 specification, is included in drafts of the upcoming 802.11e QoS standard. Frame bursting improves wireless LAN performance by eliminating some overhead traffic. As a result, more of the limited bandwidth is available to send and receive data. Broadcom is one of the first wireless LAN chip set suppliers to offer frame bursting, and markets the feature as Broadcom Xpress technology.

Wireless networking provides a shared medium; all wireless clients within range of an AP share that AP's bandwidth, and the more clients you place on the AP, the less bandwidth each individual client will receive. More devices are going wireless—in fact, according to TechKnowledge Strategies, by 2007, 75 percent of the wireless networking chip sets produced will go into something other than notebook computers. Wireless VoIP phones, PDAs, notebooks, MP3 players, digital cameras and other applications will all compete for wireless bandwidth.

In addition, wireless clients never achieve the full speed of their network (wired networks don't either, though wireless networking overhead is more substantial). For example, in an 11Mbps 802.11b network, clients can't usually exceed 6Mbps actual speed due to networking overhead (there is also a difference between the *data rate* and the *throughput*, which we'll explore later in this chapter). Every packet transmitted incurs a small amount of overhead. Unfortunately, to maintain compatibility with older standards, overhead doesn't change much even as data transmission speeds increase. For example, an 802.11g network takes less time to transmit a data packet than an 802.11b network requires, but both networks incur about the same overhead in doing so.

Frame bursting is designed to help address this problem. The original 802.11 standard requires wireless LAN devices to pause after each transmitted frame, which is basically a packet prepared for wireless transmission. These pauses allow other devices a chance to signal their intention to transmit, keeping the network working smoothly. With frame bursting, the client that is sending data is allowed to send several frames in a row without pausing—thus decreasing the total overhead while transmitting a data packet. Figure 3.4 illustrates this process.

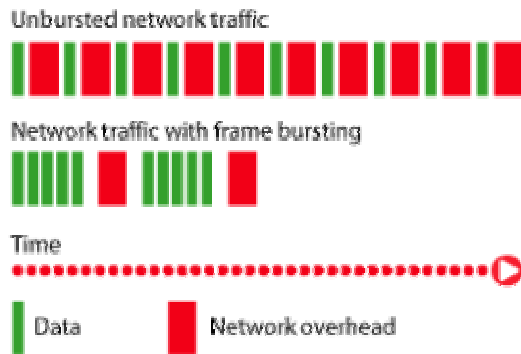


Figure 3.4: Unbursted vs. network traffic with frame bursting.




Note that transferring the data frames in 802.11g requires less time even though they contain the same amount of data; this benefit is one of the major features of 802.11g that allows it to achieve higher throughput.

Imagine a conversation in which you're required to pause for one second after every word to see whether anyone else wants to talk. If you wanted to say "nice weather we're having," it might only take half a second per word, but the entire phrase would require five seconds due to the pauses. In frame bursting, you would be allowed to get out as long as 1.5 seconds of words before pausing, meaning your phrase would only require 3 seconds—a savings of 2 seconds (a 40 percent savings).

The early 802.11 specification includes a feature called *fragment bursting* that essentially provided this savings for single packets that were divided into sub packets. Frame bursting is a standards-based technology that extends and implements this feature for multiple data packets. Frame bursting is also included in the draft 802.11e specification (in which it is called continuation transmit opportunity—CTXOP), which focuses on QOS issues such as prioritizing certain frames of time-sensitive traffic (such as streaming media). Industry leaders such as Broadcom and Microsoft are creating the Wi-Fi Multimedia Enhancements (WME), a subset of 802.11e that should be brought to market sooner than the full 802.11e specification. WME also includes frame bursting technologies.

As you can see in Figure 3.4, the performance improvement offered by Broadcom Xpress frame bursting is significant. Broadcom Xpress technology includes specific features to deal with mixed-mode environments (networks with both 802.11b and 802.11g clients). For example, in an environment with only one 802.11g client, Broadcom Xpress technology can result in an aggregate of as much as 23 percent performance improvement. With two clients, Broadcom Xpress technology shows as much as a 27 percent improvement, reflecting the savings of *both* clients eliminating some of their transmission overhead. With one 802.11g and one 802.11b client, as much as 61 percent performance improvement is possible—assuming only the 802.11b client is using Broadcom Xpress technology. In a mixed environment in which an 802.11g and 802.11b client both use Broadcom Xpress technology, the performance improvement is close to 75 percent simply by eliminating wasted transmission time.


Broadcom has introduced Broadcom Xpress technology through its OneDriver™ software, which makes frame bursting available for Broadcom's entire family of AirForce™ wireless networking products. These solutions are used in many of the major network and notebook brands.

 One advantage of Broadcom-based solutions is that the entire AirForce family (found in wireless LAN products from Apple, Dell, Hewlett-Packard, Linksys/Cisco, and others) utilizes a single software driver. This makes it easier for enterprises to maintain a single OS software image as product updates are deployed.

Radios Matter

Remember that GI Joe walkie-talkie you had as a kid? If your friend ran halfway down the block, you couldn't talk anymore, and you just couldn't imagine how the real military got by with such shoddy equipment. Obviously, the real military had better equipment, so the message is simple: all radios are not created equal. For that matter, not all digital signal processor (DSP) algorithms and antennas are created equal, and they all play an important role in the performance of wireless network hardware. One reason some notebooks seem to perform so well is that their wireless antenna is embedded in the notebook's housing and extends around the circumference of the display—providing a large antenna that tends to rise above desktop-level signal blockages.

CMOS radios are also an important technology. Because CMOS manufacturing techniques are designed for precision and reliability, CMOS radios lend themselves to consistently better performance than other chip-manufacturing technologies. First introduced in 2002, CMOS radios are the most common type of radio found in 54Mbps products. CMOS has a host of other advantages, including lower power and a smaller form factor, which helps to increase portable devices' battery life and make the technology easier to implement in a wider range of devices. Competing, more exotic technologies such as silicon germanium (SiGe) and gallium arsenide (GaAs) provide less sensitivity and higher power consumption and are typically more expensive to produce—increasing the price of the wireless LAN product you buy.

 Experts predict that, eventually, all wireless LAN radios will be CMOS. The cost savings, reliability and ease of manufacturing of the CMOS process is simply too significant. In the meantime, you can save yourself money and increase reliability by choosing wireless networking products that already incorporate CMOS radios, such as those from Broadcom.

When selecting radios, you should also look for features such as self-calibration, which enables the radio to adapt more readily to deal with walls, extended ranges and other conditions, providing consistently higher data rates without forcing the network adapter to fall back to a slower rate. Bluetooth®, a short-range wireless technology, uses the same 2.4GHz band as 802.11b and 802.11g, providing potential for interference, particularly when both technologies exist in the same device, as is becoming more common. Selecting solutions that are designed to work together, and ideally, integrated, allows them to cooperate rather than compete.

Mixed 802.11b and 802.11g Environments

If your goal is to build the fastest wireless network possible, you should be aware of a performance limitation imposed on an 802.11g network when 802.11b clients are present. 802.11g can only operate in its fastest mode when there is no need to support 802.11b devices; even a single 802.11b device will force the network into a slightly slower mode. 802.11g devices will continue to function at much higher data rates than 802.11b, but they won't reach their full throughput potential. This protocol for providing backward compatibility in mixed-mode environments is called protection mechanism, and it is part of the 802.11g standard.

Consider the network that Figure 3.5 shows, which includes two APs running on a single channel and four wireless clients. Three of the clients are 802.11g, and one is 802.11b. Because the two APs are on the same channel, they must activate protection mechanism to accommodate the 802.11b client, thereby providing support for both the 802.11b and 802.11g clients.

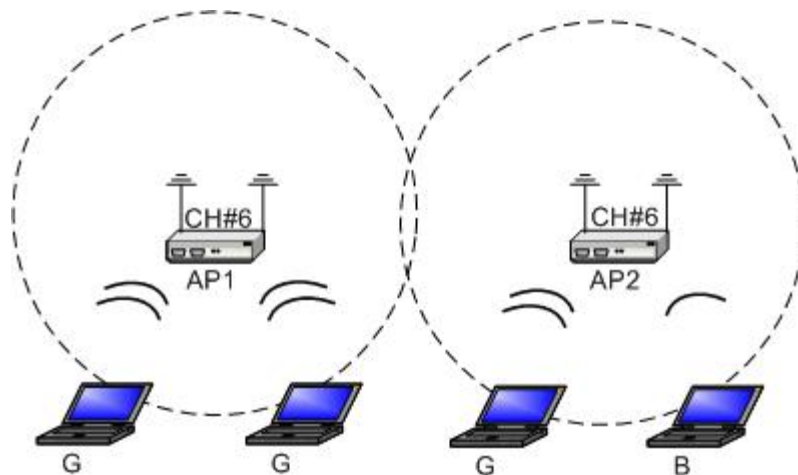


Figure 3.5: A single 802.11b client activates protection mechanism which slows the network.

Many industry observers expect that wireless networks will need to be prepared to deal with 802.11b traffic for years to come, as handheld devices that don't require the bandwidth of 802.11g can instead take advantage of inexpensive, lower-power 802.11b technology. However, if you want to provide maximum speed to your 802.11g clients, you'll need to build overlapping wireless networks on different channels, with one dedicated to serving only 802.11g clients. Figure 3.6 shows this setup.

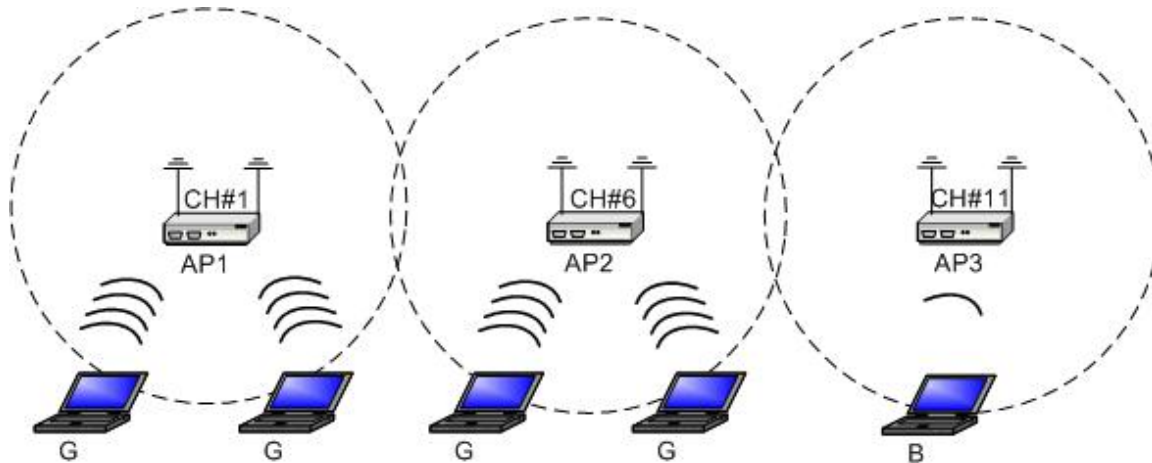


Figure 3.6: Different channels help maximize performance in mixed environments.

In this example, clients using the channel one and six APs will be able to run at full, native 802.11g speeds. Clients using the channel eleven APs will run either at 11Mbps (802.11b clients) or the slightly slower mixed-mode speeds (802.11g clients).

⚠ Don't expect 802.11b to go away just because 802.11g is available. Many devices, including PDAs and cell phones, simply have lower bandwidth needs and can do just fine with 802.11b. 802.11b is also less expensive to add to these devices, is available in single-chip implementations from manufacturers such as Broadcom, and has a long life ahead of it. Make sure your wireless network plans include 802.11b support.

Building Wireless LANs

Building a wireless network isn't totally different from building a wired one. Obviously, the key players in the wireless network are the APs, which provide a connection between your wired network and your wireless clients. Specific architecture strategies for the different modes and frequencies are a bit different, though, depending on your needs. In the next few sections, we'll discuss the major design factors and decision points for building a wireless network.

The Wired Connection

APs function as physical layer bridges, providing connectivity between disparate physical networks—specifically, wireless 802.11a/b/g networks and Ethernet wired networks. Some APs can also be configured to act as *repeaters*, simply picking up wireless signals and relaying them back to a wired AP, increasing the range of the wireless network.

Ad-hoc vs. Infrastructure

Wireless network adapters support a built-in *ad-hoc* mode designed to connect two adapters directly to one another. The wired equivalent of ad-hoc mode is an Ethernet crossover cable, and the mode is useful when you simply need to transfer a few files from place to place. Ad-hoc mode doesn't utilize APs.

Infrastructure mode comes into play with APs, allowing multiple wireless clients to connect to the AP, thereby connecting to the wired corporate LAN. Infrastructure mode is more like using an Ethernet hub.

Windows XP™ built-in wireless networking software will automatically detect APs that are advertising themselves, and generally requires users to take extra steps to establish an ad-hoc connection. The idea is that most users, most of the time, will want to use infrastructure mode to access the resources of a wired network (such as the Internet).

802.11b Architecture

Many corporations have already rolled out 802.11b wireless connectivity within their offices, and a large number of public “hot spots” are available that provide free or inexpensive wireless access. The networks providing this connectivity are generally simple. In most corporate environments, APs are placed near major areas of wireless LAN need: conference rooms, lobbies, cafeterias, employee lounges, and other areas in which mobile client devices are typically used. APs are wired back to the nearest Ethernet switch, providing connectivity to the wired network. Figure 3.6 is a simplified illustration of a typical 802.11b deployment. Note that a single 802.11b AP provides a maximum of 11Mbps data rate (not throughput), shared between all wireless clients within range.

To allow for a higher density of users and because 802.11b allows for three distinct non-overlapping channels, a configuration could be set up in which each AP handles one channel apiece. This setup provides an aggregate 33Mbps data rate shared in 11Mbps chunks with each 802.11b client on a particular channel. This type of configuration is appropriate for large conference rooms in which additional high-capacity users may be online at the same time. Many companies place APs so that their coverage areas overlap significantly around high-density areas such as large conference rooms, engineering labs, and so forth.

802.11a and 802.11g Architecture

802.11a and 802.11g each provide a maximum of 54Mbps shared bandwidth per AP. Like 802.11b, 802.11g provides for three non-overlapping channels, meaning a coverage area served equally by three APs can provide up to 162Mbps aggregate capacity. When architecting your network, however, be aware that any 802.11b clients within a channel will cause that channel to enable protection mechanisms that will result in lower bandwidth for the 802.11g clients (although they will still get better than 802.11b bandwidth).

802.11a, however, provides as many as 12 non-overlapping channels in a shorter, 180-foot range. This feature makes 802.11a ideal for especially high-density areas; as many as 12 APs can service a single coverage area, providing an aggregate raw data rate of 648Mbps. Although it is unlikely that many organizations will need that much bandwidth in such a small area, there are certainly applications—such as videoconferencing and other streaming media applications—that might make the additional dedicated bandwidth worthwhile.

One way to structure wireless networks is to deploy 802.11g (which also provides 802.11b support) to areas of normal usage, such as office spaces, smaller conference rooms, employee lounges, and so forth. You can then deploy multiple dual-band 802.11a/b/g APs to higher-density areas, such as cafeterias, larger conference rooms, or anyplace in which higher density may be required in the future. To begin, you can simply deploy one AP to each of these areas. As the need for additional aggregate bandwidth becomes evident, you can add more APs to the coverage area. If you adopt this strategy, make sure you're investing in tri-mode 802.11a/b/g clients, as well, so that your clients will be able to connect to the networks within range. You can then switch your high-density areas to provide primarily 802.11a coverage, because your clients will be able to roam between networks fairly easily.

Where Do You Need Coverage?

Your first big decision, of course, is to decide where you need wireless networking. Conference rooms, lobbies, and other meeting areas are obvious choices. Employee cafeterias and lounges may be other choices. Some companies go so far as to provide wireless LAN coverage in nearby public areas, such as an outdoor courtyard or picnic area. Large companies may also provide access at a nearby shopping mall's food court so that employees can check email while at lunch. This access may be in the form of a sponsored public "hot spot" or an extension of the company's own, authentication-required wireless network.

You'll also need to decide how much wireless coverage you need in your regular office spaces. Some companies figure that their desktop and other office computers are all wired, so there's no need to invest in additional APs. However, employees coming back from a conference may not plug their laptops into a dock or other network connection right away; providing at least minimal AP coverage in the office areas will ensure that these employees can continue to work without interruption.

Wireless Security Concepts

The idea of broadcasting your data into the air can be a little scary. After all, even though wired networks are far from immune to attack, they at least have the advantage of being physically difficult for outsiders to access. Wireless networks send your data outside your walls, where any passerby could easily eavesdrop. Another new problem brought by wireless networks is *war driving*, through which less-than-scrupulous individuals look for unsecured wireless networks and hijack bandwidth, wasting your corporate resources for their own uses. Fortunately, wireless LAN security has come a long way and is able to address these problems.

WEP

The original 802.11 specification included WEP. The intent of WEP was to make the wireless LAN connection secure through an encryption scheme. WEP required an encryption key to participate in the network. As it turned out, there were two critical flaws with WEP. First, the encryption key was static and shared by the entire network, so it proved to be easy for a computer to crack. Second, WEP provided no means of authenticating users who were approved for network access.

It was clearly time to improve upon WEP, and the IEEE created the 802.11i project to address the two shortcomings. IEEE specifications can take a long time to come to completion, so the Wi-Fi Alliance stepped in. Together with the IEEE, the Wi-Fi Alliance created Wi-Fi Protected Access (WPA), which addresses both of WEP's shortcomings and is available today.

802.11i

Currently in draft status with the IEEE, 802.11i is designed to shore up wireless LAN security with a comprehensive specification. 802.11i is being built around 802.1X port-based authentication, which we'll explore later in this chapter. 802.11i is nearing completion and should be ratified in mid-2004 according to the current pace of work. Two critical components of 802.11i are AES, a new cryptographic standard created by the United States government, and WPA's authentication scheme.

Prior to 802.11i's ratification, however, the Wi-Fi Alliance announced WPA, a new part of the Wi-Fi CERTIFIED program. The alliance requires WPA support for new products to earn the Wi-Fi CERTIFIED designation.

WPA

WPA uses the Temporal Key Integrity Protocol (TKIP), which is a bundle of data encryption features. Keys are derived differently than with WEP and are rotated frequently to prevent any one key from becoming overused and potentially compromised. WPA also adds message integrity checks to prevent forged packets.

AES

AES is a new cryptographic standard supported by the National Institute of Standards and Technology (NIST). It supports key sizes of 128, 192, and 256 bits, and serves as a replacement for the aging Data Encryption Standard (DES), which supports 56-bit keys. AES is a faster encryption algorithm than the now-common Triple-DES; a DES enhancement that basically encrypts data three times for better security. NIST describes AES as "...a symmetric block cipher that can encrypt and decrypt information." The estimated time required for modern computing equipment to crack an AES-encrypted block is 149 trillion years, compared with 4.6 billion years for Triple-DES.

AES is a significant component of 802.11i, and encrypting and deciphering every packet that comes in or out of a wireless client device or AP is a significant task. Fortunately, AES can be implemented in hardware, where it is extremely fast and places virtually no overhead on the client OS. Broadcom networking products carrying the 54g™ logo include complete on-hardware AES for full compatibility with future standards and high performance.

802.1X

An IEEE standard based on Extensible Authentication Protocol (EAP), 802.1X provides port-level authentication for networks, especially wireless networks. The idea is to only allow authenticated users on the network, both to ensure privacy and to protect corporate network resources from being wasted by outsiders.

802.1X is designed to leverage corporations' existing centralized authentication resources, primarily through the use of the Remote Authentication Dial-In User Service (RADIUS). 802.1X takes EAP and ties it to the physical medium—Ethernet or wireless LAN. EAP messages are encapsulated in 802.1X messages and referred to as EAP over LAN (EAPOL).

For wireless networks, 802.1X has three primary components:

- The *supplicant*, which is the client software trying to be authenticated
- The *authenticator*, which is the AP (or, on an Ethernet network, a hub or switch)
- The *authentication server*, which is usually a RADIUS server, although 802.1X doesn't specifically require RADIUS

The supplicant attempts to connect to the AP, which detects the client and enables its port for communications. The port is placed into an unauthorized state so that only 802.1X-related traffic is accepted and forwarded to the wired network. The supplicant is then required to send an *EAP-start* message.

The AP responds with an *EAP-request identity* message, asking to obtain the client's identity. The supplicant then sends an *EAP-response* message containing the client's identity, which is forwarded to the authentication server. The authentication server uses whatever means it wants to authenticate the client. For example, in an all-Microsoft environment, the authentication server might be a RADIUS front-end to Active Directory (AD—Microsoft provides such a front-end, called the Internet Authentication Server, with Windows® 2000 and Windows Server™ 2003). The result is the authentication server sending an *accept* or *reject* packet back to the AP.

A reject packet will cause the supplicant's port to be shut down. An accept packet will cause the port to be placed into an authorized state in which all traffic is accepted and placed onto the wired network to which the AP is connected. The last bit of 802.1X comes at logoff, when the client sends an *EAP-logoff* message to shift the port back to an unauthorized state.

Putting It All Together

So where does it all fit together? The acronyms alone can be hard to keep up with; the following list provides a summary:

- WEP is the original, outdated, and less-than-secure data encryption technique featured in the original 802.11 standard. WEP does not address user authentication.
- 802.11i is the IEEE draft specification addressing wireless LAN security from both a data encryption and user authentication standpoint.
- 802.1X is a port-level authentication scheme used to authenticate clients to a wireless network. 802.11X provides the foundation for 802.11i.
- AES is the new encryption standard created by the United States government, replacing the older DES. AES is also referenced in the 802.11i standard.
- WPA is a subset of the 802.11i draft standard that IEEE and the Wi-Fi Alliance ordained to provide an immediate replacement to WEP, while the standards-setting body hammers out the final 802.11i standard. WPA includes most of the major pieces of 802.11i, including 802.1X, TKIP encryption, and the improved message integrity check (MIC).
- RADIUS is an authentication protocol often used in conjunction with 802.1X. RADIUS can be built as a front-end to other existing authentication services, such as AD.
- EAP is a generic authentication protocol. 802.1X builds on EAP to create a port-level authentication protocol. Several specific authentication protocols, built on EAP, already exist; more are forthcoming.

The Wired Weak Point

Keep in mind that all of these features only protect communication between wireless clients and their APs; as soon as the data hits the wired network, it's completely unprotected by wireless LAN security measures. If you're concerned about the security of your wired network—a valid concern especially for traffic transmitted over the Internet—you will need to continue to employ higher-level encryption mechanisms, such as IPSec, virtual private networks (VPNs) and Secure Sockets Layer (SSL).

Architecting Secure, Next-Generation Wireless LANs

The next-generation wireless network is at your fingertips. All the technology pieces are in place, and the products are available now, you just need to deploy them to start taking advantage of faster speeds, higher client densities, better security and more privacy.

Prerequisites

You'll need to have a few extra pieces available on your network in order to build tomorrow's wireless network. The first prerequisite is planning today for future wireless LAN implementations. Many new notebooks come with built-in wireless LAN capabilities. Be sure that all new notebook purchases include built-in 802.11g, an inexpensive option that is five times faster than 802.11b. Doing so will ensure connectivity in any 802.11b or 802.11g environment you implement. If budget permits, specify a/g clients. Adding wireless LAN connectivity later can be time consuming and expensive. The following list highlights prerequisites for an efficient and successful wireless network implementation:

- A good plan is the first thing you'll need. Know your business requirements, where APs are needed, and what type of wireless LAN devices you will be supporting. Understand your users' wireless LAN bandwidth needs and make plans to meet them. Also make plans to grow the wireless network as utilization increases.
- RADIUS is almost a must in a larger business environment. Fortunately, RADIUS implementations are available for almost any environment and can leverage your existing enterprise directory, if you have one.
- Central provisioning capabilities are useful. You will want to be able to centrally configure all your wireless LAN hardware from a single desktop, if possible.

Client Software Support

More and more client devices are being built to include 802.11b, 802.11a, and 802.11g hardware; make sure your OS can handle such hardware. Windows 2000 Professional and Windows XP™ include support for wireless networks as do Linux®, UNIX® variants, Mac and more. Wireless is becoming more popular in portable devices too, such as Microsoft® Pocket PCs and Palms. The next wave of portable devices to include wireless LAN will be digital cameras, MP3 players and VoIP phones.

Hardware Support

Although it has been mentioned several times, it is worth repeating: the quality of the wireless LAN hardware you select can be critical to your wireless LAN implementation—if not today, then tomorrow. Here are some tips:

- Look for AES that is integrated into the wireless networking hardware. Simply supporting AES isn't enough; implementing AES in a software driver will place additional unnecessary processing overhead on your client computers and APs, resulting in significantly degraded performance.
- Standardize on equipment that uses lower-powered, inexpensive and reliable CMOS radios. They will be the only choice a few years from now, so there is no reason not to make the smart choice today.
- Select equipment that rigorously complies with IEEE standards. Look for the 54g™ logo for maximum performance 802.11g, and Wi-Fi CERTIFIED logos to ensure the broadest possible range of compatibility, reliability, quality, and future-proofing.

Where Can You Get the Right Wireless Hardware?

Broadcom's pioneering wireless networking products provide a completely standards-based, forward-looking approach to wireless networking. In addition, Broadcom is the power behind many of the leading brands of wireless LAN products, including Apple, Belkin, Buffalo, Compaq, Dell, eMachines, Fujitsu, Gateway, Hewlett-Packard, Linksys/Cisco, Microsoft and Motorola.

Broadcom's hardware and associated software offers everything you need for a secure, stable wireless LAN solution: single-chip 802.11b components for small-device and low-power scenarios, integrated CMOS radios, AES embedded in the hardware, a universal software driver across a product family, superior radio technologies and much more.

Management and Maintenance Concerns

Wireless networks can bring a new level of management and maintenance concerns if you're not careful. The following list highlights tips for making your deployment easier to manage now and in the long term:

- Use centralized provisioning whenever possible. Some tools can provision compatible clients with wireless encryption keys, network settings and more, making it easy to configure clients without a trip to each one.
- Use your existing central directory for 802.1X. Most directories provide RADIUS compatibility.
- Select network hardware that can utilize a single software driver for an entire family of products, such as Broadcom's AirForce family of products. You will be able to maintain fewer OS images and lower your support costs by reducing environment variables.

Summary

While you're building your wireless network of today, take the time to build the wireless network of tomorrow as well. Future-proofing is possible, particularly when you select wireless LAN equipment that is designed to be forward-looking. The following list highlights specific considerations for wireless networking equipment:

- Standards-based—Look for Wi-Fi CERTIFIED equipment as well as equipment carrying the 54g™ logo. Wi-Fi CERTIFIED equipment meets the stringent specifications created by the IEEE and provides the best interoperability between varying brands of equipment. 54g™ equipment supports WPA.
- Dual-band—Look for 802.11a/b/g equipment—both APs and clients—that provides the most flexibility for a variety of networking situations. You will be able to continue to leverage any existing 802.11b investment while taking advantage of the unique strengths of both 802.11a and 802.11g.
- 802.11e implementation—Look for equipment that implements early drafts of the 802.11e specification, including frame bursting. This equipment is designed with the future in mind, so future software updates can provide complete 802.11e compatibility.
- AES encryption in hardware—Look for equipment that includes AES capabilities built-in to the hardware—such as devices carrying the 54g™ brand—because hardware AES support provides better performance with less overhead on client computers.

Today, wireless networking is one of the most exciting areas of networking. Wireless networks are becoming more secure than wired networks, as few wired networks today offer 802.1X port-level authentication and continuous encryption. Architecting wireless networks isn't difficult, and you can build a future-proofed network by choosing equipment that is built to today's standards while looking forward to tomorrow's developments.



Broadcom®, the pulse logo, Connecting everything®, 54g™, the 54g logo, AirForce™, Broadcom Express™, OneDriver™ and SmartRadio™ are trademarks of Broadcom Corporation and/or its affiliates in the United States and certain other countries. Wi-Fi®, Wi-Fi CERTIFIED™, Wi-Fi Protected Access™ and Wi-Fi ZONE™ are trademark of the Wi-Fi Alliance. Bluetooth® is a trademark of Bluetooth SIG. Windows®, Windows XP™, Windows 2000™ and Windows Server™ are trademarks of Microsoft Corporation. Linux® is a trademark of Linus Torvalds. UNIX® is a trademark of Unix System Laboratories, Inc. All other trademarks or trade names are the property of their respective owners.