April 2001
WHITE PAPER

# DEPLOYING 802.11B (Wi-Fi) IN THE ENTERPRISE NETWORK

With the growing availability of standards-based 802.11b wireless network components, wireless networks are becoming a key element of the enterprise network. 802.11b networks enhance existing wired networks by providing convenient access to network resources for workers carrying portable computers and handheld devices (both in the office and in public facilities such as airports and hotels), and for guests or temporary workers. A wireless network can also provide a cost-effective alternative to relocating physical Ethernet jacks in environments where facilities are moved or changed frequently.

Successful deployment of an 802.11b network in "infrastructure mode" (see sidebar) requires careful planning and network design. This process includes determining network applications, coverage requirements, number of users, client device types, and equipment selection. In addition, unlike wired networks, planners must assess environmental obstacles that can impede radio frequency (RF) signal transmissions.

### Infrastructure Mode vs. Ad hoc Mode

802.11b networks can be implemented in "infrastructure" mode or "ad hoc" mode. In infrastructure mode—referred to in the IEEE specification as the basic service set—each wireless client computer "associates" with an access point (AP) via a radio link. The AP connects to the 10/100-megabits per second (Mbps) Ethernet enterprise network using a standard Ethernet cable, and provides the wireless client computer with access to the wired Ethernet network.

Ad hoc mode is the peer-to-peer network mode, which is suitable for very small installations. Ad hoc mode is referred to in the 802.11b specification as the independent basic service set.

This white paper focuses on the infrastructure-mode 802.11b networks commonly implemented in enterprise networks.

This white paper reviews 802.11b standards and presents key deployment considerations to keep in mind when planning the wireless network.

## 802.11 and 802.11b Standards

802.11b extends the original 802.11 standard, which included specifications for 1- and 2-Mbps wireless Ethernet transmissions using spread spectrum RF signals in the 2.4-GHz Industrial, Scientific, and Medical (ISM) band. The transmissions use 100 milliwatts (mw) of transmitter power in North America (and less in other parts of the world). In the original standard, two different spread spectrum transmission methods for the physical layer (PHY)[1] were defined: Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). The 802.11b standard extends the original DSSS PHY standard to provide a theoretical maximum data rate of 11 Mbps.[2]

Spread spectrum technology is a modulation technique that spreads data transmissions across the entire available frequency band in a prearranged scheme. This type of modulation makes the signal less vulnerable to noise, interference, and snooping. Spread spectrum technology also permits many users to share a frequency band with minimal interference from other users and from devices such as microwave ovens.

### FHSS

With FHSS, a transmitting and receiving station are synchronized to hop from channel to channel in a predetermined pseudorandom sequence. The prearranged hop sequence is known only to the transmitting and receiving station. In the U.S. and Europe, IEEE 802.11 specifies 79 channels and 78 different hop sequences. If one channel is jammed or noisy, the data is simply retransmitted when the transceiver hops to a clear channel. 802.11 networks using FHSS are limited to 1- and 2-Mbps data rates.

[1] The physical layer (or PHY) is layer 1 of the seven-layer Open System Interconnection (OSI) network model.

[2] These are theoretical maximum data rates. Actual throughput varies and is usually less than 11 Mbps.

## DSSS

Under DSSS, each bit to be transmitted is encoded with a redundant pattern called a chip, and the encoded bits are spread across the entire available frequency band. The chipping code used in a transmission is known only to the sending and receiving stations, making it difficult for an intruder to intercept and decipher wireless data encoded in this manner. The redundant pattern also makes it possible to recover data without retransmitting it if one or more bits are damaged or lost during transmission. DSSS is used in 802.11b networks.

## Wi-Fi Certification Program

In a heterogeneous wireless network environment, it is important to select 802.11b standards-based wireless products that are interoperable. The main measure of 802.11b equipment interoperability is the Wireless Fidelity (Wi-Fi) certification program. (802.11b networks are sometimes referred to as Wi-Fi networks.) Administered by the industry group, Wireless Ethernet Compatibility Alliance (WECA), the Wi-Fi logo (shown in Figure 1) on a product certifies its interoperability with other products containing the logo. An independent lab, the Agilent/Silicon Valley Networking Lab performs the actual testing.

**Figure 1. Wi-Fi Logo**

The Wi-Fi interoperability program tests for association and roaming capabilities, throughput, and required features such as 64-bit encryption. WECA tracks standards developments and enhances the interoperability testing to reflect these advancements.

## 802.11b Options and Proprietary Extensions

Some vendors differentiate their 802.11 products with additional features. Some are options in the 802.11 standard such as 128-bit encryption, and some are proprietary features such as security/authentication schemes, roaming capabilities, key management, and "Power Over Ethernet."[3] Using or enabling proprietary extensions usually requires that the wireless equipment, including APs and network cards, be supplied by a single vendor. Proprietary extensions are not suitable for heterogeneous environments with a mix of hardware. Although the extensions provide specific benefits, they limit future flexibility. Before choosing to implement these features, it is important to assess all the environments that must be supported in addition to the corporate wireless LAN, including home office and public (airports and hotels) wireless LANs.

## Network Design

The first step in designing a wireless network is to determine the requirements for the network. This includes identifying the areas that need to be covered, the number of users and the types of devices they will use, applications, environment, and so forth. From these requirements, network designers can begin to determine how many APs are required and where they must be placed. The goal is to ensure adequate RF coverage to stationary and roaming users of the wireless network. A key activity of this design process is to perform a site survey to determine the required coverage; number, density, and location of APs; number of users; and channel selections. In addition, the site survey can identify conditions that inhibit performance through path and multipath loss, as well as RF interference.

Path loss refers to the loss of signal power experienced between the AP and the client system as the distance between the two increases. Path loss is affected by transmission distance; obstacles such as walls, ceilings, and furniture; and the frequency of the transmission. Generally, the higher the frequency of the signal, the shorter the transmission distance that can be achieved.

Multipath loss occurs as an RF signal bounces off objects in the environment such as furniture and walls while en route to its destination. The result is that an RF signal can take more than one path, arriving as multiple signals at its destination. This can impact performance significantly. Correct network design and the use of APs and client network interface controllers (NICs) with "an-

[3] Power Over Ethernet implementations allow the AP to derive its power from the wired Ethernet network, rather than through a separate power outlet.

tenna diversity" help to correct for multipath loss. The principle of antenna diversity is to combine (in an additive fashion) two or more relatively uncorrelated signals using several methods. In 802.11b networks, antenna diversity is implemented using two antennas with supporting circuitry to improve signal reception.

RF interference is caused by other RF sources that also operate in the 2.4-GHz frequency band. These sources can include microwave ovens and cordless phones. In addition, emerging Bluetooth™ personal area network devices operate in this frequency band and can interfere with 802.11 transmissions. (See **http://www.dell.com/r&d** for an upcoming white paper on Bluetooth technology, which includes a discussion of interoperability with 802.11 networks.)

AP placement is typically determined using a combination of theoretical principles and a thorough site survey. The site survey uses building plans and physical site tours to identify optimal placement of APs. The resulting plan should take into account usage patterns and adverse conditions that can impact performance. Under good conditions, an AP can provide coverage up to approximately 150 feet (46 meters) indoors. An example of an environment where this distance could be achieved is a relatively open environment with high ceilings and no hard-wall offices or other impediments to the RF signal. In this environment, the AP can be placed high to provide an unimpeded signal to the wireless clients. In office environments with walls (including cube walls) and other impediments, a more typical range is 75 to 80 feet (23 to 24 meters).

Once the APs are installed, IT personnel can test the implementation by roaming the premises with a laptop and observing variations in signal strength. A poor signal or poor throughput at a particular location would be an indication that an adjustment in AP placement, density, or channel selection is required.

## 802.11b DSSS Channel Design and AP Placement

The 2.4-GHz frequency band contains 80 MHz of spectrum. Each 802.11b DSSS channel typically occupies 22 MHz of bandwidth (although this can vary in different implementations), and a minimum of 25 MHz is required to minimize interference between channels.[4] Thus, the 80 MHz of available spectrum accommodates up to three equivalent-width, nonoverlapping 802.11b DSSS channels. This allows up to three 802.11b APs, each programmed with one of three noninterfering channels to be located with overlapping coverage areas. Figure 2 shows a typical configuration.

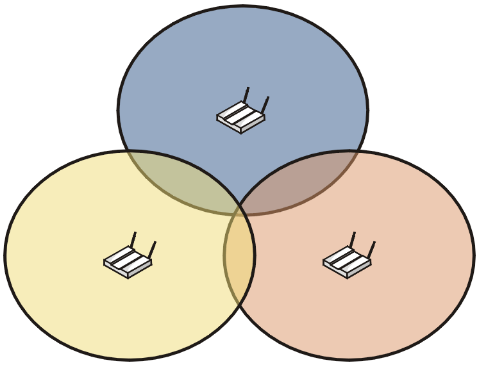


**Figure 2. Three APs with Overlapping Coverage**

## Scaling Capacity and Bandwidth

Figure 3 shows how "aggregate bandwidth" in a localized coverage area can be scaled from 11 to 33 Mbps to service a more dense population of wireless clients or to increase the bandwidth available to each wireless client in a coverage area.[5] In the example shown on the left in Figure 3, one AP provides up to 11 Mbps of bandwidth, which is shared by all wireless clients in the coverage area. As shown on the right in Figure 3, two more APs can be installed next to the original AP. Each provides an additional 11 Mbps of bandwidth to the same coverage area, for an aggregate bandwidth of up to 33 Mbps. (This solution does not provide an individual wireless client with 33 Mbps of bandwidth. In 802.11

[4] Interference is minimized, but not completely eliminated. In reality, each channel rolls off and can bleed into adjacent channels. The resulting interference is minimized through receiver design, including features such as antenna diversity.

[5] These are theoretical maximum aggregate bandwidth figures. Actual aggregate bandwidth will be lower, depending on the environment and the distribution of client systems in the coverage area. Typically, data rates fall as the wireless client computer moves farther from the AP out to the fringe of the coverage area. The rate of the decline varies depending on the AP and client NIC implementation, and physical characteristics of the environment.

networks, each client associates with only one AP at a time and shares its bandwidth with other clients associated with the AP.) This solution can increase bandwith to an existing population of wireless clients, because fewer clients share each AP's 11 Mbps of bandwidth, or it can provide additional capacity to support a denser population of wireless clients.

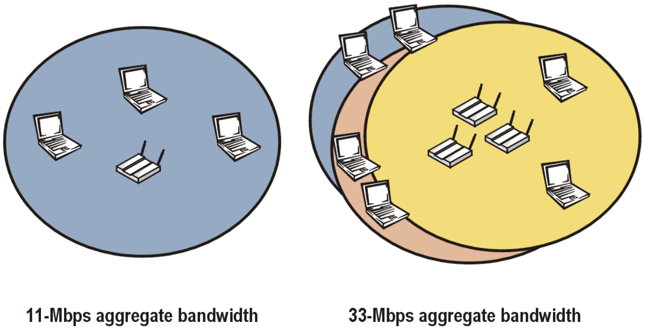
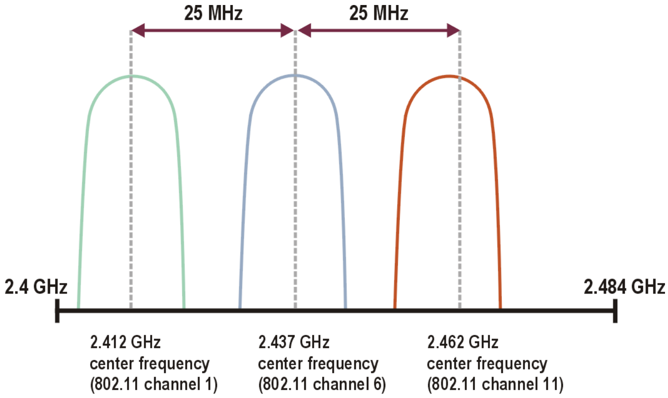


Figure 3. Scaling Aggregate Bandwidth from 11 to 33 Mbps in a Localized Area by Colocating Three APs

Capacity and bandwidth can also be scaled by reducing the size of the coverage areas. This approach is discussed in "AP Transmission Power" later in this white paper.

## Channel Selection

Within the 2.4-GHz frequency band, the 802.11 standard defines 14 "center frequency channels." Figure 4 shows a channel arrangement using channel 1 (2.412 GHz), channel 6 (2.437 GHz), and Channel 11 (2.462 GHz). Channels 1, 6, and 11 are commonly used to minimize the complexity of configuring and managing channels. These three channels, when laid out correctly, can accommodate large installations with many APs and clients.



Source: *The IEEE 802.11 Handbook: A Designer's Companion*

Figure 4. Nonoverlapping 802.11b Channels

Figure 5 shows a three-story building serviced by nine APs configured with channels 1, 6, and 11. The arrangement shown minimizes interference between APs located on the same floor, as well as APs between floors. It also eliminates the bandwidth contention that occurs when two APs with overlapping coverage are configured with the same channel. When this happens, 802.11 wireless Ethernet carrier sense multiple access/collision avoidance (CSMA/CA) mechanisms ensure that users in both coverage areas can access the network. However, instead of providing two separate 11-Mbps channels and an aggregate bandwidth of 22 Mbps, the two APs provide only one 11-Mbps channel.

## AP Transmission Power

The transmission power of most APs ranges from 1 mw up to 100 mw (in North America). Transmission power affects the effective range of the radio signal. The higher the transmission power, the longer the range of the signal (that is, the larger the coverage area). Higher power settings are appropriate in many large enterprise installations with cube-wall offices and a lot of open space. Lower settings are appropriate in environments such as test labs or small offices where the longer range is not required.

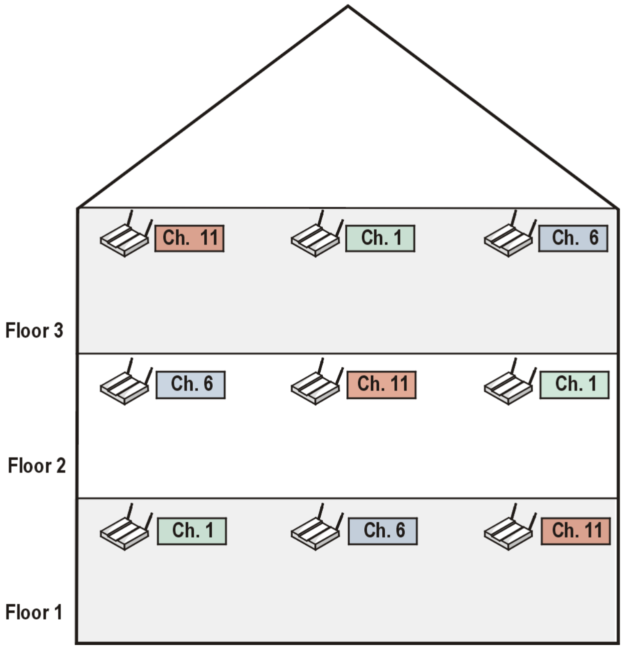


Figure 5. Sample Frequency Topology Using Channels 1, 6, and 11

Because lowering the transmission power reduces the range of an AP, lower power settings can also enable the wireless network to provide higher aggregate throughput. At lower power settings, more APs can be installed to serve a particular area than is possible at higher power levels. A coverage area serviced by three APs running at 100 mw and providing an aggregate bandwidth of 33 Mbps could instead be serviced by more APs transmitting at low power and providing more aggregate bandwidth. This approach might be appropriate in an area with a high number of wireless clients. However, the increased bandwidth must be weighed against the cost of additional APs.

## Security

Security mechanisms in 802.11b networks should be equivalent to existing mechanisms in wire-based networks. Wired network jacks are located in buildings already secured from unauthorized access through the use of keys, badge access, and so forth. A user must gain physical access to the building in order to plug a client computer into a network jack. In contrast, a wireless AP that is configured incorrectly may be accessed from off the premises (for instance, from a parking lot adjacent to the building). Properly designed wireless networks secure access to the APs and isolate the APs from the internal private network prior to user authentication into the network domain.

For a discussion of the current and upcoming access control methods available for 802.11b networks, read “802.11 Wireless Security in Business Networks” at **http://www.dell.com/r&d**. This paper reviews three approaches to securing access to an 802.11b network:

- Built-in 802.11b mechanisms—service set identifier (SSID), Media Access Control (MAC) address filtering, and Wired Equivalent Privacy (WEP).
- Virtual private network (VPN)-based security solution.
- Future solution based on the upcoming 802.1X security standard, which enables port-level access control.

## VPN

VPNs are commonly used today to provide remote workers with access to the enterprise network via the Internet. In addition, VPNs can be used to provide wireless clients with access to the wireless network. There are two main advantages of this approach. The VPN provides a secure and manageable access method, and users have a single VPN interface for remote and wireless access to the enterprise network.

### Public Access Via VPN

Users who travel may require remote VPN access to the enterprise network via public APs in airports and other public facilities. These APs are operated by third parties that provide access to the Internet and VPN access to the enterprise network.[6] These third parties provide the appropriate infrastructure for public access, and handle billing for the airtime.

These are heterogeneous environments, so Wi-Fi-certified client NICs are recommended. In addition, IT must provide infrastructure support for this type of access.

Because these networks are open to public access, appropriate security measures need to be taken to protect client data. Dell recommends a software firewall on wireless client computers to ensure adequate security. In addition, folder and disk sharing should be disabled in the operating system of the client computer.

## Managing 802.11b Networks

Two key components to a successful wireless network deployment are good management and monitoring tools. Providing a stable and manageable network infrastructure with effective support, problem detection, and problem resolution is dependent upon a good foundation of network products and tools. For the 802.11b wireless network, this includes utilities on the client computer that allow the user to monitor the health of their radio connection, and the infrastructure tools used by IT to manage and monitor the wireless network.

[6] Some of these services provide a direct Internet connection, while others provide Internet access using connection-sharing techniques such as network address translation (NAT). These connection-sharing techniques provide firewall protection to the client system, but can block some types of VPN traffic such as IPSec. In contrast, a direct connection does not block VPN traffic, but provides no firewall protection. In this case, it is especially important to have personal firewall protection on the client system.

## Client Tools

NIC selection for client computers can have a significant impact on support costs. For best results, choose client NICs with Wi-Fi certification of interoperability, as well as easy-to-use client utilities for diagnostics and determining the RF signal strength and quality. The user interface should be easy to use and should provide pertinent information on link status, network statistics, configuration options such as SSIDs, WEP keys, and so forth. It should also allow users to easily maintain multiple profiles and to switch between them as required.

## Managing Access Points

The task of managing APs can be broken down into management and monitoring/reporting. Management tools are typically provided with the AP and should be an important consideration when selecting the AP vendor. Monitoring and reporting tools are typically purchased separately and provide monitoring for a wide variety of network devices (including APs), often using standards-based agents such as the Simple Network Management Protocol (SNMP).

Management tools allow IT staff to perform initial setup and overall administration of an AP. Initial setup includes tasks such as configuring the device name, channel selection, SSID settings, IP addressing, security settings, and Ethernet settings. Administration includes tasks such as changing IP addresses and WEP settings, upgrading firmware, performing AP remote reboots, and analyzing AP network interfaces and AP client connections.

The AP management interface should be robust and should allow easy access to all configuration and management capabilities of the AP. These tools can be exposed through various interfaces such as a browser-based Web interface, command-line interface (CLI), software utility interface, and serial “console” interface. It is important to select wireless products with management tools that best meet the needs of a particular environment.

Monitoring and reporting tools can provide real-time monitoring and alerting, as well as trend reporting for wireless network devices. These tools can allow IT staff to track network device health and receive alerts of critical events or outages. IT staff can also monitor and store information over time so that longer-term network trends can be tracked and analyzed. Among other things, trend reporting is valuable when diagnosing problems and providing metrics to IT management. Purchasing high-quality monitoring and reporting tools is an integral component of any network deployment.

## Future 802.11 Technologies

There are several initiatives in progress to increase the data rates beyond 802.11b:

- In the 2.4-GHz frequency band, the IEEE is working on a higher data rate standard called 802.11g. The goal is to increase the data rate beyond 11 Mbps, and to maintain backward compatibility and interoperability with existing IEEE 802.11b products.
- In the 5-GHz frequency band, the IEEE is working on 802.11a. The goal is to achieve speeds of up to 54 Mbps.

Dell technologists continue to monitor wireless network trends and to participate in key wireless standards initiatives.

## Conclusion

Good network design techniques are required to successfully deploy an 802.11b (Wi-Fi) wireless network in an enterprise environment. These techniques include a thorough site survey, well-planned AP placement and DSSS channel design, and thorough testing of signal strength after the APs are installed. Wi-Fi-certified equipment minimizes interoperability problems. Finally, robust access control methods must be implemented and good management and monitoring tools put in place.

Dell is committed to providing wireless solutions that allow enterprise customers to implement reliable, standards-based 802.11b networks. Dell offers a full array of Wi-Fi-certified equipment, including APs and NICs for desktop and portable computers. The NICs are available in PC card format or integrated in Dell™ portable computers. These solutions allow customers to connect to the Internet from the office, from home, and while traveling.

## For More Information

- Wireless Ethernet Compatibility Alliance:
  **http://www.wi-fi.com**
- “802.11 Wireless Security in Business Networks,”
  **http://www.dell.com/r&d**

**Information in this document is subject to change without notice.**