



WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANs

Written By:

Lisa Phifer, Core Competence, Inc.

Philip Kwan, Foundry Networks, Inc.

September 2003

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANs

Introduction

The IronShield Best Practices: Deploying Wireless LANs document is designed to help network and security administrators understand the procedures and factors that go into the planning phases of an enterprise-class wireless LAN.

Contents

CONSIDERATIONS FOR 802.11 WLAN DEPLOYMENTS.....	3
UNDERSTANDING 802.11 WIRELESS LAN ALTERNATIVES	3
IEEE 802.11-1997/99: WLAN MAC AND PHY SPECIFICATIONS	4
IEEE 802.11B-1999: HIGHER-SPEED PHY IN THE 2.4 GHZ BAND.....	4
IEEE 802.11A-1999: HIGH-SPEED PHY IN THE 5 GHZ BAND.....	5
IEEE 802.11G-2003: FURTHER DATA RATE EXTENSION IN THE 2.4GHZ BAND.....	5
CHOOSING BETWEEN A, B, AND G	6
SELECTING THE RIGHT HARDWARE	7
SELECTING THE RIGHT SECURITY STRATEGY	8
AUTHENTICATION METHODS.....	9
DATA ENCRYPTION METHODS	10
COMMON WIRELESS SECURITY COMBINATIONS.....	10
WIRELESS AP PLACEMENT	12
UNDERSTANDING AND TUNING WLAN PERFORMANCE	13
CHANNEL ASSIGNMENT	14
POWER OUTPUT.....	14
ANTENNA SELECTION	15
DETERMINING REQUIRED BANDWIDTH	15
PERFORMING SITE SURVEYS.....	16
STEP 1: OBTAIN FACILITY MAP AND BUSINESS REQUIREMENTS.....	16
STEP 2: ASSEMBLE SITE SURVEY KIT	17
STEP 3: CONDUCT SITE VISIT	18
STEP 4: DOCUMENT SURVEY RESULTS.....	19
FINDING SITE SURVEY TOOLS.....	21
CONCLUSION.....	22
ADDITIONAL INFORMATION	22

Disclaimer

Although Foundry has attempted to provide accurate information in these materials, Foundry assumes no legal responsibility for the accuracy or completeness of the information. More specific information is available on request from Foundry. Please note that Foundry's product information does not constitute or contain any guarantee, warranty or legally binding representation, unless expressly identified as such in a duly signed writing.

Considerations For 802.11 WLAN Deployments

Deploying wireless local area networks (WLANs) based on IEEE 802.11 radio standards can be deceptively simple. Home users plug wireless routers into broadband links and start using them without further set-up. But, as we shall see, implementing a successful business-grade WLAN requires considerably more forethought and planning.

The factors to take into consideration when planning for an enterprise-class wireless LAN include:

- The bandwidth required to support wireless users and applications as well as the physical placement of the access points will help determine the number of access points your wireless network will need.
- The range, radio frequency (RF) interference levels, type of wireless clients, and the number of AP's that have to be deployed may dictate the radio technology that you'll implement.
- The office space layout, coverage area, and the number of users accessing the wireless LAN will determine where you place your access points.
- The type of authentication and security that your company's wireless security policy requires will help determine the complexity of your wireless rollout and the type of NIC cards and wireless client software needed.
- The size of the wireless network or the need to scale the wireless deployment in the future may have an impact on which vendor's wireless solution you purchase.
- The flexibility and the upgradeability of the hardware may have an impact on your choice of vendors.
- The price, 802.11 feature sets, management capabilities, and the ability to integrate the wireless network into your existing wired network may determine your choice of vendors.

This paper explains the differences between 802.11 radio standards, wireless security features, and how to design WLANs that can meet your needs for reach and performance. It explains how devices can be laid out and fine-tuned to optimize coverage and avoid sources of interference. The aspects of wireless security are discussed to highlight the differences in authentication, data encryption, and packet integrity technology which may affect the wireless technology selected. Finally, this paper describes how to perform a successful site survey, and includes links to free and commercial tools that can help you complete that task. If designed and implemented properly, wireless networks will provide many benefits and enhance user productivity.

Understanding 802.11 Wireless LAN Alternatives

One of the first steps in any successful deployment is to understand what IEEE 802.11 is and how 802.11a, 802.11b, and 802.11g differ from each other.

IEEE 802 is a family of standards that define physical media used to carry data between LAN stations, how multiple stations share each medium, and how data bits are framed for transmission. Ethernet LANs use IEEE 802.3 to carry data over cables between stations, hubs, and switches. Wireless LANs use IEEE 802.11 to carry data over radio waves that connect stations to access points (APs).

In Infrastructure WLANs, APs bridge traffic between wireless and wired LAN segments, letting wireless stations reach destinations inside company networks or the Internet. In Ad Hoc WLANs, a pair of stations connects directly with 802.11. Since Ad Hoc WLANs are rarely used in corporate networks, this paper focuses on Infrastructure WLANs.

Designing an Infrastructure WLAN involves distributing APs throughout the area where network access is needed so that radio waves will reach all users. 802.11 standards define several methods of modulating data into radio

waves; these methods affect maximum data rate, distance, and other spectral characteristics that are important to understand when designing a WLAN.

IEEE 802.11-1997/99: WLAN MAC and PHY Specifications

This standard serves as the foundation for all other 802.11 standards. It defines three physical carriers: Diffuse Infrared, Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS). Diffuse Infrared generates light waves in the 850-950nm range. FHSS and DSSS both transmit radio waves in the 2.4 GHz band, but in different fashions. These media do not interoperate with each other: one of these choices must be selected when deploying an 802.11 WLAN. Within two years, DSSS emerged as the industry favorite.

IEEE 802.11b-1999: Higher-Speed PHY in the 2.4 GHz Band

The 802.11b amendment focuses exclusively on DSSS. The 1997 DSSS standard uses Barker Code modulation to transmit data at 1-2 Mbps. This 1999 "high rate" amendment adds Complementary Code Keying (CCK, mandatory) and Packet Binary Convolution Coding (PBCC, optional) to transmit data at 5.5-11 Mbps. 802.11b also includes dynamic rate shifting from 11 to 5.5 to 2 to 1 Mbps to automatically adapt to changes in distance, interference, and other factors that affect signal strength.

Deploying an 802.11b WLAN does not require an exact understanding of how the Barker Code or CCK modulation works, but it is helpful to know how DSSS uses the unlicensed 2.4 GHz frequency ISM band. As shown in Figure 1, DSSS divides this band into 14 partially-overlapping channels. DSSS uses a technique called "chipping" to spread modulated data across each 22 MHz wide channel in order to tolerate some path loss.

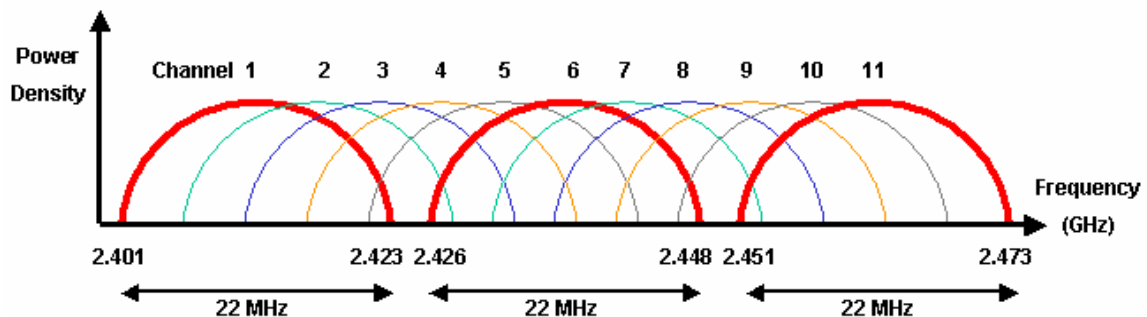


Figure 1: 2.4 GHz ISM Band Channels (US)

For example, a radio using channel 1 transmits data at 2.401 to 2.423 GHz. To avoid interfering with radios on adjacent APs, each radio should use non-overlapping channels. From Figure 1, we can see that gaps exist between channels 1, 6, and 11. Therefore, up to three (3) 802.11b APs can be harmoniously deployed on one spot.

Using DSSS, only one radio can transmit on a channel at any time. 802.11b uses collision avoidance to let several stations share each channel. A station that wants to transmit data can first send a very short Ready To Send (RTS) frame. When the channel is free, the AP responds with a Clear To Send (CTS) frame. The requesting station can then send data while other stations avoid transmitting. Because RTS/CTS frames add overhead, they should be used sparingly, such as when collision (error) rates are high.

IEEE 802.11a-1999: High-Speed PHY in the 5 GHz Band

Most existing WLANs are based on 802.11b. To further increase speed and reduce interference, the 802.11a amendment uses a new modulation method in a different frequency band.

Like the 2.4 GHz ISM band, the 5 GHz UNII band is available for use without a license. Unfortunately, the ISM band is shared by Bluetooth, other FHSS radios, cordless phones, and microwave ovens, creating many opportunities for interference (i.e., noise that increases loss). Although the UNII band is also shared by other devices -- notably radar systems and HyperLAN in Europe -- it is far less crowded.

The 5 GHz band is also wider, allowing more non-overlapping channels. As shown in Figure 2, 802.11a channels are centered 20 MHz apart in three discrete sub-bands with different transmit power limits. In the US, there are 12 non-overlapping channels defined between 5.15-5.35 GHz and 5.725-5.825 GHz. In some European countries, there are as many as 19 non-overlapping channels in the 5 GHz band.

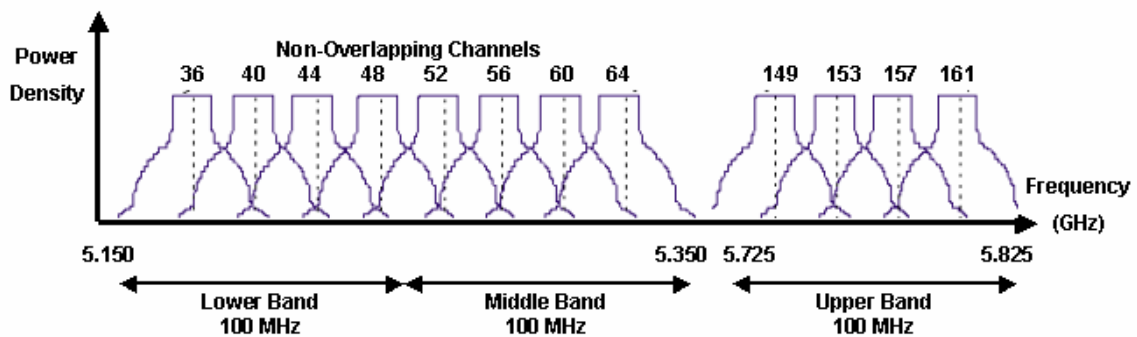


Figure 2: 5 GHz UNII Band Channels (US)

802.11a uses a more efficient modulation method, Orthogonal Frequency Division Multiplexing (OFDM), to encode more data within each channel, yielding a maximum data rate of 54 Mbps. Dynamic rate shifting adjusts data rate as needed from 6 to 12 to 24 Mbps (mandatory) and from 36 to 48 to 54 Mbps (optional). Some 802.11a chips also support a *turbo mode* that boosts the top data rate to 108 Mbps. Turbo mode can only be used between devices implementing the same proprietary turbo mode.

IEEE 802.11g-2003: Further Data Rate Extension in the 2.4GHz Band

Although 802.11a offers data rate, interference, and channel benefits, it has one significant limitation: using different bands prevents 802.11a radios from interoperating with 802.11b radios. The 802.11g amendment, ratified in June 2003, addresses this.

Like 802.11a, 802.11g employs Orthogonal Frequency Division Multiplexing (OFDM), but uses the 2.4GHz band shared by 802.11b. This lets an AP communicate at 54 Mbps with newer 802.11g stations and at 11 Mbps with older 802.11b stations with a single radio. To enable compatibility, 802.11g products support both OFDM and CCK modulation. They may also support two alternatives to achieve mid-range throughput: PBCC (the old 802.11b option) or CCK-OFDM (a new hybrid method).

When using OFDM alone, 802.11g is as fast as 802.11a. However, because 802.11g shares the 2.4 GHz band, it inherits limitations like ISM band interference and fewer channels. Therefore, companies that have no 802.11b stations at all may prefer using 802.11a.

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANS



But many WLANs will have 802.11b for quite some time. For example, most corporate APs will need to support laptops and PDAs shipping today with embedded 802.11b. When 802.11g products use the CCK-OFDM hybrid, RTS/CTS control frames may be required to share channels with 802.11b radios. In this kind of *mixed-mode* WLAN, 802.11g can achieve no more than 14.4 Mbps of effective TCP throughput, while 802.11g-only and 802.11a WLANs are capable of reaching 24.4 Mbps.

Choosing Between A, B, and G

To decide which kind(s) of 802.11 to deploy, consider business requirements for WLAN reach, application throughput, aggregate bandwidth, power consumption, etc. Table 1 summarizes the key differences between these three standards.

	802.11b	802.11a	802.11g
Maximum Data Rate	11 Mbps	54 Mbps	54 Mbps
Maximum TCP Throughput	5.9 Mbps	24.4 Mbps	24.4 Mbps
Indoor Range	~300 feet	~300 feet	~300 feet
Non-Overlapping Channels (US)	3	12	3
Access Point Density (Aggregate Bandwidth)	Lower	Higher	Lower
Noise / Interference	Higher	Lower	Higher
Power Consumption	Higher	Lower	Lower
Interoperability Testing/Certification	2000	2002	2003

Table 1: Comparing 802.11 Standards

In theory, 802.11a should have shorter range because higher wavelengths are more easily absorbed by intervening objects. However, research^{1,2} shows that indoor office reach is roughly comparable for all three standards. Three hundred feet is an approximate maximum; actual distance is affected by transmit power and environmental factors discussed later in this paper.

Note that maximum data rates (negotiated link speeds) are approximately twice the maximum effective throughput for TCP sessions (client/server application performance over wireless). This is due to the overhead incurred by frame headers, control traffic, and half-duplex network operation. As previously noted, 802.11g's maximum throughput is achieved in g-only WLANs, dropping when 802.11b stations are also present.

Although power needs are similar for all three standards, it takes longer to transmit any given file at 11 Mbps than at 54 Mbps. Therefore, 802.11b radios must transmit and receive for longer durations, consuming more total power. For example, the Atheros AR5001X chipset is roughly three times as energy efficient when using 802.11a instead of 802.11b³. Power efficiency can be an important design criteria for WLANs that include small footprint devices with limited battery life.

¹ *Indoor Propagation and Wavelength*, Dan Dobkin, WJ Communications, 2002.

² *802.11 Wireless LAN Performance*, Atheros Communications, 2003.

³ *Power Consumption and Energy Efficiency Comparison*, Atheros Communications, 2003.

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANS



As noted in Table 1, the Wi-Fi Alliance tests 802.11 products against reference implementations to promote interoperability. Certified products are important for WLANs that require multi-vendor support -- for example, when using laptops with on-board 802.11 from one manufacturer and APs by another manufacturer. Because 802.11g is newer, beware of products using non-certified pre-802.11g technology.

WLANs that require some combination of 802.11b, 802.11a, and 802.11g can use dual-band products that support all three protocols, in some cases simultaneously. Some products do this with separate radio cards; others use dual-band (tri-mode) chipsets that implement 802.11a and 802.11g/b.

Enterprise-class dual-band APs have the benefit of both higher-rate standards: 802.11a and 802.11g. They can support 802.11g/b stations at 54/11 Mbps and 802.11a stations at 54 Mbps (108 Mbps in turbo mode). By utilizing more non-overlapping channels, WLANs that use dual-band APs can provide much higher aggregate bandwidth, handling more stations in one location and/or applications that require higher data rates like voice and video.

Selecting The Right Hardware

There are many wireless vendors and solutions to select from when planning for a wireless network. Many products are designed for the small office home office (SOHO) environment while others are designed specifically for enterprise and business use. Most vendors will have a set of common features that adhere to the most common authentication, security, network, and radio standards, but enterprise-class solutions will have additional features to help secure and enhance wireless functionality.

When conducting research on which hardware to purchase, look for vendors that will support your current needs as well as your future needs. As wireless standards are ratified, the solution should be flexible enough to migrate or be upgraded effectively without requiring a repurchase of equipment. Some important areas to consider as you conduct your research may include:

Authentication features

- Does the wireless solution support the most common and latest authentication standards?
- Can the AP or WLAN switch be upgraded in the future to support newer standards such as 802.11i and AES?
- Will these upgrades be software/firmware upgrades or will they require hardware upgrades to the APs or WLAN switch?
- Does the solution support multiple authentication features for each radio (if multi-band radio is used)?
- What type of directory service can be used with the wireless solution's 802.1X authentication scheme?

Security features

- Does the solution provide the necessary encryption and packet integrity features to support the wireless LAN you are designing – both now and in the future?
- Does the vendor provide a solution for allowing visitors or guests to access the wireless network using a simpler security mechanism? Can the guest traffic be isolated from the regular employee data traffic?
- Can multiple data encryption schemes be used on the same access point - one for each radio to support different needs and provide backward compatibility with older wireless NICs?
- For high security installations, does the solution allow additional access control to regulate where the wireless user can go on the internal network once they have authenticated? Is there Dynamic VLAN or User Policy support?
- Can the system find and inform you of rogue APs and intruders who are trying to access your wireless LAN? With strong security deployed, is rogue AP detection or intrusion detection important features for your wireless LAN?

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANs



Networking features

- Can the AP be used on any Layer 2 network switch or does it have to be connected to the vendor's wireless LAN switch to function?
- Can the APs be used by itself for deployment in small remote offices or does it need to be managed by a local wireless LAN switch?
- How are the APs managed? Can they be managed individually, as group through a central management console, or through a wireless LAN switch?
- Which remote management protocols are supported and are the remote management protocols secure enough for your company's security requirements?
- What is the performance of the hardware if all of the desired security and authentication features turned on? As security is implemented, performance of the APs or WLAN switches may degrade.

Physical AP Features

- Is the AP dual radio capable to support 802.11a, 802.11b, 802.11g?
- Can the AP support extended features such as 802.11a Turbo for 108 Mbps speeds?
- Can the AP support dynamic channel assignment and does it have power controls for shaping the cell size and simplifying AP deployment?
- Can you control the number of users that can attach to the APs to offer performance SLAs?
- Is the AP's design modular allowing it to be upgradeable to newer radio technology when they become available?
- For companies installing the APs into false ceilings, is the AP Plenum rated?
- Does the AP support Power-Over-Ethernet 802.3af for easy installation?
- What are the typical distances and coverage areas provided by the AP's integrated antennas?

Vendor Criteria

- Pricing is usually a big consideration. Does the solution require more equipment than necessary to provide the features you are looking for? Does it require a dedicated WLAN switch for each wireless VLAN or can it use any Layer 2 switch for connectivity?
- The size and the stability of the vendor can play an important role in your decision. Is the vendor an established vendor or a new vendor to the market place? And what is their track record for delivering high quality solutions and support for their products?
- Is the vendor's expertise in one area or do they have other areas of expertise that can compliment their wireless solution?

There are many aspects to look at when deciding on which vendor to purchase from. Although pricing and the product's features are important, be sure to also consider the vendor's track record and their ability to support the products after the purchase.

Selecting The Right Security Strategy

The selection of the authentication, data encryption, and packet integrity security to deploy on your wireless LAN depends on several factors. Your company's wireless security policy, the type of data you are trying to secure, the complexity of the security solution you choose can all play a role in the type of authentication and data encryption scheme you choose. First, identify the security requirements that you will need to secure the wireless LAN. What are you trying to protect and who should be given access to the wireless LAN? Next, fully understand the benefits of each authentication and data encryption methods and the overhead that is required to deploy each security component. Lastly, test the security features that you have chosen with the client software and hardware and make sure they fit your needs. Once you are satisfied with the results, plan the deployment with your users and set up the necessary components.

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANs



Note: This white paper highlights the different authentication and data encryption options that are available for securing wireless LANs and does not go into great detail for each methodology. For more information on wireless security and how to select a wireless security scheme, refer to Foundry's "White Paper: IronShield Best Practices – Security & Wireless LANs".

Authentication Methods

Security schemes consist of authentication and encryption methods. Authentication is used to regulate access and control who can use the wireless network. Currently, there is a range of techniques that can be used and each has its advantages and disadvantages. The stronger the authentication, the higher the overhead in terms of hardware, software, and effort to roll out and maintain the security solution. The most common authentication methods for wireless LANs include:

- No Authentication
- Mac Address Filtering
- Shared WEP Key
- Pre-Shared Key
- 802.1X
- 3rd Party VPN Authentication

Some of these authentication methods can be combined together to create stronger security solutions. MAC Address Filtering is a separate authentication layer that can be applied to any of the other authentication methods. For example, small wireless implementations that do not need the complexity of a RADIUS server may choose Shared WEP Key authentication combined with MAC Address Filtering to control user access. For customers desiring stronger authentication, 802.1X with a secure EAP type may be the best choice. This can be combined with MAC Address Filtering in really high security deployments.

There is always a tradeoff between strong security and usability or ease of set up and rollout. Using a strong authentication scheme with 802.1X requires the selection of an Extensible Authentication Protocol (EAP) technology. Depending on your company's security requirements, the EAP method selected may complicate your rollout – especially if EAP-TLS is selected. The most common EAP types include:

- EAP-MD5
- EAP-TLS
- EAP-TTLS
- PEAP
- Cisco LEAP

EAP-MD5 is not as secure as the other EAP methods and should not be used for wireless authentication. On the other end of the scale is EAP-TLS. It is one of the most secure EAP methods and requires a unique PKI certificate for all authentication servers and wireless clients. 802.1X with EAP-TLS is also the most labor intensive authentication system to roll out and maintain. The security solution you choose will have some effect on the wireless hardware and software purchased.

Data Encryption Methods

Once you have selected an authentication method for your wireless LAN, you need to select an encryption scheme to protect your data packets traveling over the open airwaves. Some of these encryption schemes can only be used with specific authentication methods. And not all wireless network cards will support the strongest and latest security standards. If you already own wireless NIC cards, you should check with the NIC card manufacturer to see if they have software driver updates that will support your security choices. If they do not support the wireless security options you're planning to deploy, new NIC cards will have to be re-purchased.

To complicate matters, not all computer operating systems support the latest encryption methods. For example, WPA is not natively supported on all Microsoft or Unix operating systems. Third party 802.1X clients may need to be purchased if WPA is selected as your corporate standard for strong encryption. Each of the authentication methods can be combined with a data encryption method to secure the wireless LAN. The most common data encryption schemes available for wireless include:

- No Encryption
- Static WEP
- Dynamic WEP (also known as Rotating WEP)
- WiFi Protected Access (WPA with TKIP & AES-CCM)
- 3rd Party VPN Encryption

For enterprise-class wireless security, the minimum security standard that should be considered is Dynamic WEP. Dynamic WEP uses 802.1X to provide strong authentication and dynamically generates a unique WEP key for every user on the wireless LAN. Every time the user signs onto the wireless LAN, a new unique WEP key is created and assigned to the user's wireless client.

Static WEP's vulnerabilities are well publicized and there are many tools freely available to break into wireless LANs using this encryption method. For this reason, Static WEP should only be considered for wireless LANs that require low security – such as guest networks.

Common Wireless Security Combinations

As you can see, there are many security choices that can help secure the wireless airspace. As the need for security rises, the complexity of implementation and rollout also increases. When looking at the security features, you must also review what your existing wireless clients can support. Make sure that the client NICs are fully compatible with the security provided by the access point or WLAN switch. Earlier NIC cards may require a driver upgrade or may have to be fully replaced.

The most common enterprise-class authentication and security combinations are listed in the Table 2. Selecting the right security scheme will depend on the security requirements, the data being protected, and the type of service being offered by the wireless LAN.

Authentication Method	Encryption Method	EAP Needed?	RADIUS Needed?	Description and Comments
None	None	No	No	Wireless network is used as Layer 2 network with no security. Can be used for free access hot spots, guest networks with traffic VLAN'd to external network, or used with a 3 rd party VPN security solution.
Shared Key	Static WEP	No	No	Data security is not a primary concern and the ability to scale the solution is not required. Selected for ease of implementation over data security and authentication complexity. Good for guest networks and low security networks.
802.1X	WEP	Yes	Yes	Strong user authentication against a RADIUS server and unique encryption keys are generated randomly for each user per session. Requires more overhead to setup, but offers good security. Most client software and wireless NICs will support this method. Complexity of rollout depends on EAP type selected.
Pre-Shared Key	WPA	No	No	Strong data encryption is provided through WPA using TKIP or AES (multi-case cipher). Authentication is simplified through the use of pre-shared keys and scalability is compromised. Generally used in smaller wireless deployments where authentication simplicity is desired over deployment of a RADIUS server and 802.1X clients.
802.1X	WPA	Yes	Yes	Very strong security solution using a RADIUS server to authenticate each user and WPA with TKIP or AES to encrypt the data. Client NIC cards and drivers must support WPA and 802.1X clients and an 802.1X compliant RADIUS server must be deployed. Good for enterprise wireless LANs that require strong authentication of wireless users and strong data encryption. Complexity of rollout depends on EAP type selected.
MAC Address Filtering	Optional	Optional	Optional	MAC Address Filtering is a separate authentication scheme that can be applied to any of the security combinations already mentioned. It adds an additional layer of security but also adds maintenance complexity as lists of client MAC addresses must be maintained. MAC Address Filtering can be bypassed by hackers who understand MAC spoofing. Generally used with lower security schemes to provide a little extra security.

Table 2: Common Enterprise Security Schemes

Note: For more information on wireless security and how to select a wireless security scheme, refer to Foundry's "White Paper: IronShield Best Practices – Security & Wireless LANs".

Wireless AP Placement

Once you have decided on which 802.11 technology to deploy, selected the right vendor, and chosen the security scheme for your wireless deployment, the next step in WLAN design is to determine how many APs to purchase and the placement of APs to optimize network coverage, efficiency, performance, and security.

As radio waves propagate through the air, the wave front broadens and signal is scattered over an increasingly wider area until energy dissipates. Stations closest to the transmitter receive the strongest signal and can send data faster, while more distant stations receive weaker signal and must operate at slower rates. This inverse relationship between distance and data rate is illustrated in Figure 3, where three APs are used to create a WLAN covering one floor of a building.

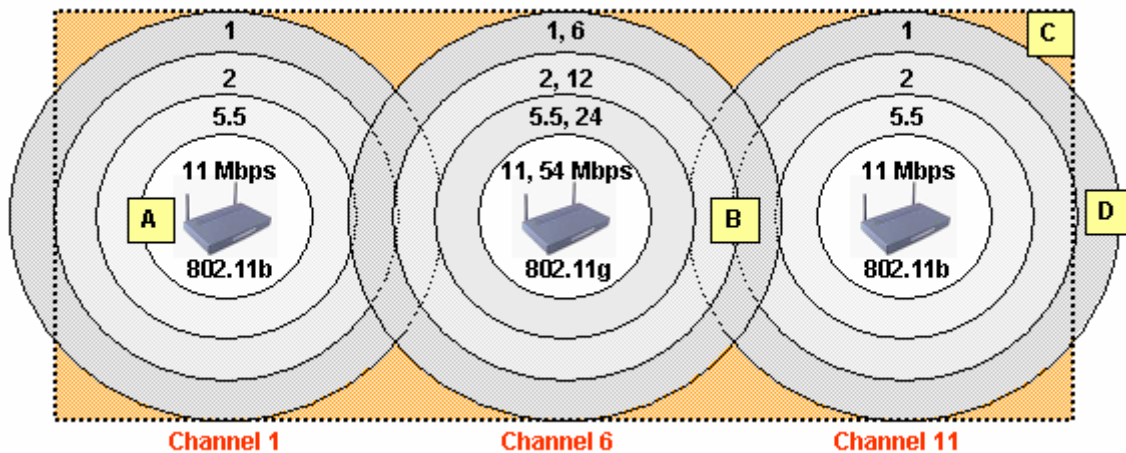


Figure 3: AP Placement, Data Rates, and Cell Overlap

Unless otherwise configured, 802.11 stations associate with (connect to) the AP that offers the strongest signal and highest data rate. If signal quality degrades, data rate drops automatically. When a station determines that conditions have changed and another AP now offers better signal, it reassociates with that new AP. For example, in Figure 3, station "A" will most likely associate with the 802.11b AP on the left. Station "B" will roam between the 802.11g AP in the middle and the 802.11b AP on the right, depending upon environmental conditions that affect actual signal strength.

Note that APs must be positioned with some coverage overlap to avoid "dead spots" (i.e., areas with no signal, shown here in orange). An optimum AP layout uses overlap to provide adequate throughput for all stations under normal conditions. In Figure 3, 2 Mbps or better should be available to all stations located along the horizontal center of this floor. Stations located along the top and bottom walls receive little or no signal -- for example, station "C" is located in a dead spot. Fortunately, corners and outside walls are often hallways and stairwells where coverage is not actually required.

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANS



So why not install more APs to provide higher throughput to all stations without any dead spots at all? This is a common question that is asked by many wireless planners. There are several things to take into consideration before deploying more APs into the same geographical area.

- Meeting business needs cost-effectively means getting the most out of each AP. In Figure 3, a high-throughput 54 Mbps *hotspot* is provided at this floor's center by deploying a single 802.11g AP. Alternatively, we could have placed both 802.11a and 802.11b AP(s) at that location. Locating more than one AP in the same spot is typically more expensive, but can support a high concentration of users (e.g., conference rooms) or high bit-rate applications (e.g., streaming video).
- Another consideration is operating efficiency. If AP coverage overlaps too much, stations in locations like "B" will repeatedly roam. Roaming for fixed stations should really be the exception, not the rule. When deploying multiple APs in one spot for high capacity/user density, choose APs that employ an inter-AP protocol to load balance associations between them.
- When coverage overlaps, co-channel interference causes signal degradation, resulting in data loss and reduced data rates. Assigning channels with maximum separation as shown in Figure 3 can minimize interference. However, 802.11 transmissions still bleed a bit outside the defined range for each channel, so some co-channel interference will exist. If unacceptable interference persists, reposition adjacent APs or reduce transmission power output.
- Note that station "D" is situated outside this building's perimeter, but within this WLAN's footprint. This illustrates the security risk created from radio signal leakage beyond intended coverage areas. Intruders or freeloaders in adjacent hallways, parking lots, or upstairs/ downstairs can take advantage of this and attempt to associate with your WLAN. Access control and authentication security measures should be used to completely address this risk, but risk should still be reduced through careful AP placement.

Understanding and Tuning WLAN Performance

Figure 3 illustrates data rate boundaries as perfect three-dimensional spheres. In reality, coverage is not this uniform. Signal strength and data rate can be affected by many factors.

Obstacles: As radio waves move through the air, they are absorbed by solid objects in their path, including wood, drywall, water, and human bodies. This *path loss* causes signal strength to be reduced, resulting in lower data rates and unexpected dead spots. Relocating APs can help -- for example, place APs in the center of a large open space instead of next to a solid-core wall or beneath a wooden desk. Alternatively, transmission power can be increased or external antennas can be used to better focus existing power output.

Interference: The unlicensed bands used by 802.11 radios can be shared by other transmission sources like Bluetooth, HiperLAN, microwave ovens, cordless phones, two-way radios, medical equipment, maritime surveillance systems, military radar, and neighboring 802.11 WLANs which may be on the floor above, on the floor below, next door, or across the street. Radio *noise* from these sources can increase error rates and degrade overall performance. In some cases, you can locate the source and eliminate the interference. Channel reassignment can improve signal quality by avoiding occupied frequencies. When broad-spectrum interference is present, using a different band (e.g., moving from ISM to UNII) may be the only effective option.

Multipath: As radio waves propagate, they bounce off reflective surfaces, causing copies of the same wave to arrive at the receiver at slightly different times. This phenomenon may cause signal to be amplified, reduced, cancelled out, or corrupted. To overcome multipath, relocate APs to avoid metal and other smooth, flat surfaces

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANS



and use APs with *diversity antennas*. Diversity antennas use the stronger of two incoming signals received through a pair of antennas, then transmit outgoing frames through the most recently used (better) antenna.

Near/Far: Stations transmitting with high power very near the AP may inhibit transmission by distant stations. This problem may be intermittent; the distant station's performance may be fine when other stations are silent, but degrade significantly when "louder" stations are active. To overcome near/far issues, reduce the power output of near stations or increase the power output of far stations.

Hidden Node: Two stations can be within an AP's coverage area without being within reach of each other. Recall that radio channels are a shared medium. Hidden nodes that cannot hear are more likely to cause collisions, resulting in loss, retransmission, and effective throughput degradation. RTS/CTS control frames can be enabled to overcome hidden node problems, at the cost of increased overhead for all data frames longer than a specified threshold. Alternatively, a station's transmit power can be increased or one of the hidden nodes can be relocated.

For many of these issues, relocating devices can be helpful, either during initial WLAN design or after. Fine-tuning can then be accomplished by adjusting channel assignments and/or power output as described below.

Channel Assignment

In most WLANs, APs are configured with fixed channel assignments, selected during network design to avoid co-channel interference. Some APs can automatically select an unused channel and then remain with that channel over time.

Some APs implement **Dynamic Frequency Selection (DFS)** to avoid frequencies that are occupied by other devices. DFS was originally defined to overcome 802.11a interference in the 5 GHz band. DFS chooses an apparently unoccupied channel to start, and then periodically listens for interference. When a signal greater than a detection threshold is encountered, the AP must retune itself to another (unused) channel within a specified time period.

Channel assignment is relevant for APs, but not usually for stations. Stations try to associate with any AP advertising a desired network name (Extended Service Set Identifier, ESSID). Stations roam across APs in the same extended service set as they move or respond to signal strength changes, changing channels as they roam. When separate APs support different user groups (e.g., corporate and visitor WLANs), stations locate the right AP by SSID, not channel. If there is a need to avoid roaming, stations can be configured to associate with specific AP(s), identified by MAC address, not by channel. In short, it is rarely useful or necessary to configure stations with channel assignments.

Power Output

Many APs and stations have variable transmit power settings that may be tuned during network design to optimize coverage. Transmit power may be increased to overcome high path loss, eliminate dead spots, and boost data rates. Transmit power may be decreased to reduce co-channel interference or leakage outside the desired coverage area.

Power settings are subject to regulatory constraints that dictate minimum and maximum outputs. For example, in North America, radios using the lower 5 GHz band can generate no more than 40 milliwatts (mW), while those using the middle 5 GHz band can output up to 200 mW. Maximum power in the upper 5 GHz band is 800 mW and is thus more suitable for outdoor use where greater distances must be spanned.

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANS



Transmit Power Control (TPC) allows 802.11 devices to operate more efficiently by automatically reducing power output. Like DFS, TPC was originally defined to facilitate international use of 802.11a. APs that support TPC broadcast beacons that advertise regulatory and local transmit power limits. Stations indicate their own minimum and maximum transmit power capabilities when they associate. Transmit power for the channel is then automatically adjusted for current conditions (e.g., path loss, interference), subject to regulatory constraints.

The power output from any transmitter passes through cables, connectors, and antenna elements before actually propagating through the air. Cables and connectors induce loss, while many antennas are designed for power gain. Output power is measured in milliwatts (mW). Loss and gain are relative measurements given in decibels (dBi). For example, a radio set to transmit at 10 mW with an antenna that yields a +6 dBi gain will actually generate 40 mW of Equivalent Isotropically Radiated Power (EIRP). Ultimately, it is EIRP (not just transmit power) that determines an AP's coverage.

Antenna Selection

Factory-default antennas can be replaced on APs (and sometimes stations) to adjust their coverage. External antennas can be positioned more flexibly -- for example, mounting antennas on ceilings or walls to provide coverage where you need it, while keeping the AP itself locked inside a wiring closet. External antennas can also focus output power in beneficial ways -- for example, spreading signal in an omni-directional sphere when placed in the center of a warehouse, or concentrating signal narrowly in one direction when placed at the end of a long, narrow hall.

The factory-default "rubber ducky" antennas included with most APs are omni-directional **Dipole** antennas. Dipole coverage looks like a squashed donut; power radiates horizontally but not out of the top or bottom of the antenna. An AP with a dipole antenna deployed on the second floor of a building will provide strongest signal to stations on the same floor, and weaker signal to stations on floors above and below, depending upon the AP's power output and the antenna's gain.

Directional antennas focus the AP's power output in one horizontal or vertical direction. **Patch** antennas are flat directional antennas, usually mounted on walls or ceilings. They produce hemispherical coverage 30 to 180 degrees wide, facing away from the antenna's mount point. **Yagi** antennas are cylinders that contain a boom crossed by thin vertical rods. Signal propagates off the front of the boom to create a narrow beam 20 to 80 degrees wide. The purpose of directional antennas like these is to improve WLAN performance without increasing risk of extending the radio coverage where it's not supposed to be or wasting power by sending available signal exactly where you need it. On the other hand, external antennas increase deployment cost and complexity, so they are not appropriate for every WLAN.

Determining Required Bandwidth

Another factor to consider is the minimum acceptable bandwidth that each wireless user should have. By default, the wireless client's 802.11 NIC will associate with the AP providing the best signal. If you have many wireless users concentrated in one area, a single AP may be supporting the majority of these users - limiting the available bandwidth as bandwidth is shared between all users that are associated with the AP. When one client transmits data, all others must wait before they can transmit.

When calculating the minimum bandwidth for each wireless client, you must take distance into consideration as well as the bandwidth supported by the AP. As clients move farther from the AP, the bandwidth capabilities will decrease. For example, if you wanted to ensure a minimum of 500 Kbps (actual maximum TCP throughput) for

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANS



each wireless user and you were using an 802.11a access point rated at 54 Mbps, the following calculation would need to be performed.

802.11a Maximum Data Rate:	54 Mbps
Actual Maximum TCP Throughput:	24.4 Mbps
Desired Minimum TCP Throughput:	500 Kbps (.5 Mbps)

Calculation to find number of supported users: $24.4 \text{ Mbps} / .5 \text{ Mbps} = 48.8 \text{ users}$

The performances that each of the 48 users would experience will also depend on the applications that are running over the wireless LAN and bandwidth patterns they produce. Large file transfers or applications that require a lot of bandwidth (streaming audio or video) will affect the performance for all users associated to the AP. Many enterprise-class APs will also allow you to limit the number of users that can be associated with each AP or radio. By limiting the number of associations, you can provide a level of service that is acceptable to your users. To provide additional coverage and capacity, you can install an additional AP in the same general area to help load balance the number of users that need to be supported.

Another commonly used formula to calculate the approximate bandwidth provided to each wireless user is:

$$(\text{AP's Maximum Data Rate} / 2) / \text{Maximum Users} = \text{Maximum Bandwidth per User}$$

For example, if the AP was programmed to support a Maximum Data Rate of 54 Mbps and it was programmed to allow 25 users to associate with it, the maximum bandwidth per user would be:

$$(54 \text{ Mbps} / 2) / 25 \text{ Users} = 1.08 \text{ Mbps per user}$$

To determine how many access points are required and where to place each access point, you should perform a site survey. The results of your site survey will help you determine the coverage patterns, capacity, channel selection and power requirements of each AP. Many enterprise-class APs can now minimize some of this work with Automatic Channel Selection and Power Control. When performing a site survey, take the minimum acceptable bandwidth into consideration. As you walk around the office to determine the coverage pattern and the signal strength of the AP, also note the maximum distance from the AP before an unacceptable performance level is reached.

Performing Site Surveys

Given a firm footing in 802.11 protocols, the basics behind wireless security, AP placement, minimum bandwidth requirements and related concepts like data rate shifting, channel selection, power output, the next step is to perform a thorough site survey. Any design created on paper must be refined to reflect the spectral characteristics of the planned deployment site. The purpose of a *site survey* is therefore to measure and document actual 802.11 behaviors to refine your design and satisfy user density, application throughput, coverage, and security requirements.

Step 1: Obtain Facility Map and Business Requirements

Before you can start plotting proposed AP placement, obstacles, and data rates, you'll need an accurate facility map of the building and floor(s) where WLAN service is to be deployed. Blueprints with actual layout and measurements are ideal. When creating a map by hand, draw rooms to scale and to include architectural

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANs



features like stairwells, elevators, and support columns. The geographic coordinates of the facility and these features can also be helpful.

Next, mark up the facility map to identify areas where WLAN users will be located, as well as public areas where coverage is explicitly undesirable. For intended coverage areas, it is best to start with a good understanding of user density, concurrent use, and application throughput and latency requirements. For example, in a modular office bullpen, identify how many stations will require WLAN access concurrently and what throughput will each require (average, maximum).

If users require non-stop WLAN access while roaming from one spot to another within the facility, it is important to identify spaces where contiguous coverage is required. For example, in a retail store, workers may need to perform price checks from any location. In a hospital, nurses and doctors may require access to patient charts from anywhere in a ward, but radio use may not be permitted from operating rooms or radiology labs. Understanding the business purpose of the WLAN is instrumental to appreciating coverage needs, performing an effective site survey, and circumventing dead spots to ensure successful deployment.

It is also helpful to identify the location of existing power sources and network equipment on your map. For example, where are wiring closets, LAN switches, and uninterruptible power supplies located? Are there existing 802.11 APs that must be integrated into (or coexist with) the new WLAN? Are there known sources of interference, like Bluetooth PANs, that the new WLAN must avoid disrupting? Plotting the location of these devices in advance can save time during an on-site visit by helping you understand what you will find there.

Obtain layer 2 and 3 (data link and IP) topology diagrams to understand where wireless APs will fit within the existing network. Although these diagrams come into play during network design, not the site survey, they can be useful to understand where APs are expected to connect to the wired LAN and the network naming conventions employed at this site for various buildings, floors, rooms, groups, etc.. Topology diagrams can also help to identify any need for wireless bridging (e.g., to connect separate buildings), in which case the site survey must include an analysis of possible locations for outdoor antenna placement.

Step 2: Assemble Site Survey Kit

During an indoor site survey, an AP will be placed in locations throughout the facility, plotting data rate boundaries, dead spots, and the impact of adjusting power output. To accomplish these tasks, you will need the following equipment and tools.

Access Point: It is convenient to use a dual-band AP with removable antenna and variable power settings to conduct site surveys. Perhaps even more important, consider bringing an AP similar to the make/model that you propose to deploy at this site.

Station: You will need at least one test station. A PDA can be more convenient, but may not run all the software and support all the radio options required. Ideally, carry both a laptop and a PDA, each with 802.11 adapters appropriate for the planned WLAN. For example, dual-band PC cards can be convenient for laptops, but a single-band CF card may be more "life-like" for a WLAN that must support small footprint handheld devices.

External Antenna and Mount/Cable/Connectors: Using an external antenna during a site survey makes it easier to position the transmitter on walls or hide above false ceilings, assuming that the survey AP can be connected to an external antenna. Because the cable length, connectors, and antenna all impact EIRP, be sure to document these in the survey results.

Battery Pack and Power Converter: It is possible to rely on local power sources during the site survey, but more convenient to bring a battery pack and DC-to-AC power converter. This lets you relocate the AP without worrying about wall sockets and extension cords. For laptops and PDAs, bring extra batteries and/or rechargers.

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANS

Adapter Client Software: Many 802.11 adapters are supplied with software utilities that monitor and display current data rate, channel, signal strength, and noise. These utilities provide a foundation to loosely plot data rate boundaries and sample ambient background noise. For small, informal site surveys, this may be sufficient.

WLAN Analyzer: To conduct more extensive surveys that require greater precision, invest in 802.11-capable WLAN analyzer software for your PC and/or laptop. These analyzers can automatically record signal and noise measurements and create a list of other wireless devices and the SSIDs and channels they are using. Many can be combined with a GPS to record the latitude and longitude associated with measurements.

Spectrum Analyzer: To understand and diagnose sources of interference in challenging radio environments (e.g., hospitals), a portable radio spectrum analyzer can be helpful. A WLAN analyzer may tell you that noise exists; a spectrum analyzer can help you pin down the noise source by examining frequency distribution.

Physical Measurement Tools: Survey kits must include tools to measure distance and location, like tape measures, string, measuring wheels, and (optionally) a handheld GPS.

Recording Tools: Finally, don't forget the basics -- your facility map, topology charts, graph paper, pencils, erasers, etc. Some analyzers and utilities can log site survey results on your laptop/PDA; when using these, establish naming conventions to make sense of results later.

Step 3: Conduct Site Visit

When scheduling a visit to conduct a site survey, request access to wiring closets, adjacent floors, and other locations that may require special permission. Arranging this in advance can save a return trip to complete the site survey. Similarly, adequate preparation during steps 1 and 2 will vastly increase the effectiveness of this on-site visit, so resist the temptation to jump ahead.

Starting with your map, tour the entire facility, and review or plot the location of noteworthy physical items, including wireless closets, power sources, elevators, and support columns (see step 1). Seek out probable radio obstacles like metal blinds, fire doors, solid core walls, and radiographic equipment. The goal is to verify and complete the facility map. The more advance planning done, the faster this will go.

During this tour, carry your laptop or PDA with WLAN analyzer software in channel-scanning mode (i.e., hopping across all channels, recording all APs or stations discovered). This output provides a starting point for further analysis. The goal is to identify all sources of potential interference, including SSID, channel, MAC address, signal strength, and (when using a GPS) location. When performing a survey without a GPS, systematically watch signal strength and attempt to walk in the direction of the transmitter until you find it -- be prepared to look upstairs, downstairs, and outside.

The next step is to rigorously plot AP coverage (data rate boundaries, signal strength, noise level, signal to noise ratio, dead spots). Place the AP in a likely/proposed location, such as the center of a large open space or on the wall at the end of a long, narrow room. Working from the edge of the room (or from the AP), move slowly towards (or away from) the AP. Use your measuring wheel and record signal strength, noise, and data rate at regular intervals. Also record distances where data rate drops; these are your data rate boundaries. Again, some analyzers make this easier by logging this information. Repeat this in all directions for each 802.11 protocol that you may consider deploying until you cover the entire facility and all proposed AP locations.

During this process, document dead spots and crosscheck against business requirements to make sure you have examined coverage in both required and undesirable areas. For example, check for *back lobes* that extend behind a directional antenna, outside the room or facility. It can also be helpful to sample effective application throughput between the station and the AP. If it becomes clear that throughput or coverage requirements are

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANs



not met by initial AP placement, move the AP/antenna and/or adjust the power output to assess the viability of likely alternatives. Repetition may be time-consuming, but a thorough survey that examines several alternatives is often needed to optimize the WLAN's design.

Step 4: Document Survey Results

The output of a site survey typically includes the facility map, marked up to show proposed AP placement, data rate boundaries, signal, noise, signal-to-noise ratio, effective throughputs, dead spots, sources of interference, and problem areas where security risk exists or performance requirements are not fully satisfied. As WLAN design is completed, recommended channel assignments and power settings should be added to this map.

Figure 4 illustrates output from a site survey -- specifically, maps documenting data rates, signal-to-noise ratios, and (implied by the absence of coverage) dead spots. Additional diagrams would be used to show other measurements. The more precise the site survey and the more sources of interference/loss discovered, the less uniform diagrams like these will be.

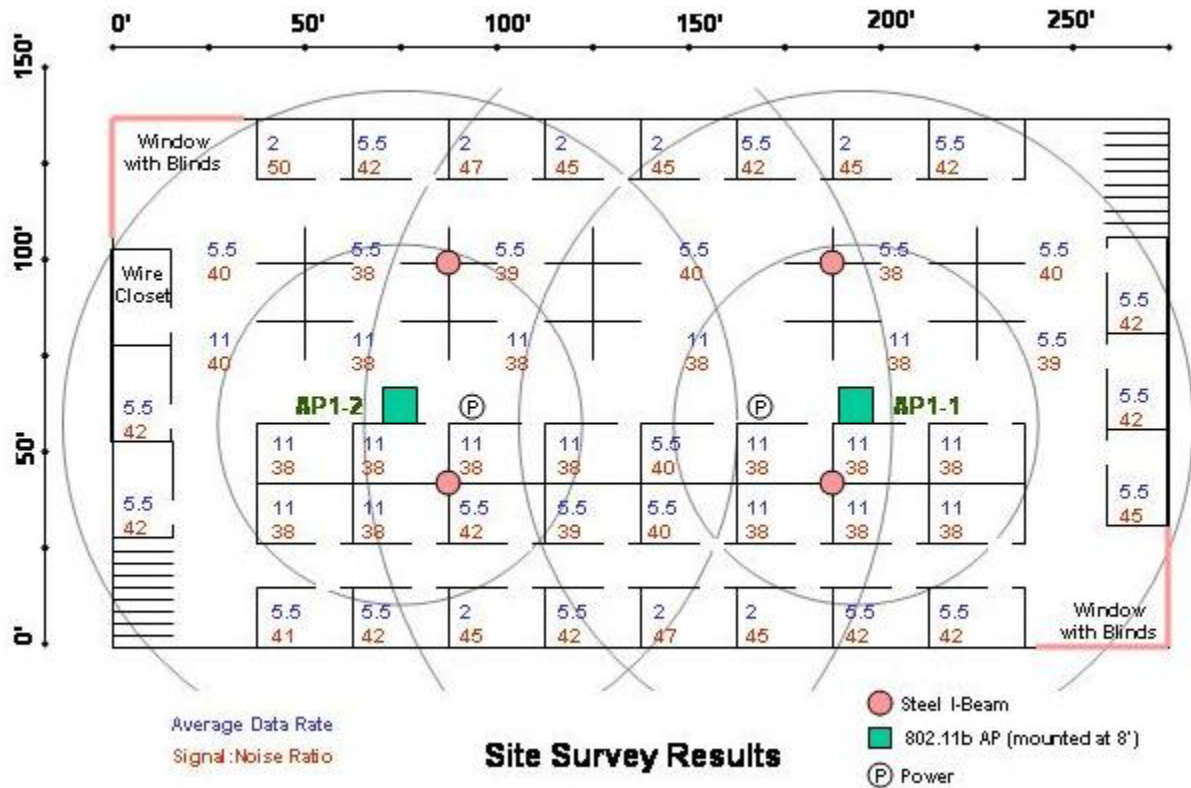


Figure 4: Site Survey Output

Table 3 illustrates a chart that can be used to help keep track of AP channel selections and power settings. Remember to take adjacent floors into consideration as radio signals can cross floors as well as walls.

	Location One	Location Two	Location Three	Location Four	Location Five
Ground Floor	Channel 1	Channel 6	Channel 11	Channel 1	Channel 6
	Power 50%	Power 50%	Power 50%	Power 50%	Power 25%
	AP 1-1	AP 1-2	AP 1-3	AP 1-4	AP 1-5
Second Floor	Channel 11	Channel 1	Channel 6	Channel 11	Channel 1
	Power 50%	Power 50%	Power 50%	Power 50%	Power 25%
	AP 2-1	AP 2-2	AP 2-3	AP 2-4	AP 2-5

Table 3: Channel & Power Survey Chart

Figure 5 illustrates further output from a site survey -- in this case, a Network Stumbler list of existing wireless LANs discovered during the site survey. Output from stumblers like these and WLAN analyzers can be logged to a file for inclusion in the survey report.

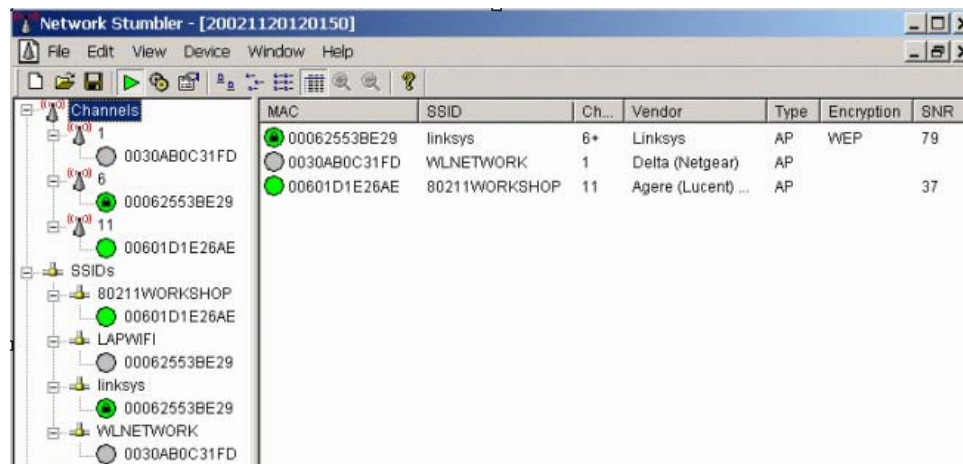


Figure 5: Site Survey Output - Part 2

After AP installation, the site survey should be repeated again to verify and fine-tune results. In most WLANs, a less extensive site survey should be repeated at regular intervals to identify new (unknown or rogue) APs and stations, coverage changes resulting from office reorganization or construction, etc.

Finding Site Survey Tools

Finally, we conclude this paper with a list of freeware and commercial tools that may prove helpful as part of your site survey toolbox. These are simply examples to help get you started; inclusion here does not imply product endorsement.

Network discovery tools passively monitor beacon and probe response frames generated by 802.11 APs and Ad Hoc mode stations, identifying discovered devices by SSID, channel, MAC address and location. Freeware examples include:

Boingo Hotspot Finder (PC, PDA)	http://www.boingo.com
BSD AirTools (BSD)	http://www.dachb0den.com/projects/bsd-airtools.html
Kismet (Several Operating Systems)	http://www.kismetwireless.net
MacStumbler (Mac OS X)	http://www.macstumbler.com
NetStumbler (PC) and MiniStumbler (PDA)	http://www.netstumbler.com
WaveStumbler (Linux)	http://www.cqure.net

WLAN analyzers capture and examine 802.11 packet content for discovery, site surveys, security and performance troubleshooting, and usage trend analysis. Examples include the following (commercial products unless noted):

AirMagnet	http://www.airmagnet.com
AirScanner Mobile Sniffer (freeware)	http://www.airscanner.com
Ethereal (freeware)	http://www.ethereal.com
Fluke Networks WaveRunner	http://www.flukenetworks.com
Network Instruments Network Observer	http://www.networkinstruments.com
Network Associates Sniffer Wireless	http://www.sniffer.com
WildPackets AiroPeek NX	http://www.wildpackets.com

Spectrum analyzers focus more exclusively on radio transmission monitoring, assisting with the detection and diagnosis of narrowband and all-band interference. Spectrum analyzers are often (but not always) specialized hardware devices. Commercial product examples include the following:

AeroComm SA3000 Spectrum Analyzer	http://www.aerocomm.com
BVS Yellowjacket	http://www.bvsystems.com
Reliawave RWA-2400A	http://www.demarctech.com
Tektronix FSQ Signal Analyzer	http://www.tektronix.com

Many 802.11 adapters include Site Survey and Link Test tools bundled with client software. A few commercial examples include the following:

NetGear Client Utility	http://www.netgear.com
Proxim ORiNOCO Client Manager	http://www.proxim.com
Symbol Spectrum24 Site Survey Tool	http://www.symbol.com

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANs



Conclusion

As we have seen, successful WLAN deployment begins with understanding how 802.11 WLANs work, alternative protocols, and how factors like channel selection and power output that affect coverage and performance. The security features to be deployed will also affect your rollout efforts and the type of client software and RADIUS servers that must be deployed to support the wireless LAN. Armed with this knowledge, you can propose a WLAN design that is theoretically capable of meeting business requirements for security, coverage, throughput, user density, and roaming.

Conducting a site survey is essential to put your proposed WLAN design to the test. By measuring the actual performance of wireless equipment in the intended WLAN location, proposed AP placements can be validated and recommend settings can be fine-tuned to meet performance and security requirements.

This paper outlines the information, tools, and steps required to complete a successful site survey. Effective surveys require rigor and detail. By employing the right tools, techniques, practice, and patience, you will find that site surveys pay off in the long run by helping to ensure that your deployed WLAN truly meets your business needs.

Additional Information

IEEE 802.1X publication: <http://standards.ieee.org/getieee802/download/802.1X-2001.pdf>

Funk: Architecting 802.1X WLANs: http://www.funk.com/radius/Solns/architecting_wlan_wp.asp

Atheros: Power Consumption White Paper: http://www.atheros.com/pt/atheros_power_whitepaper.pdf

Atheros: Wireless LAN Performance White Paper: http://www.atheros.com/pt/atheros_range_whitepaper.pdf

Foundry: Security & Wireless LAN White Paper: <http://www.foundrynet.com/solutions/wireless/index.html>

WHITE PAPER: IRONSHIELD BEST PRACTICES DEPLOYING WIRELESS LANS



Foundry Networks, Inc.
Headquarters
2100 Gold Street
P.O. Box 649100
San Jose, CA 95164-9100

U.S. and Canada Toll-free: (888) TURBOLAN
Direct telephone: +1 408.586.1700
Fax: 1-408-586-1900
Email: info@foundrynet.com
Web: <http://www.foundrynet.com>

Foundry Networks, BigIron, EdgeIron, FastIron, NetIron, ServerIron, and the "Iron" family of marks are trademarks or registered trademarks of Foundry Networks, Inc. in the United States and other countries. All other trademarks are the properties of their respective owners.

© 2003 Foundry Networks, Inc. All Rights Reserved.