WIRELESS LOCAL AREA NETWORK SITE SURVEY ADDENDUM to the WIRELESS

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 1, Release 1

31 October 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

Page

This page is intentionally left blank.

TABLE OF FIGURES

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

This *Wireless Local Area Network* (WLAN) *Site Survey Addendum to the Wireless Security Technical Implementation Guide* (STIG) is published as a tool to assist in the effective deployment of WLANs within the Department of Defense (DOD). This Addendum is meant for use in conjunction with the *Wireless STIG*. The intent is for the information in this Addendum is to supplement and enhance the security requirements found in the *Wireless STIG* by providing a more details on conducting a basic site survey in preparation for deploying WLAN equipment.

Section 2, Technology Overview, provides a technology primer describing the various transmission methods and relevant concepts. *Section 3, Identifying Requirements*, details the best practices involved in assessing user requirements. *Section 4, Basic Site Survey/Pre-WLAN Installation*, discussing access point placement and related coverage issues. *Section 5, Advanced Site Survey/Post WLAN Installation*, outlines tools used for troubleshooting and rogue monitoring.

1.2 Authority

DOD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this Addendum will provide an environment that meets or exceeds the security requirements of DOD systems operating at the MAC II Sensitive level, containing sensitive information.

1.3 Scope

This Addendum is designed to assist sites that are planning to connect to the SIPRNet using wireless products.

1.4 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG or Addendum, from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to **fso_spt@disa.mil**. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

2. TECHNOLOGY OVERVIEW

Using radio frequency (RF) technology, Wireless LANs (WLANs) transmit and receive data through the air, minimizing the need for wired connections. The IEEE 802.11a, b, and g WLAN standards define an over the air interface between a wireless client and base station or between two wireless clients. IEEE 802.11b equipment was used in constructing this guide, but the same procedures apply to IEEE 802.11a and g systems, as well.

Conventional wired networking designs require an understanding of physical and data link layers, their operation, and familiar transport via familiar physical mediums such as coaxial, twisted pair and fiber optic cables. WLANs take much of that physical medium out of the equation, and replace it with the invisible and somewhat unpredictable medium of Radio Frequency (RF) transmission. Traditional network planners and builders may not be as familiar with the concepts behind WLANs, as they are with the physical constructs of a typical wired network.

Elements of a site survey are:

- Understanding how 802.11 radios work
- Understanding RF and the effect of building structure elements and sources of external interference on RF devices
- Testing wireless communications within and outside the intended coverage area

Taking all of the above into account in designing and deploying WLANs will help ensure adequate coverage by optimizing placement of WLAN access points, and will minimize security issues involving radio signal emissions.

2.1 Radio Frequency (RF)

In its simplest form, RF is the conversion of electrical current into radio waves and transmission of those waves through the air using a defined frequency of the radio spectrum. AM and FM radios are probably the most commonly known uses of the RF spectrum. However, many devices use pieces of the radio spectrum in various ways. The Federal Communications Commission (FCC) regulates various frequency subsets of the RF spectrum for devices within the United States for non-Federal Government use.

DOD components need to obtain spectrum supportability guidance from the Military Communications Electronics Board prior to assuming contractual obligations for the full-scale development, production, or procurement of wireless devices/systems, including FCC designated Industrial, Scientific, and Medical (ISM) spectrum devices, in accordance with DODD 4650.1. For OCONUS, ISM spectrum devices must be host nation approved for use.

Presently the FCC regulates the radio spectrum between the frequencies of 9 kilohertz (KHz) and 300 gigahertz (GHz). 802.11 WLANs currently operate in the radio spectrum available to the public, commonly referred to as the unlicensed frequency band. Specifically, the 802.11 standard uses one of the three frequency bands available within the ISM band and all three of the Unlicensed – National information Infrastructure (U-NII) bands:

- 2.4 GHz (2.4-2.4835 GHz) ISM band, 802.11b and g
- 5 GHz (5.15-5.25 GHz, 5.25-5.35 GHz, and 5.725-5.825 GHz) U-NII band, 802.11a

These spectrum bands are unlicensed, and can be used by anyone providing they comply with FCC regulations. They are exempt from the Federal Government spectrum certification and frequency assignment process when used in the United States & Possessions (US&P). However, Frequency Management Officer (FMO) may require a *DD Form 1494, Application for Equipment Frequency Allocation*. Users of non-licensed devices that intend for use Outside United States & Possessions (OUS&P) must submit a DD Form 1494 for host nation coordination/approval. DOD activities will not use non-licensed devices for critical tactical or strategic command and control applications essential for mission success, protection of human life, or protection of high-value assets. Non-licensed devices must accept interference from any other Federal, non-Federal, or civilian electronic system, and therefore offer no protection of spectrum use in support of operational requirements. If non-licensed devices cause interference to a licensed user, the non-licensed user must cease operation. It is recommended that licensed devices be considered as the primary equipment.

FCC regulations govern maximum transmit power of the radios and the type of encoding and frequency modulations that can be used. Each frequency range has different characteristics. The lower frequencies exhibit better range, but with limited bandwidth and therefore lower data rates. The higher frequencies have less range and are more easily blocked by solid objects.

2.2 Attenuation, Interference, and Range

Anyone familiar with AM/FM radios is probably familiar with signal attenuation. Attenuation is the loss of signal strength during transmission. In general, the further a receiver is from the transmitter, the weaker the signal. Additionally, obstacles such as mountains and buildings can cause attenuation by blocking or weakening radio signals, causing dead zones or sporadic signal loss. Other stations operating at the same frequency can cause interference. This is evidenced whenever more than one radio station can be picked up on the same channel. WLANs are affected by the same principles that apply to AM/FM radio. Floors, walls, and ceilings (depending on what they are made of) can either strengthen or weaken WLAN signals. RF attenuation is generally measured in decibels (dB). Formulas for computing signal attenuation are beyond the scope of this guide, but some general rules of thumb will be covered in *Section 3.2.1, WLAN Attenuation and Interference.* The most common sources of interference are other devices operating at the same frequency. 2.4 GHz cordless phones are particularly troublesome for 802.11b WLANs, although microwave ovens and Bluetooth devices can also affect performance. The IEEE 802.11 standard specifies one (1) mile as the maximum coverage range for an access point. However, most 802.11b access points have an approximate range of 500 feet indoors and 1000 feet outdoors when unobstructed. More realistically, access points generally

have an effective range of 150 to 200 feet indoors, depending on building design factors such as open spaces, wall placement and composition, and interference from other devices. Careful placement of WLAN access points can mitigate interference and attenuation issues.

2.3 Transmitters, Receivers, and Transceivers

In the analogy above, a radio station would be considered a transmitter and a car radio a receiver. By comparison, CB radios, which both receive and transmit, would be transceivers. All WLAN devices are transceivers. Each component must be able to both transmit and receive IP traffic. Although both the wireless access point and wireless client adapter cards (wireless NICs) are transceivers, the location of the access point affects the range of transmission more than the NIC.

2.4 Antennas

Antennas direct RF power into the air over a coverage area. An antenna gives the wireless system three fundamental properties—gain, direction, and polarization. Gain is a measure of increase in power while direction is the shape of the transmission pattern. Polarization is typically described as vertical or horizontal, which usually corresponds to the antenna alignment. Most access point antennas are designed to operate in a vertical position, resulting in a horizontal coverage plane (polarization). Re-orienting the antenna to a horizontal position will result in a vertical plane as shown below.

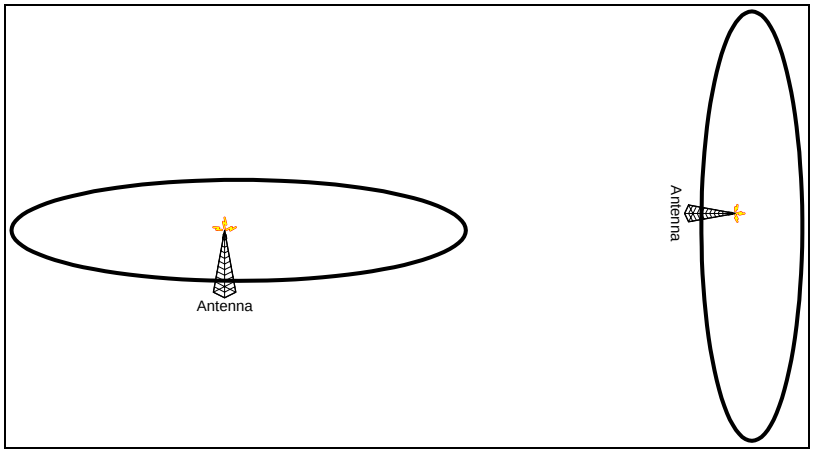

Figure 2-1. Antenna Polarization

Additional characteristics of an antenna include propagation pattern and transmit power. Transmit power is usually adjustable to accommodate various environments. Power can be adjusted to increase or decrease effective range for access points, allowing for a measure of "fine tuning" a coverage area. Transmit power should always be set to the minimum necessary to provide sufficient coverage areas, without allowing unnecessary signal leakage.

The type of antenna used by a wireless device (usually defined by its propagation pattern) can have a dramatic impact on range and coverage pattern. In general, antennas can be divided into two types—omni-directional, and directional.

2.4.1 Omni-directional

Omni-directional antennas have a 360-degree coverage pattern on a horizontal plane. The coverage pattern is shaped like a doughnut with the access point in the center. These antennas are ideal for square or somewhat square areas. Most diagrams of omni-directional antennas show only a two-dimensional view with the antenna represented as a hole in the center of a series of concentric rings.

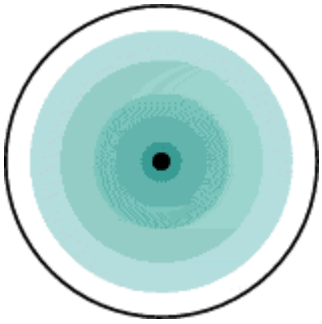

Figure 2-2. Omni-direction 2D Propagation Pattern

However, the doughnut pattern has very real implications from a signal coverage area perspective. The pattern below is a theoretical image of an isotropic omni-directional antenna. Isotropic antennas are theoretical antennas, which transmit uniformly in every direction producing an isotropic sphere.

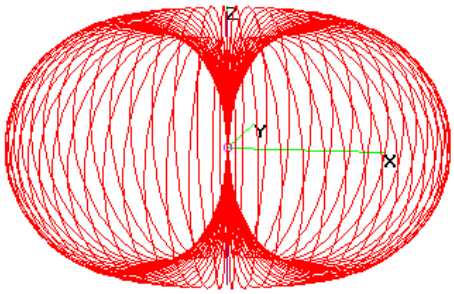

Figure 2-3. Isotropic Sphere Propagation Pattern

In reality, all real world antennas concentrate the signal into some piece of the isotropic sphere. Omni-directional antennas typically transmit a much weaker signal "below" the antenna, and a somewhat weaker signal directly "above" the antenna. In addition, both floors and ceilings (being denser than interior walls) will affect real transmission patterns. This usually results in a transmission pattern, which is flatter than the theoretical model as in *Figure 2-4, Real World Indoor Omni-directional Propagation Patterns*, as shown below.

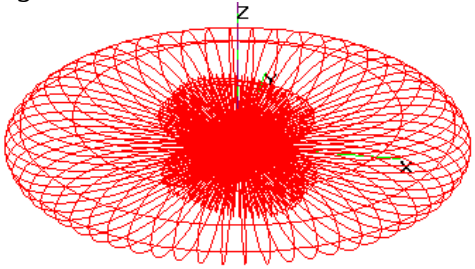

Figure 2-4. Real World Indoor Omni-directional Propagation Pattern

In addition, exterior-building walls will narrow this pattern further. However, concrete and brick walls can be penetrated by 802.11 signals. In particular, windows and doors allow signal leakage beyond exterior walls. For simplicity, a good starting point is to assume that indoor access points with omni-directional antennas, placed within a building, will have an isotropic RF emissions pattern.

2.4.2 Directional

Directional antennas focus data transmission in one direction. This will produce a conical-shaped coverage pattern, similar to that of a flashlight. The antenna directionality is specified by the angle of the beam width. Beam width angles vary from 90 degrees (somewhat directional), to 20 degrees (very directional). The focused beam allows for longer, narrower coverage patterns, which can be ideal for elongated areas, around corners, and outdoor applications such as inter-building communications in a multi-building network. As with omni-directional, most directional antennas are represented in two dimensions (as in *Figure 2-5, Directional)*; however, the actual propagation pattern is more accurately represented in three dimensions (see *Figure 2-6, Directional 3D*).

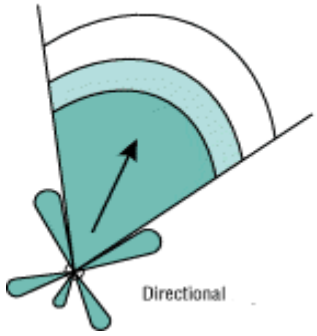

Figure 2-5. Directional

Figure 2-6, Directional 3D, depicts the RF pattern of a three-dimensional directional antenna where X and Z depict the top and bottom of the beam width, and Y represents the center of the beam pattern. The exact pattern will vary depending on the specific beam width.

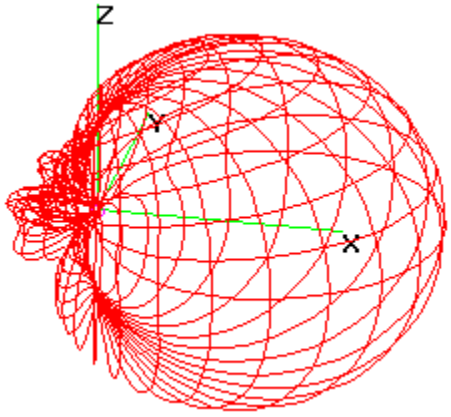

Figure 2-6. Directional 3D

2.4.3 Antenna Replacement

Most WLAN access points use omni-directional antennas. Some access points allow either the installed antennas to be replaced, or for the placement of supplemental antennas in remote locations. Depending on the results of the site survey, multiple access points and supplemental antennas may be deemed necessary. Knowing your environment can help to determine the right antenna and placement. In theory, matching the antenna provided coverage pattern to the site coverage requirements determines the correct antenna for a site. However, in many cases, equipment from vendors cannot be modified due to FCC regulations. Most WLAN equipment is certified as being FCC regulation compliant only with the OEM antenna. The FCC limits Equivalent Isotropically Radiated Power (EIRP) for all transmitting devices. Within the U.S., EIRP is restricted to four watts maximum, with additional restrictions/limitations depending on type of antenna (directional or omni-directional), and placement (indoors or outdoors). Since the FCC places restrictions on transmit power and gain allowable, replacing the OEM antenna without a thorough understanding of the effects on antenna gain and emissions could result in FCC violations.

3. IDENTIFYING REQUIREMENTS

The first stage in a wireless implementation is a careful evaluation of the current network state and a detailed assessment of what deploying WLANs is intended to accomplish. The current network state will have a lot of impact on planning the wireless deployment. The first step is to determine:

- What groups need access, such as all employees, or more restrictive groups such as engineers or inventory clerks, etc.
- What network resources should each user type be able to access?
- How many users require access in total, and how many are expected to be accessing the wireless points simultaneously in a specific area?
- What are their bandwidth requirements?
- Will users require access to data-intensive applications?

Consider the physical nature of user access to the wireless network.

- Will users be moving around a lot, such as in a warehouse environment where users are riding in vehicles such as forklifts, trucks, etc?
- Will users be stationary, such as in offices or cubicles?
- What is the WLAN designed to accomplish?

Some WLAN implementations are intended to simplify deployments to temporary facilities, where laying cables and wires would be both time and labor intensive, as in when forced to relocate offices due to catastrophic weather events such as tornadoes, hurricanes, or floods. Others may be implemented where wired LANs are prohibited by structure (e.g., a large warehouse with no internal partitions, concrete floors, walls and high ceilings), or in architecturally sensitive (possibly historic) building where typical methods (such as cutting into walls for LAN cables and jacks) are prohibited. In situations such as these, using a WLAN can save time and costs, and can be more aesthetically pleasing than traditional network infrastructure layout.

Many WLAN implementations begin with only restricted spaces such as in conference rooms, meeting rooms, even cafeterias. Other WLANs are deployed across open office spaces in order to allow users more mobility and freedom of movement from cubicle to cubicle, or even to move seamlessly from office to conference room and back.

In some cases, WLAN devices are used with directional antennas to connect multiple buildings together without having to run cables between them.

3.1 802.11 and RF

As mentioned earlier, IEEE 802.11 is a specification for Wireless Local Area Networks (WLANs). The original 802.11 specification currently includes several extensions, including 802.11a, 802.11b, and 802.11g.

3.1.1 802.11b and 802.11g

Most WLAN equipment sold today are 802.11g systems. 802.11b provides WLAN transmission rates of up to 11 Mbps, with step backs to 5.5, 2, and 1Mbps. 802.11g systems provide transmission rates up to 54 Mbps. Both 802.11b and 802.11g operate in the 2.4 GHz frequency band, specifically between 2.400 GHz (2400 MHz), and 2.484 GHz (2484 MHz). Although the 802.11 standard specifies 14 channels, in the United States, the FCC limits the operational frequencies to 11 channels of 22 MHz each covering the frequency from 2400 MHz to 2483 MHz.

NOTE: This guide applies to WLAN deployments within the territories of the United States. OCONUS deployments may have more or fewer channels available depending on local spectrum regulation.

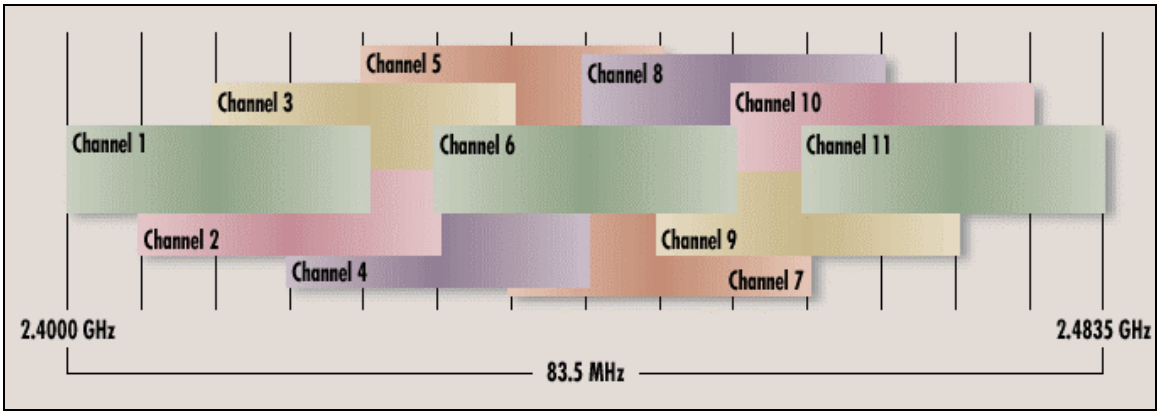

Figure 3-1. 802.11b Spectrum Coverage

As shown above, Channels 1, 6, and 11 are "non-overlapping," meaning they can all be used in the same area without causing "co-channel interference" (CCI). In this way, users can be load balanced across three channels, each providing up to 11Mbps of throughput, thereby effectively providing up to 33 Mbps of aggregate bandwidth. Therefore, larger scale WLAN deployments utilize these three channels in a "geographic space" overlapping fashion to maximize coverage area while preventing channel interference.

Visual representation of this type of deployment is shown in *Figure 3-2, 802.11b Channel Layout*.

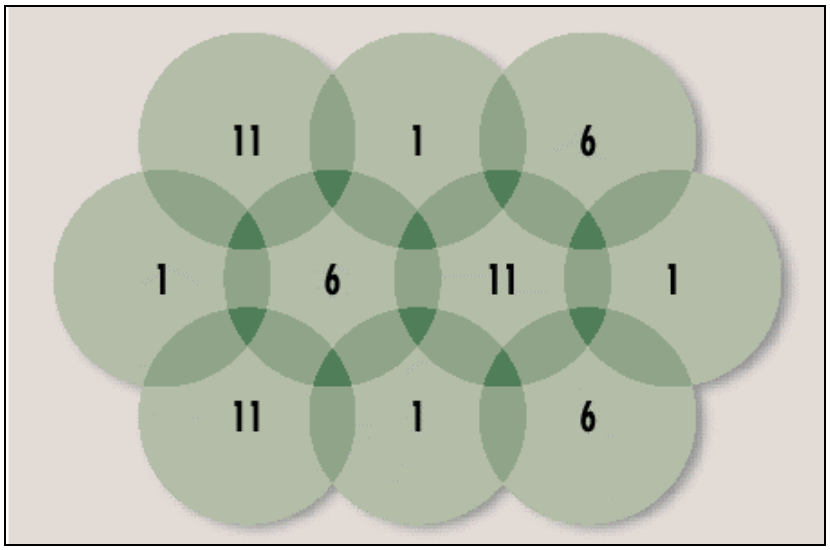

Figure 3-2. 802.11b Channel Layout

Using the three non-overlapping channels in a configuration as shown allows maximum coverage of a geographic area without cross channel interference. Since channel frequencies do not overlap, coverage areas can be laid out in a manner that ensures complete RF coverage. Since using Channels 1, 6, and 11 allows for three channels to be used without interference, it is the most popular configuration. Keep in mind that the graphic above is two-dimensional and does not accurately represent the three-dimensional nature of 802.11b RF coverage areas. This means that the signals can penetrate floors, ceilings, and walls, potentially interfering with other access points on other floors, particularly if using the same channels. In some cases, using two other non-overlapping channels could reduce interference with Channels 1, 6, and 11, and may provide adequate coverage areas. For example, Channels 4 and 9 are RF spectrum non-overlapping, as are Channels 3 and 8. Either set could be used in a geographic area already saturated by Channels 1, 6, and 11, if two channels provide an adequate coverage area. As shown below, Channels 3 and 8 overlap both 1 and 6, and 8 and 9 overlap both 6 and 11; however if power settings in both WLANs were set to the minimums necessary for applicable coverage areas, interference would be minimized. Two (2) channel operations can be determined using *Figure3-3, Non-overlap Channel Placement.*

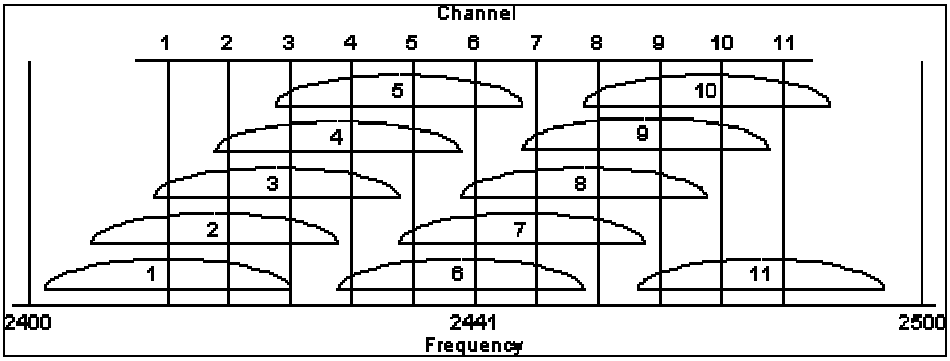

Figure 3-3. Non-overlap Channel Placement

3.1.2 802.11a

802.11a equipment operates in the 5.2 GHz frequency range, generally between 5.15 GHz (5150 MHz) and 5.83GHz (5835 MHz). Specifically (within the U.S.), 802.11a consists of twelve (12) non-overlapping channels, with eight (8) channels in the 5.15-5.35 GHz band, and four (4) additional channels in the 5.73-5.83 GHz band. By operating in the 5 GHz band, 802.11a avoids some of the problems associated with 802.11b arising from the number of devices sharing the 2.4 GHz spectrum. In addition, 802.11a also allows greater throughput (54 Mbps vs. 11Mbps in 802.11b), and more step down options with transmission speeds of 6, 9, 12, 18, 24, 36, and 48 Mbps possible (6, 12, and 24 being mandatory for all products). As 802.11a has 12 non-overlapping channels (vs. 3 in 802.11b), it allows a larger range of channels to be used without CCI (Co-channel Interference), should multiple access points need to be placed in the same geographic area.

While in theory 802.11a seems a clear winner in terms of advantages, it does have some real world disadvantages. First is availability. 802.11a products are not as readily available as 802.11b and g systems. Secondly, of the 12 available channels, only the lower eight channels are classified as suitable for indoor applications. The remaining four allow for much higher transmission powers (wattage) and have been designated as suitable for outdoor use. By using the higher 5 GHz frequency, 802.11a transmission range has been reduced; therefore in general, more 802.11a access points are required than 802.11b access points to cover the same geographic area. In addition, 802.11a signals do not penetrate walls as well as 802.11b, which can be both an advantage and disadvantage depending on the desired result. Lastly, 802.11a products are average about three to four times the price of 802.11b products, thus increasing the cost to deploy.

3.2 Rules of Thumb

Prior to beginning a formal site survey, it is best to keep in mind a couple of general rules regarding the placement of access points and interference.

- **Data rates:** Sensitivity and range are inversely proportional to data bit rates. Therefore, maximum radio range is achieved at the lowest workable data rate, and as the radio data rate increases a decrease in receiver sensitivity occurs.

- **Antenna type and placement:** Proper antenna configuration is a critical factor in maximizing radio range. As a general rule, range increases in proportion to antenna height.

- **Physical environment:** Clear or open areas provide better radio range than closed or filled areas. Generally, the less cluttered the environment, the greater the range.

- **Obstructions:** Physical obstructions such as metal shelving or a steel pillar can impact performance. Try not to place WLAN devices in a location where a metal barrier is between the sending and receiving antennas. Also keep antennas away from microwave ovens or 2.4 GHz cordless phones.

- **Access Point Placement:** The best place to begin is to try to place the AP as close as possible to the center of the area to be covered. Unless you want to be able to connect while outside the building, avoid antenna placement close to an outside wall. If you want to connect while outside, place the AP near a window.

- **Antenna Alignment:** For best results, orient the AP antenna(s) vertically. Directly under an AP (assuming the antenna is vertically oriented and omni-directional) is the worst place to be (weakest signal).

- **Water:** Try to keep AP placement away from large containers of water (i.e., fish tanks or water heaters), as water blocks 2.4 GHz RF signals.

- **Client Antenna:** Most PC card antennas are fairly directional. The horizontal orientation of the PC card antennas is not optimal. If client devices are not receiving a strong signal, try re-orienting the devices so that the PC card's antenna is pointing toward the AP.

- **Timing:** The site survey should be conducted during normal business hours to optimize coverage, taking into account possible sources of interference, including the presence of both people and equipment.

- **Building materials:** Radio penetration is greatly influenced by the building material used in construction. For example, drywall construction allows greater range than concrete blocks, and metal or steel construction is a barrier to radio signals.

3.2.1 WLAN Attenuation and Interference

As mentioned in *Section 2.2, Attenuation, Interference, and Range,* attenuation is a measure of the loss of signal strength in dB. In addition to "free space loss" (signal strength lost as a factor of the distance the signal travels through clear air), additional signal loss from typical office partitions and furniture will occur. Simply put, as the signal attenuates (weakens), it becomes more difficult for a WLAN client to clearly receive the signal, thus resulting in bit rate errors and lost packets. As packet loss increases, sending stations are forced to resend thus impacting performance (slowing down the network).

Since attenuation is measured in dB, it is first helpful to represent the signal transmitted from the access point in dB. Computing Equivalent Isotropically Radiated Power (EIRP) and receiver antenna sensitivity can get complicated. However, some rules of thumb can be used to generally predict receiver ranges and signal attenuation.

3.2.1.1 Rules of Thumb

- Most 802.11b WLAN access points have a maximum transmit power of 100 milliwatts (mW). Common power step-downs include 50, 20, 5, and 1 milliwatts. The step-down values vary between manufacturers; however a chart of available power settings should be included with the manufacturer's documentation.

- Antenna gain is measured in decibels (dBi), and is typically computed and indicated in manufacturer documentation. Antenna gain is important, because it affects the EIRP of transmitters, and EIRP is what the FCC and other regulatory agencies place restrictions upon.

- For every 3 dBi increase in antenna gain, a doubling of transmit power occurs. For example, replacing a 3 dBi antenna with a 6 dBi antenna would double a 100 milliwatt RF signal to 200 milliwatts.

- Using the formula for EIRP, at 100 mW transmit power, an 802.11b transmitter produces 20 dBm (decibels referenced to milliwatts) of transmit power. As with dBi, doubling the mW of a transmitter would result in a 3 dBm increase in transmit power. Therefore, increasing a 20 dBm 100 mW transmitter to 200 mW would result in 23 dBm of transmit power. Using these guidelines, and the manufacturer's published transmitter power options (such as 100, 50, 20, 5, and 1 mW), we get the following:

Access Point Power Setting mW	Corresponding dBm
100	20
50	17
20	13
5	7
1	0

Figure 3-4. Common Access Point Transmission Power Settings

- Receiver sensitivity is also measured in dBm, and can usually be found in the manufacturer's documentation for both access points and WLAN client adapters. Receiver sensitivity is affected by data rates. The higher the data rate, the more sensitive a receiver must be, and conversely the lower the data rate, the lower the sensitivity required. This is why the further away from the access point the client devices are located, the lower the data rate. Users at 25 feet may achieve 11 MBps throughput, where a user at 250 feet may achieve 2 MBps throughput. Depending on the bandwidth requirements of users, more or fewer access points may need to be installed to achieve the desired throughput.

- Adding receiver sensitivity and transmit power establishes acceptable levels of attenuation. For example, typical receiver sensitivity might be –85 dBm at 11 MBps. When using a typical 100 mW transmitter access point and the corresponding 20 dBm of signal, you get 20 dBm - (-85 dBm) = 105 dBm. Since some signal strength is required for connectivity, a signal could sustain approximately 104 dBm of attenuation before the signal drops below the receiver's ability to receive data error free. Using the table below in conjunction with common receiver sensitivities (as documented by the manufacturers), gives us a rough estimate of acceptable attenuation levels for varying data rates.

Access Point		11 MBps Data Rate			5.5 MBps Data Rate			2 MBps Data Rate			1 MBps Data Rate		
Power setting (mW)	Transmit dBm	Receiver dBm	Total dBm	Allowed signal loss dBm	Receiver dBm	Total dBm	Allowed signal loss dBm	Receiver dBm	Total dBm	Allowed signal loss dBm	Receiver dBm	Total dBm	Allowed signal loss dBm
100	20	-85	105	104	-89	109	108	-91	111	110	-94	114	113
50	17	-85	102	101	-89	106	105	-91	108	107	-94	111	110
20	13	-85	98	97	-89	102	101	-91	104	103	-94	107	106
5	7	-85	92	91	-89	96	95	-91	98	97	-94	101	100
1	0	-85	85	84	-89	89	88	-91	91	90	-94	94	93

Figure 3-5. Max Attenuation Values

- Unfortunately, there are many different algorithms for computing indoor signal attenuation. These formulas are much more complex than relatively standard, "free space loss" formulas used in computing outdoor signal loss, and are beyond the scope of this appendix. However, generally, at 11 MBps, you can expect 100 dBm of indoor path loss over a distance of 200 feet. Indoor path loss also increases exponentially as distance increases, therefore attenuation at 100 feet would equal 10 dBm for an 11 MBps data rate.

Once the maximum attenuation values are determined, using *Figure 2-3, Isotropic Sphere Propagation Pattern*, in conjunction with estimates of indoor path loss, can help determine both the number of access points required and their placement within the intended coverage area.

Found in most office spaces, common obstacles such as doors, windows, and walls offer fairly known levels of attenuation. These values represent attenuation in addition to the general signal strength loss over distance. The following is a general example of the attenuation values of common office construction:

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

Figure 3-6. Approximate Office Construction Material Attenuation Values

This page is intentionally left blank.

4. BASIC SITE SURVEY/PRE-WLAN INSTALLATION

The first step in a site survey involves taking a look at the physical layout of the office space and determining optimal placement and density of APs to maximize client connectivity and bandwidth. The goal is to blanket the coverage area with overlapping coverage cells so that clients might range throughout the area without ever losing network contact. The ability of clients to move seamlessly among a cluster of access points is called *roaming*. Access points hand the client off from one to another in a way that is invisible to the client, ensuring unbroken connectivity.

4.1 Building Walkthrough

It usually helps to have building blueprints in hand while doing a walkthrough to ensure accuracy. Most wireless vendors supply site survey utilities with their hardware. These are operated from a laptop with a wireless NIC and will help visualize coverage areas by showing the signal strength and quality, as well as rates of packet loss.

The simplest method for performing an RF site survey includes a laptop equipped with an 802.11 PC Card and site survey software. Most wireless PC card vendors now supply this software with the cards. The software features vary by vendor, but at a minimum, they all display the strength and quality of the signal from the access point. This helps determine the effective operating range (i.e., coverage area) between end users and access points.

For example, taking into account the rules of thumb and after "best guessing" the placement of access points for adequate coverage and overlap, this placement can be verified by simply walking around with a laptop while monitoring and noting signal levels. The intent is to verify the maximum distances that will maintain adequate signal levels. Adequate signal levels are generally defined as sufficient signal strength to enable operation at the planned data rate (e.g., 11 Mbps, 2 Mbps, etc.). If the predetermined location of an access point does not provide the required coverage, then reposition or include additional access points and repeat testing.

This page is intentionally left blank.

5. ADVANCED SITE SURVEY/POST WLAN INSTALLATION

More advanced site surveys are required when implementing large or complex WLANs, such as when users roam between multiple buildings, or if there exists RF spectrum congestion such as in urban areas, which may already contain non-DOD WLANs. Conducting these site surveys is, of course, more complex and time consuming, and can require specific knowledge of RF spectrum analyzers and experience using troubleshooting tools. Some of these tools include wireless packet sniffers and RF spectrum analyzers. These tools are most useful when troubleshooting installed WLANs, as they primarily help resolve issues such as intermittent connectivity, traffic congestion, and slow network performance. However, RF spectrum analyzers in particular can be helpful in identifying potential sources of RF interference prior to WLAN installation. Since this appendix is intended to serve as an overview of the processes, procedures, and reasons for a Site Survey and as a guide to conducting a Basic Site Survey, an in-depth look at some of the more advanced tools cannot be provided. However, a brief overview is presented here.

5.1 Wireless Sniffers

Wireless sniffers are much like their traditional wired counterparts, and in fact some of the most widely used wired products now come in wireless versions. These include products such as Sniffer Wireless 4.7 from Network Associates, Observer 8.1 Wireless Protocol Analyzer from Network Instruments, Airopeek NX from Wildpackets, as well as freeware sniffers such as Airsnort, Airosniff, and Netstumbler, to name just a few. Since these tools can capture all IP packets on the network, they are popular among hacker groups. Widely reported uses for these tools range from looking for everything from free access to the Internet via someone's unsecured access point, to being used as a new tool to break into corporate LANs/WANs while sitting outside an office building in a car.

Most wireless sniffers provide many of the same tools and features as their wired counterparts, including traffic filters and packet decoders. Although most commercial products can decode WEP when provided the encryption key, they cannot be used to "break WEP" per se. Additionally, Airopeek NX, can decode WEP encrypted traffic on the fly, raising security concerns when a "rogue" network administrator with the appropriate WEP key wants to sniff wireless traffic. Most other commercially available wireless sniffers can decode WEP traffic, but require a two-stage capture-decrypt process. Although similar to their wired counterparts, particularly when from the same company such as Network Associates, experience has shown that ample time needs to be allowed for network administrators and systems planners to familiarize themselves with everything from software/driver installation to graphical user interface (GUI) usage and filter configuration. It is not unusual for it to take a week or two of practice for an experienced network engineer to become comfortable with wireless network sniffers.

5.2 Spectrum Analyzers

More advanced 802.11 site survey tools include RF spectrum analyzers, which provide the "eyes" and "ears" of network administrators. Spectrum analyzers provide information on access point transmission characteristics and the effect of the environment on the transmission of 802.11 signals. For example, an 802.11b spectrum analyzer can graphically illustrate the amplitude of all 2.4 GHz signals within any chosen 22 MHz channel. This enables a network administrator who understands RF transmissions to distinguish 802.11 signals from other RF sources that may cause interference. This makes it possible to locate and eliminate sources of interference, as well as the placing of additional access points to resolve problems.

Another useful spectrum analyzer feature is the ability to monitor channel usage and overlap. 802.11b is limited to at most three access points operating in the same general area without interference and related performance impacts. This can cause difficulties when planning the location and assignment of channels in large networks. Spectrum analysis can display these channels, enabling network engineers to make better decisions on locating and assigning channels to access points.

Several test equipment companies currently have developed or are developing advanced site survey tools. Airmagnet, Berkeley Varitronics Systems and Softbit already have products on the market. Softbit's TriCycle software installs on a laptop equipped with a wireless client adapter card and can provide a useful display of many things, including nearby access points, association status, signal levels, and also the ability to display coverage areas. Although using TriCycle still requires network administrators to carry a laptop PC around, its features can help decrease time and increase accuracy when performing site surveys. Berkeley Varitronics Systems' Grasshopper has fewer graphical features, but is available in a small handheld form factor weighing approximately three pounds, which makes the product easier to use when mobility is important.

5.3 Advanced Summary

In addition to requiring specific knowledge of both IP traffic analysis and spectrum analyzer tools, and due to the higher cost (up to several thousand dollars) of both of these advanced tools, network administrators considering small installations of WLAN technology may forego using these advanced tools for small WLAN implementations. However, when installing multiple WLAN systems or a single complex WLAN system, experienced network administrators may want to consider purchasing and using these tools.

APPENDIX A. RELATED PUBLICATIONS

802.11 Networks: The Definitive Guide, Matthew Gast, O'Riely and Associates, 2002.

The Essential Guide to RF and Wireless, Carl J. Weisman, Prentice Hall, 2002.

Wi-Fi Experience: The Everyone's Guide to 802.11b Wireless Networking, Richard Mansfield and Harold Davis, QUE, 2002.

Wireless LANs (2nd Edition), James T. Geier, Sams, 2002.

Antennas and Coverage in WLAN, Kjell Åge Håland and Stig Erik Arnesen.
http://home.no.net/coverage/rapport/Antennas%20and%20coverage%20in%20WLAN%20intro.htm

Wireless Sniffers Put to Test, Cameron Sturdevant, eWeek.com, 22 April 2002.
http://www.eweek.com/article2/0,3959,1415,00.asp

A Guide to Wireless LANs, Network World, 25 March 2002.
http://www.nwfusion.com/wifi/2002/

Campus WLAN Design, Mobile and Wireless Technology Workshop, Dave Molta, Network Computing magazine, 13 May 2002.
http://www.nwc.com/1310/1310ws1.html

Wireless LANs Work Their Magic, Joel Conover, Network Computing magazine, 10 July 2000.
http://www.networkcomputing.com/1113/1113f2.html.

Cisco Aironet Access Point Software Configuration Guide Software Release 11.21, Cisco Systems.
http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/index.htm

Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows, Cisco Systems.
http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/windows/incfg/index.htm

This page is intentionally left blank.

APPENDIX B. LIST OF ACRONYMS

DISA	Defense Information Systems Agency
DISAI	DISA Instruction
DOD	Department of Defense
FIPS	Federal Information Processing Standard
FSO	Field Security Operations
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol
IP	Internet Protocol
IPSEC	IP Security
LAN	Local Area Network
MAC	Media Access Control
NIC	Network Interface Card
OS	Operating System
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PED	Personal Electronic Device
RF	Radio Frequency
SA	System Administrator
SRR	Security Readiness Review
SSID	Service Set Identifier
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
USB	Universal Serial Bus
WAP	Wireless Application Protocol
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WPA	Wireless Protected Access
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
WWW	World Wide Web

This page is intentionally left blank.