WIRELESS
SECURITY TECHNICAL IMPLEMENTATION GUIDE
Version 3, Release 1

15 APRIL 2004

Developed by DISA for the DOD

UNCLASSIFIED

This page is intentionally left blank.

TABLE OF CONTENTS

APPENDICES

TABLE OF FIGURES

This page is intentionally left blank.

SUMMARY OF CHANGES

GENERAL CHANGES:

–The previous release was Version 2, Release 1, dated 30 June 2003.
–Updated references to DODD 8100.bb to reflect new document version DODD 8100.2

SECTION CHANGES

SECTION 1. INTRODUCTION

–Reworded and updated the entire section with general wording and grammatical changes.
–Added reference and description of Appendix C, Wireless LAN Site Survey Guide.

SECTION 2. WLAN AND WPAN TECHNOLOGIES

–In Section 2.1, added the acronym WPAN to the section title. Added definitions for WPAN and POS.
–In Section 2.1, WIR0070 deleted.
–In Section 2.1, WIR0080 reworded to make the requirement applicable to all WPANs rather than specific to Bluetooth. WIR0083 added.
–In Section 2.2, added new opening paragraph. Added subparagraphs and definitions for 802.11e, 802.11h, 802.11j, and 802.11n standards. Updated subparagraphs for 802.11g, 802.11i, and 802.1x.
–In Section 2.2.1.1, WIR0070 was corrected to correct number, PDI WIR0090. The phrase, "if available" was replaced.
–In Section 2.2.1.1, WIR0100. The phrase, "if available" was replaced.
–In Section 2.2.1.2, added paragraph describing the new "wireless zombie" exploit.
–In Section 2.2.2.1.2, added information on impact on access point functionality with implementation of wireless network management, bridging, and wireless switching overview.
–Section 2.2.2.1.1, WIR0110 updated with CSA CTTA requirement.
–In Section 2.2.2.2.1, reference to NIAP draft protection profiles for peer-to-peer deleted. WIR0120 regarding Common Criteria peer-to-peer protection profile deleted. WIR0125 added.
–Section 2.2.2.2.2 removed. All subsequent sections renumbered. Four new requirements added regarding WLAN bridging. Removed PDI number from WIR0137 as this is a physical check.
–Section 2.2.2.2.3 added description of infrastructure WLAN
–Section 2.2.3, removed second paragraph describing 802.11b. Added paragraph discussing RSN or WPA2.
–Section 2.2.3.2, WIR0160, attached note updated.
–Section 2.2.3.3, last paragraph removed.
–Section 2.2.3.4, Renamed and last paragraph and Figure 2 detailing the RSN protocol added.
–Section 2.3.4, added reference to Draft CNSS Instruction 3034. WIR0200 added.
–Section 2.2.5, third dashed paragraph added regarding PEAP protocol. WIR0166 reworded. WIR0167 added. Figure 2 relabeled Figure 3.

–Section 2.2.6.1, added physical security requirement for classified network devices. Added PDI WIR0193.
–Section 2.2.6.2. WIR0290 was updated with the phrase "concentrator or wireless gateway". WIR0300, added phrase "network IDS/IPS or wireless IDS/IPS" in parentheses. WIR0160, changed should to will. WIR0230 reworded to required session timeout. WIR0270 added reference to Layer 2 or 3. WIR0280 updated section referenced to 3.3.3. WIR0285 updated and added last sentence. WIR0330 added the words "management console". WIR0100, deleted "if availableWIR0090, deleted "if available". Updated Figure 2.3 with the phrase "Concentrator or Wireless Gateway".
–Added Section 2.2.7 regarding WLAN Common Criteria Protection Profile requirements.
–Renamed Section 2.3 Bluetooth WPAN and made major revisions
–Section 2.3.1.1. Added WIR0182, WIR0181 and WIR0225 regarding Bluetooth devices in classified environments.
–Section 2.3.1.2. Added WIR080 and WIR083 regarding use of Bluetooth in Unclassified environments.
–Section 2.4. Replaced old section on WMAN technology with new Section 2.4 on Wireless Mice and Keyboards requirements. Added WIR0010 and WIR0132.
–Added Section 2.5 discussing requirements for VoIP. Added WIR0133.

SECTION 3. REMOTE ACCESS WIRELESS TECHNOLOGIES

–Section 3.1. General editing.
–Section 3.2. Heading change to "Cellular Technologies, Protocols, and Security.
–Section 3.2.1.1. Added last paragraph.
–Section 3.2.1.4. Entire section updated and reorganized.
–Section 3.2.2, third paragraph, replace Motorola with General Dynamics.
–Section 3.2.3. Added two WIR0356 and WIR0371 policies for cellular/PCS telephones with digital cameras in classified environments. Added two PDIs regarding 3G phones used with laptop or PDA devices. These PDIs are not yet assigned PDI numbers.
–Inserted new Section 3.3 on Wireless Broadband Technologies, Protocols, and Security.
–Section 3.3.5.1. Added requirements WIR0376, WIR0377, and WIR00378 to this new section on Classified Broadband Wireless Systems.
–Section 3.3.5.2. Added requirements WIR0379 and existing requirement WIR0040 to this new section on Unclassified Broadband Wireless Systems.
–Section 3.4.1.3. Updated last paragraph with Symbian OS licensee changes.
–Section 3.4.5. Changed heading name. Major editing.
–Section 3.4.5.1. WIR0030 deleted. Added WIR0356
–Section 3.4.5.2. WIR0050 and WIR0460 updated to remove "if available" and category code changed to CAT IV. WIR0470 was updated to add CTTA consultation requirement for IR. WIR0490 updated to add last dashed item regarding removing modems when not in use.

SECTION 4. WIRELESS TWO-WAY MESSAGING AND E-MAIL TECHNOLOGIES

–Section 4.1. Updated dates.
–Section 4.2.1. Deleted footnote.
–Section 4.2.3.2. PDI WIR0480 changed to 0050 and words “if available removed.
–Section 4.2.3.2. Added WIR00020.
–Section 4.3. Introductory sections streamlined. Subheadings renumbered throughout. WIR0050 updated to match DISA requirements for 14-day updates and Category code changed to CAT IV. WIR0600 updated to remove “if available”.
–Section 4.4.2. Updated paragraph with information on Blackberry S/MIME and URL.
–Section 4.4.3.2. Deleted WIR0005 regarding use of only S/MIME BlackBerry.

APPENDIX A. RELATED PUBLICATIONS

–Reference information for the following publications were updated: A.1.1, A.1.2, A.1.4, A.1.5, and A.2.1.
–Reference A.2.13 was added.

APPENDIX B. INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) COMPLIANCE

–Format and editorial changes. Patch server web site address added.

APPENDIX C. WIRELESS LAN SITE SURVEY GUIDE

–Removed old Appendix C. Renamed appendices.
–General editing updates

APPENDIX D. WLAN REFERENCE MODEL

–Newly added appendix. Document added in separate pdf file.

APPENDIX E. LIST OF ACRONYMS

–Updated throughout with new acronyms.

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

This *Wireless Security Technical Implementation Guide* (STIG) is published as a tool to assist in the improvement of the security of Department of Defense (DOD) commercial wireless information systems. The document is meant for use in conjunction with the Network STIG and appropriate operating system STIGs.

Use of wireless technologies can improve productivity of DOD employees, however wireless systems and handheld devices may also introduce security vulnerabilities, which, if left unmitigated, can expose government information systems to attack. In the last five years, there has been a dramatic evolution in wireless technologies, standards, and implementation practices. These changes impact the security of both wireless and wired networks. The pace of these changes is not expected to decrease for the foreseeable future, therefore solid security engineering practices and wireless network implementation policies are crucial to ensure that DOD wireless systems are deployed and operated in a secure manner. To that end, this STIG provides an overview of each wireless technology and the security impact associated with incorporating these wireless devices into the DOD environment.

Although there are a number of different wireless services available today (including two-way pagers and e-mail services, Bluetooth wireless networks, and automobile telemetrics), there are three services that are of primary interest to government agencies—wireless local area networks (WLANs); wireless connectivity to the agency network via the Internet (wireless remote access); and wireless two-way e-mail services. Each of these services has different implementation and security issues.

In general, developing a wireless network security architecture is more complicated than developing a wired network security architecture. Limits on wireless device transmission bandwidth, processing power, data storage, and mobility require that, in most cases, different security mechanisms be used to provide user authentication and data encryption. For example, the Wireless Transport Layer Security (WTLS) protocol is used to encrypt data in many wireless networks instead of Secure Socket Layer (SSL). Additionally, most wireless Internet service providers (WISPs) and wireless device manufacturers preset many of the security features of the network and client devices, thus the security manager may not be able to control all security aspects of the system. When designing and implementing a wireless network and wireless security architecture, the project manager and security manager must carefully evaluate the security requirements of the system against the security features of the wireless gateway, WISP, and wireless device.

Security mechanisms can be found at three layers within the International Standards Organization (ISO) Open Systems Interconnection (OSI) 7-layer protocol model of a wireless network (*see Figure 1-1, The OSI Model)*.

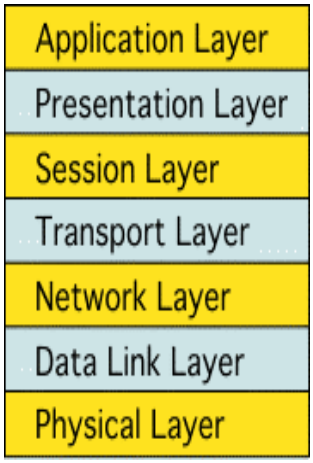


Figure 1-1. The OSI Model

At the Physical/Data Link layers many transmission protocols provide encryption and device identification. For WLANs, the Wired Equivalent Privacy (WEP) protocol, which is part of the IEEE 802.11 standard, and the Wi-Fi Protected Access (WPA) protocol provide these security services. For wireless PDAs, two-way e-mail devices, and cell phones, the radio/air interface protocol (e.g., CDPD [cellular digital packet data], GSM, CDMA, or TDMA) may provide these services between the wireless device and the wireless service provider base station.

At the Network/Transport layers, many wireless network providers provide secure Virtual Private Network (VPN) tunnels using standard protocols (e.g., IPSEC) or proprietary protocols. These secure tunnels encrypt all data between the wireless device and the wireless gateway (which may be located at the wireless service provider or on the government operated network) and may provide device identification and/or user authentication security services.

The third layer where security is found in the OSI model is at the presentation/application layer where user authentication and data encryption services are offered. End-to-end security is provided between the client application on the wireless device and the application server located in the government operated network. A number of standard and proprietary protocols are used to provide these security services including SSL and WTLS. In addition, several biometric security solutions are now available including fingerprint scanning and signature recognition. For a WLAN system, security services at the application layer are usually the same as those found in the wired part of the network.

This STIG supports the design, implementation, and management of wireless devices and networks that are used to provide e-mail and other information technology services to mobile workers in the DOD and provides implementation guidance for DODD 8100.2. Additional information on wireless systems can be found on the DOD Wireless Community of Practice

Knowledge Management (CoP KM) Web site at http://acc.dau.mil. Select the "DOD Wireless" workspace from the main web page.

This document does not cover every wireless system or network in use, or being considered for use, in DOD. The target is for commercial wireless systems, networks, or devices that are used to provide office environment type services (e.g., e-mail, travel applications, connections to office networks) using commercially available wireless equipment and wireless carriers. The intent is for the requirements in this STIG to supplement other OS and network STIGs so that a seamless security infrastructure can be maintained within the DOD enterprise.

DODD 8100.2 excludes RFID technologies from being within the scope of the directive. Provisions do not exist to implement RFID technologies to restrict reading of the tags to only "authorized" people, or to encrypted tag ID's when they are read. However, there may be some R&D efforts in this area. Security implementation guidance based on RFID policy and/or RFID technology, cannot be provided at this time.

In an effort to ensure that the STIG reflects the latest wireless technology, usage trends, and DOD wireless policies and guidance, the document is updated on at least an annual basis. In this version you will find that Chapter 3 has been completely reorganized based on the convergence of wireless devices and the wide deployment of broadband wireless services. We can no longer accurately differentiate wireless laptops from Portable Electronic Devices (PEDs), Personal Digital Assistants (PDAs), and cell phones.

To simplify the discussion, wireless devices and technologies are divided into three categories. *Section 2, WLAN and WPAN Technologies*, discusses WLAN and WPAN network technologies and security policies. *Section 3, Remote Wireless Access Technologies*, discusses remote access devices such as mobile telephones and personal data devices and various wireless protocols (e.g., cellular, WWAN) used to provide Internet and remote DOD network connectivity for these devices. Lastly, *Section 4, Wireless Two-Way Messaging and E-mail Technologies* discusses wireless messaging technologies such as two-way paging and e-mail. Wireless devices and systems that do not meet the security requirements of this STIG or of DODD 8100.2 should not be used to store, process, or transmit DOD information unless approved by the DAA as necessary to meet specific mission requirements.

Appendix C, Wireless LAN Site Survey Guide, provides procedures for a critical component of a WLAN system design, which is the site survey. The new DISA Wireless LAN Security Framework document can be found at Appendix D. The Framework is designed to assist in coordinating wireless LAN acquisition, development, architecture design, and implementation.

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 STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the MAC II Sensitive level, containing unclassified but sensitive information.

1.3 Scope

This document is a requirement for all DOD administered systems and all systems connected to DOD networks. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**" implies mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This will make all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" is considered a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "[*N/A: CAT III]* ").

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that has a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

1.6 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG 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/. The Secret Internet Protocol Router Network (SIPRNet) URL is http://iase.disa.smil.mil/. Access to the STIGs on the IASE web server requires a network connection that originates from a **.mil** or **.gov** address. The STIGs are available to users that do not originate from a **.mil** or **.gov** address by contacting the FSO Support Desk at DSN 570-9264, commercial 717-267-9264, or e-mail to **fso_spt@ritchie.disa.mil**.

1.7 Document Revisions

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

2. WLAN AND WPAN TECHNOLOGIES

2.1 Introduction

Wireless Local Area Networks (WLANs) and Wireless Personal Area Networks (WPANs) provide authorized users access to resources that they are not physically connected to, just as if they were sitting at their desk. WLANs are generally developed as an extension to an existing wired infrastructure, although they may be standalone as well. The mobility of WLANs introduces security issues that must be addressed. Standards bodies and industry are consistently working on evolving the technologies that will improve data rate, range, and security in wireless networking solutions. WPANs operate in the Personal Operating Space (POS) of a user, which extends 10 meters in any direction.

The majority of all short-range WLAN and WPAN standards development has occurred in two systems—IEEE 802.11 and IEEE 802.15 (Bluetooth).

- *(WIR0010: CAT III) The IAO will ensure that WLAN systems are approved by the DAA prior to installation.*

- *(W1R0015: CAT IV) The IAO will maintain a list of all DAA approved WLAN devices. The list will include access point MAC address; access point IP address; wireless client IP address; wireless client MAC address; wireless channel set for each access point; access point DHCP range; type of encryption enabled; encryption key used; access point SSID; manufacturer, model number, and serial number of wireless equipment; equipment location; and assigned users with telephone numbers.*

- *(WIR0030: CAT III) The IAO will ensure that wireless devices that connect directly or indirectly (hot-sync) to the network are added to the site SSAA.*

- *(WIR0060: CAT II) The IAO will ensure that WLAN systems are compliant with overall network security architecture, appropriate enclave security requirements, and DODD 8100.2 before they are installed.*

- *(N/A: N/A) The IAO will ensure that WLAN systems are designed using a defense-in-depth approach using multiple layers of security as described in Section 2.2.6, IEEE 802.11 WLAN Implementation Compliance Requirements.*

- *(WIR0080: CAT II) The IAO will ensure that WPAN wireless devices (e.g., Bluetooth) are not used to transfer, receive, store, or process DOD information unless FIPS 140-2 compliant cryptographic modules are used to encrypt the data during transmission*

2.2 IEEE 802.11 Wireless LAN Systems

The Institute of Electrical and Electronic Engineers (IEEE) 802.11 wireless local area network standard defines the interoperability requirements for wireless local area networks operating in

the 2.4 and 5 GHz unlicensed bands. Products using the 802.11b standard operate in the 2.4 GHz band at a maximum data rate of 11Mbps while products using the 802.11g standard operate in the same frequency range as 802.11b equipment but at a data rate of up to 54 Mbps. Products using the 802.11a standard operate in the 5 GHz band with a data rate of up to 54 Mbps.

The IEEE 802.11 standards group primarily defines the WLAN standard. There is a sub-committee or sub-group for each component of the 802.11 standard.

- IEEE 802.11a is the standard for high speed WLANs in the 5 GHz band. The standard defines data rates between 6-54 Mbps with 6, 12, and 24 Mbps required for any implementation. Most vendors have implemented either WEP or WPA security services in 802.11a products.

- IEEE 802.11b is the standard for WLANs in the 2.4 GHz band. The standard defines 1, 2, 5.5, and 11 Mbps data rates. Most vendors have implemented either WEP or WPA security services in 802.11b products.

NOTE: A number of WLAN vendors have released IEEE 802.11b WLAN products that can operate at 22 Mbps data rates. These products are based on proprietary extensions to the IEEE 802.11b standard and will not interoperate at 22 Mbps with other vendors' WLAN systems (but can dynamically adjust to operate at standard 802.11b data rates with other 802.11b/g WLAN systems).

- IEEE 802.11e is a developing standard that will specify Quality of Service (QoS) for WLAN systems that require QoS support (e.g., VoIP WLAN systems).

- IEEE 802.11g is the standard for high speed (up to 54 Mbps) WLANs in the 2.4 GHz band. Most vendors have implemented either WEP or WPA security services in 802.11g products.

NOTE: A number of WLAN vendors have released "Super G" WLAN systems, which operate at 104 Mbps. Super G products are based on proprietary extensions to the IEEE 802.11g standard and will not interoperate at 104 Mbps with other vendors' Super G systems (but can dynamically adjust to operate at standard 802.11b/g data rates with other 802.11b/g WLAN systems).

- IEEE 802.11h is a developing standard that specifies dynamic channel selection and transmission power control for WLAN systems. Its purpose is to minimize interference between IEEE 802.11a WLAN systems and other systems operating in the 5 GHz frequency band such as radar systems, Earth Exploration Satellite Service (EESS) systems, and Space Research Service (SRS) systems.

- IEEE 802.11i (802.11TGi). Task Group I is working to develop enhanced security capabilities for the 802.11 standard. IEEE 802.11i is scheduled for released in mid 2004 and is expected to consist of two components: IEEE 802.1x and Robust Security Network (RSN). See *Section 2.2.3.4, Wi-Fi, WPA, and RSN,* for a description of RSN.

- IEEE 802.11j is the standard for WLAN systems operating in the 4.9 – 5 GHz frequency band in Japan.

- IEEE 802.11n is a developing WLAN standard that will provide data rates in excess of 100 Mbps.

- IEEE 802.1x is the Port Based Network Access Control standard. Included in the IEEE 802.1x standard is Extensible Authentication Protocol (EAP), which provides multiple user-based authentication methods (smart cards, Kerberos, Public Key Infrastructure (PKI), etc.). EAP provides a standard method for user authentication in WLAN systems. Various WLAN vendors have implemented proprietary versions of EAP including:

    - Extensible Authentication Protocol – Transport Layer Security (EAP-TLS): Provides very strong security, but requires that each WLAN user be running a client certificate. Used primarily in enterprises that already have deployed a PKI infrastructure. EAP-TLS provides for certificate-based, mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication; dynamically generated user- and session-based keys are distributed to secure the connection. Windows XP includes an EAP-TLS client.

    - Extensible Authentication Protocol – Tunneling Transport Layer Security (EAP-TTLS): An extension of EAP-TLS, which provides for certificate-based, mutual authentication of the client and network. Unlike EAP-TLS, however, EAP-TTLS requires only server-side certificates, eliminating the need to configure certificates for each WLAN client. EAP-TTLS uses TLS records to tunnel the client authentication.

    - Protected Extensible Authentication Protocol (PEAP): Is similar to EAP-TTLS; however, with PEAP, only EAP may be carried as a protocol inside the tunnel.

    - Lightweight Extensible Authentication Protocol (LEAP): Used primarily in Cisco WLAN access points. It encrypts data transmission using dynamically generated WEP keys, and supports mutual authentication.

    - EAP-MD-5: Provides only minimal authentication capability and is not recommended because of significant security vulnerabilities. Duplicates CHAP password protection.

2.2.1 IEEE 802.11 WLAN Components

To understand WLANs and their associated security, you should understand the two basic elements of a wireless network, namely, the wireless station and the access point.

2.2.1.1 Stations

A wireless station can be a laptop, desktop PC, handheld device, access point, or any other device that utilizes wireless communication, as it's primary means of communicating with other network devices. Stations may be mobile, portable, or stationary and can be used to transmit data or voice (e.g. Voice over IP (VoIP) phones). Wireless NICs are manufactured in the same form factors as their wired counterpart (e.g. Personal Computer Memory Card International Association (PCMCIA) cards, Peripheral Component Interconnect (PCI) cards, Industry Standard Architecture (ISA) cards, Compact Flash (CF) cards, Universal Serial Bus (USB) cards).

The requirements for wireless stations are as follows:

- *(WIR0040: CAT III) The IAO will ensure that all wireless devices, particularly laptops, comply with applicable operating system STIGs.*

- *(WIR0090: CAT II) The IAO will ensure that password protection mechanisms are placed on folders and files on all 802.11-enabled devices.*

- *(W1R0105: CAT III) The IAO will conduct periodic audits and reviews of the WLAN to identify unauthorized devices (unauthorized MAC addresses) connecting to the network.*

2.2.1.2 Access Points

An access point is the entry point from a wireless station to a WLAN, from a WLAN to a wired LAN, or between WLANs. Access points generally consist of a radio, a wired network interface, and management and bridging software. Access point functionality can be implemented using a hardware device or an application installed in another network device (a router for example) and is configured based on architecture requirements. Some vendors have removed the management and bridging software from the access point and placed these features into a wireless switch and then all access points on the network are managed and configured from the wireless switch. In a WLAN system with wireless switches, the access points are usually called access ports and are essentially transceivers (transmitter/receiver of data) with a network interface.

A number of software applications are now available that can be used to turn a laptop computer acting as a wireless station (wireless client) into an access point. A new trick by wireless hackers is to compromise an unsecured wireless laptop and then download access point software onto the laptop, thereby creating a "wireless zombie". The wireless zombie is then configured to attempt to associate with nearby wireless clients by masquerading as a legitimate access point. After a client has been successfully hijacked, the laptop will forward the connection to the hacker's IP address.

2.2.2 Technology Overview

WLANs may utilize infrared technology, narrowband technology, or radio frequency transmission. Data is placed onto a radio wave through a process called modulation, and the

carrier wave acts as the transmission medium (replacing the copper or fiber optic cable of the wired network). In addition to the 2.4 GHz Industrial, Scientific, and Medical (ISM) band, WLAN products are also available that operate in the 5 GHz Unlicensed National Information Infrastructure (UNII) band (IEEE 802.11a), which uses orthogonal frequency division multiplexing (OFDM) as its carrier.

2.2.2.1 Data Transmission

WLANs transmit and receive data using several different methods. IEEE 802.11b standard defines three different physical layers—Baseband Infrared, Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS). The IEEE 802.11a and 802.11g standards specify OFDM as the transmission method.

2.2.2.1.1 Infrared

Infrared-based WLANs are best suited for wireless networks whose requirements are for use within a small group or subnetwork. Infrared signals do not penetrate solid objects, such as walls and floors in a building. There are few commercial implementations of infrared WLANs because access points and stations must be within line of sight when using this transmission method.

Most commercially available infrared transceivers produce a signal even when the device is turned off via software. Covering the transceiver with metallic tape or placing the wireless device into a container with electromagnetic shielding can secure infrared transceivers.

- *(WIR0110: CAT IV) The IAO will ensure that infrared WLAN receivers and transmitters are disabled when not required. The local Certified TEMPEST Technical Authority (CTTA) should be consulted to determine appropriate methods for disabling a specific Infrared wireless device.*

2.2.2.1.2 Spread Spectrum

Most WLANs utilize spread spectrum technology for transmission. FHSS transmissions jump around frequencies at a pre-determined rate/interval. DSSS uses a redundant chipping code. Both technologies rely on the fact that the schemes are known only by the transmitter and receiver (i.e., between wireless devices and access points). FHSS and DSSS do not interoperate. DSSS is used by nearly all 802.11b wireless LAN radios. Radio waves using the 802.11b standard which operated at 2.4 GHz, easily penetrate building walls and have a coverage range of up to a few hundred feet, which is useful when signal must traverse larger areas, such as multi-floor and campus environments.

2.2.2.1.3 OFDM

OFDM is the modulation scheme used by 802.11a and 802.11g WLANs. This method transports data using many carrier waves, with each wave carrying part of the message. The OFDM method has the following advantages when compared to spread spectrum modulation: higher

data rate over a smaller bandwidth; more non-overlapping channels; increased resistance to reflected multipath signals; increased resistance to interference

2.2.2.2 IEEE 802.11 WLAN Topologies

2.2.2.2.1 Infrastructure WLANs

The most common WLAN topology is the infrastructure mode where WLAN stations connect to the wired network through access points. *Figure 2-1, Enclave WLAN Architecture*, shows an example of an infrastructure mode WLAN.

2.2.2.2.2 Ad Hoc Wireless Networks

WLANs may be configured into a peer-to-peer (also known as ad hoc or independent) network that permits devices to communicate directly. This type of implementation can be as basic as two laptops with wireless NICs transmitting data back and forth where no access point is required. Peer-to-peer WLAN communications can bypass DOD required encryption and authentication mechanisms and therefore, these transmissions are vulnerable and could be easily intercepted, providing unauthorized access to DOD data. To mitigate this risk, peer-to-peer WLAN networks must be used only with DAA approval and must comply with the requirements outlined in *Sections 2.1, 2.2.1.1, 2.2.5,* and *2.2.6*. Additionally, the following requirements apply:

- *(WIR0130: CAT II) The IAO will ensure that WLAN Network Interface Cards (NICs) that do not have the capability to turn off or otherwise disable peer-to-peer WLAN communications are not used.*

- (WIR0125: CAT II) The IAO will ensure that mutual authentication between each station on the peer-to-peer network occurs before data is transmitted between stations Wireless LAN Bridges

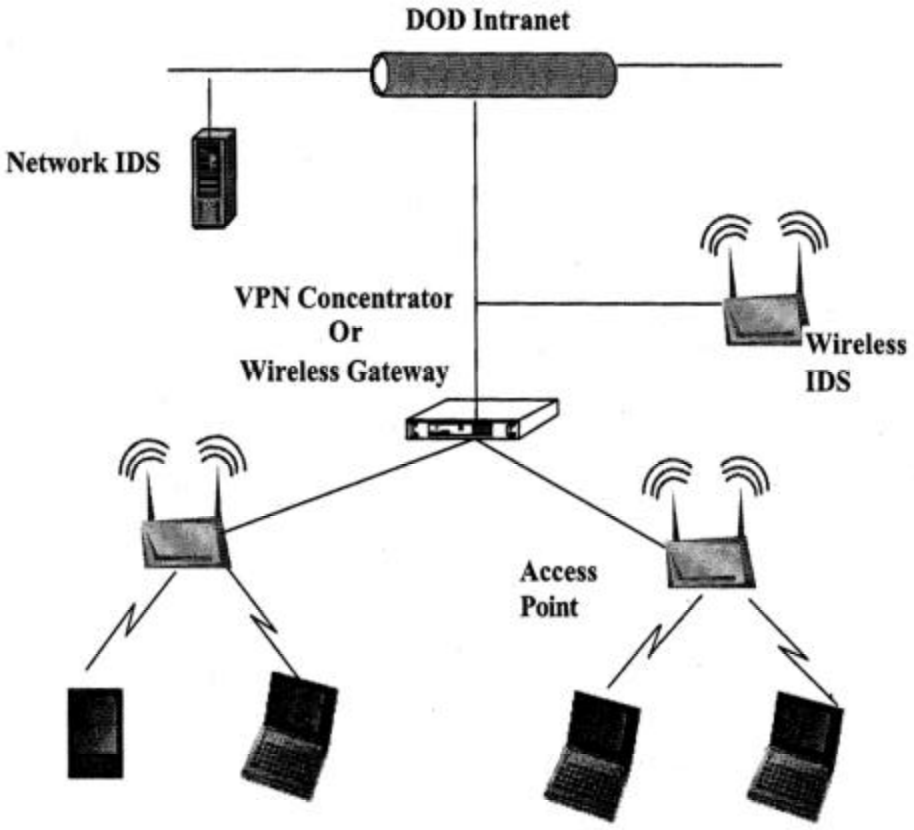


Figure 2-1 Enclave WLAN Architecture

2.2.2.2.3 Wireless LAN Bridges

IEEE 802.11 WLAN systems can be used to provide a wireless communications link (or bridge) between two wired LANs, typically located in adjacent buildings. The hardware used in a wireless LAN bridge is similar to a wireless LAN access point, but instead of only connecting wireless clients to the wired network, bridges are primarily used to connect other wireless LAN bridges to the network.

NOTE: Most wireless LAN bridges can connect to both clients and other bridges. If a WLAN bridge is configured to allow connections to WLAN clients, the bridge should be configured IAW Section 2.2.6 of this STIG.

- *(WIR0270: CAT II) The IAO will ensure that a FIPS 140-2 compliant VPN or security gateway (layer 2 or 3 with Triple Data Encryption Standard (3DES) or AES) are used to secure the WLAN bridge wireless communications channel.*

The IAO will ensure that wireless bridges are protected from attack as follows:

- *(WIR0290: CAT II) The IAO will ensure that bridges are placed in an isolated subnetwork, DMZ, or Virtual LAN (VLAN) from the DOD network by placing a VPN or security gateway between the bridge and the local DOD network.*

- *(NET0210: CAT II) The IAO will ensure that wireless bridges are physically secured to prevent tampering/reprogramming (prevent unauthorized physical access).*

- *(WIR0320: CAT II) The IAO will ensure that HTTP and SNMP interfaces are turned off after initial configuration.*

- *(WIR0330: CAT I) The IAO will ensure password access to the wireless bridge is turned on.*

2.2.3 802.11 Wireless LAN Security

Like all IEEE 802 standards, the 802.11 standards (802.11a, 802.11b, and 802.11g) focus on the bottom two levels of the OSI model—the physical and data link layers. Security mechanisms of the 802.11 standard, such as access control and encryption, operate at the data link layer, particularly the Media Access Control (MAC) sublayer. The 802.11 MAC sublayer can work seamlessly with standard Ethernet, via a bridge or access point, to provide a connection between wireline and wireless nodes. For this reason, once the access point is reached, the same security standards supported by other 802-compliant LANs for access control (such as network operating system logins) and encryption applies (such as IPSec or application-level encryption).

The number of deployments using Wi-Fi has grown dramatically both inside and outside of DOD even though the initial security mechanisms were severely flawed. The IEEE and an industry group, the Wi-Fi Alliance, however, have moved to improve the security of Wi-Fi based networks via a series of stepwise improvements. The first step was the release of the Wi-Fi Protected Access (WPA) definition (described below). WPA fixes a number of the known

security problems with the original 802.11 standard and will work with most legacy equipment, but WPA still does not meet DOD requirements. WPA equipment, as well as software and firmware to upgrade legacy equipment, is now available. The next step in the improvement process is the ratification of the IEEE 802.11i. These changes will be known as the Robust Security Network (RSN) (or WPA2). RSN capable products should be available in late 2004 or early 2005. Upgrading to RSN, however, will require the purchase of new equipment. Also, while RSN is a substantial increase in the security of Wi-Fi networks, it will not provide protection against denial of service attacks.

2.2.3.1 Service Set Identifier (SSID)

Although advertised as a means of simple access control for an access point or group of access points, the SSID should not be considered a safe or reliable access control mechanism. The SSID is an alphanumeric code that corresponds to a specific wireless network (or subsystem). Usually, in the default configuration of an access point, the SSID is transmitted in the clear as a part of a periodic beacon that is sent by the access point or it may be requested in a probe-request frame when a wireless client attempts to associate with an access point with a specific SSID. Most access points permit the broadcast of their identifier so that wireless stations within range know that the access point is available for a client to connect to it. Good security practice dictates that an access point should not advertise its presence and should only respond to clients that know its SSID.

- *(WIR0140: CAT III) The IAO will ensure that SSIDs are changed from the manufacturer's default to a pseudo random word consisting of a combination of characters, numbers, and special characters.*

- *(WIR0150: CAT II) The IAO will ensure that the SSID broadcast mode is disabled. WLANs that do not allow the SSID broadcast mode to be disabled will not be used.*

2.2.3.2 MAC Address Filtering

Just as an access point or group of access points can be identified by the SSID, a client in a WLAN can be identified by the unique MAC address of its 802.11 wireless NIC. Therefore, another type of access control can be implemented based on permitting access to only those MAC addresses that are known to belong to legitimate users. Only devices having MAC addresses matching those on the list are permitted access to the WLAN. MAC related information in the header of a datagram is sent in the clear so it is possible that the MAC address can be obtained by eavesdropper and spoofed in an attempt to gain access to the WLAN. Although MAC address filtering provides only minimal security, it should be implemented as a deterrent to the casual hacker.

- *(WIR0160: CAT II) The IAO will ensure that MAC address filtering is turned on at each access point.*

NOTE: MAC address filtering may not be practical for large WLAN implementations, unless the WLAN management system allows for MAC distribution lists to be centralized and automatically distributed to the point of authentication.

2.2.3.3 Wired Equivalent Privacy (WEP) Protocol

There are two types of authentication/access control defined by the WEP protocol—open system authentication and shared key authentication. With open system authentication, the access point grants access to stations with an authorized SSID. With shared key authentication, both the access point and any station authorized to connect to the access point share a key that is used for both authentication and encryption.

Most WLAN products offer both 64-bit and 128-bit WEP encryption. The WEP encryption key is comprised of a shared key and a 24-bit initialization vector (IV). The 64-bit WEP key is formed by combining a 40-bit shared key and the IV, while the 128-bit WEP key is formed by combining a 104-bit shared key and the IV. Some WLAN products allow the IV to be changed periodically, including as often as after every transmission.

Unfortunately, the WEP protocol is a flawed application of cryptographic principles and design. Some known attacks exploit problems with both the encryption and authentication provided by WEP. These flaws occur because the current WEP standard uses static, reusable shared secret keys and a poor implementation of the RC4 algorithm. In addition, the IV is transmitted in clear text and is usually changed in a predictable pattern. Several studies have concluded that with minimal hardware/software and statistical analysis (intercepting a minimal amount of wireless traffic), WEP keys can be easily determined. Then with these keys exploited (shared secret key and IV), an unauthorized individual can determine the encryption key and gain access to the data that is being transmitted over the air as well as, potentially, to all connected backend resources within the environment.

2.2.3.4 Wi-Fi, WPA, and RSN

Wi-Fi is a trade-group certified wireless networking standard that relies on the IEEE 802.11x specifications. When a wireless LAN product is identified as Wi-Fi compliant, the product has been evaluated by the Wi-Fi Alliance trade group and found to meet the requirements found in the IEEE 802.11x standards.

The Wi-Fi Alliance requires that Wi-Fi Protected Access (WPA) be included in WLAN devices in order for the device to be certified as Wi-Fi compliant. WPA relies on an interim version of the IEEE 802.11i WLAN security specification.

WPA does not rely on fixed WEP encryption keys, but instead uses a network password that initiates a key rotation every 10,000 bytes of data using the 802.11i's Temporal Key Integrity Protocol (TKIP). Since WPA still uses the RC4 encryption algorithm found in WEP, Wi-Fi certified wireless LAN products with WPA will not meet DOD security requirements.

Robust Secure Network (RSN) uses dynamic negotiation of authentication and encryption algorithms between access points and stations. The authentication schemes are based on IEEE 802.1x and EAP with AES as the encryption algorithm. Dynamic negotiation of the authentication and encryption algorithms allows the use of new algorithms as they are developed. Figure 2-*2, Robust Secure Network,* details the steps of the RSN protocol.

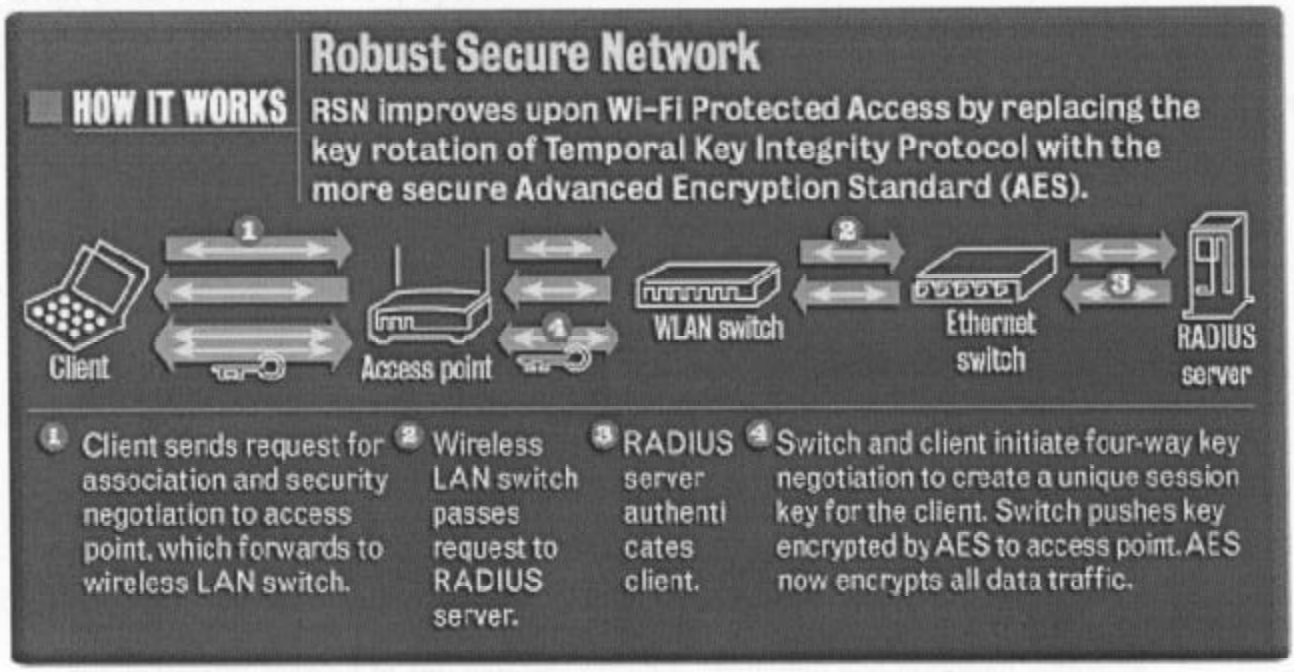


Figure 2.2. Robust Secure Network

2.2.4 SecNet-11™

The Secure Wireless Local Area Network (SecNet-11™) developed by Harris, provides transparent, NSA Type 1 encrypted data communications in a WLAN environment. The SecNet-11 wireless network interface card uses a Harris Sierra™ Encryption Module, Intersil PRISM™ II chipset, and Baton encryption algorithm. The card operates in the unlicensed 2.4 GHz Industrial, Scientific, and Medical (ISM) frequency band using a modified IEEE 802.11b protocol, which takes into account crypto delays. The cryptographic function is embedded in the card. SecNet-11 users can send and receive secure data, voice, and video between and among equipped wireless stations. The SecNet-11 is certified for processing data classified up to DOD SECRET.

The SecNet-11 only provides data encryption; it does not have any user identification or authentication capabilities. Therefore, when the SecNet-11 is used to secure a wireless LAN, additional identification and assurance equipment is needed to meet the security requirements of *DOD Directive 8100.2*.

NSA distributes both classified and unclassified operational keys for the SecNet-11 WLAN; therefore, SecNet-11 is available for unclassified WLANs that process highly sensitive information. COMSEC accounts are required for organizations that plan to use the SecNet-11.

Draft CNSS Instruction 3034, Operational Security Doctrine for the SecNet-11 Wireless Local Area Network Interface Card, should be reviewed before implementing a SecNet-11 WLAN.

Harris is developing a new NSA Type 1 certified WLAN product called the SecNet-54™, which will provide a WLAN based on the IEEE 802.11a, b, or g standards (depending on which radio adapter is used). The SecNet-54 is expected to be available by Q3 CY 2005 and will be certified to process classified information up to Top Secret.

- *(WIR0200: CAT III) The IAO will ensure that the CTTA has been notified before installation and operation of WLANs intended for use in processing or transmitted classified data, including the SecNet-11.*

2.2.5 Security Issues with Windows XP and Embedded Wireless Systems

Windows XP has inherent wireless support features, provided by the Wireless Zero Configuration (WZC) service. The WZC service has a number of security vulnerabilities:

- The Automatic Network Detection and Association feature, which is enabled by default in Windows XP (pre XP SP1), causes the computer to automatically detect and attempt to associate (connect) to any wireless device that can be "seen" by the wireless NIC in the computer. When Windows XP SP1 is installed, the WZC service will attempt to automatically connect to wireless networks based on the networks listed in the "Preferred Networks" list. This default setting can be changed to allow the WZC service to automatically connect to any wireless network, including non-preferred networks.

- Windows XP will "leak" SSID information on any registered and approved SSID to which it has been previously connected. A list of all the access points to which the computer has ever connected is stored in XP. Upon boot-up or when out of access point range, the computer continually transmits queries, attempting to reconnect to an access point. These queries contain the SSID of all access points to which the computer has previously connected. A hacker can easily sniff the content of these queries, obtain the embedded SSIDs, and use the information to program a rouge access point. (This is an example of why SSIDs are not a good security mechanism.)

- When a third party PEAP utility is used for authentication, each 802.11-associated update to Windows XP may overwrite the PEAP settings. In most cases the PEAP utility will have to be reinstalled.

- *(WIR0163: CAT III) The IAO will ensure that the Windows XP WZC service is disabled in any Windows XP computer that is used on a wireless LAN. This setting should be verified whenever new software or XP updates are installed on the computer.*

- *(WIR0164: CAT III) The IAO will ensure that only WLAN drivers and WLAN management software from third party sources that do not depend on the Windows XP WZC service are used in Windows XP computers. (Check with WLAN vendor prior to purchasing equipment.)*

NOTE: The Windows XP WZC service may not be used to manage WLAN connections to the computer. Instead, the WLAN software that is usually provided by the WLAN interface card vendor should be installed and used.

- *(WIR0165: CAT III) The IAO will ensure that WLAN users with Windows XP computers remove the WLAN NIC whenever wireless service is not being used.*

Laptop computers with embedded wireless LAN cards (mini PCI cards) are particularly susceptible to the Windows XP wireless vulnerabilities described above. Most laptop vendors provide a software utility to manage WLAN connections for the embedded wireless cards. The utility usually provides a feature that allows a laptop user to turn off the WLAN card radio. The default setting of all embedded WLAN card radios should be set to the ***"OFF"*** setting.

- *(WIR0166: CAT III) The IAO will ensure that Windows XP computers with embedded wireless LAN cards will only be purchased after it has been verified by test that the installed WLAN interface card can be operated with the Windows XP WZC service disabled and that the laptop vendor provides a WLAN card management utility. The WLAN card management utility should have the capability to turn off the radio of the embedded WLAN card.*

- *(WIR0167: CAT III) The IAO will ensure that laptops with embedded WLAN cards have the WLAN card radio set to OFF as the default setting.*

2.2.6 IEEE 802.11 WLAN Implementation Compliance Requirements

The compliance requirements in this section apply to WLAN access points, bridges (that allow wireless client connections), stations (clients), gateways and switches.

- *(WIR0011: CAT IV) The IAO will ensure that WLAN devices installed outside the United States have been approved by the local US Forces command and /or host nation.*

2.2.6.1 Classified WLAN Systems

Currently there are no NSA approved WLAN devices for storing, processing, or transmitting classified (Top Secret) and/or SCI information.

- *(WIR0170: CAT II) The IAO will ensure that WLANs are not used to store, process, or transmit classified (Top Secret) and/or SCI information.*

- *(WIR0180: CAT II) The IAO will ensure that WLAN devices (for all classification/sensitivity level of information) are not permitted in a permanent, temporary, or mobile Sensitive Compartmented Information Facility (SCIF).*

- *(WIR0190: CAT II) The IAO will ensure that computers with embedded WLAN systems that cannot be removed by the user are not used to store, process, or transmit classified information).*

- (*WIR0011 CAT IV) The IAO will ensure that WLAN devices installed outside the United States have been approved by the local US Forces command and/or host nation.*

The DAA has the responsibility to ensure that only NSA Type 1 certified WLAN systems are used for the wireless transmission of classified information. All wireless systems must receive the approval of the Defense Security Accreditation Working Group (DSAWG) prior to connecting them to the SIPRNet. Currently, the Harris SecNet-11 is the only NSA Type 1 certified commercial WLAN for storing, processing, or transmitting classified (Secret and Confidential) information.

- *(WIR0010: CAT III) The IAO will ensure WLAN systems used for processing classified (SECRET and Confidential) information are approved by the DAA.*

- *(WIR0203: CAT I) The IAO will ensure that only NSA Type 1 certified WLAN systems are used for wireless transmission of classified information.*

- *(WIR0204: CAT I) The IAO will insure that all WLAN systems connected to the SIPRNet have been approved by the DSAWG.*

- *(WIR0210: CAT II) For WLANs approved by the DAA for processing Secret or Confidential information, the IAO will ensure high assurance DOD PKI certificates are used for user authentication in compliance with DOD policy. (SecNet 11 does not provide user identification and authentication.)*

- *(WIR0220: CAT II) For WLANs approved by the DAA for processing Secret or Confidential information, the IAO will ensure file system encryption is used on all WLAN client devices with an NSA Type 1 encryption software or technique.*

- *(WIR0225: CAT II) The IAO will ensure that WLANs are not operated in areas where classified information is electronically stored, processed, or transmitted unless:*

  - *Approved by the DAA in consultation with the CTTA.*

  - *The WLAN equipment is separated from the classified data equipment the distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented.*

- *(NET0210: CAT II) The IAO will ensure that access points and clients for wireless devices processing classified data, including the SecNet-11, are physically secured to prevent tampering/reprogramming (prevent unauthorized physical access).*

- *(WIR0193: CAT II) The IAO will ensure that all laptop computers connected to the SIPRNET do not have internal wireless NIC.*

2.2.6.2 Unclassified WLAN Systems

With DAA approval, 802.11a, 802.11b, and 802.11g solutions will be used for unclassified data provided all of the following conditions are met:

- *(WIR0140: CAT III) The IAO will ensure that SSIDs are changed from the manufacturer's default to a pseudo random word consisting of a combination of characters, numbers, and special characters.*

- *(WIR0150: CAT II) The IAO will ensure that the SSID broadcast mode is disabled. WLANs that do not allow the SSID broadcast mode to be disabled will not be used.*

- *(WIR0160: CAT II) The IAO will ensure that MAC address filtering is turned on at each access point.*

- *(WIR0230: CAT II) The IAO will ensure that the wireless LAN provides a session timeout capability and the timeout is set for 15 minutes or less depending on local security policy.*

- *(WIR0240: CAT II) The IAO will ensure that PKI certificates are used for identification and authentication (I&A) of the user.*

- *(WIR0250: CAT II) The IAO will ensure that the WLAN access point is set to the lowest possible transmit power setting that will meet the required signal strength of the area serviced by the access point.*

- *(WIR0260: CAT II) The IAO will ensure that file system encryption is used on all WLAN client devices*

- *(WIR0270: CAT II) The IAO will ensure that a FIPS 140-2 compliant VPN (Layer 2 or 3 with 3DES or AES) or security gateway is used to secure the WLAN system.*

- *(WIR0280: CAT II) The IAO will ensure that if a wireless LAN device is to be used to access a DOD network via the Internet through a public WLAN/Internet gateway (e.g., airport or hotel "hotspot"), the requirements for PDAs for remote Internet access listed in Section 3.4 of the Wireless STIG and the requirements in the Secure Remote Computing STIG will also be met.*

- *(WIR0075: CAT III) The IAO will ensure that the organization periodically screens for unauthorized or rouge access points, stations, and bridges. Local security policy will address the frequency for which these screenings should occur.*

The IAO will ensure that access points are protected from attack as follows:

- *(WIR0290: CAT II) The IAO will ensure that access points are placed in a screened subnet (DMZ), or Virtual LAN (VLAN) and separated from the wired internal network. A VPN concentrator or wireless gateway is placed between the access point and the local DOD network as shown in Figure 2-1, Enclave WLAN Architecture.*

- *(WIR0300: CAT II) The IAO will ensure an Intrusion Detection System (IDS) (network IDS/IPS or wireless IDS/IPS) is used to monitor the wireless network.*

It is recommended that a wireless IDS be used to continuously monitor approved wireless networks and search for unapproved "rouge" wireless networks at all DOD sites with either wired and wireless computer networks. Most likely the next version of the Wireless STIG and Enclave STIG will list this recommendation as a requirement.

- *(NET0210: CAT II) The IAO will ensure access points are physically secured to prevent tampering/reprogramming (prevent unauthorized physical access).*

- *(WIR0320: CAT II) The IAO will ensure HTTP, SNMP, and other management ports are turned off after initial configuration. These ports are turned on only for firmware upgrades.*

- *(WIR0330: CAT I) The IAO will ensure password access to the access point management console is turned on and configured with a password, which complies with DOD password policies.*

The IAO will ensure that client stations are protected as follows:

- *(WIR0100: CAT III) The IAO will ensure that a personal firewall is implemented on each 802.11-enabled wireless device.*

- *(WIR0090: CAT III) The IAO will ensure that password protection mechanisms are placed on folders and files on the 802.11-enabled wireless device.*

- *(WIR0040: CAT II) The IAO will ensure that all stations comply with applicable operating system STIGs*

WLAN stations (e.g. PCs, laptops, PDAs) should only be purchased after it has been verified that a personal firewall, antivirus software, and file encryption software are available for that equipment.

2.2.7 WLAN Common Criteria Protection Profiles

NSA is developing a suite of protection profile (PP) requirement documents focused on wireless networking technologies. For Wireless LANs, the first protection profile, the "US Government Wireless Local Area Network (WLAN) Access System for Basic Robustness Environments Protection Profile," focuses on IEEE 802.11a/b wireless LAN access devices. This PP specifies

the minimum-security requirements for a WLAN Access System used by the US Government in Basic Robustness Environments. The target robustness level of "basic" is specified in DOD Instruction 8500.2.

A wireless LAN access system can be defined as one or more components that provide secure wireless access to a wired or wireless network. This PP discusses a typical wired to wireless configuration. However the PP does not preclude any other wireless configuration that may exist. This wireless access system may vary in the type of components used to provide access to the wired LAN. This PP does not dictate a particular configuration. Instead the PP addresses the security requirements for the system that allows access to the wired network while performing management functions within the system. The security requirements of the Target of Evaluation (TOE) are identification and authentication (I&A), audit, encryption, information flow control, and administration. This PP requires privacy and integrity of communications over a WLAN, using commercially available cryptographic algorithms. The assurance requirements specified in the PP are Evaluation Assurance Level (EAL) 2 augmented with flaw remediation, assurance maintenance and misuse analysis.

In early October 2003, the Wireless Access System PP received approval from the National Security Agency (NSA) PP Review Board (PPRB) and an accredited Common Criteria (CC) Test Lab submitted it to NIAP for evaluation. Once the lab completes evaluation of the Wireless Access System PP, the PP will be available as the official US Government security requirements for wireless access systems used on US Government systems at the Basic robustness level.

NSA is also developing a WLAN Client for Basic Robustness Environments PP. The final draft of this profile was submitted to the PP Review Board. This PP specifies similar requirements as in the wireless access system PP, with the exception of auditing requirements at the client device.

2.3 Bluetooth WPAN

The Bluetooth Special Interest Group (SIG), which is a group of companies interested in promoting Bluetooth wireless solutions, developed the Bluetooth specification. IEEE 802.15 Wireless Personal Area Networks (WPANs) formalizes the specification. The primary goal of the specification is to define wireless connectivity for fixed, portable, and moving devices within or entering a Personal Operating Space (POS) of the user. The goal is to achieve interoperability (e.g., no radio interference) between a WPAN device and any IEEE 802.11 WLAN device. Interference between WLAN technology and Bluetooth (IEEE 802.15 WPAN) networks can be a significant problem, as they both operate in the same frequency band. The IEEE 802.15 Task Group 2 (TG2) is developing coexistence mechanisms for the two standards. The IEEE 802.15.1 standard defines device-level authentication at the data link layer and data encryption at the physical layer.

Bluetooth enabled electronic devices connect and communicate wirelessly via short-range (100m or less) in ad hoc networks called piconets. Bluetooth and 802.11 wireless technologies share some characteristics and overlap slightly in some usage models, but they serve fundamentally different purposes.

Security for a Bluetooth network can be found at both the physical and link layers of the protocol. Bluetooth uses FHSS modulation that provides a 1600 hops/sec frequency hopping rate and, along with low output transmission power (100 mw max transmission power) and short transmission range (most devices transmit <10 m [while transmitting at 1 mW]), provides a formable barrier to anyone trying to eavesdrop on a connection. However, a hacker can synchronize a rogue Bluetooth device to any Bluetooth connection by catching only one packet of a transmission since the hardware address in each data packet defines the hopping frequency being used.

At the link layer, Bluetooth provides both authentication and encryption. Each Bluetooth device has a unique device address that is used to authenticate the devices. Either one-way, two-way, or no authentication may be specified. For encryption, Bluetooth uses an algorithm where the key length is selectable between 8 and 128 bits. This allows Bluetooth to be used in countries that limit the length of encryption keys. The encryption key size in a specific Bluetooth device must be set at the factory in order to prohibit the user from overriding the permitted key size.

Bluetooth has many of the same security management problems found with the IEEE 802.11b standard in that no process is defined for managing the process for issuing, validating, and revoking link keys. Bluetooth provides for built-in encryption and authentication, but like 802.11b, additional security products must be used to mitigate this standard's inherent security shortcomings. There were no Bluetooth specific FIPS 140-2 security products available at the time this document was released. One vendor claims that their FIPS 140-2 certified wireless VPN (Certicom's movianVPN GSE) will work with Bluetooth systems.

2.3.1 Bluetooth Compliance Requirements

2.3.1.1 Classified Information

- *(WIR0182: CAT III) The IAO will ensure that Bluetooth devices are not used to send, receive, store, or process classified messages.*

- *(WIR0181: CAT II) The IAO will ensure that Bluetooth devices are not permitted in a permanent, temporary, or mobile SCIF unless the transmit capability (RF and IR) is rendered completely inoperable.*

- *(WIR0225: CAT II) The IAO will ensure that Bluetooth Devices are, if allowed, operated in areas where classified discussions or data processing takes place only when:*

  - The DAA, in consultation with the CTTA, has approved that Bluetooth devices can be brought into the facility and/or used in the facility.

  - The device's voice recording capability is rendered inoperable.

  - The Bluetooth devices are separated from the classified data equipment a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented.

2.3.1.2 Unclassified Information

- *(WIR0080: CAT II) The IAO will ensure that Bluetooth devices are not used to store, process, or transmit DOD information, unless FIPS 140-2 validated cryptographic modules are used to encrypt the data during transmission.*

- *(WIR0083: CAT III) The IAO will ensure that the Bluetooth capability is removed or disabled from the wireless device if FIPS 140-2 validated cryptographic modules are not used.*

2.4 Wireless Mice and Keyboards

Interest in using wireless keyboards and mice by DOD offices has been increasing. These systems use a number of wireless technologies for transmitting data to the computer, including WLAN, Bluetooth, and infrared. A wireless mouse transmits only telemetry data (right, left, etc.) and therefore poses little to no security risk to DOD systems. Wireless keyboards, on the other hand, transmit users' keystrokes, which can be easily read by a nearby receiver and, therefore, can be a significant security risk.

The following conditions will be met prior to the use of wireless mice or keyboards:

- *(WIR0010: CAT III) The IAO will ensure that wireless mice and keyboards are used only after the approval of the DAA.*

- *(WIR0132: CAT II) The IAO will ensure that if wireless keyboards are used, applicable requirements listed in the Wireless STIG, Sections 2.2.6 and 2.3 are followed.*

2.5 Voice Over IP (VoIP) WLAN Systems

Wireless VoIP systems offer the convenience of a mobile or cellular phone combined with the cost savings of a VoIP telephone system.

The following conditions will be met prior to the use of wireless VoIP systems:

- *(WIR0010: CAT III) The IAO will ensure that wireless VoIP are used only after the approval of the DAA.*

- *(WIR0133: CAT II) The IAO will ensure that all wireless VoIP systems comply with applicable requirements in the Wireless STIG, Section 2.2.6, and the VoIP STIG.*

3. WIRELESS REMOTE ACCESS TECHNOLOGIES

3.1 Introduction

The use of Personal Electronic Devices (PEDs), including cell phones and PDAs, is widespread in the DOD. Various wireless technologies are in use, including cellular, broadband cellular (3G), broadband wireless, and WLAN that provide wireless network connectivity for PEDs. The convergence of mobile phone, PDA, and wireless email into one device has made it more difficult to determine the security requirements of these devices when used in the DOD environment.

This section will focus on cellular, broadband cellular (3G), and broadband wireless (WWAN) technologies and the secure use of cell phones and PDAs that use these wireless technologies to connect to the Internet and DOD networks

3.2 Cellular Technologies, Protocols, and Security

3.2.1 Wireless Telephone Protocols

This section provides an overview of radio interface standards and protocols used by wireless carriers in the United States.

Analog wireless communications protocols, in general, provide no security services. Analog cellular calls can be easily intercepted and the Mobile Identification Number (MIN) and Electronic Serial Number (ESN) can then be extracted from the intercepted call. Analog wireless phones can be easily cloned using intercepted MINs and ESNs. However, nearly all analog wireless carries have added device-level authentication, which is cross-referenced to the MIN and ESN, and ensures that a wireless phone is registered with the network before a call will be connected. Voice encryption services are not provided.

All digital wireless carrier systems provide device level authentication and data encryption. Some networks, such as GSM, also provide user authentication.

3.2.1.1 1st Generation (1G) Technologies (Analog)

The AMPS (Advanced Mobile Phone Service) has been the American analog cellular standard since the 1970s. Developed by AT&T, this standard uses FDMA (frequency division multiple access) whereby the assigned radio spectrum is divided into channels and each channel is used for either the receive or the transmit portions of the wireless phone call (see *Figure 3-1, Wireless Radio Interface Protocols*). One of the shortcomings of AMPS is the lack of inherent security features (authentication and data encryption) in the standard.

(For an on-line tutorial of cellular history and technology, visit the following web site—http://www.privateline.com/Cellbasics/Cellbasics.html.)
Currently, the FCC requires all US cellular carriers to provide analog cellular services. In August 2002 the FCC ruled that US cellular carriers could begin to phase out analog cellular services in five years.

3.2.1.2 2nd Generation (2G) Technologies (Digital)

- *Code division multiple access (CDMA).* TIA IS-95, published by the Telecommunications Industry Association (TIA), is the CDMA standard developed by Qualcomm. CDMA currently provides 12-16 times the channel capacity over AMPS. CDMA has been implemented by a number of national wireless carriers, including, Verizon, and Sprint PCS. CDMA provides data services with rates of about 9.6 kbps. With CDMA, the frequency spectrum is shared by all calls. Each call is assigned a pseudo random code and the receiver in both the mobile phone and base station will only accept the call with the correct code (see *Figure 3-1, Wireless Radio Interface Protocols*).

- *Time division multiple access (TDMA).* TDMA is the generic name for an air interface technology that is used by a number of standard digital radio systems including IS-136 and GSM. The IS-136 standard is published by the TIA and is the current United States standard for both the cellular (850 MHz) and PCS (1.9 GHz) spectrums. TDMA has been implemented by a number of national wireless carriers including Cingular and AT&T Wireless. (In 2003 Cingular started transitioning many of their TDMA customers over to their new GSM system.) Each communications channel is divided into six time slots with two being used for each wireless connection. TDMA provides a three to one gain in network capacity over an analog cellular network (see *Figure 3-1, Wireless Radio Interface Protocols*) and data rates of about 9.6 kbps. (IS-136 is also known as D-AMPS or Digital-AMPS.)

- *Iridium.* The Iridium satellite phone system is a TDMA system but it does not operate in the cellular frequency band.

- *Global System for Mobile communications* (*GSM).* GSM is the primary digital wireless phone standard throughout the world, except for primarily North America and Japan. The 3rd Generation Partnership Project (3GPP) of the European Telecommunication Standards Institute (ETSI), a European standards group, manages the GSM standard. GSM is a form of TDMA, but it has a different timing standard than the IS-136 version of TDMA. Security features, including customer billing, authentication information, and data encryption are recorded on a SIM (Subscriber Identity Module) card, which must be inserted into the phone before a call can be sent or received. The standard GSM data rate is 9.6 Kbps, but this capacity can be upgraded to 14.4 Kbps. T-Mobile (formerly VoiceStream), AT&T, and Cingular operate GSM networks in the U.S.

- *Integrated Dispatch Enhanced Network (iDEN).* iDEN is a TDMA based digital wireless phone technology that is used by Nextel for their nationwide wireless telephone service. iDEN is a proprietary specification that was developed by Motorola and integrates four wireless services into one digital network—dispatch radio, voice, data, and short message service (SMS). Nextel operates the only iDEN system in the U.S.

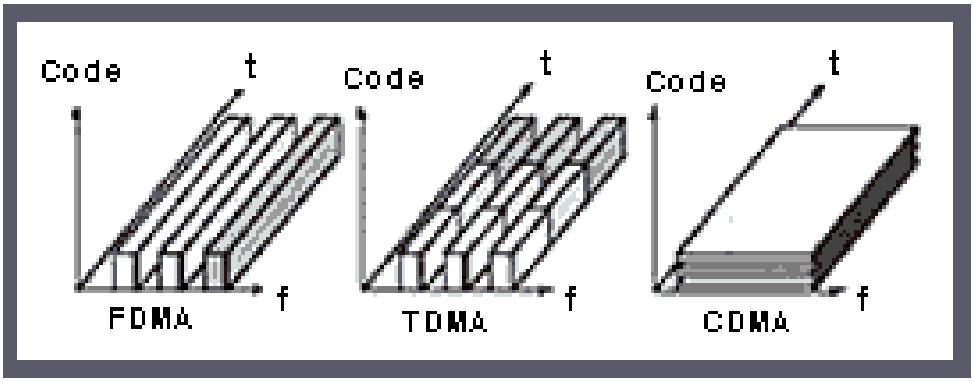


Figure 3-1 Wireless Radio Interface Protocols

3.2.1.3 2.5 Generation (2.5G) Technologies

General Packet Radio Service (GPRS). GPRS is a packet-based digital wireless service and is considered an interim phase for GSM networks transitioning to 3G wireless systems. GPRS is deployed over GSM networks by overlaying a packet based air interface over the existing circuit-switched network. A version of GPRS has also been developed for IS-136 networks, but most U.S. based wireless carriers are using a GSM network as the foundation for their GPRS service. GPRS has maximum theoretical data rate of 171.2 Kbps with a typical user throughput of 56 – 115 Kbps. GPRS is considered an interim step from the transition of 2G wireless services to 3G. Cingular, T-Mobile (formerly VoiceStream), and AT&T Wireless are among the U.S. wireless carriers that have deployed GPRS service to selected markets. The European Telecommunications Standards Institute (ETSI) maintains the GPRS standard.

3.2.1.4 3rd Generation (3G) Technologies

Universal Mobile Telecommunications System (UMTS) is the International Telecommunications Union's (ITU) IMT-2000 vision for a global family of 3G wireless communications systems and consists of five 3G wireless communications standards:

- IMT-2000 CDMA Direct Spread (DS), also known as the Universal Terrestrial Radio Access (UTRA) Frequency Division Duplex (FDD) and includes WCDMA (or W-CDMA) which stands for Wideband Code Division Multiple Access. The Universal Mobile Telecommunications System (UMTS) and UTRA are developed by the 3rd Generation Partnership Project (3GPP).

- IMT-2000 CDMA Multi-Carrier (MC), also known as cdma2000 (3X) was developed by 3GPP2. IMT-2000 cdma2000 includes 1X components (e.g.cdma2000 1X EV-DO).

- IMT-2000 CDMA Time Division Duplex (TDD), also known as UTRA TDD and Time Division - Synchronous Code Division Multiple Access (TD-SCDMA). TD-SCDMA was developed in China and is supported by the TD-SCDMA Forum.

- IMT-2000 TDMA Single Carrier, also known as UWC-136 Enhanced Data Rates for GSM Evolution (EDGE) which is supported by Universal Wireless Communications Consortium (UWCC).

- IMT-2000 Digital Enhanced Cordless Telecommunications (DECT) which is supported by the DECT Forum.

The IMT-2000 family of 3G systems includes three types of Core Network technologies:

- GSM based (using Mobile Application Part (MAP) protocols on top of SS7 protocols for signaling)

- ANSI-41 based (IS-634 protocols for signaling)

- Internet Protocol based

In the U.S., TDMA and GSM carriers will transition to EDGE while CDMA carriers plan to deploy either CDMA 2000 or WCDMA systems. CDMA2000 and WCDMA (UMTS) were developed separately and are 2 separate ITU approved 3G standards.

Enhanced Data Rates for Global Evolution (EDGE) is a TDMA based 3G wireless radio interface standard that provides a migration path for GSM and IS-136 networks to 3G services. EDGE is the standard for IMT-2000 Single Carrier (also called Universal Wireless Communications-136 (UWC-136) and provides three to four times the data rates and throughput over GPRS (up to 384 Kbps theoretical with 115 Kbps considered the typical user data rate). Cingular, AT&T Wireless, and T-Mobile have announced plans to use EDGE for their 3G wireless services. The EDGE standard is supported by both the ITU and ETSI.

NOTE: EDGE is essentially a relatively low cost upgrade for a GSM carrier when compared to other 3G upgrades. This is why most US TDMA carriers, including Cingular, started transitioning their customers to GSM networks in late 2002 and early 2003.

- CDMA 2000 is a trademark of the TIA and has been proposed as the IMT-2000 Multi Carrier standard. CDMA2000 1xRTT, cdma2000 1xEV-DO (Evolution, Data Only) and future CDMA2000 3x were developed to be backward compatible with cdmaOne. Both 1x types have the same bandwidth and chip rate and can be used in any existing 2G cdmaOne frequency band and network. Backward compatibility was a requirement for successful deployment for the USA market. Deployment is straightforward because operators do not need new frequencies. (A list of the complete cdma2000 family of standards can be found at the TIA web site, http://www.tiaonline.org/standards/search.cfm?keyword=IS+2000*). Two interim versions of CDMA 2000 have been deployed or will be piloted in the United States:

    - 1xRTT CDMA (RTT – Radio Transmit Technology) will support up to 144 Kbps packet data in its first release and up to 614 Kbps in the second release. The second phase, 3x, completes the 3G evolution of the IS-95 CDMA

standard. Verizon and Sprint PCS are deploying 1xRTT CDMA systems in select U.S. markets.

- 1xEV-DO (1x Evolution Data Only) is an enhancement to cdma2000 air interface technology optimized for packet data transfer. It is one of the most promising techniques for enabling third-generation (3G) wireless communications systems to deliver Internet Protocol (IP)-based services such as e-mail, Web browsing, e-commerce and telematics. 1xEV-DO technology allows a standard 1.25 MHz cdma2000 wireless communication channel to provide a peak data rate of 2.4 Mb/sec on its forward link, effectively tripling the capacity of each CDMA2000 channel. Verizon has been testing 1xEV-DO networks in several locations in the U.S. 1xEV-DO offers an "always on" user experience, so that users are free to send and receive information from the Internet and their corporate intranets, anytime, anywhere.

- Wideband Code Division Multiple Access (WCDMA) is another approved 3G standard developed by DoCoMo, the dominate Japanese wireless carrier. WCDMA provides data rates up to 2 Mbps and will be piloted by AT&T in several locations in the United States. WCDMA (UMTS) was developed mainly for countries with GSM networks, because these countries have agreed to free new frequency ranges for UMTS networks. Because it is a new technology and in a new frequency band, new radio access networks have to be built. The advantage is that the new frequency band gives plenty of new capacity for operators. 3GPP is overseeing the standard development and has kept the core network as close to the GSM standard as possible. A complete list of the WCDMA family of standards can be found at the 3GPP web site: http://www.3gpp.org/ftp/Specs/html-info/status-report.htm.

3.2.1.5 Other Important Standards

ANSI 41 (with Revisions A, B, C, and D) is the Industry standard for intersystem networking. This provides standards for communications between separate wireless carriers to support seamless roaming by wireless subscribers. Revision D provides the means to validate a wireless phone's MIN and ESN before a roaming call is connected. This is the method that all wireless carriers in the U.S. use to authenticate/validate a phone prior to setting up a wireless phone call.

3.2.2 Cell Phone Security

No conversation transmitted across radio frequencies is completely secure, but you have a higher level of security with digital and personal communications service (PCS) phones than with analog phones. Conversations on analog phones can be intercepted and decoded on inexpensive and readily available radio scanners. However, conversations on digital phones are encoded, which makes them more difficult to decode when intercepted. Now that cellular phones are in use for the transmission of data, the security that the phone and cellular networks provide is even more important.

- Smart cards were introduced in the wireless telephones by the GSM standard as Subscriber Identity Module (SIM) cards. SIM cards were designed as separate tokens located in cellular phones to hold and protect data and applications and to provide a barrier to subscription cloning. Over the years, SIM card functions have been enhanced and now provide secure user authentication and encryption services.

Several cellular phones are now available from General Dynamics and Qualcomm to secure sensitive and classified voice and data cellular communications and meet the NSA Type 1 requirements:

- The Motorola Sectéra Secure GSM (SGSM) cellular phone (available from General Dynamics) provides end-to-end high assurance security over commercial GSM cellular systems. The handset is designed to support hardware clip-in modules and is compliant with the Future Narrow Band Digital Terminal (FNBDT) standard[1]. The Sectéra Security Module utilizes the Type 1 security core developed for Motorola's Iridium® Security Module and Sectéra Wireline Terminal. The Sectéra Wireline Terminal provides secure voice and data when connected to a standard analog handset or PC and provides a transition from STU-III to FNBDT standards. This wireline terminal produces Type 1-4 encryption with PIN access.

- The Qualcomm QSec™-800 is the first cellular phone to provide end-to-end encrypted communications using existing, commercial cellular phone networks implementing CDMA data services. This phone provides high-grade voice security and normal cell phone operation in a single handset. The QSec™-800 offers secure interoperability with STE terminals that are based on the U.S. government's FNBDT-compliant technology and equipment.

- The QSec®-2700 is a new secure cellular phone from Qualcomm that is expected to be available by mid 2004. The phone will provide Type 1 secure-voice communications and secure-data connectivity and will operate over 800 MHz and 1900 MHz CDMA commercial wireless networks. In addition, the QSec 2700 will provide a variety of 3G CDMA2000 1X technology wireless features with data speeds up to 153 Kbps.

3.2.3 Cell Phone Compliance Requirements

- *(WIR0010: CAT III) The IAO will ensure that the DAA has approved the use of any cellular or PCS phone that is used to transmit classified or unclassified DOD information.*

- *(WIR0030: CAT III) The IAO will ensure that wireless devices that connect directly or indirectly (hot-sync) to the network are added to site System Security Authorization Agreements (SSAAs).*

[1] The FNBDT standard defines the process for negotiating the security thread between communications products.

- *(WIR0350: CAT II) The IAO will ensure that only NSA approved Type 1 cellular or satellite phones are used for classified voice or classified data wireless telephone transmissions. The classification level of information transmitted over the phone will not exceed the classification level approved for the phone.*

- *(WIR0360: CAT II) The IAO will ensure that no cellular phones are permitted in a permanent, temporary, or mobile SCIF unless the transmit capability (RF and IR) is rendered completely inoperable.*

- *(WIR0370: CAT II) The IAO will ensure that cellular phones are allowed or operated in areas where classified discussions or data processing takes place only when:*

  - The DAA, in consultation with the CTTA, has approved that cellular phones can be brought into the facility and/or used in the facility.

  - The device's voice recording capability is rendered inoperable.

  - The phones are separated from the classified data equipment a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented.

  - Wireless phones are not connected via hot-sync to a workstation in a SCIF.

- *(WIR0020: CAT II) The IAO will ensure that the 3G cellular wireless data system is used on a laptop computer; the security compliance requirements in paragraph 3.3.5, Broadband Wireless System Compliance Requirements are followed.*

- *(WIR0356: CAT II) The IAO will ensure cellular/PCS phones with digital cameras (still and video) are not allowed in any SCIF or other area where classified documents or information is stored, transmitted or processed.*

- *(WIR0371: CAT III) The IAO will ensure cellular/PCS phones with digital cameras (still and video) are allowed in a DoD facility only if specifically approved by site physical security policies.*

The IAO will ensure that 3G cellular data systems are protected as follows:

- *(WIR0020: CAT III) If the 3G cellular wireless data system is used on a laptop computer, the security compliance requirements in paragraph 3.3.5, Broadband Wireless System Compliance Requirements are followed.*

- *(WIR0020: CAT III) If the 3G cellular wireless data system is used on a PDA, the security compliance requirements in paragraph 3.4.5, PDA Compliance Requirements, are followed.*

3.3 Wireless Broadband Technologies, Protocols, and Security

3.3.1 Introduction

Commercial wireless data services began in the US in the early 1990s as low speed (less then 30 Kbps) data networks and have been used primarily for pagers and wireless PDAs and email devices (e.g. Blackberry). In the late 1990s wireless data broadband services (100 Kbps – 1+ Mbps) started to become available. The development and subsequent deployment of wireless broadband services has followed two paths: cellular based standards (3G services) and IEEE standards based services. This section discusses both legacy wireless data services and IEEE standards based broadband wireless services.

3.3.2 Legacy PDA Wireless Air Interface Protocols

This section describes the two most prevalent slow speed radio interface protocols that have been used in the United States for PDA and laptop wireless Internet access. Most wireless carriers are expected to discontinue these servers starting in 2004.

- Cellular Digital Packet Data (CDPD) is an open standard for packet data service that is integrated with existing AMPS and IS-136 TDMA networks. CDPD provides data rates up to 19.2 Kbps and is one of the primary data protocols for wireless PDA services. CDPD provides device-level authentication and data encryption between the wireless device and the carrier base station. In addition, the standard includes sophisticated anti-cloning protection. AT&T Wireless, Verizon, and GoAmerica provide CDPD services.

- Mobitex is an open standard for a narrow band data packet switching network that is used by several wireless PDAs and the BlackBerry e-mail device. Verizon and AT&T Wireless operate national Mobitex networks. Mobitex security primarily consists of device-level authentication using an embedded device ID number, but this number is subject to the same cloning problems as analog cellular phones. Although the standard includes data bit scrambling, this is done for technical reasons and should not be considered data encryption. Most wireless PDA service providers, including Palm.net, provide secure application level data encryption services.

3.3.3 IEEE 802.16 Broadband Wireless Access (BWA) Technology

The IEEE 802.16 (BWA) standard (also known as Wi-MAX) defines interoperability requirements for Wireless Metropolitan Area Networks (WMANs) that will operate in the 2 – 66 GHz frequency range. These networks offer subscriber local loop service (similar to a local telephone service) and wireless hotspots for Internet connections (similar to an 802.11b WLAN hot-spot) and are expected to compete with both public 802.11 and broadband 3G cellular services. BWA networks focus on the first mile/last mile connection in WMAN networks and provide broadband alternatives to DSL, cable, or T-1 services. Data rates for BWA systems will vary, depending on the specific implementation but subscribers are expected to see rates equal to or greater than T-1 and DSL (1.5 Mbps+).

BWA systems are usually deployed in a PMP (Point to Multipoint) topology where the base station services multiple subscribers located in the broadcast area of the base station. The base station is collocated with an entry point of the service provider's backhaul system and connects to the Internet backbone through the backhaul system. The BWA standard defines an optional topology, called Mesh Mode, for areas of high user density or areas were subscribers do not have line of sight to a base station located at the backhaul system entry point (airhead). In a mesh network, intermediate base stations (intermediate devices) have the capability to route traffic to other intermediate devices until the airhead is reached. Mesh networks are designed so that there are multiple paths between each intermediate device and the airhead, thus providing system redundancy.

WMANs are beginning limited deployment in the United States. In general, WMAN systems do not include security services. Therefore, DOD WMAN subscribers should assume that the WMAN system does not meet DOD security requirements and that additional security measures are required before using these systems.

3.3.4 IEEE 802.20 Mobile Broadband Wireless Access (MBWA) Technology

The emerging MBWA specification is designed to address performance gaps between high data-rate low mobility services of WLAN and WMAN systems and high mobility cellular networks. The goals of the specification are to provide user data rates in excess of 1Mbps, support mobile users in vehicles traveling up to 250 Km/h (150 miles/h), and operate in frequency bands below 3.5GHz. MBWA systems are expected to compete directly with cellular 3G broadband services. Deployment of MBWA systems is not expected until at least 2005.

3.3.5 Broadband Wireless System Compliance Requirements

3.3.5.1 Classified Broadband Wireless Systems

Currently there are no NSA approved Broadband wireless devices for storing, processing, or transmitting classified and/or SCI information.

- *(WIR0373: CAT II) The IAO will ensure that broadband wireless systems are not used to store, process, or transmit classified and/or SCI information.*

- *(WIR0374: CAT II) The IAO will ensure that broadband wireless system devices are not permitted in a permanent, temporary, or mobile Sensitive Compartmented Information Facility (SCIF).*

- *(WIR0375: CAT II) The IAO will ensure that broadband wireless systems are not operated in areas where classified information is electronically stored, processed, or transmitted unless:*

  - Approved by the DAA in consultation with the CTTA.

- The broadband wireless systems is operated in an area where classified information is electronically stored, processed, or transmitted, the broadband wireless system equipment will be separated from the classified data equipment the distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented.

3.3.5.2 Unclassified Broadband Wireless Systems

With DAA approval, broadband wireless systems solutions will be used for unclassified data provided all of the following conditions are met:

- *(WIR0376: CAT II) The IAO will ensure that PKI certificates are used for identification and authentication (I&A) of the user.*

- *(WIR0377: CAT III) The IAO will ensure that a FIPS 140-2 compliant VPN (Layer 2 or 3 with 3DES or AES) are used to secure the broadband wireless systems system.*

- *(WIR0378: CAT III) The IAO will ensure that the requirements in the Secure Remote Computing STIG are met.*

The IAO will ensure that client stations are protected as follows:

- *(WIR0379: CAT III) The IAO will ensure that a personal firewall is implemented on each broadband wireless client device.*

Broadband wireless client equipment (e.g. PCs, laptops, PDAs) should only be purchased after it has been verified that a personal firewall is available for that equipment.

- *(WIR0040: CAT II) The IAO will ensure that all client devices comply with applicable operating system STIGs.*

3.4 PDA Technologies, Protocols, and Security

PDAs can be categorized based on the OS that is used. Currently Palm OS, developed by Palm, and Windows Mobile (formerly Win CE), developed by Microsoft, have the largest market share. Symbian, a joint venture between Ericsson, Motorola, Nokia, and Psion, developed a third operating system called Symbian OS, originally called EPOC. In addition, JAVA and Linux based PDAs are now available. Most newer PDA operating systems provide security application programming interfaces (APIs) that application developers can use to enhance the security of their applications.

PDA manufacturers provide several security-related applications, including password protection of data and other security services stored on the PDA device. When activated, users are required to enter a password before any PDA functions or applications can be used. Unfortunately, built-in password protection mechanisms can be inadequate. Several vendors offer enhanced

authentication capabilities, including signature, voice, and token-based authentication that provide user identification and access control. In addition, there are several products available from security vendors that provide enhanced on-device encryption schemes that are configurable to encrypt confidential files, applications, and data.

Enhanced encryption and authentication can be provided from the device to the content server by implementing Wireless Application Protocol (WAP) PKI, also known as Wireless PKI (WPKI). Through the use of digital credentials, a secure framework can be implemented to protect transactions. WPKI can also be implemented on WAP enabled cellular phones and smartphones.

3.4.1 PDA Device Security Capabilities

3.4.1.1 Palm Devices

The current version of Palm OS (version 5) has many enhanced security features compared to previous versions. These security features include:

- Built in Palm OS security APIs.

- Secure user authentication including support for biometrics and the CHAP, MS-CHAP, and PAP authentication protocols. Palm OS allows users to specify a set of rules (e.g., password, biometric token) that must be met in order to access the device.

- Data integrity and confidentiality encryption (128 bit). RC4 and SH-1 are included in PALM OS. Several third party vendors incorporate other cryptographic algorithms, including AES, via the Palm OS security APIs.

    - Signed code support. When implemented, only applications that have a valid digital signature may access certain data and resources.

    - SSL 3.0 and VPN (IPSec and PPTP) support.

    - Device password protection. Can be set to automatically lock the device on power off, at a specific time, or after a specific period of inactivity.

    - Password protection for select records stored on the PDA.

    - Device level authentication to networks via the PDA Flash ID, Mobile Access Number (MAN), or Electronic Serial Number (ESN).

Palm OS also supports infrared, IEEE 802.11, Bluetooth, and cellular add-on modems that are built in features of many PDA devices.

3.4.1.2 Windows Mobile

Microsoft has renamed their operating system for mobile handheld devices to Windows Mobile. Windows Mobile 2003 has been released in three versions:

–Pocket PC 2003 – Features include storing and retrieval of e-mail, contacts, appointments; play multimedia files and games; exchange text messages with MSN Messenger; and browse the Web. Data can also be synchronized with a desktop computer. Pocket PC 2003 provides improved WiFi support compared to Pocket PC 2002 including Zero Configuration WiFi that is similar to Wireless Zero Configuration (WZC) in Microsoft XP (see *Section 2.2.5*).

–Pocket PC Phone Edition – Combines all the standard functionality of Pocket PC 2003 with that of a feature-rich mobile phone. Provides wireless Internet access via a connection through a wireless service provider.

–Smartphone – Integrates PDA-type functionality into a voice-centric handset. Designed for one-handed handset operation with keypad access to both voice and/or data features. Optimized for voice and text communications, wireless access to Outlook information, and encrypted browsing to corporate and Internet information and services.

Windows Mobile 2003 improves security over previous versions of the WinCE platform. Microsoft has included a long alphanumeric password, but configuration settings will still permit a four-digit PIN. A user is allowed only three guesses of the password before erasing all of the data in the device's memory. Secure remote access functionality is included in Windows Mobile, including PPTP, SSL and WTLS.

Windows Mobile includes power-on password protection and support for Secure Sockets Layer (SSL) and Private Communication Technology (PCT), the CryptoAPI 1.0 application programming interface and Windows 2000 challenge/response authentication.

Smartphone supports code signing of applications whereby any application that is downloaded is assigned to one of three trust levels:

- Privileged Trust means the application has a valid signature and a certificate that allows it access to all system resources. Very few applications should need this level of trust.

- Unprivileged Trust means the application has a valid signature, but a less trusted certificate, which means access to system resources, is restricted. Most applications will operate at this level.

- Untrusted means the application is either not signed or the certificate is not recognized. If the Smartphone enforces code signing, then such an application will not be allowed to load onto the device.

Since Windows Mobile is built on the modular WinCE operating system, each device manufacturer (HP, Casio, etc.) has the option of choosing which features to implement, therefore not every Windows Mobile security feature may be available in a specific Windows Mobile PDA or Smartphone.

3.4.1.3 Symbian OS

Symbian OS includes a multi-tasking multithreaded core, a user interface framework, data services enablers, application engines, and integrated Personal Interface Module (PIM) functionality and wireless communications. Symbian is actively working with emerging standards, such as Java 2 Platform, Micro Edition (J2ME), Bluetooth, WAP, Multi-media Message Service (MMS), Synchronization Markup Language (SyncML), IPv6, and Wide band CDMA (WCDMA).

Symbian OS is the common core of APIs and technology that is shared by all Symbian OS phones. Symbian OS includes a multi-tasking kernel, middleware for communications, data management and graphics, the lower levels of the GUI framework, and application engines. Symbian OS security includes full-strength encryption and certificate management; secure communications protocols (including HTTPS, WTLS, and SSL); and certificate-based application installation.

Substantial security features were added in Symbian OS Version 6.0 (and included in Version 7.0, the latest release), primarily in two modules—the cryptography module and the certificate management module. Security features include standard cryptography algorithms, hash key generation, random number generation, and certificate management. The certificate management module certificate lifecycle services include storage and retrieval of certificates, assignment of trust status to a certificate on an application-by-application basis, certificate chain construction and validation, and verification of trust of a certificate.

Support is initially limited to X.509 certificates along with a PKIX certificate usage profile. The architecture allows for other certificate formats and profiles to be added.

Symbian's licensees include Ericsson, Samsung, Matsushita (Panasonic), Nokia, Siemens, and Sony.

3.4.1.4 Wireless Java

The Java Technology for the Wireless Industry (JTWI) Roadmap 1 specification defines the version of the Java operating system for mobile devices. The latest edition of the Java toolkit (J2ME Wireless Toolkit 2.0), used by developers to build wireless Java applications and Java operating system packages for PDAs, contains a set of security APIs that provide the following features:

–Permissions and Code Signing – These APIs verify that an application is signed with a trusted digital signature. Access to resources and network connections are granted based on the digital signature verification.

–Server Authentication.

–SSL and TLS data encryption services.

NOTE: Security features available in a specific wireless Java PDA will depend on what security features the PDA vendor has implemented.

3.4.1.5 Linux

Many PDA developers believe that Linux is a better choice for mobile devices than other mobile/wireless operating systems because the operating system supports numerous installation methods that work in many heterogeneous environments and needs smaller resources.

A wide range of security features are available in Linux PDAs because vendors can include any available Linux operating system authentication, access control, and encryption security component or include various Linux security applications in their product.

3.4.2 On-Device File Encryption

The first line of defense for protecting data stored in mobile devices is the power-on password that comes built into the device. The second line of defense is to encrypt the data on the device. This provides security against data compromise attacks that can take place when a malicious individual has physical access to a lost/stolen PDA. Several vendors offer products that encrypt selected applications, content, and passwords on the device and support AES 128-bit encryption. FIPS 140-2 certified PDA file/data encryption products are available from several vendors by mid 2003.

3.4.3 Handheld Virus Security

With the expanding role that handheld devices are playing in the federal, corporate, and personal computing environment, the threat from handheld viruses is expanding. PDAs are increasingly making wireless connections to the Internet and agency networks, therefore providing more means for being infected by a virus.

It is speculated that the reason crippling viruses have not been a significant issue for PDAs is due to the fact that the simple PDA operating systems make it hard to write malicious code that will spread automatically. Also, most PDAs do not have hard drives; rather they operate limited Read Only Memory (ROM) and Random Access Memory (RAM) and any preinstalled applications reside in ROM where they are not susceptible to viral attacks. Conversely, third-party applications and user information are stored in RAM and are vulnerable to viruses.

The three methods for transmitting viruses to handheld devices are outlined in the following paragraphs.

Synchronization: Each PDA OS has a means of syncing up information from the desktop to the PDA. This is the primary method by which applications are transferred onto the handheld device and is used primarily to synchronize data stored on the device with data stored on the desktop computer, to backup data to the desktop computer, and to install new device applications. This method provides the easiest means of introducing a virus or malicious code onto the handheld device.

IrDA: Most handhelds contain Infrared (IR) communications capability. If the IR transmission method is complaint with Infrared Data Association (IrDA) specifications, it can directly interface with the IR capabilities of another handheld device. This allows the device to send and receive data from a remote device using a standard protocol. The handheld is then able to send and receive applications and, potentially, malicious code. A malicious program could potentially speak to another infected device and exchange information and code all unbeknownst to the user.

Network Access: By using a PDA with wireless broadband access, a user has access to many standard Internet Protocols such as TCP/IP. This allows the user to directly access the web and e-mail or download files and attachments. This capability also makes it possible to establish a connection with other computers on the Internet and transfer data (including viruses) to the device and makes it possible for a hacker to access a user's confidential data on the handheld device.

There are three basic ways that anti-virus software can be deployed to combat viruses on a handheld device. The first approach is for the handheld anti-virus software to be resident on the desktop computer where data sync is performed with the handheld device and then the handheld is scanned for a virus when synchronization occurs. The anti-virus software can also scan software resident on the desktop for handheld viruses and ensure that virus is eradicated before it is moved to the handheld. The second method is for the anti-virus software to be resident on the handheld and to be searching for viruses on the handheld. The third method is to have anti-virus software running on the desktop and on the handheld.

There are a number of companies in the market place supplying anti-virus software, and a review of the handheld anti-virus market shows that currently the following companies are offering handheld anti-virus products—Symantec, McAfee, Computer Associates, and F-Secure.

- *(WIR0050: CAT II) The IAO will ensure that DOD CERT approved anti-virus software is installed on all wireless devices and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus definition tables every 14 days or less.*

3.4.4 Wireless Application Security

Many vendors offer software development kits (SDKs) for developing security features for handheld devices including PDAs, smartphones, cellular phones, etc. Security features included in applications are dependent on the PDA OS, on which programming and content development options used (Java and J2ME, C, C++, Visual BASIC, WAP, JavaPhone, Smartphone, etc.), as

well as by various vendors' security libraries. Palm, Microsoft, Symbian, RSA, and Certicom offer toolkits to facilitate wireless application development and security.

3.4.5 PDA Compliance Requirements

3.4.5.1 Classified Information

- *(WIR0010: CAT III) The IAO will ensure that the DAA has approved the use of any PDA that is used to transmit, receive, store, or process classified information.*

- *(WIR0380: CAT II) The IAO will ensure that PDAs that are used to transmit, receive, store, or process Classified data use NSA-approved, Type-1 end-to-end encryption for data being transmitted, received, stored, or processed.*

- *(WIR0390: CAT II) The IAO will ensure that PDAs are not permitted in a permanent, temporary, or mobile SCIF unless the transmit capability (RF and IR) is rendered completely inoperable.*

- *(WIR0400: CAT III) The IAO will ensure that PDAs are permitted in an area where classified data is discussed or processed only when:*

  - The DAA, in consultation with the CTTA, has approved that PDAs can be brought into the facility and/or used in the facility.

  - The PDAs are separated from the classified data equipment a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented.

  - The device's voice recording capability is rendered inoperable.

- *(WIR0410: CAT II) The IAO will ensure that users do not connect PDAs directly to workstations located in a SCIF or in other classified areas that store, process, or transmit classified data.*

- *(WIR0420: CAT II) The IAO will ensure that synchronization software will not be loaded on systems processing classified information. Classified information will not be synched. PDAs will not be connected via hot-sync to a classified workstation in a SCIF.*

- *(WIR0425: CAT II) The IAO will ensure that classified data stored on PEDs is encrypted using NSA approved encryption consistent with the classification level of the data stored on the device.*

- *(WIR0356: Category II) The IAO will ensure PDAs with digital cameras (still and video) are not allowed in any SCIF or other area where classified documents or information is stored, transmitted or processed.*

3.4.5.2 Unclassified Information

- *(WIR0010: CAT III) The IAO will ensure that the DAA has approved the use of any PDA that is used to transmit, receive, store, or process unclassified information.*

- *(WIR0010: CAT II) The IAO will ensure that only DAA approved devices, applications, and network/PC connection methods and wireless services are used.*

- *(WIR0010: CAT II) The IAO will ensure that no personally owned devices are used to transmit, receive, store, or process DOD information.*

- *(WIR0371: CAT II) The IAO will ensure PDAs with digital cameras (still and video) are allowed in a DoD facility only if specifically approved by the site physical security policies.*

- *(WIR0450: CAT I) The IAO will ensure that password protection, which meets the following requirements, is used to protect access to device data and applications.*

    - A password meeting DOD password policies is used, if this capability is available, and the password is changed at least every 90 days.

    - The password protection feature will not permit its bypass without zeroing all data stored on the device.

    - The password protection feature is enabled at all times.

- *(WIR0460: CAT II) The IAO will ensure that tools are used to encrypt data and files on PDAs.*

- *(WIR0010: CAT III) The IAO will ensure that only DAA certified and approved applications and operating systems are loaded on PDAs that transmit, receive, store, or process DOD information.*

- *(WIR0465: CAT II) The IAO will ensure that mobile code is not downloaded from non-DOD sources and is downloaded from only trusted DOD sources over assured channels).*

- *(WIR0470: CAT II) The IAO will ensure that PDAs that are used in areas where DOD information is processed have IR ports disabled when IR transmissions are not being used. Data exchange via the IR port should be limited to only trusted DOD devices. The local Cognizant Security Authority (CSA), CTTA should be consulted to determine appropriate method for disabling the IR port on the PDA.*

Synchronization of wireless and handheld devices with applications or data located on a workstation or server (e.g., Microsoft Outlook) via a hot-sync cable or cradle can expose the DOD to significant security risks. Some synchronization systems will operate even if the workstation is locked and the wireless or handheld device is not registered with the synchronization application on the workstation. Therefore, the following procedures will apply:

- *(WIR0480: CAT III) The IAO will ensure that if the hot-sync management software does not require a password, the following is implemented:*

  - The hot-sync management software is only launched when hot-syncing the PDA and is closed as soon as the hot-sync operation is completed, if the hot-sync software does not require a password before use.

  - The hot-sync management software is not launched as part of the computer boot-up process, if the hot-sync software does not require a password before use.

- *(WIR0480: CAT III) The IAO will ensure that only DOD-approved synchronization access control software is used.*

- *(WIR0480: CAT III) The IAO will ensure that the user disables wireless operations when a PDA is connected to the DOD wired network via a hot-sync or other interface cable.*

- *(WIR0480: CAT III) The IAO will ensure that PDAs that transmit, receive, store, or process DOD information are not synced to home or personally owned PCs.*

- *(WIR0490: CAT II) The IAO will ensure that PDAs used for wireless Internet remote access to DOD networks meet the following standards and criteria:*

  - Data encryption meeting the FIPS 140-2 (3DES or AES) standard is used on the device.

  - PKI certificates are used for identification and authentication (I&A) of users.

  - Only DAA approved PDAs, wireless service providers, and network access gateways are used.

  - PDA wireless modems (e.g., IEEE 802.11, cellular, etc.) are removed or turned off when wireless data connections are not being used.

  - DOD CERT approved anti-virus software is installed on the device and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus definition tables every 14 days or less.

  - A personal firewall is implemented on the device.

PDA devices should only be purchased after it has been verified that file encryption software is available for that equipment. PDAs that will be used for wireless Internet remote access to DOD networks should only be purchased after it has been verified that FIPS 140-2 certified data encryption software, anti-virus software, and personal firewall software is available for that equipment. PDAs with Bluetooth radios should not be purchased unless the Bluetooth radio transmission can be secured with FIPS 140-2 certified data encryption software or the Bluetooth radio can be removed or disabled.

4. WIRELESS TWO-WAY MESSAGING AND E-MAIL TECHNOLOGIES

4.1 Introduction

Wireless messaging is the most prevalent wireless service used by the DOD. Wireless messaging can be categorized into three types of services—Short Messaging Service (SMS), two-way paging, and two-way e-mail. Many wireless paging services have been discontinued due to low demand as wireless customers move to wireless messaging services that combine two-way e-mail and SMS with wireless phone services.

4.2 Short Message Service (SMS)

4.2.1 SMS Technology Overview

SMS is a standard protocol for GSM systems. TDMA and CDMA carriers are using several different, and in many cases, proprietary SMS protocols. Several U.S. wireless carriers are now providing messaging services that allow a user to send an SMS to another user on a competitor's wireless network. SMS is used to transmit short messages between wireless phones and provides no security features. Although all digital wireless carriers encrypt data between the phone and the carrier base station, SMS messages are not normally encrypted as they transit the wireline network.

An advanced form of SMS, called Multimedia Messaging Service (MMS), is now available on a number of 3G wireless networks. Photos, graphics, video, and other forms of multimedia can be transmitted via MMS,

Wireless two-way messaging services are sold by a number of wireless vendors including cellular, wireless data, and two-way paging service providers. SMS services are rarely sold as a stand-alone wireless service and are usually bundled with wireless phone, data, or e-mail services.

4.2.2 SMS Security

Most SMS service providers implement some form of message encryption and device and/or user-level authentication in addition to the security mechanisms that may be included in the airlink protocol, but these security features cannot be relied on to provide strong end-to-end security. No commercial SMS message service incorporates an assured channel employing a 140-2 certified encryption process, or NSA-approved, Type 1 end-to-end encryption.

4.2.3 SMS Compliance Requirements

4.2.3.1 Classified Information

- *(WIR0500: CAT III) The IAO will ensure that SMS devices are not used to send, receive, store, or process classified messages.*

- *(WIR0510: CAT III) The IAO will ensure that SMS devices are not permitted in a permanent, temporary, or mobile SCIF unless the transmit capability (RF and IR) is rendered completely inoperable.*

- *(WIR0520: CAT III) The IAO will ensure that SMS devices are not permitted in or used in areas where classified data processing takes place unless:*

  - The DAA, in consultation with the CTTA, has approved that the SMS device can be brought into the facility and/or used in the facility.

  - The SMS device is separated from the classified data equipment at a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented.

4.2.3.2 Unclassified Information

SMS devices and wireless services do not meet the security requirements of *DODD 8100.2* for storing, processing, and transmitting unclassified information. Therefore, SMS devices will not be used unless the following conditions are met:

- *(WIR0010: CAT III) The IAO will ensure that the DAA has approved the use of the device based on mission needs.*

- *(WIR0030: CAT III) The IAO will ensure that wireless devices, that connect directly or indirectly (hot-sync) to the network are added to site System Security Authorization Agreements (SSAAs).*

- *(WIR0540: CAT III) The IAO will ensure that the SMS device is used to send and receive unclassified routine/administrative type information only.*

- *(WIR0560: CAT II) The IAO will ensure that no personally owned SMS devices are used to transmit, receive, store, or process DOD information.*

- *(WIR0570: CAT II) The IAO will ensure that only DOD authorized SMS wireless service providers are used.*

- *(WIR0050: CAT IV) The IAO will ensure that DOD CERT approved anti-virus software is installed on all wireless SMS devices and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus definition tables every 14 days or less.*

- *(WIR0580: CAT I) The IAO will ensure that password protection, which meets the following requirements, is used to protect access to device data and applications. The IAO will ensure that password protection, where a password must be entered in order to access device data and applications, is used.*

  - A password meeting DOD password policies is used, if this capability is available, and the password is changed at least every 90 days.

  - The password protection feature will not permit its bypass without zeroing all data stored on the device.

  - The password protection feature is enabled at all times.

- *(WIR0020: CAT II) The IAO will ensure that when SMS services are used on a cellular phone or PDA, the cellular phone or PDA security guidelines found in Section 3 of this Wireless STIG.*

4.3 Wireless Two-way Paging

Wireless pagers have almost become a technology of the past, having been replaced by wireless phone messaging services. Some vendors offer paging services with two-factor authentication and FIPS 140-2compliant 128-bit 3DES encryption. Currently no vendors offer two-way pagers and their associated services that provide an assured channel employing NSA-approved, Type 1 end-to-end encryption.

4.3.1 Wireless Two-way Paging Compliance Requirements

4.3.1.1 Classified Information

- *(WIR0500: CAT II) The IAO will ensure that wireless two-way pagers are not used to send, receive, store, or process classified messages.*

- *(WIR0510: CAT III) The IAO will ensure that wireless two-way pagers are not brought into a permanent, temporary, or mobile SCIF unless the transmit capability (RF and IR) is rendered completely inoperable.*

- *(WIR0520: CAT III) The IAO will ensure that two-way pagers are not permitted or used in an area where classified data processing takes place unless:*

  - The DAA, in consultation with the CTTA, has approved that the two-way pager can be brought into the facility and/or used in the facility.

  - The two-way pager is separated from the classified data equipment a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented.

4.3.1.2 Unclassified Information

Wireless two-way pagers services do not meet the security requirements of *DOD 8100.2* for storing, processing, and transmitting unclassified information. Therefore, wireless two-way pagers will not be used unless the following conditions are met:

- *(WIR0010: CAT III) The IAO will ensure that the DAA has approved the use of the pager based on mission needs.*

- *(WIR0540: CAT III) The IAO will ensure that the wireless two-way pagers are used to send and receive unclassified routine/administrative type information only.*

- *(WIR0550: CAT III) The IAO will ensure that the paging service provides some type of data encryption for the wireless link.*

- *(WIR0560: CAT III) The IAO will ensure that no personally owned wireless two-way pagers are used to transmit, receive, store, or process DOD information without DAA approval.*

- *(WIR0050: CAT IV) The IAO will ensure that DOD CERT approved anti-virus software is installed on all wireless two-way pagers and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus definition tables every 14 days or less.*

- *(WIR0450: CAT I) The IAO will ensure that password protection, where a password must be entered in order to access device data and applications, is used.*

    - A password meeting DOD password policies is used, if this capability is available, and the password is changed at least every 90 days.

    - The password protection feature will not permit its bypass without zeroing all data stored on the device.

    - The password protection feature is enabled at all times.

4.4 Wireless Two-way E-mail

4.4.1 Wireless Two-way E-mail Overview

There are no specific standards used for wireless e-mail services. Wireless phone carriers and e-mail service providers use a number of protocols, some of them proprietary, for their e-mail service. Some form of account verification and data encryption is provided by most wireless e-mail services.

Wireless two-way e-mail has become the fastest growing wireless service using handheld devices in the government. There are essentially two different e-mail services being offered by wireless e-mail service providers.

The most popular wireless e-mail service for government users redirects a user's e-mail to a wireless e-mail device. Either an e-mail redirector application is installed on the user's computer, or a redirector server is connected to the government e-mail server to redirect all incoming e-mail, via the Internet, to the wireless e-mail vendor's wireless gateway. The wireless gateway then transmits the e-mail to the wireless e-mail device. The wireless e-mail gateway also sends a copy of any e-mail sent from the handheld device, also via the Internet, back to the user's corporate e-mail servers so that a copy of the e-mail can be placed in the user's e-mail outbox.

For the second type of e-mail service, the wireless e-mail vendor provides a wireless e-mail account to users. E-mail that is sent to this account is transmitted to the wireless handheld e-mail device by the vendor's wireless gateway. A user can have their government e-mail account forward all incoming messages to the wireless e-mail account when they are out of the office.

In addition to e-mail, some wireless service providers offer other wireless services including airline flight information, news headlines, and stock market updates. Several wireless e-mail vendors also provide a SMS that will allow subscribers to send short messages to other subscribers (peer-to-peer communications).

4.4.2 Wireless Two-way E-mail Security

Security features of wireless two-way e-mail services vary from vendor to vendor and depend a large part on which wireless handheld device is offered by the vendor. Most wireless e-mail vendors provide some type of device-level authentication and data scrambling or encryption as part of the air interface protocol (e.g., CDPD). In addition, the majority of all redirector based wireless e-mail services provide some form of application layer end-to-end encryption of e-mail data from the wireless device to the redirector application on the user's workstation or to the redirector server.

End-to-end encryption is not provided for wireless e-mail services that require the user to have a wireless e-mail account separate from their government agency e-mail account. Although e-mail is usually encrypted between the wireless e-mail gateway and the wireless device, it is not encrypted when it is sent on the Internet between the user's government e-mail account and the wireless e-mail account.

A number of different encryption protocols are used to secure e-mail data including SSL, TLS, WTLS, and proprietary protocols. DES, ECC, 3DES, and AES are the most common encryption algorithms in use. Several wireless e-mail services offer FIPS 140-2 compliant encryption. Currently, no vendors offer wireless e-mail devices and services that provide an assured channel employing NSA-approved, Type 1 end-to-end encryption.

Several handheld wireless e-mail devices have strong password protection for the data on the device. When this feature is enabled, a password is required to unlock the device and gain access to data and applications on the device.

All Research In Motion (RIM) BlackBerry email devices are FIPS 140-2 certified and use 3DES encryption. Several RIM Blackberry models are S/MIME capable, which provides end-to-end e-mail encryption, even if the sender or recipient is not a BlackBerry user. The S/MIME Enhanced BlackBerry or "CryptoBerry" is the RIM 957-8 Blackberry and is the only NSA evaluated and recommended RIM S/MIME Blackberry device. NSA has not evaluated other S/MIME BlackBerry devices. Each DAA should determine which RIM BlackBerry device is most appropriate for their operational environment. Additional information on the S/MIME Enhanced BlackBerry can be found at http://www.smimeblackberry.net/.

4.4.3 Wireless Two-way E-mail Compliance Requirements

4.4.3.1 Classified Information

- *(WIR0500: CAT II) The IAO will ensure that wireless two-way e-mail devices are not used to send, receive, store, or process classified messages.*

- *(WIR0510: CAT III) The IAO will ensure that wireless two-way e-mail devices are not brought into a permanent, temporary, or mobile SCIF unless the transmit capability (RF and IR) is rendered completely inoperable.*

- *(WIR0520: CAT III) The IAO will ensure that two-way e-mail devices are not permitted or used in areas where classified data processing takes place unless:*

  - The DAA, in consultation with the CTTA, has approved the two-way e-mail device for entry and use in the facility and/or used in the facility.

  - The two-way e-mail device is separated from the classified data equipment a distance determined by the CTTA and that appropriate countermeasures, as determined by the CTTA, have been implemented.

- *(WIR0530: CAT II) The IAO will ensure that hot-sync software will not be loaded on computers processing classified information.*

4.4.3.2 Unclassified Information

The Research in Motion (RIM) BlackBerry wireless e-mail service is currently the only wireless two-way e-mail service that is compliant with a majority of the security requirements of *DODD 8100.2* for storing, processing, and transmitting unclassified information.

- *(WIR0010: CAT III) The IAO will ensure that the DAA has approved the use of the BlackBerry device and service based on mission needs and has approved all applications and operating systems loaded on the device."*

- *(WIR0030: CAT III) The IAO will ensure that wireless devices, which connect directly or indirectly (hot-sync) to the network, are added to site the SSAA.*

- *(WIR0050: CAT II) The IAO will ensure that DOD CERT approved anti-virus software is installed on all wireless BlackBerry devices and the software is configured in accordance with the Desktop Application STIG and is kept up-to-date with the most recent virus definition tables every 14 days or less.*

The RIM 957-8 Blackberry uses digital signatures to validate the authenticity of all software installed on the device, which mitigates the requirement to install anti-virus software on the device.

- *(WIR0560: CAT III) The IAO will ensure that no personally owned BlackBerry devices are used to transmit, receive, store, or process DOD information.*

- *(WIR0590: CAT II) The IAO will ensure that only the S/MIME BlackBerry enterprise server e-mail redirector is used.*

- *(WIR0600: CAT II) The IAO will ensure that tools are used to encrypt data and files on the BlackBerry device.*

The RIM 957-8 Blackberry encrypts all email messages stored on the device.

- *(WIR0605: CAT III) Mobile code will not be downloaded from non-DOD sources and is downloaded from only trusted DOD sources over assured channels.*

- *(WIR0610: CAT II) The IAO will ensure that the BlackBerry device IR port is disabled when IR transmissions are not being used. Data exchange via the IR port should be limited to only trusted DOD devices.*

- *(WIR0620: CAT II) The IAO will ensure that a BlackBerry device is deactivated at the BlackBerry server if it is reported lost or stolen.*

- *(WIR0630: CAT II) The IAO will ensure that password protection, where a password must be entered in order to access device data and applications, is used.*

    - *A password meeting DOD password policies is used and the password is changed at least every 90 days.*

    - *The password protection feature will not permit its bypass without zeroing all data stored on the device.*

    - *The password protection feature is enabled at all times.*

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

Applicable Federal Policies and Guidelines

Current and Future Requirements for Federal Wireless Services in the United States, December 2001. (http://www.fwuf.gov/Documents/rev_dec01.pdf)

*Federal User's Wireless Telephone Security Risks(*http://www.fwuf.gov/Documents/FWUR_PT1.PPT)

FCC Rule 22.919, "Cellular Fraud" (http://wireless.fcc.gov/services/cellular/operations/fraud.html)

NIST Special Publication 800-46 "Security For Telecommuting and Broadband Communications," Sept 2002, (http://csrc.nist.gov/publications/nistpubs/index.html)

NIST Special Publication 800-48,*Wireless Network Security: 802.11, Bluetooth, and Handheld Device*, Nov 2002, (http://csrc.nist.gov/publications/nistpubs/index.html)

OMB Circular A-130, *Management of Federal Information Resources* (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)

Federal Communications CFR, Title 47, Part 15 (http://www.access.gpo.gov/nara/cfr/waisidx_00/47cfr90_00.html)

NTIA Manual of Regulations & Procedures for Federal Radio Frequency Management, January 2000 Edition with 2001 Revisions (http://www.army.mil/spectrum/library/regulations.htm)

Applicable DOD Policies and Guidelines

DOD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2004.

DOD Directive 8500.1, *Information Assurance*, 24 October 2002.

Director's Policy Letter 2003-7, *Portable Electronic Devices*, 1 July 2003.

DOD Instruction 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003.

Office of the Secretary of Defense Memorandum, Department of Defense (DOD) Information Assurance Vulnerability Alert (IAVA).

OASD C3I Memorandum, Defense-wide Information Assurance Program Implementation Plan, 12 February 1999.

OASD C3I Memorandum, Increasing the Security Posture of the Unclassified but Sensitive Internet Protocol Router Network, 22 August 1999.

DOD Directive 8800.aa, Global Information Grid (GIG).

National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, January 2000.

DISA CIO Guideline, Guidelines for S/MIME BlackBerry Orders, 16 Dec 2002.

DISA CIO Memorandum, Deployment of the Secure Multipart Internet Mail Extensions (S/MIME) Blackberry Device.

Draft CNSS Instruction 3034, Operational Security Doctrine for the SecNet-11 Wireless Local Area Network Interface Card.

The following industry and professional groups are involved in developing and/or sponsoring the development of wireless and wireless security standards:

Formal Standards Groups

American National Standards Institute (ANSI)
European Telecommunications Standards Institute (ETSI)
International Standards Organization (ISO)
Institute of Electrical and Electronics Engineers (IEEE)
International Telecommunications Union (ITU)
National Information Assurance Partnership (NIAP)
Telecommunications Industry Association (TIA)

Government Agencies

FCC Homeland Security Policy Council
Federal Communications Commission (FCC)
Federal Wireless Policy Committee (FWPC)
Federal Wireless Users Forum (FWUF)
National Institute of Standards and Technology (NIST)
National Telecommunication Information Administration (NTIA)

Industry Associations

Bluetooth Special Interest Group (SIG)
CDMA Development Group (CDG)
Cellular Telecommunication and Internet Association (CTIA)
Electronic Industry Association (EIA)
GSM Association
Infrared Data Association (IrDA)
Internet Engineering Task Force (IETF)
Personal Communications Industry Association (PCIA)
WAP Forum
Wireless LAN Alliance (WLANA)

WEP Vulnerability Web Links

Intercepting Mobile Communications: The Insecurity of 802.11 – DRAFT.
By Nikita Borisov, UC Berkeley; Ian Goldberg, Zero-Knowledge Systems; David Wagner, UC Berkeley.
http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

Using the Fluhrer, Mantin, and Shamir Attack to Break WEP, Revision 2.
By Adam Stubblefield, Rice University; John Ioannidis, AT&T Labs; Aviel D. Rubin, AT&T Labs.
http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

Weaknesses in the Key Scheduling Algorithm of RC4.
By Scott Fluhrer, Cisco Systems; Itsik Mantin, The Weizmann Institute; Adi Shamir, The Weizmann Institute.
http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

An Initial Security Analysis of the IEEE 802.1x Standard.
University of Maryland, Department of Computer Science
Mishra, Arunesh and Arbaugh, William A.
http://www.cs.umd.edu/~waa/1x.pdf

This page is intentionally left blank.

APPENDIX B. INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) COMPLIANCE

IAVM Wireless Related Notices

No Notices at this time.

CERT Wireless Related Notices

Vulnerability Note VU#107186 **—** Multiple vulnerabilities in SNMPv1 trap handling
Vulnerability Note VU#854306 **—** Multiple vulnerabilities in SNMPv1 request handling
Vulnerability Note VU#898931 — Multiple vendors' RADIUS implementations do not adequately validate user input, thereby permitting DOS and arbitrary command execution via "**radiusd**" daemon.

APPENDIX C. WIRELESS LAN SITE SURVEY GUIDE INTRODUCTION

C.1 Introduction

Using radio frequency (RF) technology, Wireless LANs (WLANs) transmit and receive data through the air, minimizing the need for wired connections. The IEEE 802.11x 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 802.11 A & G systems, as well.

C.2 Purpose

This appendix is intended to give an overview of the importance of, and instructions for, conducting a basic site survey in preparation for deploying Wireless LAN (WLAN) equipment. Conventional WAN and LAN 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:

1. **Understanding how 802.11 radios work.**
2. **Understanding RF and the effect of building structure elements and sources of external interference on RF devices.**
3. **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.

C.3 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 radio 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 ISM band. Specifically, the 802.11 standard uses two of the three frequency bands available within the ISM band. The ISM bands are distributed as follows:

–900 MHz (902-928 MHz) is not widely used in WLANs
–2.4 GHz (2.4-2.4835 GHz) 802.11 and its subset 802.11b
–5 GHz (5.15-5.35 GHz and 5.735-5.835 GHz) 802.11a

These spectrum bands are classified unlicensed, and can be used by anyone providing they comply with FCC regulations. They are exempt from the federal spectrum certification and frequency assignment process when used in the United States & Possessions (US&P). However, a *DD Form 1494, Application for Equipment Frequency Allocation,* may be required by the Frequency Management Officer (FMO). 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.

C.3.1 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 C.4.2.1, WLAN Attenuation and Interference*. The most common sources of interference are other devices operating at the same frequency. Newer 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.

C.3.2 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.

C.3.3 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.

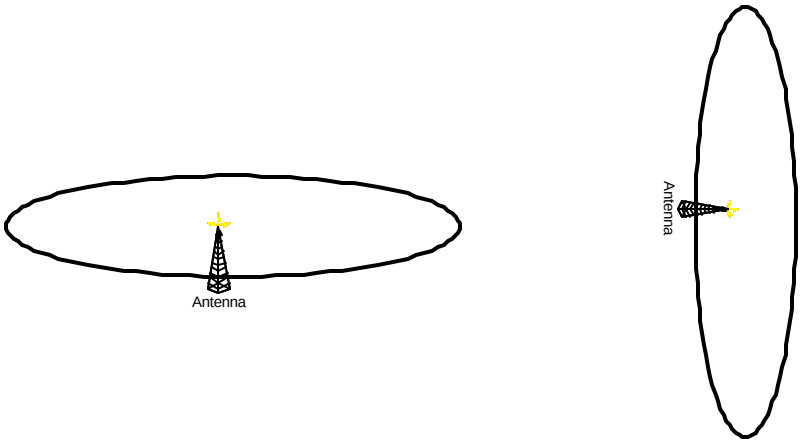


Figure C-1. Antenna Polarization

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.

C.3.3.1 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.

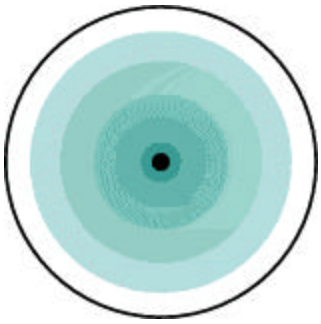


Figure C-2. Omni-direction 2D Propagation Pattern

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.

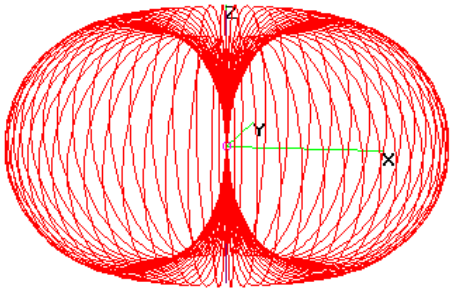


Figure C-3. Isotropic Sphere Propagation Pattern

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 4, Wireless Radio Interface Protocols*.

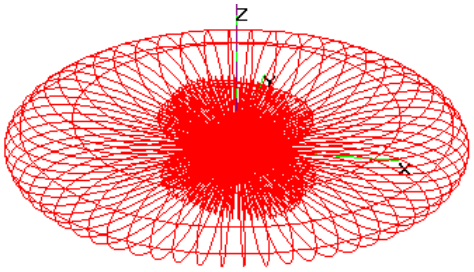


Figure C-4. Real World Indoor Omni-directional Propagation Pattern

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.

C.3.3.2 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 C-5, Directional*); however, the actual propagation pattern is more accurately represented in three dimensions (see *Figure C-6, Directional 3D*).

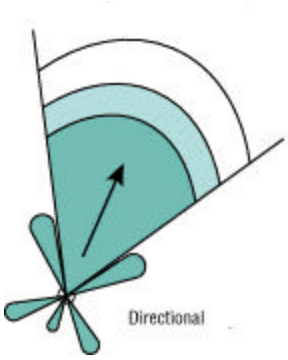


Figure C-5. Directional

Figure C-1, Antenna Polarization, 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.

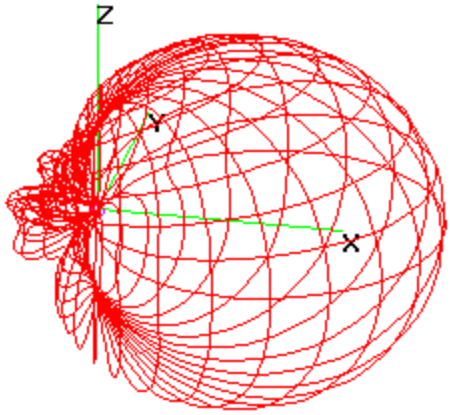


Figure C-6. Directional 3D

C.3.3.3 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.

C.4 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.

C.4.1 802.11 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.

C.4.1.1 802.11b 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.

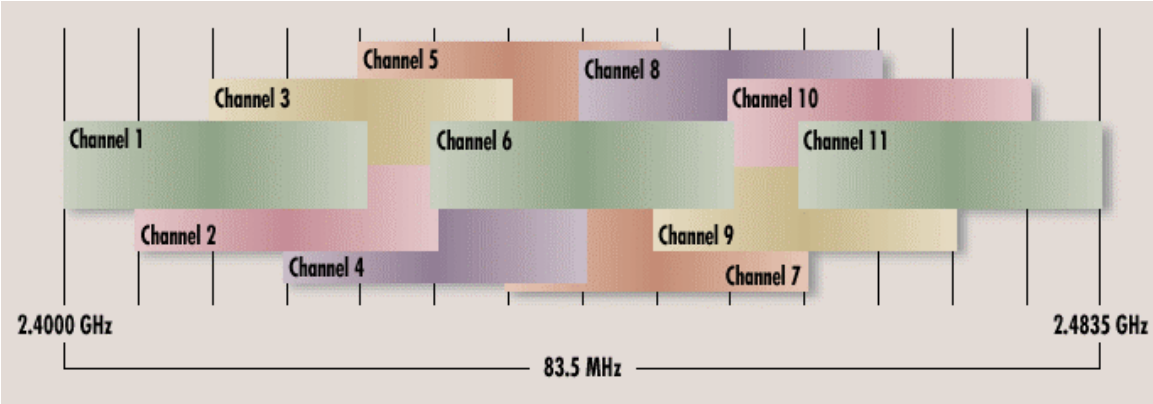


Figure C-7. 802.11b Spectrum Coverage

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 C-8* below:

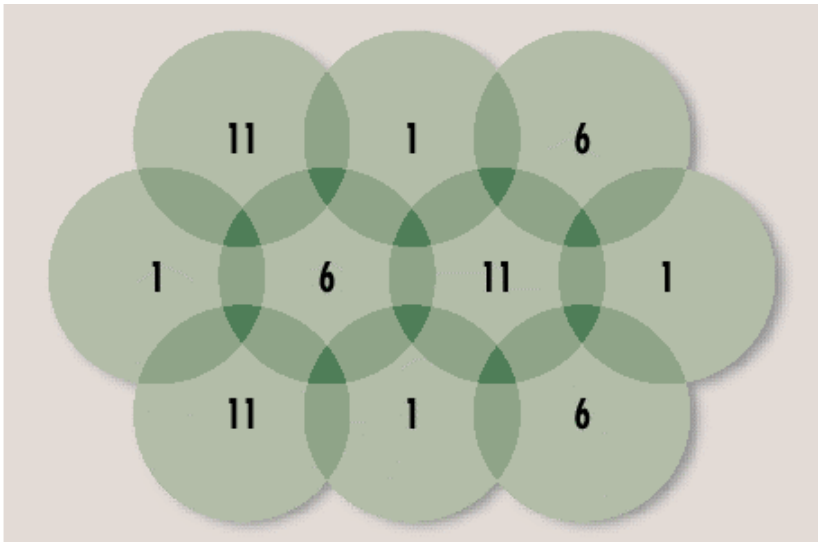


Figure C-8. 802.11b Channel Layout

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 *Figure C-9, Non-overlap Channel Placement*.

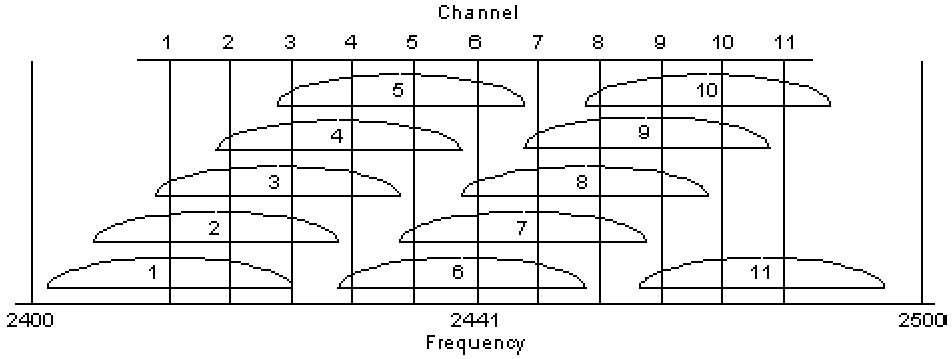


Figure C-9. Non-overlap Channel Placement

C.4.1.2 802.11a

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 US), 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 just recently entering the market. 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 some instances, it may require more 802.11a access points than 802.11b access points to cover the same geographic area. In addition to generally shorter range, 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, since 802.11a products are relatively new to the market, they currently average about 25-30% higher in price than comparable 802.11b products, thus increasing the cost to deploy as well.

C.4.2 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.

C.4.2.1 WLAN Attenuation and Interference

As mentioned in *Section C.3.1, 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.

C.4.2.1.1 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 C-10. 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 C-11. 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 C-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 C-12. Approximate Office Construction Material Attenuation Values

C.5 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.

C.5.1 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.

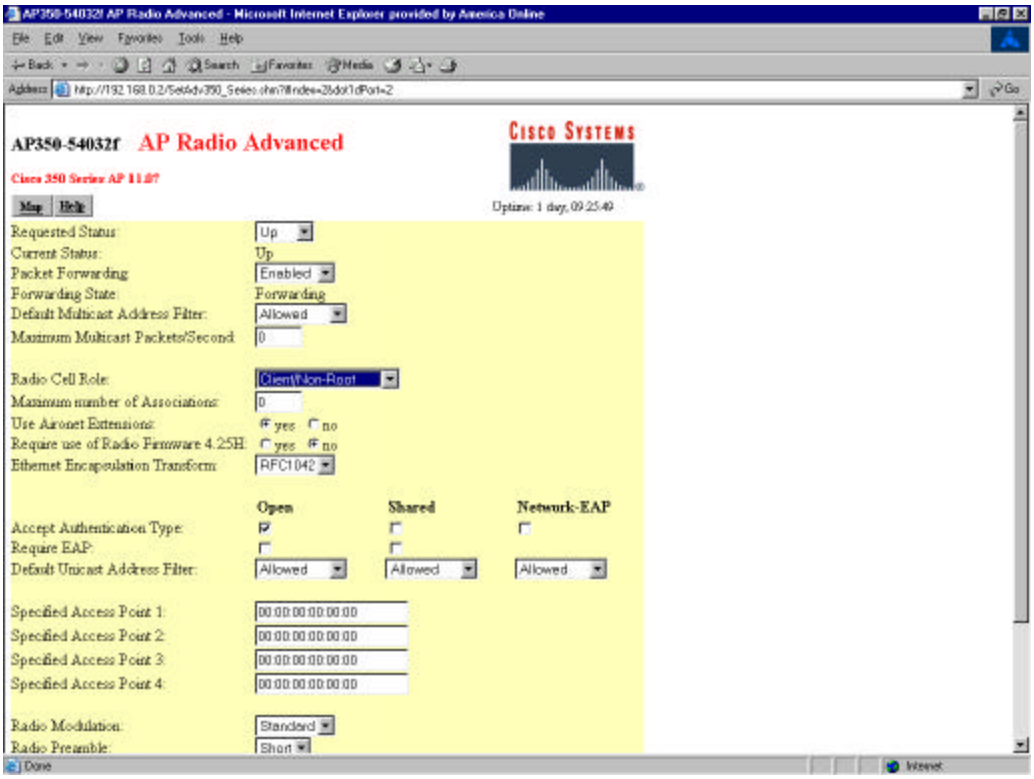
The simplest method for performing an RF site survey includes a laptop equipped with an 802.11 PC Card and site survey software. Most wireless PC card vendors now supply this software with the cards. The software features vary by vendor, but at a minimum, they all display the strength and quality of 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.

C.5.2 Configuring the Cisco Aironet 350 for Site Survey

For best results during a site survey, turn off all wireless networking devices within range of the access point except the device with which you are trying to communicate.

Change the Aironet 350's "role" on the "AP Radio Advanced" page:



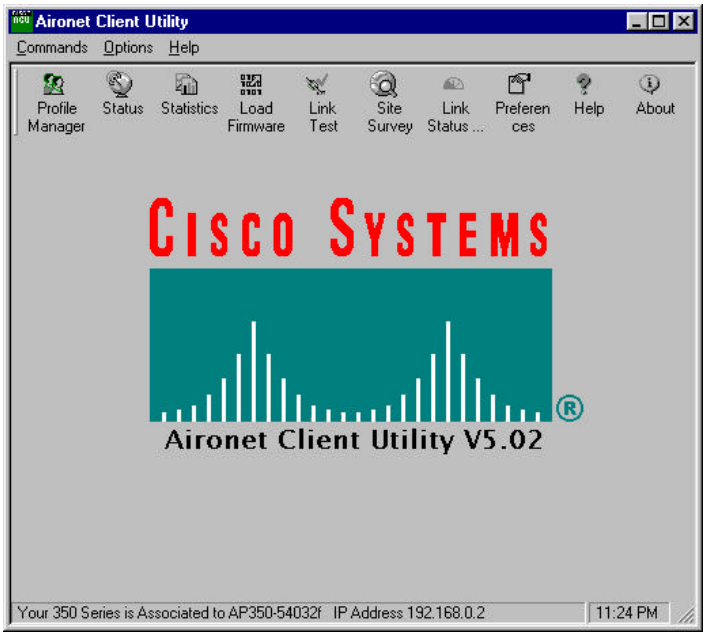
- Summary Setup
    - Setup
        - AP Radio-Advanced

In the *Radio Cell Role:* drop down menu, change the selection to "Client/Non-root." This allows the access point to test communications with other wireless devices, without accepting association requests from clients.

C.5.3 Configuring the Aironet 350 Client Adapter

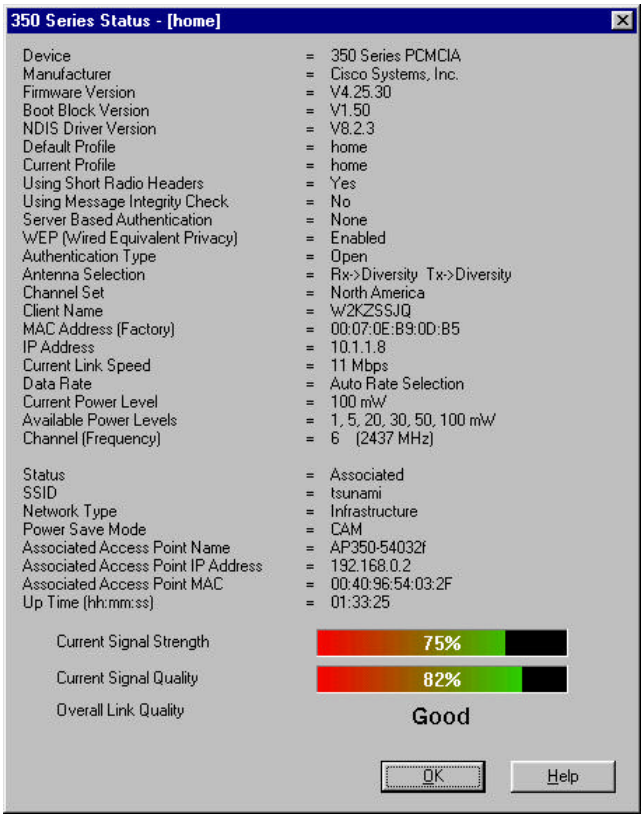
The Cisco Aironet 350 client adapter card (NIC) can be set to Site survey mode. From a Windows laptop:

- Start
    - Programs
        - Cisco Aironet-Aironet Client Utility (ACU)



Selecting the Status icon on the screen will bring up the Status page.

The Status page is one way to view the current connection state.



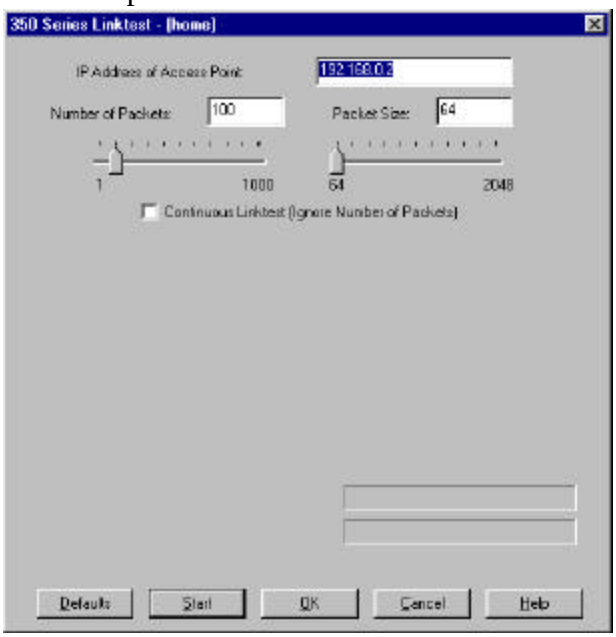
The Current Signal Strength denotes the current strength of the received RF signal from the access point.

Current Signal Quality describes the quality of that signal.

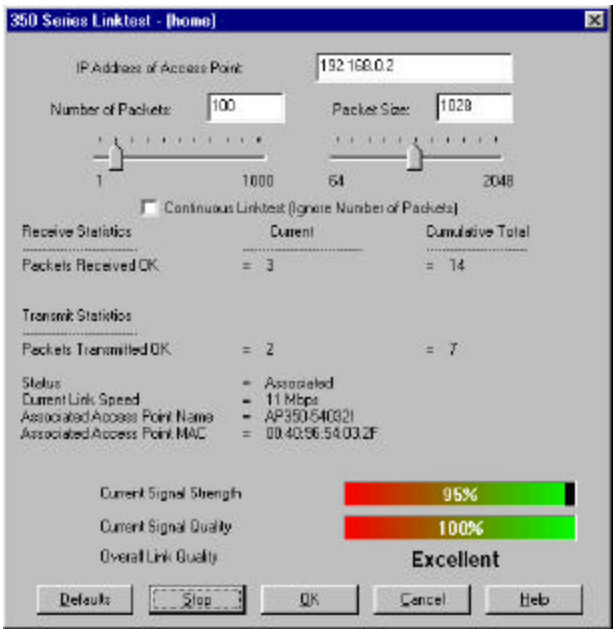
The Overall Link Quality describes the ability of the Cisco Aironet client adapter to communicate with the access point. Values include Excellent, Good, Fair, and Poor.

Also on this page, the Current Link Speed line shows the current transmission rate between the access point and the client.

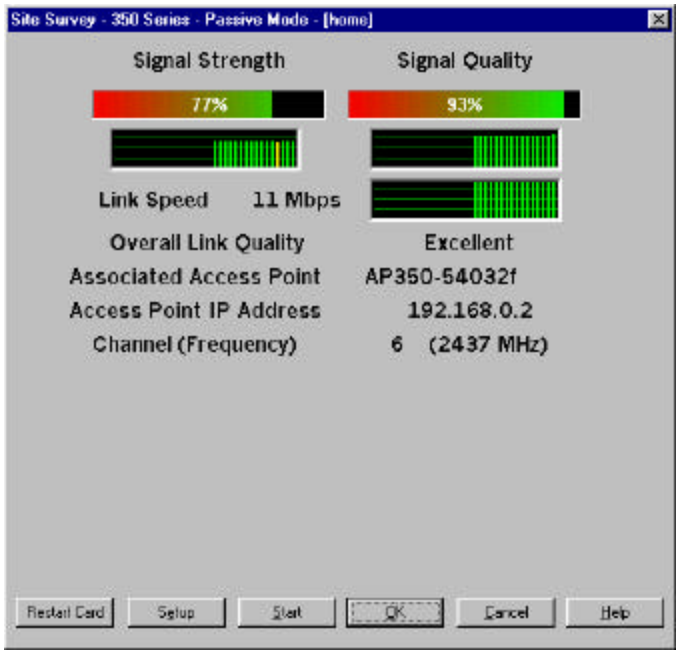
Selecting the Link Test icon will open the Linktest page, where test packets can be sent to measure performance.



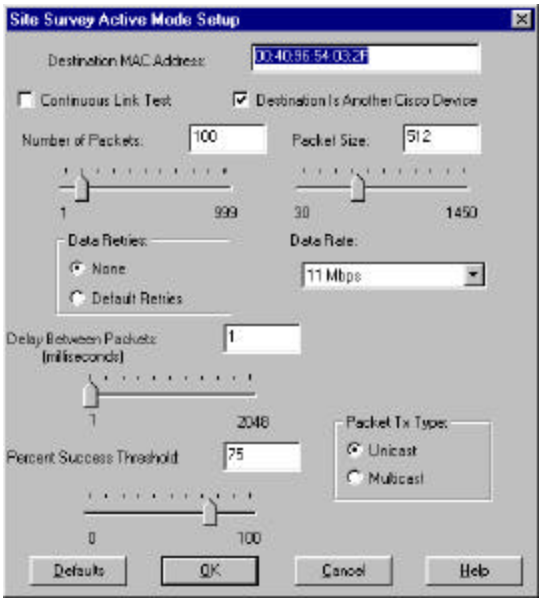
Clicking on the Start button will begin packet transfers to test the link. You can select the number of packets and packet sizes in the appropriate fields. This screen is best utilized to test performance in cases where you know users will be transferring large files or quantities of data. This screen allows for simulation of a production environment.



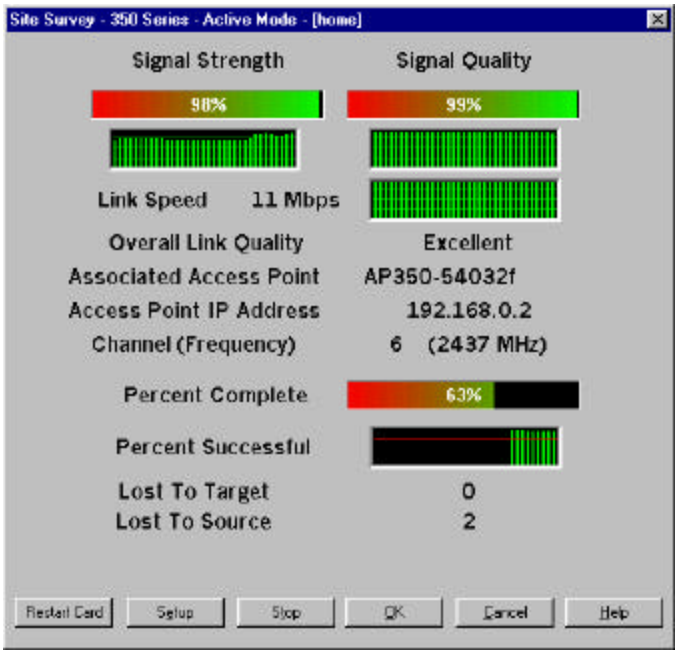
Selecting the Site Survey icon will bring up a scrolling status meter showing the link quality.



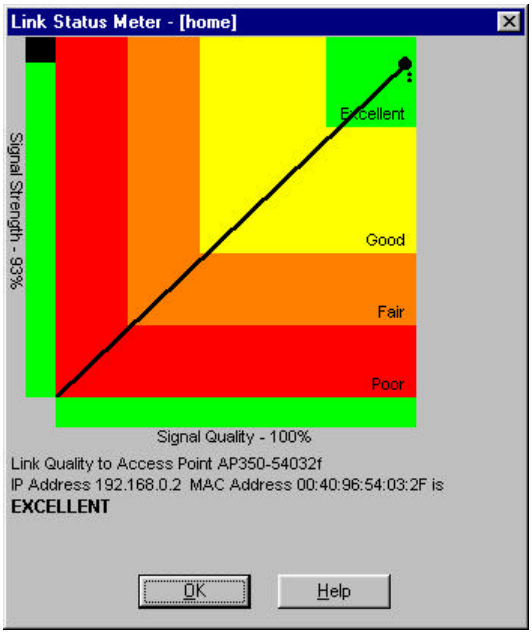
This screen functions in two modes—Active and Passive. Default is passive, where the Client adapter card is listening but not initiating any RF traffic. Clicking on the Setup icon from the Aironet Client Utility allows you to set the parameters of Active mode.



Again, both the number and size of packets can be customized, along with the data rate, and delay between packets. Also, the Packet Tx Type, Unicast (to a single IP), or Multicast (broadcast) can be changed. After setting parameters, and clicking on OK, selecting Start from the Site Survey main screen will begin the active test.

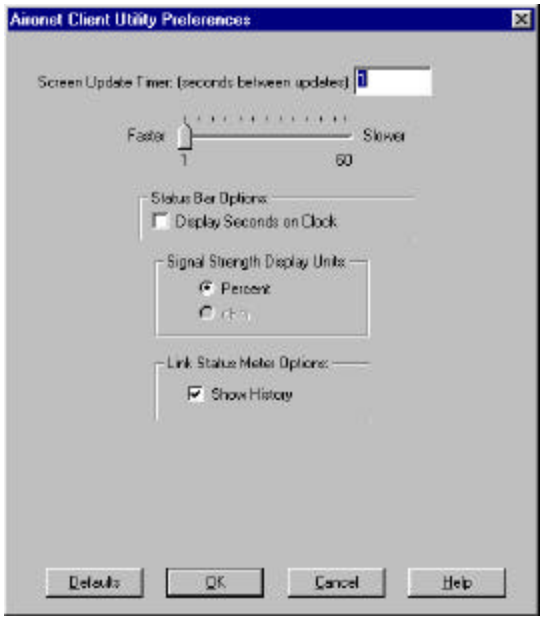


Selecting Link Status will open the screen showing a graphical status of the link state.



Values again range from Excellent to Poor, and will change over time and if the client device is moved. This is an excellent way to do an initial walkthrough of spaces intended for coverage by a WLAN.

Selecting the Preferences icon will open the preference screen. On this screen, you can select between displaying signal strength as a percentage, or in dB. This may prove useful for documenting specific signal loss due to walls, doors, windows, etc., within the intended coverage areas.



C.5.4 Basic Disadvantages

It can be physically demanding to lug a laptop around a building all day when doing the testing. The physical demands can be mitigated by using 802.11 CompactFlash cards and a handheld device, such as the Compaq iPAQ, Casio Cassiopeia, or HP Jornada. While this may reduce some of the physical demands, some functionality may be lost, such as the detection of RF interference between access points and from other RF sources, such as Bluetooth devices, microwave ovens, and wireless phones. However, for one-time installations, especially smaller facilities, using the steps outlined in the Basic Site Survey should be sufficient. You can relocate the limited number of access points easily enough until everything works together properly.

C.6 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.

C.6.1 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.

C.6.2 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. 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.

C.6.3 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.

References:

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

APPENDIX D. WIRELESS LAN SECURITY FRAMEWORK

The Wireless LAN Security Framework document can be found in the same .zip file as the Wireless STIG document. Both documents are available at the IASE web site (See *Section 1.8* of the Wireless STIG for site addresses.) WLAN developers, system architects, System Administrators, and users should use the WLAN Reference Model document as a guide to the implementation of secure WLANs. The document is intended to supplement the policies in the Wireless STIG, Wireless Checklist, and other applicable DOD policy documents.

This page is intentionally left blank.

APPENDIX E. LIST OF ACRONYMS

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AIS	Automated Information Systems
AMPS	Advanced Mobile Phone Service
ANSI	American National Standards Institute
API	Application Program Interface
ARP	Address Resolution Protocol
ASDC3I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
BRAN	Broadband Radio Access Network
C2	Level C Security for Computer Products (provides Discretionary Access Control [DAC])
C&A	Certification and Accreditation
CA	Certificate Authority
CCI	Co-channel Interference
CDG	CDMA Development Group
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CF	Compact Flash
CGI	Common Gateway Interface
CHAP	Challenge Authentication Protocol
CICS	Customer Information Control System
CJCS	Chairman, Joint Chiefs of Staff
COMSEC	Communications Security
COTS	Commercial-Off-The-Shelf
CRT	Display Monitor (Cathode Ray Tube)
CSA	Command, Service, and Agency
CSA	Cognizant Security Authority
CTIA	Cellular Telecommunications & Internet Association
CTTA	Certified TEMPEST Technical Authority
DAA	Designated Approving Authority
DAC	Discretionary Access Control
dBi	Decibel (measure of antenna gain in decibels)
DECC	Defense Enterprise Computing Center
DECC-D	Defense Enterprise Computing Center-Detachment
DES	Data Encryption Standard
DH	Diffie Hellman
DISA	Defense Information Systems Agency
DISAI	DISA Instruction

DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DOD	Department of Defense
DOS	Denial of Service
DSAWG	Defense Security Accreditation Working Group
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAS	Extended Assistance Support
ECC	Eliptic Curve Cryptogrophy
EDGE	Enhanced Data Rate for Global Evolution
EIA	Electronic Industry Association
EIR	Equipment Identity Register
E-mail	Electronic Mail
EMS	Extended Maintenance Support
ESAF	External Subsystem Attachment Facility
ESN	Electronic Serial Number
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
FNBDT	Future Narrow Band Digital Terminal
FSO	Field Security Operations
FWPC	Federal Wireless Policy Committee
FWUF	Federal Wireless Users Forum
GHz	Gigahertz
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HSCSD	High-Speed Circuit-Switched Data
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol
HTTPS	Hyper Text Transport Protocol - Secure
I&A	Identification and Authentication
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IAVA	Information Assurance Vulnerability Alert
iDEN	Integrated Dispatch Enhanced Network
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange

IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPSEC	IP Security
IrDA	Infrared Data Association
ISA	Industry Standard Architecture
ISM	Industrial, Scientific, and Medical
ISO	International Standards Organization
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	nformation Technology
ITU	International Telecommunications Union
IV	Initialization Vector
LAN	Local Area Network
LEAP	Lightweight EAP
MAC	Media Access Control
MBPS	Megabits Per Second
MD5	Message Digest 5
MIC	Message Integrity Check
MIN	Mobile Identification Number
MMS	Multi-Media Message Service
NETSEC	Network Security
NIC	Network Interface Card
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network
NIST	National Institute of Standards and Technology
NSO	Network Security Officer
OFDM	Orthogonal Frequency Division Multiplexing
OS	Operating System
OSI	Open Systems Interface
OUS&P	Outside United States & Possessions
PAN	Personal Area Network
PCI	Peripheral Component Interconnect
PCIA	Personal Communications Industry Association
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Service
PCT	Private Communication Technology
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PED	Personal Electronic Device
PIM	Personal Interface Module
PIN	Personal Identification Number

PKI	Public Key Infrastructure
PPP	Point-to-Point-Protocol
PPTP	Point-to-Point Tunnel Protocol
RADIUS	Remote Access Dial-in User Service
R & D	Research and Development
SA	System Administrator
SCI	Secure Compartmented Information
SGSM	Secure GSM
SHA	Secure Hash Algorithm
SID	System Identifier
SIG	Special Interest Group
SIM	Subscriber Identity Module
SIPRNet	Secret Internet Protocol Router Network
SM	Security Manager
SMF	System Management Facility
S/MIME	Secure Multipurpose Internet Mail Extensions
SMS	Short Message Service
SRR	Security Readiness Review
SRRDB	SRR Database
SSAA	System Security Authorization Agreement
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSN	Subsystem Name
STE	Secure Terminal Equipment
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TIA	Telecommunications Idustry Association
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneling TLS
UMTS	Universal Mobile Telecommunications System
UNII	Unlicensed National Information Infrastructure
US&P	United States & Possessions
USB	Universal Serial Bus
VCTS	Vulnerability Compliance Tracking System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WCDMA	Wide band CDMA

WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WID	Wireless Information Device
Wi-Fi	Wireless Fidelity
WIM	WAP Identity Module
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN
WLANA	Wireless LAN Association
WMAN	Wireless Metropolitan Area network
WPA	Wireless Protected Access
WPAN	Wireless Personal Area Network
WPKI	WAP or Wireless Public Key Infrastructure
WTLS	Wireless Transport Layer Protocol
WWAN	Wireless Wide Area Network
WWW	World Wide Web
WZC	Wireless Zero Configuration