Securing Wireless LANS in Microsoft Networks using Wi-Fi Protected Access^{TM} and Digital Certificates

John Holmblad
SANS GIAC/GCWIN Practical

January 6, 2004
(Revised Feb 10, 2004)

Table of Contents

This page intentionally left blank

1 Abstract

This objective of this paper is to provide a comprehensive overview of the implementation of a secure 802.11 wireless networking environment based on a combination of enterprise grade 802.11 a/b/g wireless LAN[1] components from Proxim, Cisco/Linksys, Lucent, Netgear, and Microsoft with Microsoft Small Business Server 2003 Premium Edition, Microsoft 2000 Advanced Server, and Microsoft Server 2003 Enterprise Edition. The focus of this paper will be to examine the ease of deployment and use claims of each supplier with respect to their Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access^{TM} (WPA) capabilities. WPA will be tested with three different authentication methods:

- pre-shared key,
- Extensible Authentication Protocol- Transport Layer Security (EAP-TLS) mode, and
- Extensible Authentication Mode – MS Challenge Handshake Protocol V.2 (PEAP- MS CHAP V.2).

Both EAP-TLS and PEAP-MS CHAP V.2 will be tested with Digital Certificates produced by the Microsoft Certificate Services Server. A secondary goal of this testing will be to confirm interoperability of the various 802.11 base stations and client hardware used to perform the tests in a mixed Microsoft OS and networking environment. The paper next provides an assessment of the suitability of each of the security technologies for deployment in the small business environment and considers the extension of this solution to a mixed operating system wireless network environment through the addition of a Linux based SAMBA file server to the solution over the wireless LAN. Finally, the paper makes specific recommendations on how to deploy WPA in two specific Microsoft network environments, a Windows Workgroup network and a Windows Active Directory network.

2 Introduction

2.1 Objectives

It takes no stretch of the imagination to believe that if large and medium size businesses are having a significant challenge in securing their network environments against insider and outsider threats, then the situation is even more challenging for the small Internet enabled business. The small business market segment in the United States serves as the true backbone of the economy and an engine of continuous economic renewal not to mention innovation and job growth. In his recent trip to the Asia, President George Bush spoke in the Philippines on the subject of terrorism and made the point of clearly linking the negative consequences of terrorism on the world's economies[2]. By extension, cyber-terrorism, and, more generally, cyber-crime similarly exert a cost and economic drag on the information economies of the world and the

United States in particular. This is felt particularly strongly in the small business sector, here defined as businesses with up to 100 so called “seats” or workstations of various types along with one or more server computers and other telecom and Information technology systems. This segment of the enterprise market is finally starting to see the benefits of networked computer systems and the Internet that larger enterprises have reaped over the last decade. It is now possible for businesses with just a few employees and a modest revenue stream to acquire powerful and flexible computing and networking assets and to put those assets to productive use. Continued price/performance improvements (so called “Moore’s law” improvements)[3], geometric productivity gains through networking (so called “Metcalfe’s Law” improvements)[4], and the dominance of “ease of use” and cost reduction engineering over the often times (but not always) cost increasing and performance decreasing impact of security engineering have all contributed to this situation. As a result, these small organizations with little or no professional IT support can deploy and use such assets. This is particularly true of wireless LAN technology based on the IEEE 802.11 a/b/g standards which have been phenomenally successful in the last three years in the US market. The downside of course is that these assets are rarely, if ever, properly secured. A key objective of this paper is to assess the degree of difficulty in deploying improved wireless LAN security in the small business environment. This assessment is based on conducting tests in a lab environment that attempts to approximate the mix of workplace computer and network systems as are typically found in a small business information technology enabled workplace.

After briefly summarizing the current state of 802.11 security in sections 2 and 3, and the technology and architecture of the test network in sections 4 and 5, section 6 of this paper presents the results of the conduct of 8 different test protocols. In the discussion of the test results, an assessment is also made of the ease of use of the underlying security technologies under plausible real-life conditions of use. The major components of 802.11 wireless LAN security that are tested and evaluated in this paper include the following:

- ➔ Secure 802.11 Access Point (AP) Administration
- ➔ Detection and reporting of unauthorized (so called “rogue”) Access Points
- ➔ Network Access Control using MAC Address Filtering
- ➔ Privacy and message integrity using Wired Equivalent Privacy (WEP)
- ➔ Network Access Control, privacy, and message integrity using Wi-Fi Protected Access^{TM} (WPA)

2.2 Security Services and Supporting Standards

The principal underlying industry standards on which these security technologies are based include the communications protocols identified in **Table 2.2.1** below. While this is not an exhaustive list it does represent the major components that are utilized as the key ingredients for any secure system which is intended to provide one or more of the following services to a group of communicating entities:

- Privacy
- Integrity
- Non-repudiation
- Authenticity
- Availability

Standard			Responsible Standards Body	Purpose
Acronym	Name	Documentation Number/Name		
SSL	Secure Sockets Layer	AOL/Netscape Standard	Internet Society/Internet Engineering Task Force (ISOC/ITEF)	Provide privacy for documents transmitted via HTTP
WEP	Wired Equivalent Privacy	802.11[5]	IEEE 802.11 Committee	Provide authentication, privacy, and message integrity for 802.11 wireless networks
WPA	Wi-Fi Protected Access™	WPA[6]	WIFI Alliance	Provide improvements to WEP to eliminate flaws in WEP design
802.1x	Port Based Network Access Control	802.11x[7]	IEEE 802.11 Committee	Provide port based network access control for Local Area Networks
802.11i	Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security Draft 3.0	802.11i[8]	IEEE 802.11 Committee	Provides a specification for improved security over that of the original 802.11 standard.
X.509	The Directory: Public-key and attribute certificate frameworks	X.509[9]	International Telecommunications Union (ITU)	Provides an International standard for Digital Certificate based credentials
EAP	PPP Extensible Authentication Protocol	RFC 2284[10]	ISOC/ITEF	Provides an extensible Link Control Protocol which allows negotiation of an Authentication Protocol for authenticating its peer before allowing Network Layer protocols to transmit over the link
TLS	Transport Layer Security	RFC 2246[11]	ISOC/ITEF	Provides a means for client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery
EAP-TLS	EAP – Transport Layer Security	RFC 2716[12]	ISOC/ITEF	Provide authentication using the TLS protocol
PEAP-MSChapV2	Protected EAP MS Challenge Handshake Protocol V2	draft-josefsson-pppext-eap-tls-eap-07.txt[13]	ISOC/ITEF	Provide authentication using the Microsoft CHAP V.2 protocol
RADIUS	Remote Authentication Dial-In User Service	RFC 2138[14]	ISOC/ITEF	Provide for the transport of authentication, authorization, and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server.

Relevant Security Related Standards
Table 2.2.1

The focus of this paper is on the Microsoft networking environment, and the Microsoft operating system technologies summarized in **Table 2.2.2** below are directly relevant to the discussion of security technologies. These technologies with the exception of the IAS Proxy Server function, which first became available in the Microsoft Windows Server 2003 family, are utilized in the test network whose configuration is discussed in detail in section 5 of this paper. These technologies are well understood, well documented by Microsoft and others, and are widely used in networks of all sizes and uses.

Microsoft Network Technology	Purpose
Active Directory Forest/Domain Controller	Provides centralized management of computer, user, and other resources in a Microsoft network including Kerberos authentication.
Certificate Services Server	Provides for the creation, distribution, and management of a Digital Certificate based Public Key Infrastructure
Integrated Authentication Services (IAS) Server	Provides RADIUS services
IAS Proxy Server	Provides RADIUS proxy between RADIUS clients and a RADIUS server
Domain Name Server (DNS)	Provides Domain Name Service

Microsoft Network Technologies
Table 2.2.2

For the reader who is familiar with the structure of, and the known weaknesses in the security methods utilized in the IEEE 802.11 standard you can advance to section 4 of this paper, Technology Underpinnings of a Secure **Microsoft Wireless Network**

. Otherwise please proceed to the following section to learn more about wireless network security.

3 The Security Challenges of Wireless Networks

Since 1895, when Guglielmo Marconi, a self-taught 21-year-old from Bologna, Italy, successfully propagated electromagnetic radiation for the purpose of communications[15], the world has had to contend with the security consequences of what, after all, is a fundamentally insecure medium. As with many if not most inventions, whose ultimate value to society is not well perceived at the start, Marconi had to work hard to find believers in the value of his work and he had to travel abroad to England to pursue his ideas. One hundred years on, however, the ubiquitous application of wireless communications has transformed civilization and pervaded almost every aspect of our lives. Consequently, security professionals who specify, design, implement, and support systems using the wireless medium have an important responsibility to assure that such systems properly deliver the security related services outlined in Section 2.2, **Security Services and Supporting Standards**

of this paper.

3.1 Attacks on Wireless Networks

In chapters 3 and 4 of their text, “Real 802.11 Security, Wi-Fi Protected Access and 802.11i”[16], authors Jon Edney and William A. Arbaugh, provide a concise yet thorough review of the types of attackers and the types of attack that can be mounted against networks in general, and specifically against wireless LANS. The attacker types are summarized in **Table 3.1.1** below along with this author’s assessment of the degree of economic risk to the victim organization that each class of attacker represents in the aggregate. The economic risk to the victim is greatest from the “profit or revenge” attacker because such attackers generally understand where the economically valuable information is located with the victim organization and/or they have the intention to get at it, and, having obtained access to it, to then use it for their own benefit. Of course any given attack, even one which “accidentally” compromises and/or destroys valuable information can be devastating to the victim firm, but the table below assumes that the victim organization has fully implemented the necessary backup/recovery procedures to mitigate the risk of such “accidents”.

The classes of attack are summarized in **Table 3.1.2**

Attacker Type	Motivation	Economic Risk to Victim
Gaming	Thrill or fun seeker	Low
Profit or Revenge	Theft or destruction of Economic Value	High
Ego	Boost Self-Esteem in the Cracker community	Medium

Attacker Motivation
Table 3.1.1

Attack Class	Potential Uses	Examples
Data Compromise	→ Gain access to sensitive information of economic value → Obtain information (e.g. passwords) to mount other attacks on the victim system	→ Theft of password secrets to compromise various systems on the victim’s network → Extraction of financial account (e.g. credit card) information
Data Modification	→ Cause redirection of information useful to the attacker (e.g. for known plaintext attacks) for mounting further attacks → Denial of service to cause economic harm to the victim → Produce economic gain for the attacker	→ Increasing transaction value of an otherwise legitimate transaction to the advantage of the attacker → Capture of plaintext in order to mount a known plaintext attack on the victim’s cryptographic system
Impersonation	→ Gain access to valuable information assets on the victim’s network	→ Rogue service that appears to be legitimate but actually results in compromise of sensitive information of the victim to the attacker
Denial of Service (DOS)	→ Create economic loss for the victim → Divert victim attention while attacker mounts a different attack	→ TCP “SYN” flooding → Various application level DOS attacks

Attack Classification
Table 3.1.2

3.2 Flaws in the Original 802.11 Security Protocols

It is well documented by now that, despite the excellent worldwide reputation of the IEEE with respect to the production of useful and well designed engineering standards, the committee which developed 802.11 did not fulfill its aforementioned responsibility with respect to the design of the 802.11 security features. The original standard contains a set of security related services known as Wired Equivalent Privacy, or WEP, and it has been amply documented that each of these services can be compromised at an almost trivial economic cost. The list of these security related services in WEP is shown in **Table 3.2.1** below along with a brief statement of the vulnerability which leads to the security compromise of that particular service. Perhaps the most fundamental mistake of the 802.11 standard designers was to use a fast, proprietary cryptographic algorithm developed by RSA Security, Inc[17], and known as RC4, in a medium, free space, in which ciphertext can be easily sniffed and analyzed. The simplicity and speed of RC4 is achieved through the use of bitwise exclusive or'ing (XOR) of the plaintext message with a keystream that is derived from an RC4 key of variable length[18]. This simplicity and speed of the mathematical operation of XOR (XOR is, after all, one of the fundamental or "atomic" if you will, mathematical operations of a computer or for that matter any digital logic system) along with the well understood vulnerabilities of the RC4 algorithm to

- ➔ certain so-called "weak key" values
- ➔ the reuse of previously used key values, and
- ➔ short key lengths

make the RC4 algorithm susceptible to various attacks in situations where the attacker can easily obtain knowledge of only the ciphertext of the message, as is the case with respect to wireless communications. The mistake of using the RC4 algorithm, which in and of itself is a fundamentally useful and widely used algorithm in applications such as Oracle's Secure SQL and the Cellular Digital Packet Data specification[19], was further magnified by other design decisions which only made things worse from a security perspective. For example, in the case of client authentication, the attacker can obtain the plaintext as well as the ciphertext and mount a straightforward known plaintext attack on the cryptographic system of WEP.

802.11/WEP Security Service	Vulnerability	Attack Method	Result
a) Client Authentication to Access Point (AP) (shared key authentication)	➔ Authentication message exchange (challenge/response) is based on RC4 and the exchange (ciphertext & plaintext) is accessible to an attacker	Eavesdropping & capture of challenge/response sequence followed by XOR of challenge with response to produce WEP key stream	Compromise of Message Encryption (WEP) Key
b) AP Authentication to client	Not defined in 802.11		
c) Message Integrity & Authenticity	➔ Linear CRC Method used to calculate Message Integrity Value (ICV) ➔ No Message replay protection	Eavesdropping & capture of a message and selective modification to create a modified message which nonetheless has a correct ICV	Message Modification and message replay by attacker
d) Message Privacy	➔ RC4 encryption Key reuse as a consequence of the use of a relatively short (24 bit) Initialization Vector ➔ weak WEP RC4 key values	Eavesdropping & capture of sufficient ciphertext to deduce the keystream	Compromise of Message Encryption (WEP) Key

WEP Vulnerabilities, Attack Methods, and Consequences
Table 3.2.1

The implementation of the Client to Access Point authentication is so seriously flawed that some implementers of 802,11 products don't even support the feature. Where it is supported it should be turned off to avoid exposing the WEP key to disclosure.

These vulnerabilities in the cryptographic aspects of WEP give rise to the potential for all manner of easily mounted and successful attacks on a network which utilizes the 802.11 protocol including:

- ➔ Message Interception
- ➔ Rogue Access Points masquerading as a legitimate Access Point
- ➔ Message Forgery

A thorough explanation of the weaknesses of and attack methods on WEP can be found in chapter 6 of the text, "Real 802.11 Security"[20]. The attacks on the WEP cryptographic methods are also documented in the papers "Intercepting Mobile Communications: The Insecurity of 802.11[21] and "Weaknesses in the key scheduling algorithm of RC4"[22].

There should be no doubt in the reader's mind that the aforementioned weaknesses in the 802.11 security protocols can be exploited in the real world. At the recently completed WIFI Planet Conference in December 2003, Tech world reporter Peter Judge reported[23] that AirDefense monitored Wi-Fi traffic at the trade event and observed 21 attempted man-in-the-middle (MITM) attacks of which 16 were successful for a success rate of 76%. This represents a substantial increase in the percentage of successful attacks of this type from the similar event just six months earlier in June 1002 where only 3 of 32 or ~9% of MITM attacks were successful. Air Defense also recorded 75 Denial-of-Service (DOS) attacks and 125 MAC spoofing attacks. In addition, at least one cracker was able to construct a "rogue" ad hoc network with an SSID of "wifiplanet" which was real enough to trick at least 10 delegates into associating with that rogue network.

Of course, the aforementioned weaknesses in WEP security have not stopped users from utilizing 802.11 based networks, just as the high vulnerability of first generation mobile voice networks based on the Advanced Mobile Phone System (AMPS) standard to eavesdropping did not stop users from using that service starting in the early 1980's. What is different today, of course, is that 802.11 based networks are being used extensively inside of the perimeter defenses of enterprises and, in many cases, government agencies where the weaknesses in WEP can expose the whole business or government network to unauthorized access, theft, and destruction of information

3.3 Short Term and Medium Term Replacements for WEP

Unfortunately for the users of 802.11 wireless technologies, the true extent of the vulnerabilities of 802.11 WEP were fully understood and communicated only **AFTER** the standard had been embedded in systems produced by numerous suppliers and literally millions of units of products containing WEP had been deployed worldwide. This led to a crash effort on the part of a consortium of suppliers of 802.11 technologies known as the WI-FI alliance (www.wi-fi.com) to develop an interim "fix" to WEP security known as Wi-Fi Protected Access^{TM} (WPA). In the meantime. the IEEE itself has been working on a more extensive and, of course, more cryptographically robust replacement for WEP known as 802.11i which is currently in draft form and is expected to be ratified sometime in 2004. The security architecture for 802.11i is also referred to as Robust Security Network (RSN) and it utilizes the IEEE 802.1x[24,25] standard as the underpinning for the access control, authentication, and cryptographic key management functions associated with 802.11i.

The W-Fi alliance has been careful to design the WPA standard to have both downward compatibility with many (but not all) previously deployed WEP based systems as well as upward compatibility with the still to be finalized/ratified IEEE 802.11i draft standard (draft 3.0 in fact). The balance between downward and upward compatibility in the WPA standard shows itself in the area of the choice of cryptographic methods for message privacy. Although the 802.11 supports two alternative cryptographic methods, the Advanced Encryption Standard[26] and the Temporal Key Integrity Protocol[27] (TKIP), the WPA standard only requires the TKIP alternative (AES support is supplier optional). This is because TKIP can be more easily implemented through a software/firmware retrofitting of the already extant 802.11 equipment than can the more cryptographically secure but more computationally intense AES standard. Furthermore there is one useful but not as critical feature of 802.11i/RSN, which is authenticated roaming access, which is not yet finalized by the 802.11i standards committee and so that feature was left out of WPA altogether.

As this paper goes to press, WPA compliant products (Access Points and various client radio PC adapter products) are just coming into the commercial market along with the necessary software and firmware to support the WPA feature set.

The essential features of WPA are summarized in **Table 3.3.4** below along with a brief explanation of the mitigating effect of each such WPA feature on the risk of attack against an 802.11 wireless network.

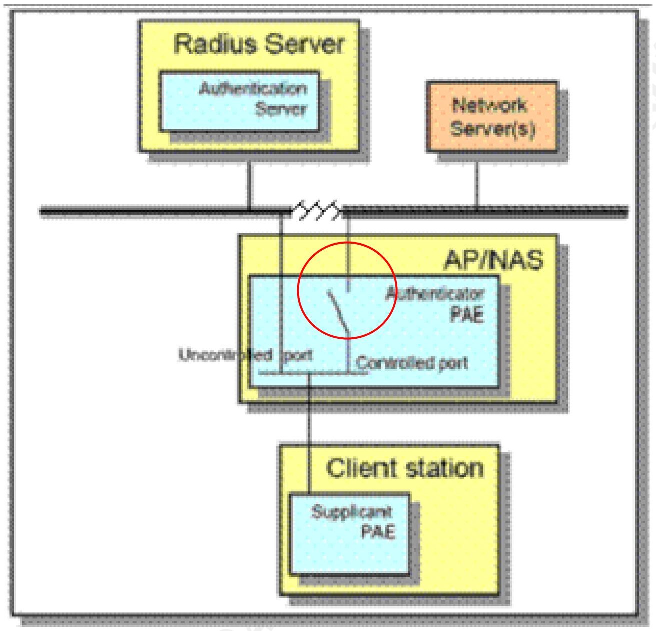
WPA Security Component		Solution	Required for Wi-Fi Alliance WPA certification?	How the Solution mitigates the risk of successful Attack
TKIP	Message Privacy	→ Modifications to WEP Keying protocol	YES	→ 32 bit vs 24 bit initialization vector → Key mixing protocol changes key with each message → Weak keys are avoided → Mechanism to automatically change broadcast message key
	Message Authenticity	→ Michael Message Integrity Check		→ The use of a strong message integrity protocol eliminates the threat of message modification by an attacker
	Message Anti-Replay	→ TKIP Sequence Counter (TSC)		→ Allows the message recipient to detect and discard "out of sequence" messages which may be replay forgeries
AES-CCMP	Message Privacy	→ AES-Counter Mode	NO	→ Highly secure symmetric key encryption algorithm with no known vulnerabilities to ciphertext only attacks
	Message Authenticity	→ AES – CBC-MAC		→ The use of a strong message integrity protocol to eliminate the threat of message modification by an attacker
	Message Anti-Replay	→ CCMP Header Packet Number (PN)		→ Allows the message recipient to detect and discard "out of sequence" messages which may be replay forgeries
802.1X-Extensible Authentication Protocol (EAP)	Client authentication to Access point	→ Use 802.1x with EAP method	YES	→ 802.1x EAP provides strong authentication by means of a) Digital Certificates for both client and AP (EAP-TLS) or b) a Digital Certificate for the AP followed by a password for the Client (PEAP-MS-CHAP-v2). Dynamic keying can then take place over an encrypted channel.
	Access Point authentication to client			
802.1X-Preshared Key (PSK)	Client authentication to Access point	→ Pre-shared 256 bit key, which can optionally be derived from a pre-shared passphrase	YES	→ WPA-PSK provides mutual authentication by means of a shared secret. Dynamic keying can then take place over an encrypted channel using the shared key for encryption on that channel.
	Access Point authentication to client			

WPA Security Components, Methods, and Risk Mitigants
Table 3.3.4

As **Table 3.3.4** indicates, the WPA standard makes use of the 802.1x standard for mutual authentication of the Client, which is referred to as the Station in the WPA standard, and the Access Point, which is referred to as the Authenticator in the WPA standard. Although 802.x was first introduced to support authentication in a wired LAN environment, it has been extended to support wireless device authentication as well. In so doing the WPA standard leverages the broad base of experience with the RADIUS authentication protocol which has been proven in widespread use for over 10 years in dial-up networking environments.

Figure 3.3.1 below shows the architectural elements of an 802.1x based authentication environment. The Access Point (a.k.a. authenticator) implements a virtual switch function to control the access of the Client station (a.k.a.

supplicant) to the Network Server(s) on the LAN. Prior to authentication of the Client station by the RADIUS Server (a.k.a. Authentication Server), the Access Point allows communication ONLY between the Client Station and the RADIUS Server. Once the Client station has successfully authenticated to the RADIUS Server, the Access Point "throws" the switch shown in the diagram to the position that allows the Client station to access the LAN and the Network Server(s) thereupon.

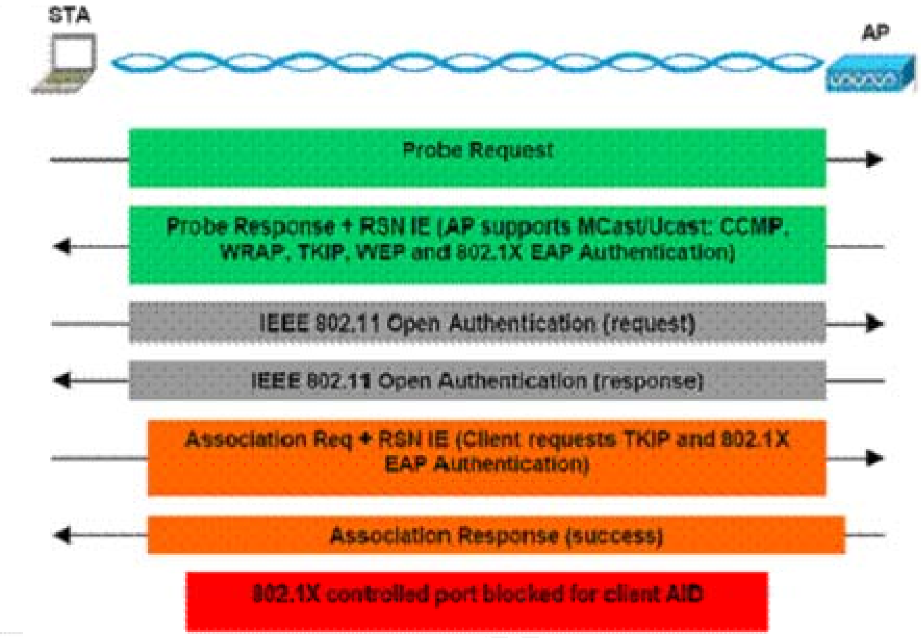


802.1x Component Architecture[28]
Figure 3.3.1

With respect to the mutual authentication of the supplicant and the access point using 802.1x/EAP, the supplicant, authenticator, and authentication server go through a phased process by which mutual authentication using EAP is achieved. The process is described in detail in section 8.5 of the IEEE standard 802.11i Draft 3.0[29] and summarized here. The Figures 3.3.2-3.3.5 below are derived from those in the 802.11i Draft 3.0 specification.

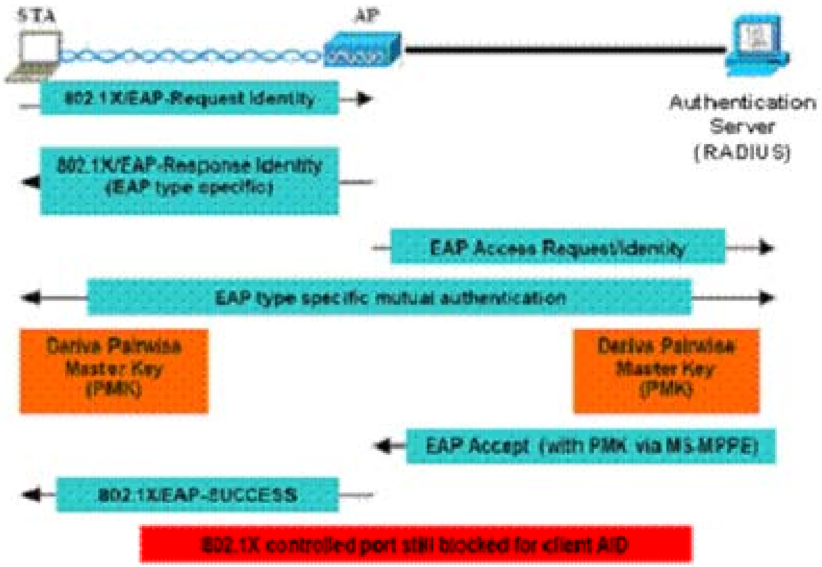
In the first phase, the supplicant sends a probe request frame and receives a probe response from the AP wherein the AP identifies the cipher suites that it supports. The supplicant then performs and Open Authentication sequence to the AP just as is done in 802.11, after which the supplicant responds to the AP indicating what type of cipher suite that the supplicant would like to use and the AP affirms the response with an Association Response success frame. This sequence is shown in **Figure 3.3.2**

. At this point the supplicant and the AP are associated but NOT authenticated so the virtual switch shown in **Figure 3.3.1** is set to the open position so that ONLY 802.1x frames can be passed between the supplicant and the AP.


STA
AP
Probe Request
Probe Response + RSN IE (AP supports MCast/Ucast: CCMP, WRAP, TKIP, WEP and 802.1X EAP Authentication)
IEEE 802.11 Open Authentication (request)
IEEE 802.11 Open Authentication (response)
Association Req + RSN IE (Client requests TKIP and 802.1X EAP Authentication)
Association Response (success)
802.1X controlled port blocked for client AID

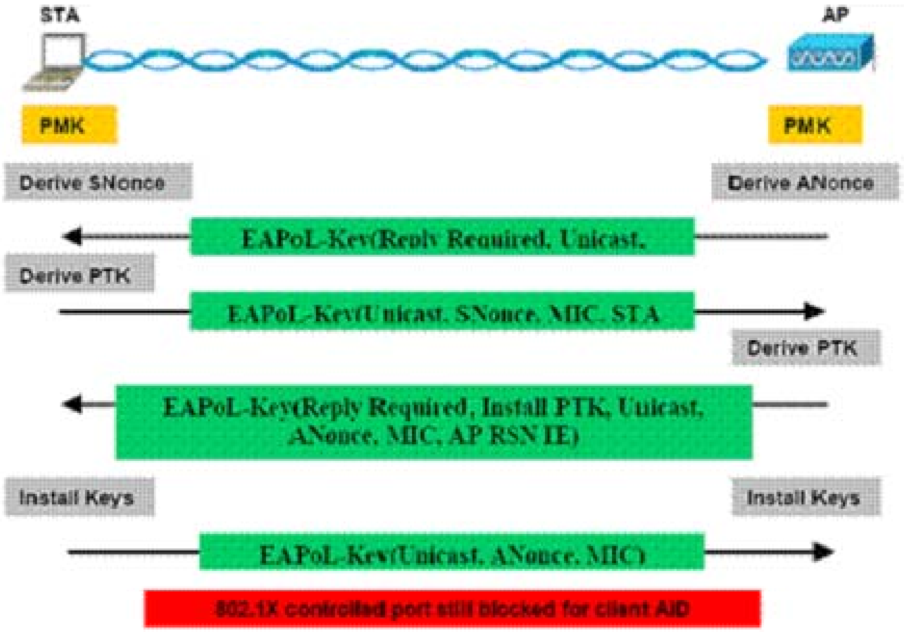
Phase I
Association via Open Authentication and Negotiation of the Security Policy
Figure 3.3.2

The next phase in the authentication process is for the supplicant and the authentication server to perform mutual authentication according to the EAP method that was agreed in phase 1 described above and using the AP as a mediator for the authentication transactions. Once mutual authentication is achieved, the supplicant and the authentication server each derive the Pairwise Master Key (PMK) using information that was shared between the two parties during the just completed authentication. In addition, the authentication server sends a copy of the PMK to the access point in an EAP success frame via its secure channel to the AP. The AP then removes the PMK from the received frame and sends an EAP/802.1X Success EAPOL frame to the supplicant. At this point both the supplicant and the AP have the same keying material in the form of the PMK from which they immediately construct a secure (i.e. encrypted channel) for completing the installation of the aforementioned cipher suite. From this point forward, the remaining steps to install the cipher suite are performed between the supplicant and the AP. In other words the work of the authentication server is completed.


STA
AP
Authentication Server (RADIUS)
802.1X/EAP-Request Identity
802.1X/EAP-Response Identity (EAP type specific)
EAP Access Request/Identity
EAP type specific mutual authentication
Derive Pairwise Master Key (PMK)
Derive Pairwise Master Key (PMK)
EAP Accept (with PMK via MS-MPPE)
802.1X/EAP-SUCCESS
802.1X controlled port still blocked for client AID

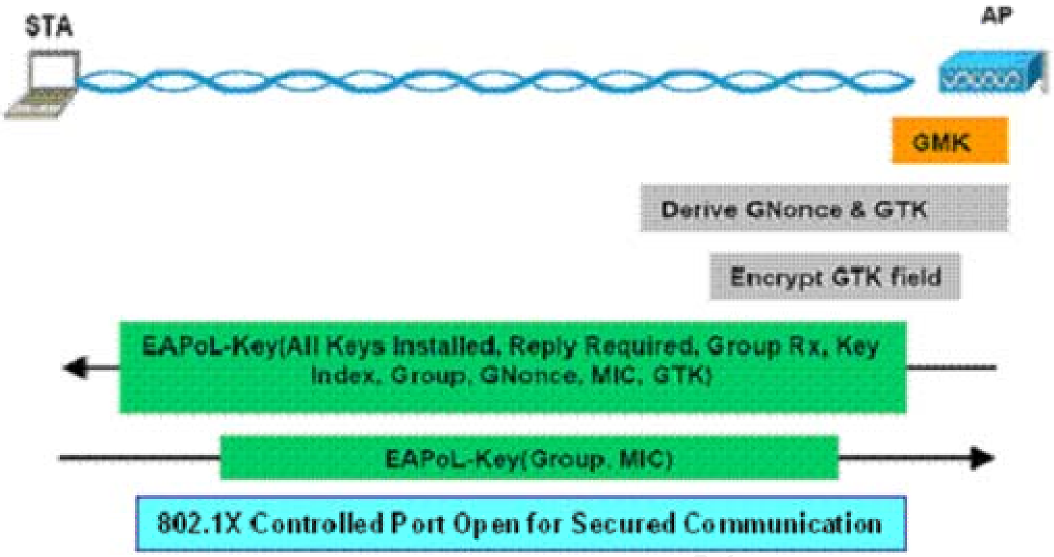
Phase II
Mutual Authentication and Derivation of the Pairwise Master Key (PMK
Figure 3.3.3

In the next phase the supplicant and the AP use the aforementioned channel that is secured by the Pairwise Master Key to create a unique (i.e. never used before) Pairwise Temporal Key (PTK) that will be used to encrypt all data frames once the EAP negotiation is completed. Nonces from both the supplicant and the AP are used to assure uniqueness of the PTK. The protocol sequence that takes place at this point is referred to as a 4-way handshake because it involves the exchange of 4 messages to complete the installation of the Pairwise Temporal Key. This phase is shown in **Figure 3.3.4**.


STA
AP
PMK
PMK
Derive SNonce
Derive ANonce
EAPoL-Key(Reply Required, Unicast,
Derive PTK
EAPoL-Key(Unicast, SNonce, MIC, STA
Derive PTK
EAPoL-Key(Reply Required, Install PTK, Unicast, ANonce, MIC, AP RSN IE)
Install Keys
Install Keys
EAPoL-Key(Unicast, ANonce, MIC)
802.1X controlled port still blocked for client AID

Phase III
Creation of the Unicast Pairwise Temporal Key
Figure 3.3.4

Because the 802.11 standard also provides for the transmission of broadcast and multicast traffic, a means must be established for protecting such traffic from eavesdropping. In this case however, all of the supplicants must have the same cryptographic key, otherwise, the communications of broadcast/multicast frames between the AP and the supplicants would be unwieldy as the AP would have to send such broadcast/multicast traffic serially, that is, one frame at a time, changing the keying material for each frame, thus defeating the whole concept of a broadcast or multicast transmission. For this reason the supplicant and the AP undergo a final phase by which the AP transmits the Group Master Key for use by the supplicant to decrypt broadcast/multicast transmissions. Note that this key is used for one direction of communications only, that is, from the AP to the supplicants.


STA
AP
GMK
Derive GNonce & GTK
Encrypt GTK field
EAPoL-Key(All Keys Installed, Reply Required, Group Rx, Key Index, Group, GNonce, MIC, GTK)
EAPoL-Key(Group, MIC)
802.1X Controlled Port Open for Secured Communication

Phase IV
Exchange of the Group Master Key
Figure 3.3.4

The WPA specification provides implementers of the standard with guidance with respect to the optional and mandatory features of that standard for both client cards (Network Interface Cards) as well as for Access Points. **Table 3.3.5** below summarizes that guidance. Of significant note is that the implementation of a pairwise key cipher (requirement number 25 in **Table 3.3.5**) is optional, not required, for Access Points. This suggests that a compromise was made for manufacturers who could not support the retrofit of pairwise keying in their currently deployed systems. The same is true no doubt with respect to WPA requirement number 31, “Group key update on a disassociation of a authenticated station”.

WPA Requirement		Required /Recommended /Optional for	
#	Explanation	NIC	AP
1	48 bit TKIP (including phases 1 and 2)	Required	Required
2	Fragmentation of TKIP Data Packets (Note: the station will not be able to send full size 802.11 MPDU's if fragmentation is not supported)	Required	Required
3	De-fragmentation of TKIP data packets	Optional	Optional
4	Use of integrity check and IV for replay protection	Required	Required
5	Michael	Required	Required
6	Michael counter measures	Required	Required
7	WPA information element in beacon, probe response, association/re-association request	Required	Required
8	Privacy bit set in capability information element Beacon/Probe response/association/re-association request	Required	Required
9	4-way handshake	Required	Required
10	Validation of WPA Information Element in beacon/probe response/association/re-association request with WPA IE in 4-way handshake	Required	Required
11	Group key update	Required	Required
12	Pairwise Request (with or without error)	Required	Required
13	Group Request (with or without error)	Required	Required
14	Encryption of 802.1x messages with Pairwise Key	Required	Required
15	802.1x messages not encrypted with Group Keys	Required	Required
16	WPA authentication mode	Required	Required
17	WPA-PSK authentication mode	Required	Required
18	WPA-None authentication mode	Optional	Required
19	Open 802.11 MAC authentication for all WPA authentication modes	Required	Required
20	WPA-PSK ASCII passphrase hash	Required	Required
21	WPA-PSK 256 bit key	Recommended	Recommended
22	Non-WPA support	Recommended	Recommended
23	Non-WPA and WPA mixed mode	Recommended	Recommended
24	Group key cipher	Required	Required
25	Pairwise key cipher	Required	Recommended
26	No sending of non-802.1x data packets until the correct key is installed. (Note: This is the Group key for multicast/broadcast from AP or from station if Pairwise key is not installed. This is the Pairwise key for unicast from AP or all traffic from station if a Pairwise key is installed)	Required	Required
27	Queuing of EAPOL-Key messages when in power save mode	Required	Required
28	Saving of IBSS Initialization Vector (IV)	Required	Required
29	Support for Radius	Not Applicable	Required
30	Group Key Update on a time interval	Recommended	Recommended
31	Group key update on a disassociation of a authenticated station	Optional	Optional
32	Use of PRF for Pairwise key generation	Required	Required
33	Use of PRF for Group Key generation	Required	Required
34	Use of random number on AP for master key for Group Key generation	Required	Required
35	Initialization Key Counter	Required	Required
36	Initialization of EAPOL-IV from Key Counter	Required	Required

WPA Optional and Required Features

Table 3.3.5

4 Technology Underpinnings of a Secure Microsoft Wireless Network

4.1 The Technology Framework for a Secure Wireless Network

Although it may be many years before all of the cryptographic methods utilized in WPA and 802.11i are shown to be secure through user experience, cryptologists generally agree that both WPA and 802.11i are secure in their design. As a consequence, with respect to WPA, suppliers have moved very quickly to implement this much needed replacement for WEP while the final details of the 802.11i/RSN standard are resolved, hopefully, in 2004.

Because the elements of implementing an 802.11 network using the WPA security methods and protocols are now available, the author of this paper decided that it would be useful to test these methods out under various scenarios in a Microsoft networking environment using the latest software, firmware, and hardware available from the relevant suppliers and to compare their ease of implementation with that of the older WEP standard.

4.2 Network Test Protocol

A suite of 8 tests was conducted over a period of two weeks across a variety of predominantly Microsoft operating system based servers and workstations along with a single Redhat Linux based server system. The tests also incorporate a variety of 802.11 NIC's and depending upon the test, utilize one of the three 802.11 standards summarized in **Table 4.2.1**

.

Standard	Frequency Band (ghz)	Multiplexing Method	Maximum Baseband Bandwidth
802.11a	2.4	Orthogonal Frequency Division Multiplexing (OFDM)	11
802.11b	5.4	Direct Sequence Spread Spectrum (DSSS)	54
802.11g	2.4	Orthogonal Frequency Division Multiplexing (OFDM)	54

802.11 Standard Modes of Operation
Table 4.2.1

It should be noted that, with respect to baseband bandwidth, some suppliers (for example, Proxim) support proprietary extensions to the standard that double the maximum achievable bit rate with some of the frequency bands/multiplexing methods. The tests described in this paper however are based entirely on features that are in conformance with the 802.11 a/b/g standards so such enhanced but non-standard features were not tested.

Time did not permit the running of every test over each of the three frequency bands but this author used his best judgment to construct a suite of tests that fairly indicate the capabilities of the equipment and software in each of those three bands. It should be noted that the newest of three standards is the 802.11 g standard, which achieved commercial market penetration starting in 2003.

The specific tests that were performed are summarized in
Table 4.2.2
. The first three tests are relatively easy to implement and bear little relationship to the operating systems being used on the computer systems that are being networked using 802.11. However the author felt it was important to conduct these tests in order to

a) observe the correct functionality being tested and assess any performance impacts, and

b) determine the ease of deployment of the feature or features being tested in the kind of network that a small enterprise or government agency might encounter.

Tests 4 and 5 are of intermediate complexity, requiring modifications to the operating systems of the networked computers. The most complex test protocols are 6-8, each of which requires a digital certificate infrastructure and a Microsoft Active Directory based network along with Microsoft's RADIUS component, Internet Authentication Server (IAS). Furthermore test 8 is conducted to determine whether the Lucent Orinoco client cards, which DO NOT support the WPA standard, can nonetheless be configured to support one or more of the EAP methods designed into the Microsoft operating systems.

Test Protocol		Purpose
#	Description	
1	SSL Implementation for HTTP Administrative Interface on the Access Point	Determine the performance and functional impact of enabling SSL to protect HTTP/HTML communications between the Access Point and the network administrator's workstation
2	Rogue Access Point Detection	Confirm the ability of the Access Point to accurately detect rogue access points
3	MAC Address Filtering on the Access Point	Assess the ease of implementation of MAC address filtering
4	104 bit WEP with Open Authentication	Assess the ease of deployment and performance of WEP across multiple OS's/systems/Wireless Client Cards
5	WPA with Pre-Shared Key (WPA-PSK)	Assess the ease of deployment and performance of WPA-PSK across multiple OS's/systems/Wireless Client Cards
6	WPA with EAP-TLS	Assess the ease of deployment and performance of WPA based EAP-TLS
7	WPA with PEAP MS-CHAP –v2	Assess the ease of deployment and performance of WPA based PEAP MS-CHAP-v2
8	WEP with PEAP MS-CHAP –v2	Assess the ease of deployment and performance of WEP based PEAP MS-CHAP-v2

802.11 Test Protocol
Table 4.2.2

5 Test Network Architecture and Test Protocol Design

5.1 Test Network Architecture – Network Backbone

The test network architecture consists of a LAN connected to a Router, DSL Modem, and the Internet. Although most of the tests were conducted entirely within the LAN environment itself, access to the Internet was required for the numerous firmware updates that were needed to insure that all of the software/firmware/drivers were at the latest revision levels. In addition, tests 3-8, which included wireless supplicants, required Internet access to verify that the activation of the security methods under test did not inadvertently result in blockage of Internet related services such as DNS, etc.

In all cases the operating systems used in the lab test were configured with the latest revision levels except in the case of the system running Redhat Linux 8.0. Disc memory partition size on the Linux system was insufficient to allow the system to load all of the latest security patches from the Red Hat Network (RHN). However the absence of these patches did not affect the outcome of the one test, number 4, which utilized this system.

In the case of the Microsoft Server operating systems

- ➔ Microsoft Windows 2000 Advanced Server
- ➔ Microsoft Windows Server 2003 Enterprise Edition
- ➔ Microsoft Small Business Server 2003 EE

The test configuration afforded the author to determine whether or not the wireless NIC cards and their associated drivers and client configuration utility software would operate correctly on the server OS's. This is an important implicit test because most of the providers of wireless NIC cards do NOT explicitly specify whether or not their products are compatible with the Microsoft server operating system families.

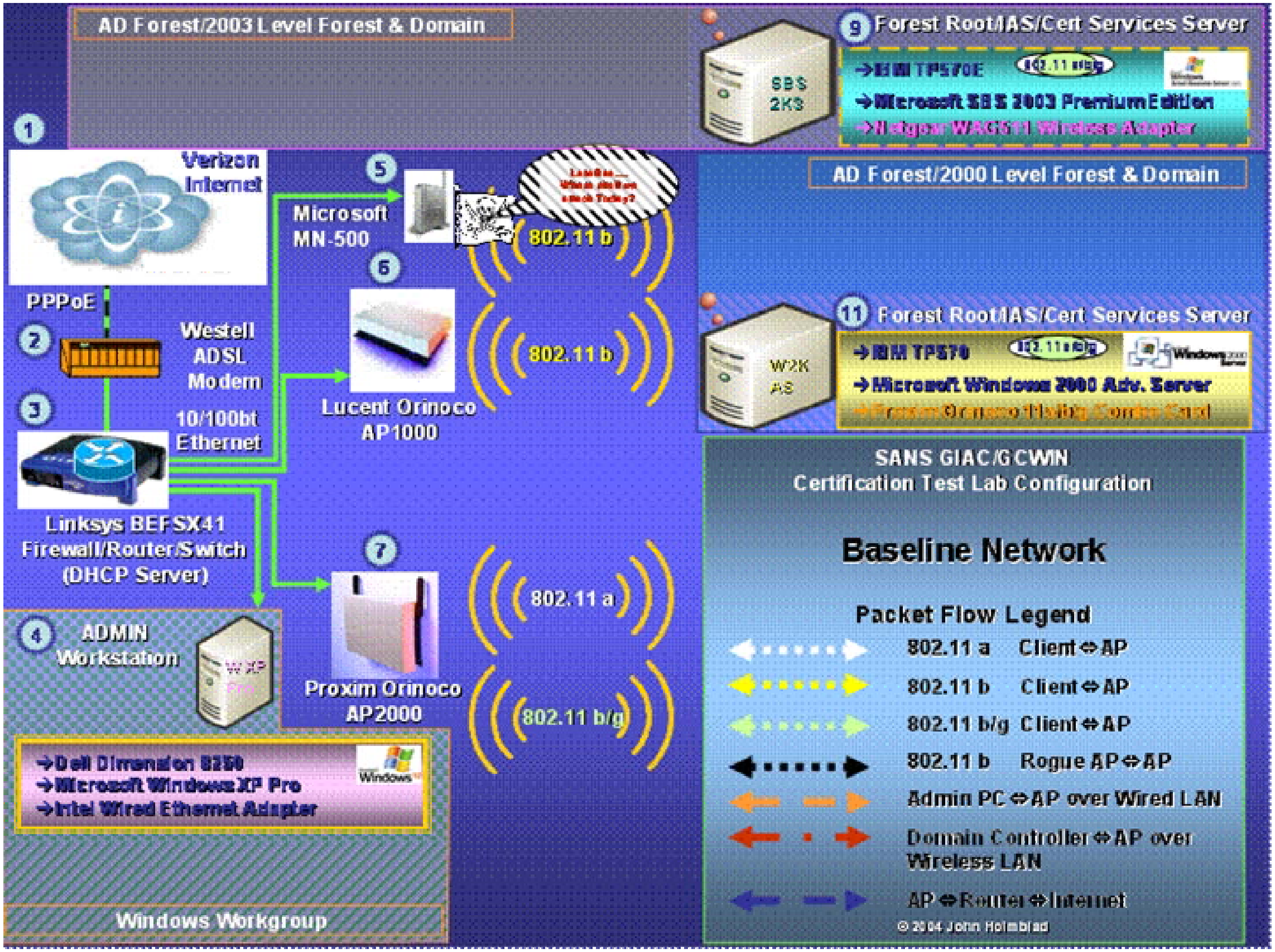
The LAN has a single routed segment that is managed by a Linksys router. The LAN has five branches each of which is served by either a LAN switch or Wireless Access Point operating in LAN Bridging mode as indicated in **Table 5.1.1** below.

LAN Branch				Served by
#	Hardware Component Diagram #	Type	MAC Layer	
1	3	Wired	802.3	4 Port layer 2 switch embedded in a Linksys BEFSX41 Firewall/Router/Switch
2	5	Wireless	802.11 b	Microsoft MN-5000 Access Point configured in LAN bridging mode
3	6	Wireless	802.11 b	Lucent Orinoco AP-1000 configured in LAN bridging mode
4	7	Wireless	802.11 a	Proxim Orinoco AP-2000 configured in LAN bridging mode (Slot A radio)
5	7	Wireless	802.11 b/g	Proxim Orinoco AP-2000 configured in LAN bridging mode (Slot B radio)

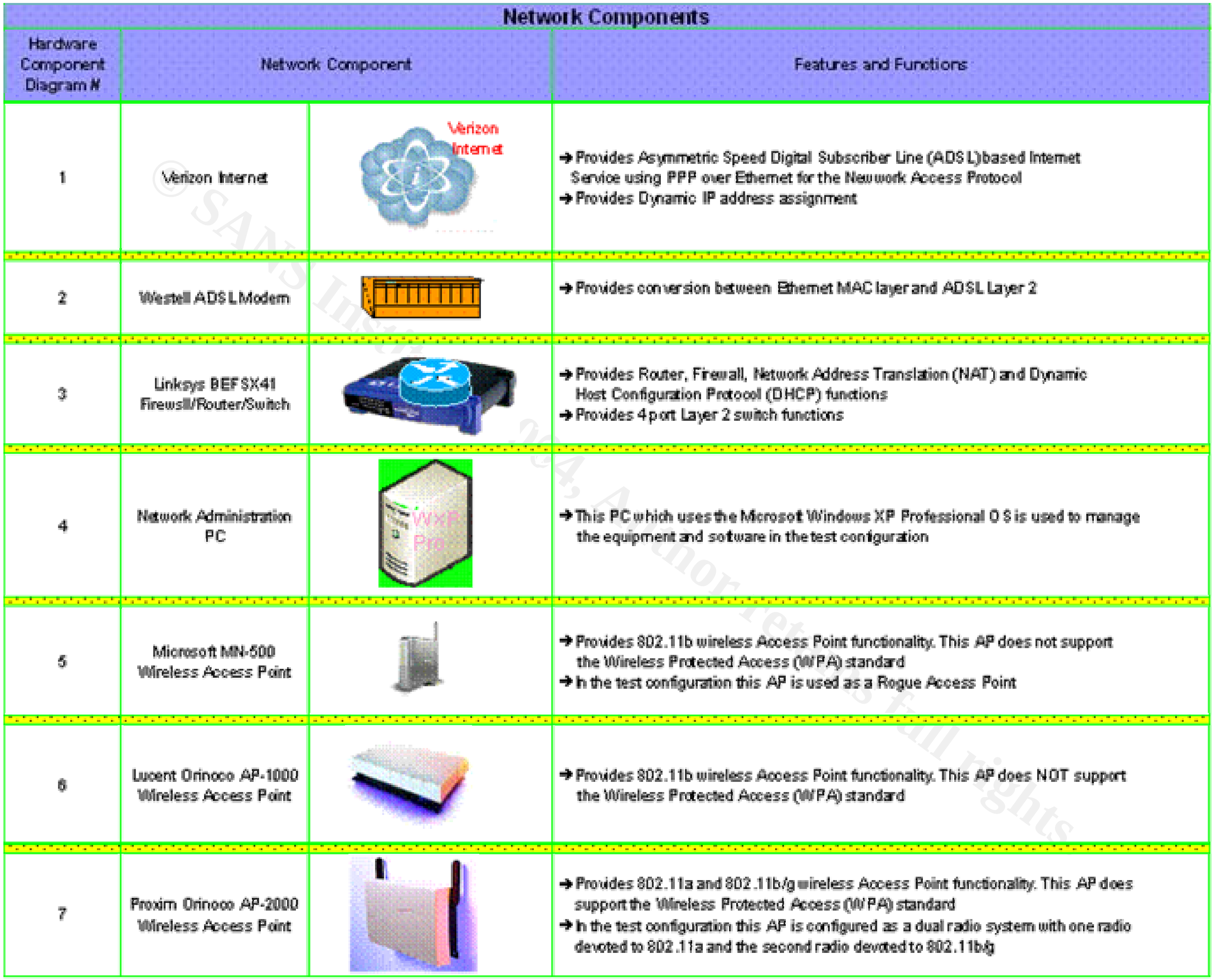
Test LAN Configuration
Table 5.1.1

The complete baseline network is shown in **Figure 5.1.1** below and a more detailed explanation of the network components is provided in **Table 5.1.2** below. **Figure 5.1.1** includes a legend that is used in subsequent figures to identify relevant packet flows of different categories across the wireless and wired branches of the LAN.

The network is administered using a PC running Microsoft Windows XP Professional. Wherever possible the Microsoft Remote Desktop (RDP) protocol is used to manage the other computers in the network whether they are server computers or 802.11 client (supplicant) systems. In addition, although it was not strictly a part of the test protocol for this paper, the author was able to also configure and test the HTTP based administrator capabilities built into Microsoft Windows Server 2003 Enterprise Edition and the even more extensive such capabilities built into Microsoft Small Business Server (SBS) 2003 Premium Edition. The combination of RDP and these HTTP based portals to the administrative functions of the tested systems greatly facilitated the testing.


AD Forest/2003 Level Forest & Domain
9 Forest Root/IAS/Cert Services Server
SBS 2K3
→IBM TP570E
802.11 a/b/g
→Microsoft SBS 2003 Premium Edition
→Netgear WAG511 Wireless Adapter
1
Verizon Internet
5
Microsoft MN-500
802.11 b
6
Lucent Orinoco AP1000
802.11 b
AD Forest/2000 Level Forest & Domain
11 Forest Root/IAS/Cert Services Server
W2K AS
→IBM TP570
802.11 a/b/g
→Microsoft Windows 2000 Adv. Server
→Proxim Orinoco Mobile Combo Card
PPPoE
2
Westell ADSL Modem
3
10/100bt Ethernet
Linksys BEFSX41 Firewall/Router/Switch (DHCP Server)
7
Proxim Orinoco AP2000
802.11 a
802.11 b/g
4 ADMIN Workstation
WXP Pro
→Dell Dimension 8250
→Microsoft Windows XP Pro
→Intel Wired Ethernet Adapter
Windows
Windows Workgroup
SANS GIAC/GCWIN
Certification Test Lab Configuration
Baseline Network
Packet Flow Legend
802.11 a Client⇔AP
802.11 b Client⇔AP
802.11 b/g Client⇔AP
802.11 b Rogue AP⇔AP
Admin PC⇔AP over Wired LAN
Domain Controller⇔AP over Wireless LAN
AP⇔Router⇔Internet
© 2004 John Holmblad

Test Network Components
Figure 5.1.1


Verizon
Internet
WXP
Pro

Network Components			
Hardware Component Diagram #	Network Component		Features and Functions
1	Verizon Internet	Verizon Internet	→ Provides Asymmetric Speed Digital Subscriber Line (ADSL) based Internet Service using PPP over Ethernet for the Neuwork Access Protocol → Provides Dynamic IP address assignment
2	Westell ADSL Modem		→ Provides conversion between Ethernet MAC layer and ADSL Layer 2
3	Linksys BEFSX41 Firewall/Router/Switch		→ Provides Router, Firewall, Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) functions → Provides 4 port Layer 2 switch functions
4	Network Administration PC	WXP Pro	→ This PC which uses the Microsoft Windows XP Professional OS is used to manage the equipment and software in the test configuration
5	Microsoft MN-500 Wireless Access Point		→ Provides 802.11b wireless Access Point functionality. This AP does not support the Wireless Protected Access (WPA) standard → In the test configuration this AP is used as a Rogue Access Point
6	Lucent Orinoco AP-1000 Wireless Access Point		→ Provides 802.11b wireless Access Point functionality. This AP does NOT support the Wireless Protected Access (WPA) standard
7	Proxim Orinoco AP-2000 Wireless Access Point		→ Provides 802.11a and 802.11b/g wireless Access Point functionality. This AP does support the Wireless Protected Access (WPA) standard → In the test configuration this AP is configured as a dual radio system with one radio devoted to 802.11a and the second radio devoted to 802.11b/g

Test Network Components
Table 5.1.2

5.2 Test Network Architecture – Microsoft Networking Components

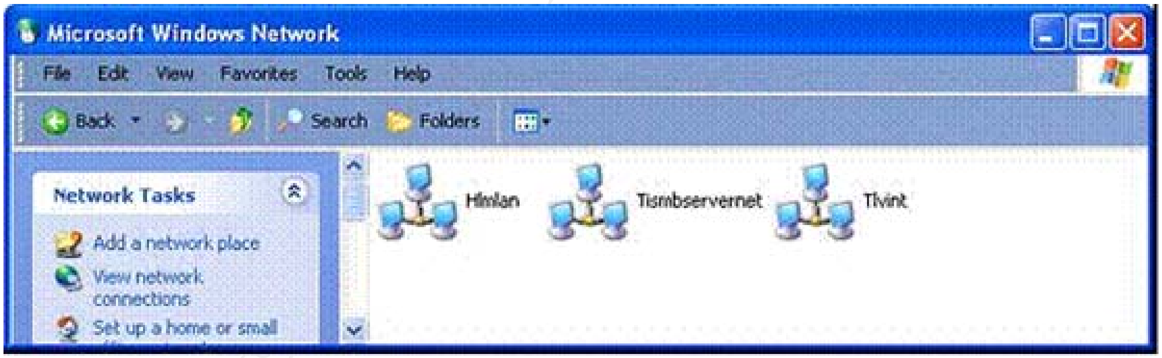
To approximate the kinds of networks that are typically encountered in a small business environment, the test network was configured with three separate Microsoft Networks on the same LAN depicted in **Figure 5.2.1** below:

- ➔ (Hlmlan) A Windows Workgroup network consisting of 5 PC's running various Microsoft OS's and one PC running RedHat Linux 8.0 with a SAMBA Client/Server configured on that system

- ➔ (Tlvint) A Windows Active Directory Forest managed by one PC running Microsoft Windows 2000 Advanced Server and one domain member computer running Windows XP Professional. The Forest and Domain are configured to operate in Windows 2000 mode.

- ➔ (Tismbservernet) A Windows Active Directory Forest managed by one PC running Microsoft Windows Small Business Server 2003 Premium Edition and one domain member computer running Windows XP Professional. The Forest and Domain are configured to operate in Windows 2003 mode.

With respect to the Microsoft Active Directory forests there is no cross-forest trust configured between the forests, Tlvint and Tismbservernet.



Microsoft Networks Comprising the Test
Figure 5.2.1

For test protocols 6-8, the Windows Server (either Server 2003 or SBS 2003) is also configured to support the following additional services besides Active Directory:

- ➔ Certificate Services for creation of machine & user digital certificates

- ➔ Internet Authentication Service (IAS) for providing RADIUS authentication on behalf of wireless supplicants and the AP's

- Domain Name Service (DNS) for providing Domain Name⇔IP address mapping services for the Domain

The motivation for testing with both a Windows 2000 Forest/Domain and a Windows 2003 Forest/Domain is twofold:

- to gain a sense of some of the differences between the Windows 2000 and Windows 2003 Active Directory, Certificate Services, and Internet Authentication Services

- To create a test framework for future testing of IAS Proxy Server Service, which service is a new capability that has been added to IAS as a part of the Windows Server 2003 family.

5.3 Test Network Architecture – Wireless Supplicants

As mentioned earlier in this paper one of the objectives of the test protocols is to get a sense of the degree of the ease of deployment of wireless security across a range of Microsoft operating systems. To that end a broad cross section of currently supported Microsoft operating systems was selected for testing including the following:

- Windows Millennium Edition
- Windows 2000 Professional
- Windows XP Professional
- Windows 2000 Advanced Server
- Windows Server 2003 Enterprise Edition
- Windows Small Business Server 2003 Premium Edition

In addition a system running Redhat Linux 8.0 Professional was configured with SAMBA in order to test it out in a mixed Microsoft/Linux environment including wireless access.

Most of the computer systems used in the test are actually IBM ThinkPad systems (570's, 570/E's, and an R32), in each case, configured with sufficient memory and disc capacity to support the testing requirements.

The 802.11 wireless client NIC cards were of 6 distinct types & manufacturers as shown in **Table 5.3.1** below. It should be noted that, despite the large number of NIC suppliers, many of them utilize the same underlying microchip technology which helps to assure the interoperability of these systems.

Manufacturer	Name/Model	802.11 Operating Modes Supported			Support for WPA?
		a	b	g	
Lucent	Orinoco Gold	--	✓	--	No
IBM	Integrated Wireless Adapter	--	✓	--	No
Microsoft	MN-520 Wireless Adapter	--	✓	--	No
Linksys	Wireless G Adapter		✓	✓	Yes
Netgear	WAG511 Wireless Adapter	✓	✓	✓	Yes
Proxim	Orinoco Gold 11 a/b/g Combo Card	✓	✓	✓	Yes

802.11 Client NIC Card Types
Table 5.3.1

It should also be noted that the Microsoft Windows server systems used in tests 6-8 respectively are configured for open authentication with WEP enabled to access the wireless Access Point and are therefore NOT subject to the 802.1x/EAP authentication process. In other words the wireless access of these servers is NOT actually a part of the test protocols of 6-8. The use of wireless access for these servers in tests 6-8 was simply for testing convenience.

The details of the wireless supplicant systems utilized in tests 2 and 4-8 are provided in **Table 5.3.2** below. This table identifies the PC hardware, operating software, and 802.11 client NIC utilized on that particular system. Note that hardware component 4 in the table, which is utilized as the network administration system does NOT have a wireless NIC since it is configured on the wired branch of the LAN.

Supplicant/Admin/Domain Controller PC Component Details								
Hardware Component Diagram #	**PC Hardware**			**PC Operating System**	**802.11 Supplicant Components**			**Comments**
	Manufacturer/Model	**Processor/Speed**	**RAM**		**Hardware**	**Radio Operating Modes**	**Supplicant Software**	
8	IBM Thinkpad 570E	Intel Pentium III 497 mhz	320 mb	Microsoft Windows xp	Linksys WPC54G Wireless Adapter	802.11b/g	Microsoft WZC w WPA Update	
9	IBM Thinkpad 570E	Intel Pentium III 497 mhz	320 mb	Microsoft Windows Small Business Server 2003	Netgear WAG511 Wireless Adapter	802.11 a/b/g	Nedtgear Client Utiliti	
10	IBM Thinkpad 570	Intel Pentium II 366 mhz	192 mb	Microsoft Windows xp	Lucent Orinoco Gold Wireless Adapter	802.11 b	Microsoft WZC w WPA Update	
11	IBM Thinkpad 570	Intel Pentium II 366 mhz	192 mb	Microsoft Windows 2000 Server	Proxim Orinoco 11 a/b/g Combo Card Gold World	802.11 a/b/g	Proxim Client Utility w WPA Update	
12	IBM Thinkpad 570E	Intel Pentium III 497 mhz	320 mb	Microsoft Windows Server 2003	Linksys WPC54G Wireless Adapter	802.11b/g	Linksys Client Utility	
13	IBM Thinkpad 570	Intel Pentium II 366 mhz	192 mb	Microsoft Windows 2000	Microsoft MN-520 Wireless Adapter	802.11 b	Microsoft Client Utility	Microsoft provides Automatic Update Service similar to Windows Update
14	IBM Thinkpad R32	Intel Pentium IV /3.02 ghz	??? Mb	Microsoft Windows xp	IBM Integrated Wirelss Adapter	802.11 b	Microsoft WZC w WPA Update	
15	IBM Thinkpad 570	Intel Pentium II 366 mhz	192 mb		Lucent Orinoco Gold Wireless Adapter	802.11 b	Redhat Linux Client Utility	Time did not permit the procurement/installation/testing of a Linux 802.1x/EAP Supplicant. A beta test version of a 802.11 WPA supplicant that is compatible with the newer Proxim a/b/g client card is available at www.sourceforge.net/projects/madwifi.
16	HP Pavillion 8720	Intel Pentium III 1 ghz	256 mb	Microsoft Windows Me	Lucent Orinoco Gold w PCI Adapter	802.11 b	Lucent/Proxim Client Utility w/o WPA	
4	Dell Dimension 8250	Intel Pentium IV 3.02 ghz	1 gb	Microsoft Windows xp	--NA--	--NA--	--NA--	This system is used for Network Administration

Test Network Components
Table 5.3.2

5.4 Test Network Architecture – Putting it all Together

As might be anticipated in a test environment this complex, a lot of effort went into simply putting all of the components together into an interoperable framework. The system running Microsoft Windows SBS2003 PE had to be built from a bare disk and because of the relatively small amount of RAM (320 MB) on the PC, the build took ~5 hours to load, configure, and test due to frequent page faulting. It should be noted that Microsoft does not recommend that SBS be deployed on a system with less than 500 mb of RAM. Nonetheless the software DOES install properly and runs somewhat slowly, again due to page faulting.

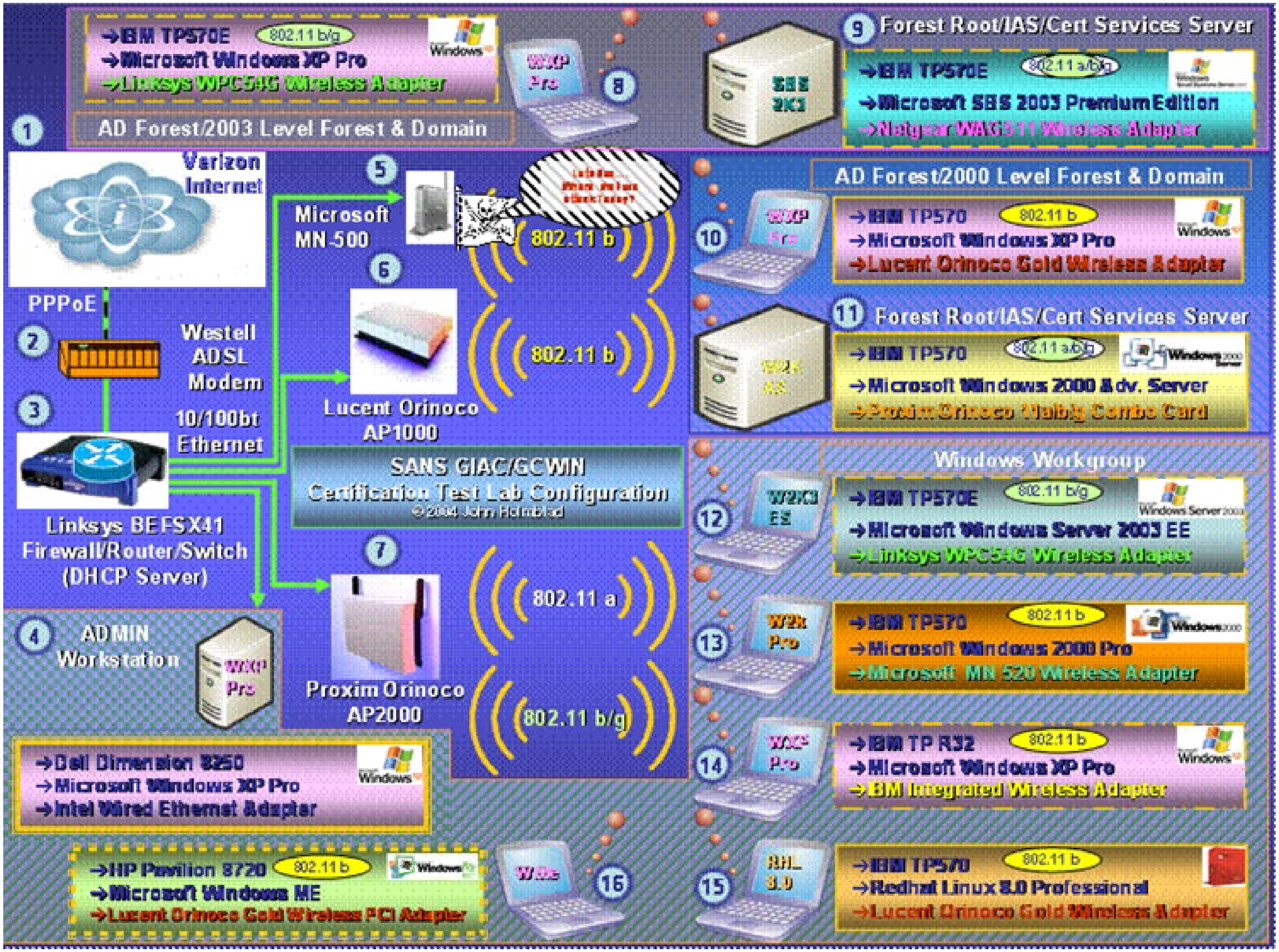
Because the Wireless Protected Access TM feature set has become available, in some cases, only as of early December of 2003, it was necessary to update the software/firmware/drivers on all of the systems that were specified to support WPA capabilities. This included products from Microsoft (WPA client), Proxim, Linksys, and Netgear. As of the writing of this paper the author has been unable to locate a version of Microsoft's WPA client that will install correctly on either Windows Server 2003 or Windows SBS 2003.

To provide additional operational flexibility in the author's test lab, two of the IBM ThinkPad systems were configured as dual boot systems as follows:

➔ Dual Boot System #1
  - IBM ThinkPad 570E
  - OS #1 - Microsoft Windows XP Professional
  - OS #2 - Microsoft Windows Server 2003 Enterprise Edition

➔ Dual Boot System #2
  - IBM ThinkPad 570E
  - OS #1 - Microsoft Windows 2000 Advanced Server
  - OS #2 – RedHat Linux 8.0 Professional
  -

Figure 5.4.1 provides a composite picture of the whole network and the most salient details. In that figure each of the 16 constituent components of the test network is labeled with a number from 1 to 16. Subsequent sections of the text, tables, and figures will make use of this numbering scheme where necessary in order to simplify the discussion. The next section discusses each test in turn and focuses on the equipment configuration that is relevant to each specific test protocol.


1
AD Forest/2003 Level Forest & Domain
→IBM TP570E
802.11 b/g
→Microsoft Windows XP Pro
→Linksys WPC54G Wireless Adapter
Windows
WXP Pro
8
9 Forest Root/IAS/Cert Services Server
SBS 2K3
→IBM TP570E
802.11 a/b/g
→Microsoft SBS 2003 Premium Edition
→Netgear WAG511 Wireless Adapter
Verizon Internet
PPPoE
2
Westell ADSL Modem
3
10/100bt Ethernet
Linksys BEFSX41 Firewall/Router/Switch (DHCP Server)
5
Microsoft MN-500
802.11 b
6
Lucent Orinoco AP1000
802.11 b
SANS GIAC/GCWIN Certification Test Lab Configuration
© 2004 John Holmblad
7
Proxim Orinoco AP2000
802.11 a
802.11 b/g
4
ADMIN Workstation
WXP Pro
→Dell Dimension 8250
→Microsoft Windows XP Pro
→Intel Wired Ethernet Adapter
Windows
→HP Pavilion 8720
802.11 b
→Microsoft Windows ME
→Lucent Orinoco Gold Wireless PCI Adapter
Windows
W Me
16
AD Forest/2000 Level Forest & Domain
10
WXP Pro
→IBM TP570
802.11 b
→Microsoft Windows XP Pro
→Lucent Orinoco Gold Wireless Adapter
Windows
11 Forest Root/IAS/Cert Services Server
W2K AS
→IBM TP570
802.11 a/b/g
→Microsoft Windows 2000 Adv. Server
→Proxim Orinoco 11a/b/g Combo Card
Windows 2000 Server
Windows Workgroup
12
W2K3 EE
→IBM TP570E
802.11 b/g
→Microsoft Windows Server 2003 EE
→Linksys WPC54G Wireless Adapter
Windows Server 2003
13
W2k Pro
→IBM TP570
802.11 b
→Microsoft Windows 2000 Pro
→Microsoft MN 520 Wireless Adapter
Windows 2000
14
WXP Pro
→IBM TP R32
802.11 b
→Microsoft Windows XP Pro
→IBM Integrated Wireless Adapter
Windows
15
RHL 8.0
→IBM TP570
802.11 b
→Redhat Linux 8.0 Professional
→Lucent Orinoco Gold Wireless Adapter

Test Network Components
Figure 5.4.1

6 Test Description and Test Results

This section describes each test protocol and the results, observations, and insights gained during the execution of the tests. The complete test protocols are summarized in **Table 6.1.1**
below, which indicates, for each test, which Network/Admin and wireless supplicant components were utilized in that particular test. In addition the table indicates whether or not each test was successful. Failed tests are indicated in the table with red shading. The core Network/Admin system components except for the Windows Server systems are highlighted in **blue** shading, the Wireless Supplicant components are indicated in **yellow** shading and the Windows Server Forest/Domain Controller components are highlighted in **green** shading. It should be noted that in tests 4 and 5 the Windows Server systems were also used as Wireless Supplicants to test out their support for 104 bit WEP and WPA-PSK respectively.

Securing Wireless LANS in Microsoft Networks using Wireless Protected Access ™ and Digital Certificates

802.11 Compatibility Testing in a Mixed Microsoft OS Environment

Test #	Test Name	Status	Result	Test Components																					
				Functional Components						Physical Components															
				802.11 Supplicant OS	802.11 Supplicant 802.11 HW	Supplicant 802.11 Operating mode	802.11 Access Point Authenticator	Rogue 802.11 Access Point	Radius Authentication Server	Network/Admin							Wireless Supplicant or Sever								
										1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	SSL implementation for HTTP Admin Interface	Tested	Success	--NA--	--NA--	--NA--	Proxim AP-2000	--NA--	--NA--			✓	✓			✓									
2	Rogue AP Detection	Tested	Failure	--NA--	--NA--	--NA--	Proxim AP-2000	Microsoft MN-5000 Wireless Base Station	--NA--	✓	✓	✓	✓	✓		✓									
3	MAC Address Filtering - Local	Tested	Success	Microsoft Windows XP Pro	Lucent Orinoco Gold	802.11b	Proxim AP-2000	--NA--	--NA--	✓	✓	✓	✓			✓			✓						
4	104 Bit WEP with Open Authentication	Tested	Success	Microsoft Windows XP Professional	IBM Integrated Wireless Adapter	802.11b	Lucent AP-1000	--NA--	--NA--	✓	✓	✓	✓		✓								✓		
		Tested	Success	Microsoft Windows XP Professional	Lucent Orinoco Gold Wireless Adapter	802.11b	Lucent AP-1000	--NA--	--NA--	✓	✓	✓	✓		✓				✓						
		Tested	Success	Microsoft Windows 2000 Professional	Microsoft MS 520 Wireless Adapter	802.11b	Lucent AP-1000	--NA--	--NA--	✓	✓	✓	✓		✓							✓			
		Tested	Success	Microsoft Windows Me	Lucent Orinoco Gold Wireless Adapter	802.11b	Lucent AP-1000	--NA--	--NA--	✓	✓	✓	✓		✓										✓
		Tested	Success	Microsoft Windows 2000 Adv Server	Proxim Orinoco 11 a/b/g Como Card	802.11b	Lucent AP-1000	--NA--	--NA--	✓	✓	✓	✓		✓					✓					
		Tested	Success	Microsoft Windows Server 2003 Enterprise Edition	Linksys WPC54G Wireless Adapter	802.11b	Lucent AP-1000	--NA--	--NA--	✓	✓	✓	✓		✓						✓				
		Tested	Success	Microsoft Small Business Server 2003 Premium Edition	IBM Integrated Wireless Adapter	802.11b	Lucent AP-1000	--NA--	--NA--	✓	✓	✓	✓		✓			✓							
		Tested	Success	Redhut Linux 8.0 Professional	Lucent Orinoco Gold Wireless Adapter	802.11b	Lucent AP-1000	--NA--	--NA--	✓	✓	✓	✓		✓									✓	
5	WPA with Pre-Shared Key (WPA-PSK)	Tested	Failure	Microsoft Small Business Server 2003 Premium Edition	Netgear WAG511	802.11a	Proxim AP-2000	--NA--	--NA--	✓	✓	✓	✓			✓		✓							
		Tested	Success	Microsoft Windows 2000 Adv Server	Proxim Orinoco 11 a/b/g Como Card	802.11b/g	Proxim AP-2000	--NA--	--NA--	✓	✓	✓	✓			✓				✓					
		Tested	Success	Microsoft Windows XP Professional	Linksys WPC54G Wireless Adapter	802.11b/g	Proxim AP-2000	--NA--	--NA--	✓	✓	✓	✓			✓	✓								
6	WPA with EAP TLS	Tested	Success	Microsoft Windows XP Professonal	Linksys WPC54G Wireless Adapter	802.11g	Proxim AP-2000	--NA--	IAS on Microsoft SBS Server 2003	✓	✓	✓	✓		✓	✓	✓	✓							
7	WPA with PEAP MS-CHAP V2	Tested	Success	Microsoft Windows XP Professional	Proxim Orinoco 11 a/b/g Como Card	802.11g	Proxim AP-2000	--NA--	IAS on Microsoft Windows 2000 Advanced Server	✓	✓	✓	✓		✓	✓	✓			✓					
8	WEP with PEAP MS-CHAP V2	Tested	Success	Microsoft Windows XP Professional	Lucent Orinoco Gold Wireless Adapter	802.11a	Proxim AP-2000	--NA--	IAS on Microsoft Windows 2000 Advanced Server	✓	✓	✓	✓		✓	✓			✓	✓					

Test Protocols
Table 6.1.1

Sections 6.1-6.8 below provide the details of each test and an explanation of the known or suspected cause of any test failures.

Tests 6, 7, and 8 of the test protocol require the use of a RADIUS authentication server and Digital Certificates and the tests are based on the use of 802.1X authentication. The first of these tests, test 6, uses EAP-TLS along with the WPA/TKIP cipher. EAP-TLS uses Digital Certificates for authentication of both the supplicant and the authentication server to one another. The Authentication Server in this test is Microsoft Small Business Server 2003 Premium Edition.

Test 7 uses PEAP-MS-CHAP V2 which, although it is still a draft ISOC/IETF standard, has already been implemented by Microsoft in their operating systems. With this EAP method, the identity of the Supplicant is protected from eavesdropping, In addition, although the authentication server authenticates to the supplicant by means of a digital certificate, the supplicant uses a password and NOT a Digital Certificate to authenticate to the authentication server. This method obviates the requirement to have user/computer digital certificates installed on the supplicant systems. Test 8 also uses PEAP-MS-CHAP V2 except in test 8 the Authentication Server is Windows 2000 Advanced Server.

MS CHAP V2 is a mutual authentication process based on a irreversible encryption method (one way hash) of a shared secret and in concept it is similar to mutual authentication based on the use of digital certificates. MS-CHAP V2 improves on the earlier MS-CHAP standard that was utilized in earlier Microsoft operating systems in a number of ways as summarized in **Table 6.1.2**
below.

MS-CHAP version 1 issue	MS-CHAP version 2 solution
LAN Manager encoding of the response used for backward compatibility with older Microsoft remote access clients is cryptographically weak.	MS-CHAP v2 no longer allows LAN Manager encoded responses.
LAN Manager encoding of password changes is cryptographically weak.	MS-CHAP v2 no longer allows LAN Manager encoded password changes.
Only one-way authentication is possible. The remote access client cannot verify that it is dialing in to its organization's remote access server or a masquerading remote access server.	MS-CHAP v2 provides two-way authentication, also known as mutual authentication. The remote access client receives verification that the remote access server that it is dialing in to has access to the user's password.
With 40-bit encryption, the cryptographic key is based on the user's password. Each time the user connects with the same password, the same cryptographic key is generated.	With MS-CHAP v2, the cryptographic key is always based on the user's password and an arbitrary challenge string. Each time the user connects with the same password, a different cryptographic key is used.
A single cryptographic key is used for data sent in both directions on the connection.	With MS-CHAP v2, separate cryptographic keys are generated for transmitted and received data.

MS-CHAP V2 vs. MS-CHAP

Table 6.1.2

Table 6.1.3
below summarizes, for each test, the authentication server operating system, the type of authentication credential that is used by each party, and the data encryption cipher that is used once the 802.1X/EAP process is completed and the connection goes into the open data transfer state.

Test #	EAP Method	Credential used for the specified direction of authentication		Cipher for Data Encryption	Authentication Server OS
		Supplicant authenticating to Authentication Server	Authentication Server authenticating to Supplicant		
6	EAP-TLS	Digital Certificate	Digital Certificate	WPA/TKIP	Microsoft SBS PE
7	PEAP-MS CHAP V.2	Password	Digital Certificate	WPA/TKIP	Microsoft SBS PE
8	EAP-TLS	Digital Certificate	Digital Certificate	WPA/TKIP	Microsoft Windows 2000 Advanced Server

Credential Differences between EAP Methods in Tests 6-8
Table 6.1.3

For tests 6-8, on the authentication server the following Microsoft server functions are utilized:

- Active Directory Service
- Domain Name Service (DNS)
- Certificate Services
- Internet Authentication Service (IAS)

On Windows XP Professional for tests 6 - 8 the following services are utilized:

- Windows WPA Client
- Domain Logon Service

For tests 6-8 configuration guidance was derived from two Microsoft documents[30,31] from the Microsoft www site as well as the Microsoft Press text, “Deploying Secure 802.11 Wireless Networks with Microsoft Windows”[32]. In addition, guidance for the configuration of the Windows 2000 Server to work with 802.1x and the WEP cipher was obtained from the text “Building Secure Wireless Networks with 802.11”[33].

The network connections to the server computers in tests 6-8 happen to be wireless connections although these connections are not themselves authenticated/authorized using the EAP methods under test.

6.1 Test 1 – SSL Implementation for HTTP Admin Interface

6.1.1 Test 1 – Configuration Details

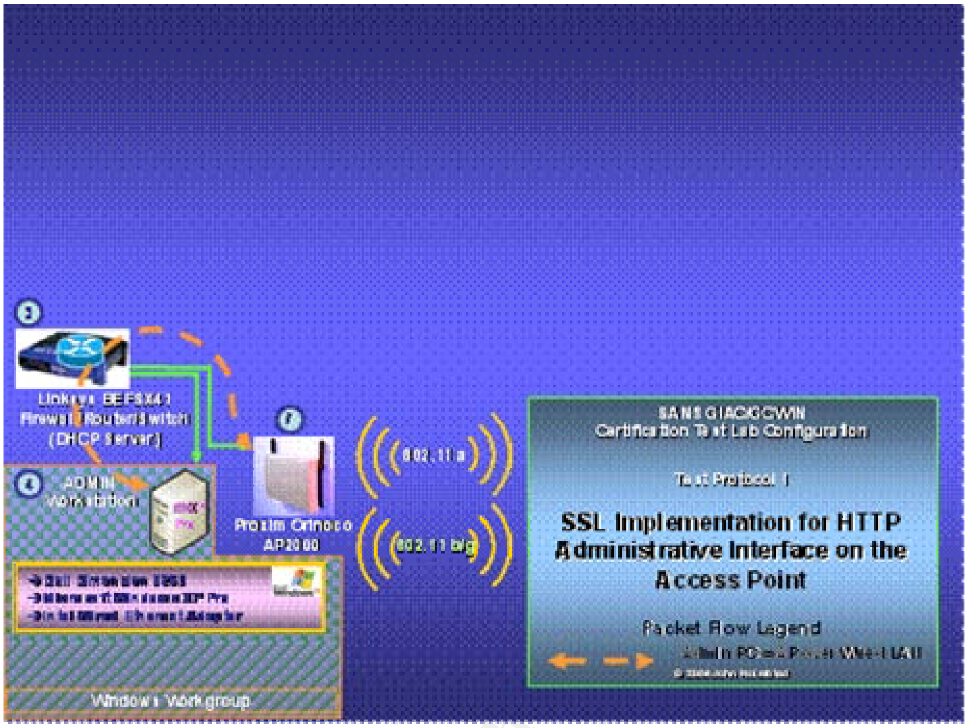
The Proxim AP-2000 Access Point supports three forms of access to administer the AP-2000 as follows:

- HTTP Protocol Access via a Browser
- Command Line Interface (CLI) via the Telnet protocol
- SNMP access via the SNMP protocol

Section 13.1 of this paper entitled **Table 12.1**
provide a display of typical screen shots for this HTTP/HTML based Graphical User Interface (GUI). For small networks of one or two AP's this is the most convenient way to manage the device.

Furthermore. with its latest release of the firmware for this product, Proxim has implemented the option to enable Secure Sockets Layer (SSL)[34] protocol on the HTTP interface. The benefit of using this feature is to protect the administrative interactions between the AP and the controlling system with its HTTP Browser from unwanted surveillance/eavesdropping. Many suppliers of telecommunications equipment now ship their products with similar HTTP based access to the equipment administration functions of such equipment but often times these interfaces are not at all secured.

The first test was to enable and assess the performance impact of using Secure Sockets Layer (SSL) for the administrative interface to the Proxim Orinoco AP-2000 Access Point. The configuration for this test is shown in **Figure 6.1.1.1**. With SSL enabled the packet flows shown in the figure as shaded in orange are protected using SSL based encryption.



SANS GIAC/GCWIN
Certification Test Lab Configuration

Test Protocol 1

SSL Implementation for HTTP Administrative Interface on the Access Point

Packet Flow Legend

Test 1 Configuration - Implementation for HTTP Admin Interface Figure 6.1.1.1

6.1.2 Test 1 – Results

The main impact of implementing SSL encryption is that it takes noticeably longer (~2x as long as in the case where SSL is NOT enabled) to upload pages from the AP. This is because the AP does not have any hardware cryptographic acceleration and so the encryption of each HTML page has to be done in software. Nonetheless the implementation of this feature is straightforward in the Proxim product line and it is recommended by this author to always have it enabled. The Proxim AP-2000 is delivered with a pre-configured http web server digital certificate installed in the AP-2000 firmware. For the purpose of this test, when the Internet Explorer 6.0 browser provided the warning concerning a certificate without a trusted root certificate it was necessary to simply click “yes’ to install the certificate and continue the test. Proxim provides a means to download to the AP-2000 a server certificate of the user’s choosing during the installation of the AP-2000. For operational use of the AP-2000 this author recommends that the user either generate a certificate using their own trusted certificate server or, alternatively, obtain a certificate from a provider of certificate services and to then install this certificate on the AP prior to putting the AP into production use.

6.2 Test 2 – Rogue Access Point Detection

As mentioned in section 3, **Attacks on Wireless Networks**
, Wireless LANS are vulnerable to impersonation attacks and these attacks can come from both so called "rogue" clients and "rogue" Access Points. To combat this threat, several companies including, Air Defense (http://www.airdefense.net/), and AirMagnet (http://www.airmagnet.com/) have developed hardware/software intrusion detection technologies to ferret out such rogue 802.11 devices. Of course this same kind of intrusion detection technology can potentially be implemented within an access point itself and Proxim has done so with their Proxim Orinoco AP-2000 product line. While purpose built products such as those of Air Defense and AirMagnet will generally provide a more feature rich set of capabilities than a built in solution on a standard Access Point such as that of Proxim, it is still worthwhile to have this feature built into an Access Point.

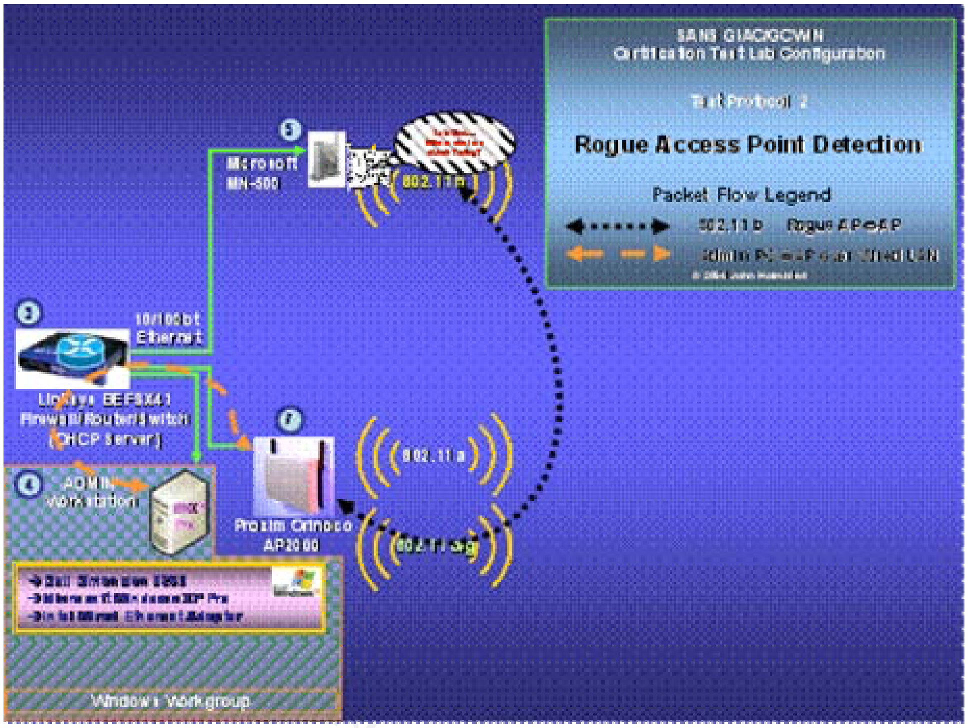
The Proxim capability works by allowing the network administrator via one of the three aforementioned methods to configure a time interval (minimum interval is 15 minutes) in the Proxim AP-2000 between full scans by the AP of the frequency band/operating mode in which the AP is operating (i.e. 802.11 a, b, or g or both in the case of a dual radio AP such as the AP-2000 used for this test) for other AP's within radio proximity of the scanning AP. **Figure 13.1.1**
provides a screen shot of the configuration TAB for this feature which Proxim refers to as RAD (Rogue AP Detection).

The scan is performed in the background and interleaved with normal traffic between the AP and its associated clients so as not to disrupt the operation of those clients or cause disassociation with the AP. At the end of each scan the scan process generates and SNMP trap to a previously configured IP address on the LAN to report any other Access Points that are discovered in the same band along with their SSID's. Now it is always possible especially in an enterprise that has multiple Access Points deployed, or even in the case of a small business in a building that has numerous other access points operating in the same frequency band/operating mode, that this rogue AP detection process will pick up a signal from such system even though they are not actually malicious systems. Thus it is necessary for a filter to be implemented at the receiving end of such SNMP traps to filter out such false positives.

The second test, in summary, is to enable the rogue AP detection on the test Proxim Orinoco AP-2000 and observe whether or not the AP was able to detect the other AP's operating in the same frequency band/operating mode.

6.2.1 Test 2 – Configuration Details

The configuration for test 2 is shown in **Figure 6.2.1.1**, and includes a Microsoft MN-500 Access Point (hardware component 5) which operates in 802.11 b mode and serves as a rogue access point. In lieu of installing and configuring Rogue AP detection software on the network ADMIN workstation (hardware component 4), Ethereal software was installed on that workstation and configured to filter on incoming SNMP packets in order to detect the receipt of traps from the AP-2000 that designate the presence of potential rogue AP's.



Test 2 Configuration - Rogue Access Point Detection
Figure 6.2.1.1

6.2.2 Test 2 – Results

Once the configuration for this test was set up, the Proxim Orinoco-2000 AP began sending SNMP traps at the configured interval of 15 minutes as shown by the Ethereal traces at the Network Admin workstation. However the AP did NOT report any other access points as having been detected despite the fact that there were two other 802.11b AP's (the aforementioned rogue AP + the Lucent Orinoco AP-1000 AP) within radio range. This problem has been reported to Proxim and they are investigating it as this paper goes to press. The author surmises that the problem may arise because the AP has been configured to scan for rogue AP's for both the A radio (operating in 802.11 a mode) and the B radio (operating in 802.11 b/g mode).

6.3 Test 3 – MAC Access Control on the Access Point

The Proxim Orinoco AP-2000 also supports the capability to block access to the wired network through the AP on the basis of the MAC address of the client/supplicant system. This feature is enabled on an AP-wide basis, that is, if the system is configured for two radios, and the MAC Access Control feature is enabled, then the blocking will be performed on frames received on both radios. **Figure 13.1.4** provides a screenshot of the feature tab for this capability.

Furthermore this feature can be implemented in one of two modes:

- Passthru (allow access ONLY for devices whose MAC address is on the list)
- Block (block access ONLY for devices whose MAC address is on the list)

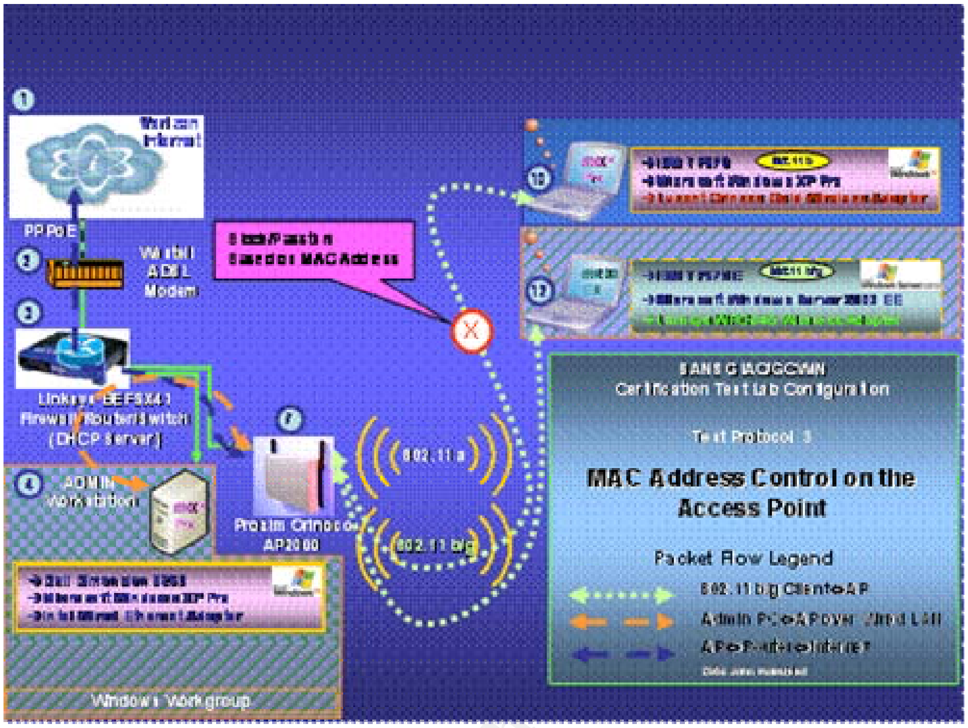
It should be noted that the Proxim-AP-2000 also supports a more sophisticated form of filtering which was not tested as a part of this test and which supports filtering based on four different criteria:

- Filtering based on Ethernet Protocol Number
- Filtering based on Ethernet MAC Address
- Filtering based on packet protocol (IP/ARP, IPX/RIP.IPX/SAP,IPX/LSP, IP/Broadcast, IP/Multicast)
- Filtering based on TCP/UPD Port number

Figure 13.1.5 provides a screen shot for the four tabs associated with this set of filtering capabilities. The second of these four types of filtering provides a richer form of filtering than the basic MAC Access control which is the subject of this test.

6.3.1 Test 3 – Configuration Details

To perform this test, the AP-2000 MAC Access Control list was configured with the MAC address of Hardware component 10 (Thinkpad570/Windows XP Pro/Lucent Orinoco Gold Client Card). The test configuration is shown in **Figure 6.3.1.1**
below. In addition Hardware component 12 was used as the control system in this test, that is, its MAC address was NOT added to the MAC access control list. The test then proceeded in two steps, first to test the "Passthru" mode and second to test the "Block" mode of this feature. Activation of this feature, in each case requires a reboot of the AP which takes approximately 15-20 seconds.


1
Verizon Internet
PPPoE
2
Westell ADSL Modem
3
Linksys BEFSX41 Firewall/Router/Switch (DHCP Server)
4
ADMIN Workstation
7
Proxim Orinoco AP2000
802.11a
802.11b/g
Block/Passthru based on MAC Address
10
12
Windows Workgroup
SANS GIAC/GCWIN Certification Test Lab Configuration
Test Protocol 3
MAC Address Control on the Access Point
Packet Flow Legend
802.11b/g Client⇔AP
Admin PC⇔AP over Wired LAN
AP⇔Router⇔Internet

Test 3 Configuration – MAC Address Control on the Access Point
Figure 6.3.1.1

6.3.2 Test 3 – Results

When the test was performed with the "Block" mode enabled, the supplicant (#10 in the figure) whose MAC address was configured in the Access Control Table was in fact blocked from access to the wired network, while the second supplicant (#12 in the figure) was still able to reach the wired LAN. Interestingly, the supplicant nonetheless remained associated with the AP (since it was in fact authenticated via open authentication) but the supplicant was unable to reach the DHCP service to obtain an IP address which is configured on the wired side of the LAN. Furthermore, attempts to browse the www were unsuccessful.

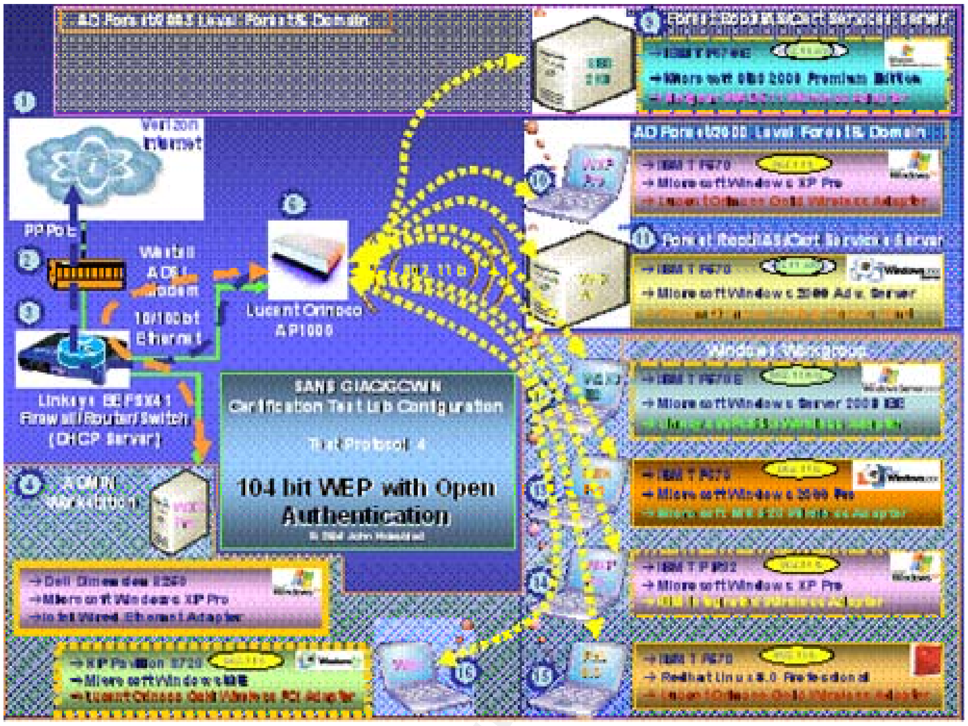
When the test was performed with the "Passthru" mode enabled, as expected, the opposite result was achieved, that is the supplicant (#10 in the figure) whose MAC address was configured in the Access Control Table was able to access the wired segment of the LAN while the supplicant (#12 in the figure) was unable to access the wired segment of the LAN.

6.4 Test 4 – 104 Bit WEP with Open Authentication

The purpose of this test was to verify that the full range of supplicant operating systems Microsoft + Linux) and supplicant wireless NIC cards that are specified in the test protocol can operate properly with a wireless access point that is configured with WEP enabled. The stronger mode of the WEP encryption standard was utilized which is based on a 104 bit WEP cryptographic key that is supplemented by a 24 bit Initialization Vector (IV) which is automatically generated for each frame that is transmitted. For this reason some suppliers refer to this mode as 128 bit encryption.

6.4.1 Test 4 – Configuration Details

As indicated in **Figure 6.4.1.1**
 a total of 9 different supplicant systems were utilized for this test along with all 6 of the supplicant wireless NIC adapter types identified in **Table 5.3.1**. The access point used for this test is the Lucent Orinoco AP-1000, although any of the three AP's could have been used. The WEP keys were configured manually by going to each supplicant in turn, and configuring the 13 hexadecimal digit key into the Microsoft Windows Wireless Networks Tab in the case of the Microsoft based systems and into the Wireless Settings Tab of the Linux Wireless Device Configuration window on the RedHat Linux 8.0 server system.


Verizon Internet
PPPoE
Westell ADSL Modem
10/100bt Ethernet
Lucent Orinoco AP1000
802.11b
Linksys BEFSX41 Firewall/Router/Switch (DHCP Server)
ADMIN WORKSTATION
AD Forest 2000 Level Forest & Domain
→ IBM T P70
→ Microsoft Windows XP Pro
→ Microsoft Windows 2000 Adv Server
Windows Workgroup
→ Microsoft Windows Server 2003 EE
→ Microsoft Windows 2000 Pro
→ Dell Dimension
→ Microsoft Windows XP Pro
→ Microsoft Windows ME
→ Redhat Linux 8.0 Professional
SANS GIAC/GCWIN
Certification Test Lab Configuration
Test Protocol 4
104 bit WEP with Open Authentication

Test 4 Configuration – 104 Bit WEP with Open Authentication
Figure 6.4.1.1

6.4.2 Test 4 – Results

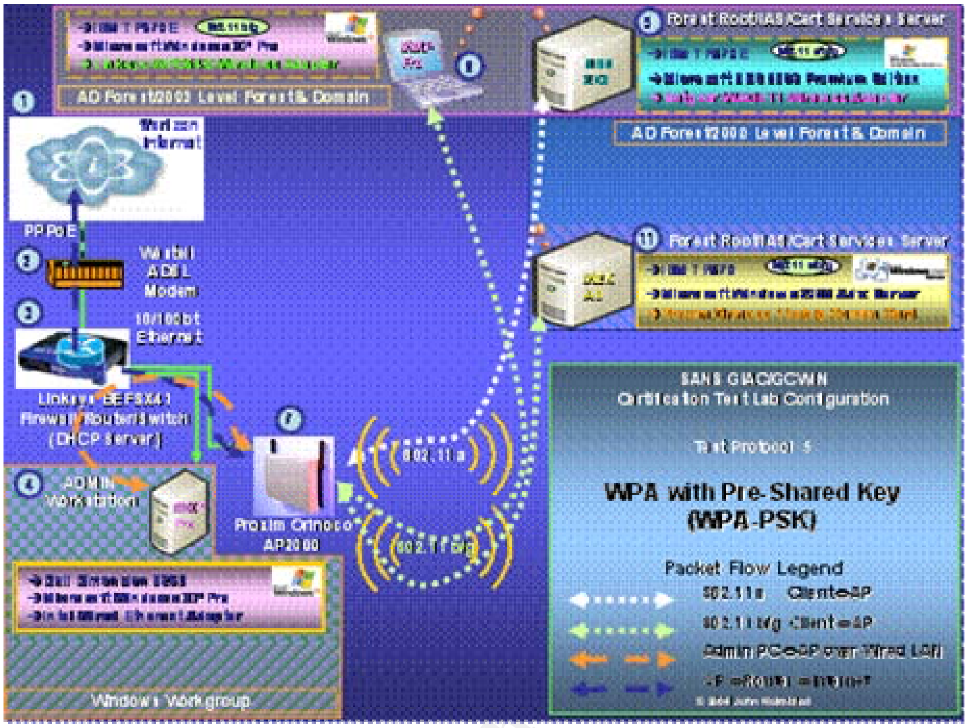
This test completed successfully without difficulty after configuring each supplicant with the WEP key. It took approximately 5 minutes per system to perform the key installation. Although it was not a part of the test protocol, it so happens that the author's lab network has several other wireless supplicants from Linksys (a wireless Print Server and a Wireless Ethernet bridge) which were also successfully configured to support 104 bit WEP.

6.5 Test 5 – WPA with Pre-shared Key Authentication

Test 5 is the first test in the test suite that utilizes Wireless Protected Access (WPA). The purpose of test 5 is to verify the operation of WPA when utilized in Pre-Shared Key mode. The Pre-Shared Key mode was introduced into the WPA standard[35] to facilitate supplicant⇔access point authentication in environments (e.g. small office/home office or SOHO) that did not have the necessary computing/software resources to support a RADIUS based authentication method. The WPA standard acknowledges that, of course, this option is somewhat less secure because each supplicant is configured with the same pre-shared key. However it should be emphasized that even when WPA is used in pre-shared key mode, the use of WPA will ensure that a strong cryptographic method (either TKIP or AES) and NOT the original WEP cryptographic method is utilized for supplication⇔access point communications for that particular supplicant. The primary risk of this pre-shared key method is if the pre-shared key gets compromised by some other means that via a cryptanalytic attack.

6.5.1 Test 5 – Configuration Details

The configuration for test 5 is shown in **Figure 6.5.1.1**
below. The test was conducted using three supplicants Two of the supplicants, the system with Microsoft Windows XP Professional installed and the system with Microsoft Windows 2000 Advanced Server installed (#8 and 11 in the figure) were configured to operate in the 802.11b frequency band/mode. The third supplicant, the system with Microsoft SBS 2003 Premium Edition system installed (#9 in the figure) was configured to operate in the 802.11 a frequency band/mode. The access point utilized for this test is the Proxim Orinoco AP-2000. Splitting the systems this way provided a convenient method to test WPA-PSK for both the frequency bands/modes that are supported by the Proxim product.


AD Forest2003 Level Forest & Domain
1
Verizon Internet
PPPoE
2
Westell ADSL Modem
3
10/100bit Ethernet
Linksys BEFSX41 Firewall/Router/switch (DHCP Server)
4
ADMIN Workstation
Windows Workgroup
7
Proxim Orinoco AP2000
802.11a
802.11b/g
8
9
Forest Root/IAS/Cert Services Server
AD Forest2000 Level Forest & Domain
11
Forest Root/IAS/Cert Services Server
SANS GIAC/GCWIN
Certification Test Lab Configuration
Test Protocol 5
WPA with Pre-Shared Key (WPA-PSK)
Packet Flow Legend
802.11a Client⇔AP
802.11b/g Client⇔AP
Admin PC⇔AP over Wired LAN

Test 5 Configuration – WPA with Pre-Shared Key (WPA-PSK)
Figure 6.5.1.1

6.5.2 Test 5 – Results

To simplify the key installation procedure, this test took advantage of the option within the WPA-preshared key mode of operation to key in a passphrase instead of a 64 hexadecimal digit key directly.

The pre-shared key using the passphrase option was first installed on the Proxim AP-2000 using the HTTP admin interface.

Once the AP was configured with the preshared key but before the supplicants were so configured, testing confirmed the supplicant systems could NOT associate with the AP precisely because they did not have the necessary preshared crypto key.

The next step was to configure the pre-shared key on the supplicant systems (#8, 9, and 11 in the Figure) The pre-shared key was configured on the Windows XP Professional system by means of the Microsoft WPA client and the same key was configured on the Windows 2000 Advanced Server system by means of the Proxim a/b/g client utility. As of the writing of this paper, Microsoft does not have a WPA client that can be installed on the Windows 2000 Server or Professional product lines, or, for that matter, on the Windows Server 2003 family (see comment in the next paragraph).

The attempt to install a pre-shared key on the system with Microsoft Small Business Server PE installed failed because a) the Microsoft WPA client will not install on the Microsoft Server 2003 family of products, and b) the Netgear client utility installs correctly on the SBS 2003 server but it DOES NOT allow the pre-shared WPA key to be configured.

On the aforementioned systems where the pre-shared key was successfully installed, the supplicant systems were subsequently able to associate with the AP and to obtain access to the wired portion of the LAN and the Internet.

6.6 Test 6 – WPA with EAP-TLS Authentication

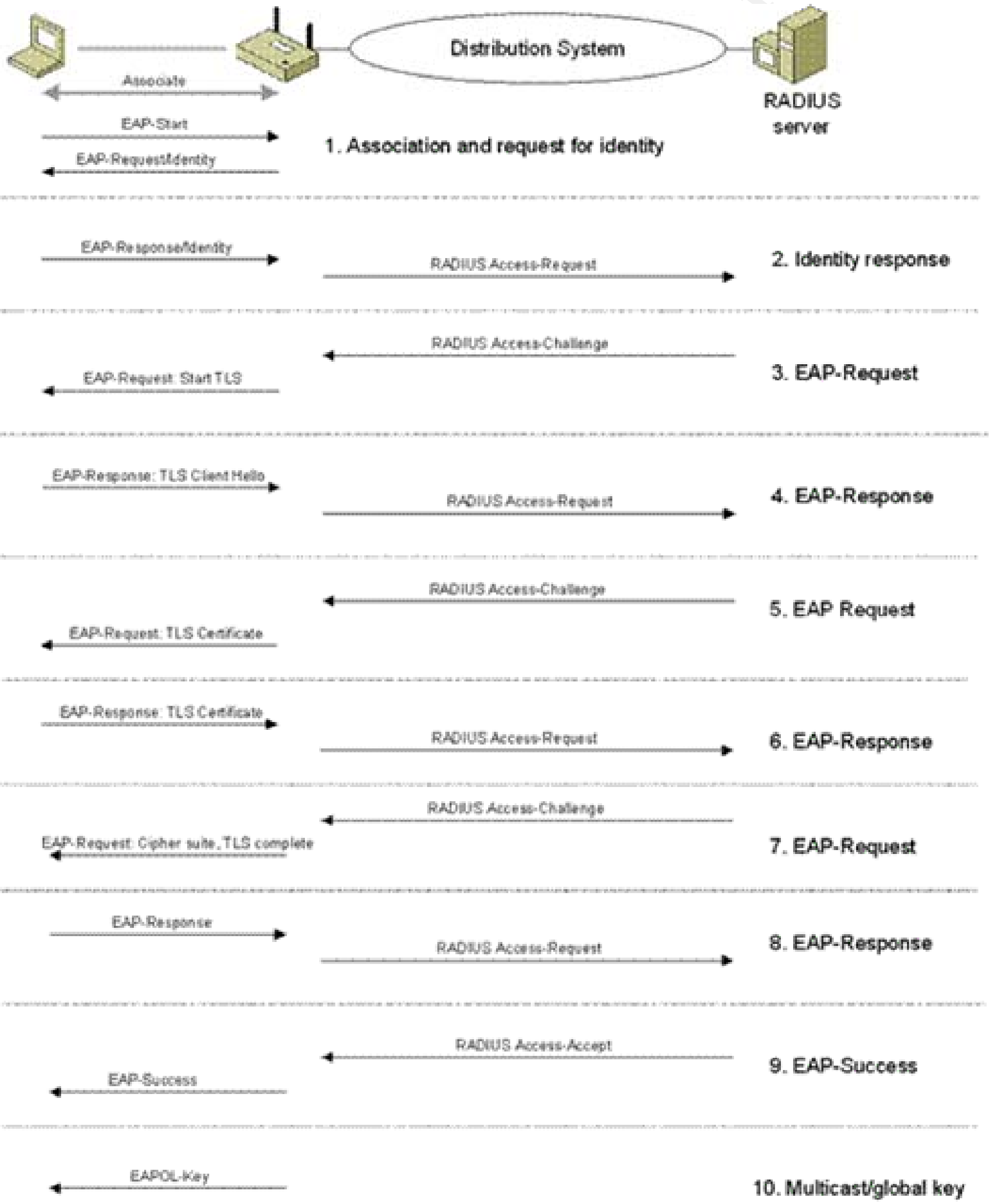
In this test the Microsoft server components are configured and utilized to verify the correct operation of EAP-TLS. Setting up this test and tests 7, and 8, and getting them to work properly took the overwhelming degree of effort among all of the tests because there were so many "moving parts" with which to deal. A number of systems and services, had to be installed and configured In addition to the 802.11 equipment from Proxim and Linksys, including the following Microsoft Windows operating system components:

➔ Small Business Server 2003 Premium Edition
  - Active Directory
  - Integrated Authentication Service (IAS)
  - Certificate Authority\Certificate Services\Certificate Web Enrollment
  - Internet Information Server (IIS)
  - Network Monitor (similar to Ethereal for packet/frame tracing)
  - Event Logging

For this test an Active Directory domain, "tismbservernet.local", was created with Windows SBS 2003 Premium Edition as the forest root. The test supplicant computer was named "eaptlsclient".

Operating system event logging was utilized for tracking IAS success/failure events and security event logging was utilized for tracking of logon/logoff success/failure events. The Network monitor was used to perform packet tracing of RADIUS message flow between the Proxim AP-2000 and the Microsoft SBS 2003 system. IIS was required in order to enroll/install a user certificate on the Windows XP Pro supplicant system using the Certificate Authority HTTP based service. Because it was not possible to install the Windows XP computer certificate using this method, the certificate was first created on the Windows SBS Certificate Authority and then exported (with private key material) to the supplicant PC. It turns out that the certificate web services capability does NOT provide a simple way to request and receive a computer certificate, even with the advanced certificate request option.

As mentioned previously in this paper, Microsoft has extensive documentation on deploying wireless technology and the Microsoft white paper, "Windows XP Wireless Deployment Technology and Components Overview"[36] provides an excellent review of the technologies that were used in this tests as well as in tests 7 and 8 and therefore will not be repeated here. A diagram of the EAP-TLS message exchange taken from that white paper is provided in **Figure 6.6.1**
below:

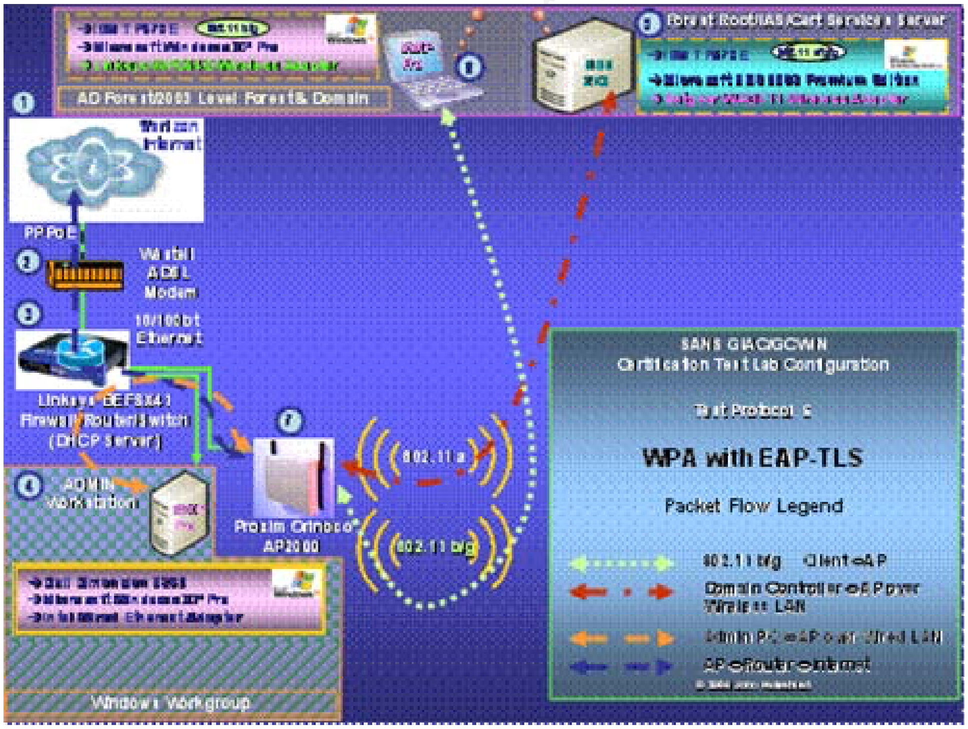


EAP-TLS and IEEE 802.1X Authentication
Figure 6.6.1

This EAP method requires installation of a computer certificate AND a user certificate on the supplicant system and both of these certificates must be associated with both computer and user objects that are members of the AD domain to which the Internet Authentication Server (IAS) is registered. This technique allows AD Kerberos to be utilized for both computer and user authentication in the same way that Kerberos authentication is used in a wired network environment,

6.6.1 Test 6 – Configuration Details

The components used in this test are shown in **Figure 6.6.1.1**
below. The wireless settings on the supplicant computer Windows XP system were set to allow the OS to authenticate as the computer when an AD domain user account is not active on the computer. This configuration option is shown in the Windows XP Wireless Zero Configuration screenshot in **Figure 13.5.10**.



Test 6 Configuration – WPA with EAP-TLS
Figure 6.6.1.1

6.6.2 Test 6 – Results

After a significant amount of configuration debugging of certificate services, IAS, and the Linksys wireless client, the test was successfully carried out in accordance with the above diagram. It turned out that if the Linksys client utility software is installed on the computer, then it configures itself to run automatically on startup and this interferes with the correct operation of the card when the Windows WPA client functionality is also being used. This was solved by using msconfig to remove the Linksys client utility from the system startup sequence.

The screen shots of the system and security log events that record the successful EAP-TLS authentication of component number 8 in the figure above are provided in **Figure 13.2.1**
 to **Figure 13.2.5** of section **13.2** . The first four figures are from the security event log and pertain to the authentication and authorization process for first the computer account, "tismbservernet.local/eaptlsclient", and then the user account, "john a. holmblad', The last figure is from the system event log and shows the successful IAS authentication event log record for the just completed authentication process.

The testing also confirmed that when the AD domain user is logged off of the Windows XP system, the Linksys NIC maintained its association with the Proxim AP-2000 and its security association with the Windows AD domain. Thus it was possible, from another computer on the same LAN, to browse file shares that had been configured on the subject Windows XP system. In addition, when the Windows XP system was rebooted but prior to any user logon, it was possible to confirm that the Linksys NIC formed an association with the Proxim AP-2000 and that the EAP-TLS protocol successfully authenticated and authorized the subject computer to access the wired LAN via the wireless interface & AP.

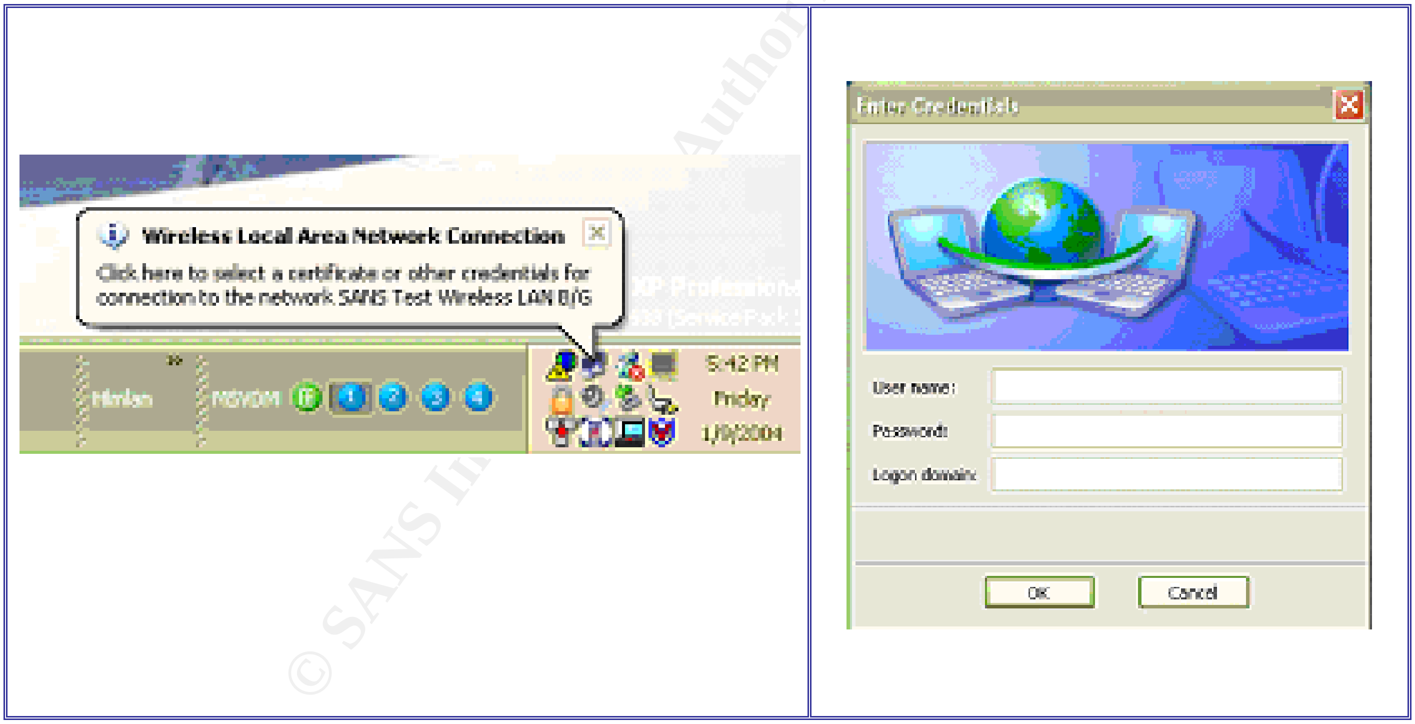
6.7 Test 7 – WPA with PEAP MS-CHAP V.2 Authentication

The second EAP method that was tested as a part of the test protocol is PEAP MS-CHAP V.2. This is a protected EAP method, wherein the channel over which the supplicant authentication information is sent to the authentication server is accomplished by means of an encrypted channel which is created after the authentication server authenticates to the supplicant but BEFORE the supplicant authenticates to the authentication server. This EAP method has the benefit that the supplicant computer does not have to have a user digital certificate installed on that computer. The PEAP protocol standard is currently in draft form within the ISOC/IETF[37].

In the Windows operating system environment it s also possible to use a protected EAP (PEAP) method to protect EAP-TLS authentication, however, this operation of PEAP was not tested as a part of the test protocol. Furthermore it is possible to combine EAP-

TLS and PEAP-MS CHAP V.2 by using EAP-TLS to authenticate the computer BEFORE the user logs on to the AD domain and then using PEAP-MS-CHAP V.2 upon user logon. The benefit of this alternative is the same as mentioned in the explanation of test 6 above, that is, the computer can then be associated with and authenticated to the Windows AD domain controller even when there is no user logged on. Of course this alternative requires that the computer digital certificate is present on the supplicant for this mixed alternative to work.

Furthermore the Windows XP wireless client provides the option under the PEAP authentication method to configure Windows XP to prompt the user for his/her credentials instead of automatically using the user's Windows XP login credentials for the PEAP authentication. A screen shot of this credential request screen is provided below in **Figure 6.7.1**. This is a useful feature because it means that a computer using Microsoft Windows XP can be configured to associate with and authenticate to an 802.11 network protected by an Active Directory integrated IAS server even though the computer itself is NOT a member of the domain of the user (or of any domain for that matter) who is being authenticated.



Wireless Local Area Network Connection

Click here to select a certificate or other credentials for connection to the network SANS Test Wireless LAN B/G

PEAP Credentials Prompt from Windows 802.11 WPA Client
Figure 6.7.1

In this test the following Microsoft server components are configured and utilized to verify the correct operation of PEAP MS-CHAP V.2.

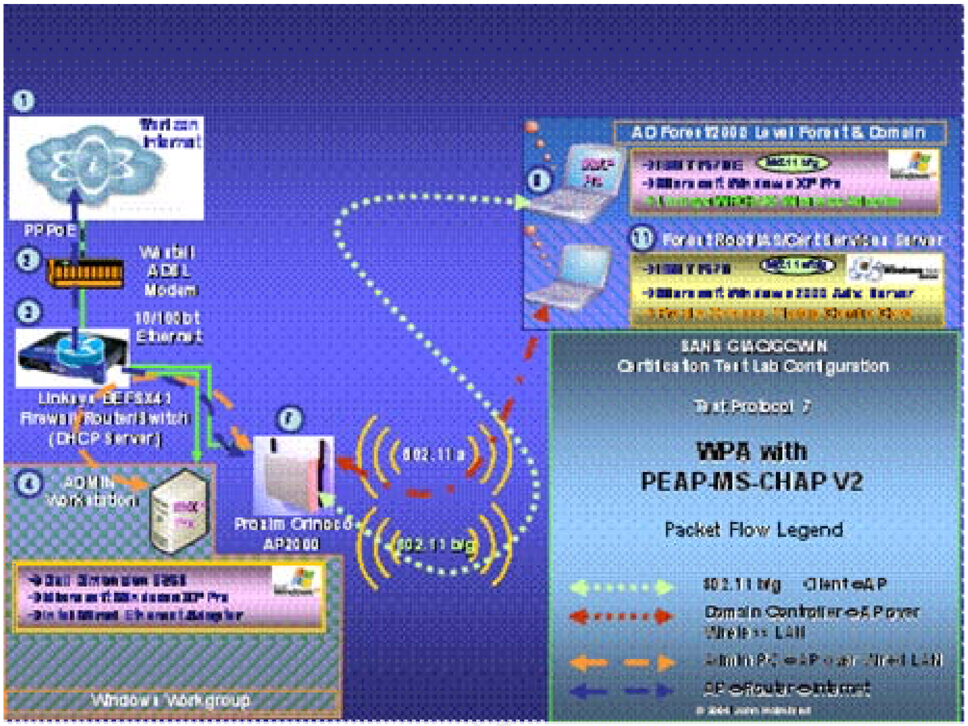
➔ Small Business Server 2003 Premium Edition

- Active Directory
- Integrated Authentication Service (IAS)
- Certificate Authority\Certificate Services\Certificate Web Enrollment
- Internet Information Server (IIS)
- Network Monitor (similar to Ethereal for packet/frame tracing)
- Event Logging

For this test an Active Directory Domain, “tismbservernet.local”, was created with Windows SBS 2003 Premium Edition as the forest root. The test supplicant computer was named “eaptlsclient”

6.7.1 Test 7 – Configuration Details

The configuration for test 7 is provided in **Figure 6.7.1.1**
. The same computers as were used in test 6 were used for this test so it was simply a matter of modifying the EAP method to be used in the WPA wireless client software on the Microsoft Windows XP system and on the Microsoft SBS 2003 Premium Edition IAS server. There were no changes required to the Proxim AP-2000 in order to switch over to this method.



Test 7 Configuration – WPA with PEAP-MS-CHAP V2
Figure 6.7.1.1

6.7.2 Test 7 – Results

This test was successful and the results are shown in the screen shots shown in **Figure 13.3.1**

of section **13.3**. This screen shot shows the IAS System Event log record that was produced by the SBS 2003 server upon successful PEAP authentication of the user "TISMBSERVERNET\John A. Holmblad" as a result execution of this test.

6.8 Test 8 – WEP with PEAP MS-CHAP V.2 Authentication

Test 8 is a repeat of test 7 with two important differences:

- ➔ Windows 2000 Advanced Server is used for the AD/IAS/DC functions
- ➔ The Windows XP Professional supplicant uses an older WEP compliant (but NOT WPA compliant NIC card – the Lucent Orinoco Gold card).The motivation to run this test was to determine the degree of downward compatibility of the Windows XP WPA client with older versions of 802.11 client NIC's as well as the IAS/AD environment of Windows 2000.

In this test the following Microsoft server components are configured and utilized to verify the correct operation of PEAP MS-CHAP V.2.

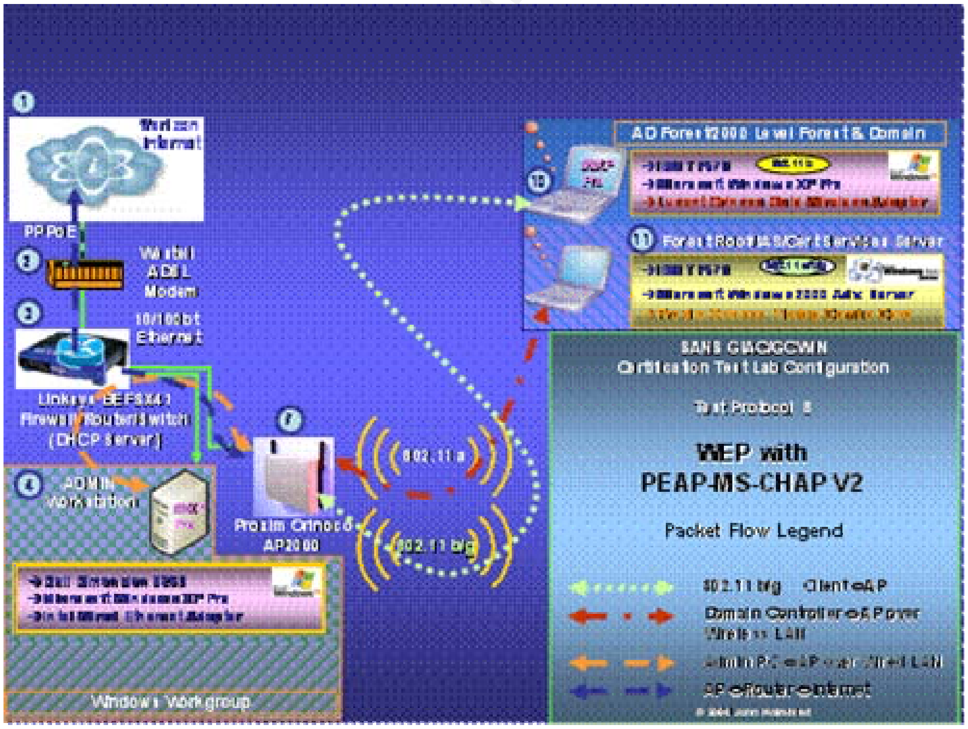
➔ Windows 2000 Advanced Server

- Active Directory
- Integrated Authentication Service (IAS)
- Certificate Authority\Certificate Services\Certificate Web Enrollment
- Internet Information Server (IIS)
- Event Logging

For this test a different Active Directory Domain from that used in tests 6 and 7, "tlvint.net", was created with Windows 2000 Advanced Server as the forest root. The test supplicant computer was named "newthinkpad570"

6.8.1 Test 8 – Configuration Details

The configuration for test 8 is shown in **Figure 6.8.1.1.**



Test 8 Configuration – WEP with PEAP MS-CHAP V2
Figure 6.8.1.1

6.8.2 Test 8 – Results

The screen shots of the system and security log events that record the successful PEAP MS-CHAP V2 authentication of component number 8 in the figure below are **Figure 13.4.1** to **Figure 13.4.4** of section **13.4**. The first three figures are from the security event log and pertain to the authentication and authorization process for first the computer account, “tlvint/newthinkpad570”, and then the user account, “john a. holmblad’, The last figure is from the system event log and shows the successful IAS authentication event log record for the just completed authentication process.

7 Implementation Lessons Learned

7.1 Implementation Lessons – Product Interoperability

These tests confirmed what, in the author's opinion, is a high degree of interoperability, not only among the 802.11 radio technologies from the range of suppliers whose systems were tested, but also among the very recent implementations of Wireless Protected Access (WPA) from Proxim, Linksys, Netgear, and Microsoft. This is important because for the reasons mentioned earlier in this paper it is vital that WPA gets quickly deployed in the commercial market in order to diminish the security risks posed by most implementations of WEP in enterprise and government networks today.

7.2 Implementation Lessons - Testing Methodology

Interoperability testing always represents challenges, especially when the technologies being tested are fairly new. Documentation from all suppliers on their WPA implementations is very Spartan to say the least!

The test effort was greatly facilitated by having systems that were small (laptop computers) that could be stacked, networked using 802.11, and all controlled from a common console using the Microsoft Remote Desktop Protocol (RDP). Furthermore, the Server 2003 family offers enhanced administration capabilities via HTML.HTTP interfaces and a www browser.

7.3 Implementation Lessons – Differences between Windows 2000, Windows XP, Windows 2000 Server and Windows Server 2003

These tests revealed some important differences in how the Microsoft Windows operating systems handle 802.11 wired and wireless interfaces. These differences are summarized in **Table 7.3.1** below.

Category	Feature or Function	Microsoft Operating System			
		Windows 2000 Professional	Windows XP Professional	Windows 2000 Server	Windows Server 2003
Network Connections	Support for Internet Connection Firewall	NO	✓	NO	✓
	Support for Wireless Zero Configuration Service including wireless network configuration that is "per network/per interface"	NO	✓	NO	✓
	Support for Wireless Protected Access™ Client Update	NO	✓	NO	NO
Internet Authentication Server	Support for IAS Proxy Server	na	na	NO	✓
	Support Logging to an SQL Server	na	na	NO	✓
Group Policy	Group Policy Template support for Wireless Networks using WEP	na	na	NO	✓
	Group Policy Template support for Wireless Networks using WPA	na	na	NO	NO
	Group Policy Template support for computer certificate distribution	na	na	✓	✓
	Group Policy Template support for user certificate distribution	na	na	NO	✓

Documented and/or observed differences between Microsoft Windows Operating Systems
Table 7.3.1

8 Suitability for Use in the Small Business Environment

Based on the level of effort for the implementation of each of the 8 test protocols the author has developed guidance on the level of expertise that is required in the Information Technology organization of any firm that chooses to implement and support the features that were tested. This guidance can be found in **Table 8.1** below. The main difference with the last three features from the first five in the table is that the IT staff in the organization that plans on using features 6, 7, or 8 must be reasonably well versed in the use of Microsoft AD and Public Key Infrastructure (PKI). Microsoft Small Business Server 2003 provides a simplification of operation for the small enterprise in that with SBS 2003 it is possible to house the AD domain controller, Certificate Services Server, Internet Authentication Services Server and IIS www server all on the same computer system as long as that system is **well protected from intrusion with multiple layers of defense, e.g. firewall and IPSEC wherever possible between the AD domain controller and the other systems attached to the LAN.**

Security Feature		Degree of Difficulty to implement/support	
#	Description	Rating	Commentary
1	SSL Implementation for HTTP Administrative Interface on the Access Point	1	Implementation is trivial. The only ongoing impact is that serving of HTML pages by the AP is slowed by the SSL encryption on the AP-2000. This situation may be different for other AP's from other suppliers
2	Rogue Access Point Detection	3	Implementation requires a network management and administration function to collect SNMP traps and filter received Rogue AP reports from the AP
3	MAC Address Filtering on the Access Point	2	Requires collection of NIC MAC addresses and installation on the AP's that will perform the filtering. Once this is done the support is trivial.
4	104 bit WEP with Open Authentication	2	Requires installation of WEP keys on all client computers and AP's. Once this is done the support is trivial except for periodic updating of the keys which may be a major effort depending upon the size of the network if it has to be done manually.
5	WPA with Pre-Shared Key (WPA-PSK)	2	Requires installation of WPA preshared keys on all client computers and AP's. Once this is done the support is trivial except for periodic updating of the keys which may be a major effort depending upon the size of the network if it has to be done manually.
6	WPA with EAP-TLS	5	Requires Microsoft AD/IAS/Digital Certificate Infrastructure and therefore the SYSADMINs have to be trained in designing and deploying a PKI infrastructure even on a small scale. Because this technology requires user certificates it ranks slightly higher in difficulty than 7 and 8.
7	WPA with PEAP MS-CHAP –v2	4	Requires Microsoft AD/IAS/Digital Certificate Infrastructure and therefore the SYSADMINs have to be trained in designing and deploying a PKI infrastructure even on a small scale.
8	WEP with PEAP MS-CHAP –v2	4	

802.11 Security Features – Level of Difficulty to Implement
Table 8.1

9 Extending the solution to a Mixed Linux/Microsoft Network Environment

As mentioned earlier in the paper, one of the tests, number 4, 104 Bit WEP with Open Authentication, included a Linux system. As Linux finds its way into the Small and Medium Enterprise (SME) market it will be important for it to interoperate seamlessly with Microsoft network environments. This means that EAP methods and RADIUS authentication must be implemented so that they can be supported across a mixed platform environment. Although the aforementioned Linux system was NOT tested with any EAP method, it should be possible to develop a digital certificate based method that can work successfully in a Microsoft AD/IAS authentication environment, at least at the level of computer association/authentication/authorization with an 802.11 WPA enabled AP.

Although there is not yet available a set of Linux drivers for the Proxim Orinoco a/b/g World Card from Proxim, there is an effort underway by the Opensource community to develop a set of drivers. Their work can be found at the following URL:

http://sourceforge.net/projects/madwifi

10 Recommendations for Deployment of 802.11 Wireless Protected Access^{TM} in a Microsoft Network for Small Business

By now the reader should have a good understanding of how Wireless Protected Access™ operates and a sense of the numerous ways that a Microsoft Windows based network COULD be configured to provide secure communications using WPA based on the various laboratory test scenarios that were described in section 6. This section provides the reader with specific guidance on how this technology can be deployed in two specific Microsoft network and server scenarios to provide significant improvements in wireless security by deploying WPA in place of the earlier Wired Equivalent Privacy Standard.

It should be noted here that a key objective in performing the aforementioned tests was to ascertain interoperability of the wireless security standards, both WEP and WPA, in a wide array of Microsoft and even non-Microsoft systems and in a controlled laboratory environment. In everyday practice, this author does NOT recommend the use of such a broad array of technologies and suppliers in a single network. This author has found through his own business experience that it is best to thoroughly evaluate a reasonable set of suppliers based on your commercial and technical requirements including those pertaining to information security, and then to select the top two for production use. Having two suppliers will help you achieve ongoing competitive pricing and service quality by

- ➔ Maintaining sufficient purchasing volume with each supplier, and
- ➔ keeping both suppliers in play for your business,

and also provide you protection against a supply chain failure of most kinds (e.g. one supplier runs out of parts in their manufacturing plant). The extra cost and complexity of maintaining staff "fluency" in more than one technology is generally offset by the aforementioned positive effects of competition especially with potentially high volume products such as 802.11 wireless access points and client NIC cards.

For the purpose of recommending specific Microsoft network designs, two scenarios, which are typically found in a small business, are considered in this section. A small business is here defined as one having fewer than 100 computers and other smart devices (e.g. 802.11 enabled pda's and the like) which need to be taken into consideration in the design of the network. The first scenario is the simpler of the two and is referred to herein as the Windows Workgroup network scenario. The second scenario is somewhat more complex but much more scalable and is referred to as the Windows Active Directory Domain network scenario. Each is described in turn below along with guidance on implementing WPA in each type of network.

For the purpose of simplicity of description, both scenarios assume that the network is being deployed with 802.11equipment from a single supplier, comprising the Proxim Orinoco a/b/g Combo Card Gold NIC card and the Proxim Orinoco AP-2000 Access Point. Although the testing was conducted with a Proxim Orinoco AP-2000 operating with two radios, an 802.11a radio and an 802.11b/g radio, the scenarios described below will assume only a single 802.11 b/g radio is present. At the end of this paper the author does however suggest how a second radio in the base station could be used with a Virtual LAN (VLAN) to provide guest access to the Internet by means of the enterprise 802.11 network.

In each network design the desktop and laptop computers are assumed to be running Microsoft Windows XP Pro SP1 and in the case of the second scenario the server computer is assumed to be running either Microsoft Small Business Server 2003 Standard Edition or Windows Server 2003 Standard Edition.

For both networks the 802.11 Service Set Identity (SSID) is assumed to be "XYZ Enterprise Wireless LAN"

In the description of each scenario, security enhancing configuration practices are highlighted in **bold red letters**.

For larger deployments of 802.11 access points this author recommends the deployment of an access point management software product such as that of Wavelink (http://www.wavelink.com/) whose Wavelink Mobile Manager[38] software supports the

802.11 wireless access point products of several different suppliers. In addition to easing the management of multiple AP's on a single network, such software can provide other services such as rogue activity detection, SNMP trap logging and many other useful network management tasks. Unfortunately the time available to the author for this project did not permit the testing of such specialized network management software.

10.1 Windows Workgroup Network Scenario with WPA Pre-Shared Key

Since the time of first release of the Microsoft Windows 2000 operating system, Microsoft has placed great emphasis on the scalability, performance, and security benefits of its Lightweight Directory Access Policy (LDAP) based directory service known as Active Directory (AD). Indeed the architecture of AD and the features related to it, such as Group Policy, sites, domains, organization units, Kerberos based authentication, cross-forest trusts, shortcut trusts, etc. afford the Microsoft network system administrator (sysadmin) a myriad array of options for configuring and managing the network for which he or she is responsible. This power, however, comes at the cost of complexity and in a very small business there may not even be a full time sysadmin to command the IT "ship**.** On the other hand the average computer competency level of the employees of such small organizations may be sufficient so that each employee can take responsibility for their own computer system and play an active role in maintaining overall workplace information security**.** Fortunately for a small business of 10 or so computers where such conditions hold, there is a simpler although less secure alternative to an AD based network which is herein referred to as Windows Workgroup (WW) networking. WW networking is actually a form of peer-to-peer networking where each system is responsible for its own security and there is no central authority to manage credentials, access rights to systems and services, log security related events, etc. Earlier versions of the Microsoft operating system (Windows for Workgroups 3.1) from the early 1990's were the first in Microsoft's product line to support this technology and it was then known as Windows for Workgroups. Microsoft continues to support WW networking even in its newest server products and there is a text which covers this subject extensively entitled, "Configuring Windows 2000 Without Active Directory"[39]. The text provides excellent guidance on best practices for non-AD network configuration of Windows 2000 computers and includes for example, an explanation of how to utilize Microsoft Group Policy on a computer by computer basis (Local computer mode only of course) to get at the hundreds of parameters (e.g. IPSEC policies, security templates, administrative templates, etc.) that are simply not accessible with the Local Security Policy Microsoft Management Console (mmc) snap-in. Of course, since a WW network lacks the AD infrastructure that is necessary to automatically push such policies out to tens, hundreds, or thousands of desktops, there are obvious limits on how far this WW approach can reliably scale. Furthermore the only component of a Local Group Policy object that can be exported to a file (.inf suffix) and easily shared with other computers in the workgroup is the security component. In other words in a Microsoft network that is not operating with Windows Active Directory services, it is NOT possible to export a complete GP from one computer and to import it into another.

As stated in **Table 3.3.4** of section **3.3** of this paper, the developers of WPA included an operating mode called "Pre-shared Key" that is useful for networks that do not have a central RADIUS authentication service. In order for this method to work, the pre-shared key (256 bits or 64 hexadecimal digits) has to be installed on each wireless client and also on the AP. In order to ease the burden on the sysadmin of entering such long character strings, some suppliers have chosen to support the implementation of a passphrase solution which then automatically generates a 256 bit key using the passphrase as keying material input. While this feature has been implemented on the Proxim equipment, unfortunately it is NOT, as far as this author can determine, implemented in the Microsoft Windows WPA Client Update. Obviously, this approach does not scale, just as the original WEP standard did not scale because of the requirement for the entering of keying material. While it may be possible to write a script to automate the key installation, so far there does not appear to be any guidance from Microsoft on how to script the configuration of the Wireless Zero Configuration (WZC) client.

The core network protocols above and beyond TCP/IP and UDP/IP, DHCP, DNS, and ICMP that are now used between computers running Microsoft operating systems in WW networks include the Server Message Block (SMB)/Common Internet File System[40] (CIFS) protocol for file and print sharing, and the Remote Procedure Call (RPC) protocol, and the Remote Desktop Protocol (RDP) for remote access to a Windows XP desktops. In addition, if the WW network has an internal http server then of course such protocols as http and https will be present. It should be noted that SMB/CIFS is also used on a Linux server running SAMBA to emulate the workings of Windows file sharing so that such Linux servers can participate in a WW network. These Linux based systems running SAMBA offer a good solution for file sharing and provide additional security against malware that is most often targeted to the Windows operating system. This kind of operating system diversity can be thought of as a kind of "security through diversity". In configuring the security of a WW network, it is important to be aware of the presence of the aforementioned protocols in the context of securing the network so that the services supported by these protocols are not inadvertently prevented from operating on the LAN due to an improperly configured firewall.

10.1.1 Windows Workgroup Network Configuration

Figure 10.1.1.1 below depicts the Windows Workgroup network configuration. This is the kind of configuration one might find in a small business of a few employees. Below is a bulleted description of the configuration.

- ➔ The network consists of 5 computers (objects numbered 5-9 in the figure), 4 laptops and 1 desktop each running Windows XP Pro SP1.

- The 4 laptops are networked using a single Proxim Orinoco AP-2000 (object 4 in the figure) running in 802.11 b/g mode.

- The AP-2000 is connected in turn to a Small Office/Home Office (SOHO) router, in this case, the Cisco/Linksys BEFSX41 (item 3 in the figure) and the router is connected to a DSL or Cable Modem (item 2 in the figure) and the Internet (item 1 in the figure).

- The 5th computer is connected to the network with a wired (100bT) connection to the Linksys router.

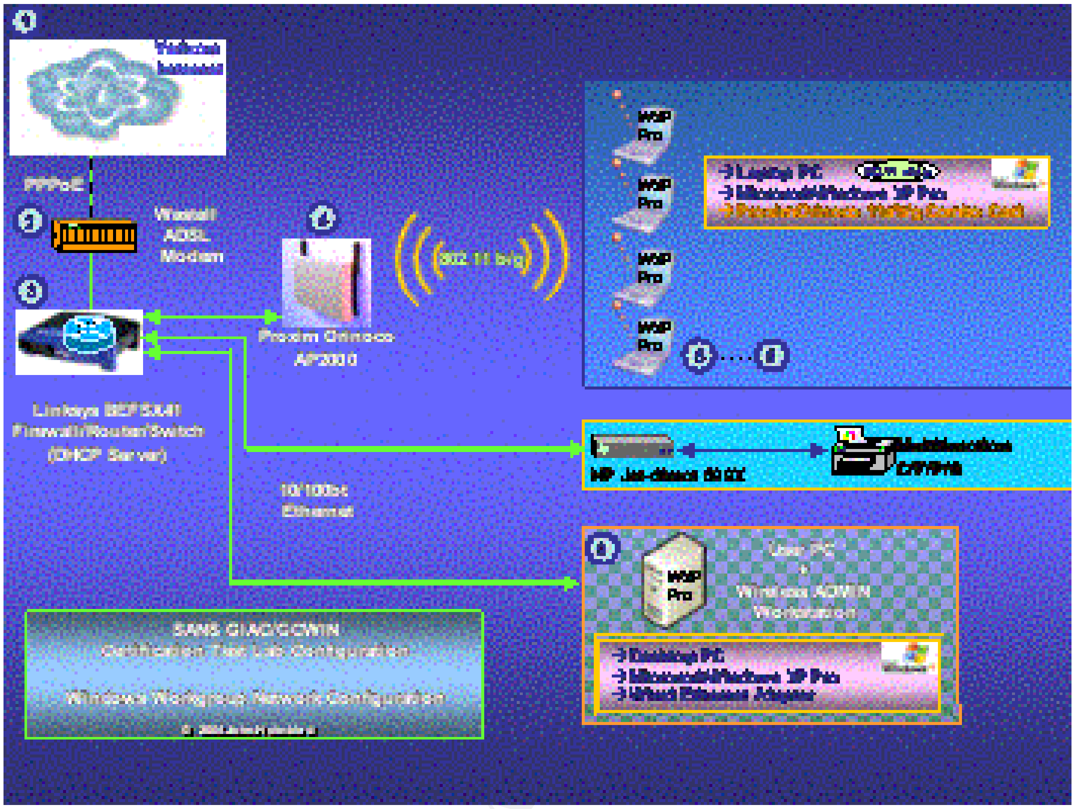
- In addition there is a shared multifunction (print/copy/fax/scan) printer, connected to a HP Jetdirect print server and the print server joins the network via a wired connection to the Linksys router. Since the printer is shared via the stand alone print server, each computer can have its own instance of the printer installed with a TCP/IP printer port connection to the Jetdirect print server. Consequently, the Windows XP printer sharing feature is not required. The Jetdirect print server is configured with a static IP address.

- In order to share files, the network is set up with a file share on each system and each user has read privileges but not “write” or “modify” privileges on that share.

- The router supports Domain Host Control Protocol (DHCP) service and is configured to do so for the computers on the LAN.

- Domain Name Service (DNS) is assumed to be provided by the Internet Service Provider that also delivers the cable modem or DSL service.

- Because this network scenario presumes the use of WPA with pre-shared key there is no need for a central Radius server to provide authentication and authorization services.


PPPoE
Westell ADSL Modem
Proxim Orinoco AP2000
802.11 b/g
Linksys BEFSX41 Firewall/Router/Switch (DHCP Server)
10/100bt Ethernet
WXP Pro
Laptop PC
Microsoft Windows XP Pro
WXP Pro
User PC + Wireless ADMIN Workstation
Desktop PC
Microsoft Windows XP Pro
Wired Ethernet Adapter
SANS GIAC/GCWIN Certification Test Lab Configuration
Windows Workgroup Network Configuration

Windows Workgroup Network Configuration
Figure 10.1.1.1

Table 10.1.1.1 and **Table 10.1.1.2** below provide a high level step by step summary of implementing WPA-PSK in this environment. The explanation provided in these tables assumes that the Linksys router has already been configured and is operating with the following parameter settings:

- a non-routable IP address range of 192.161.1.1/24 on the LAN.
- the necessary configuration parameters from the WAN side of the network including the ISP's primary and secondary DNS addresses and the encapsulation protocol if any (e.g. Point to Point Protocol over Ethernet – PPPoE)
- DHCP service enabled with a DHCP address scope of 192.168.1.100 – 192.168.1.105.
- **Stateful firewall enabled**

- → **NO mappings of incoming IP address/port combinations from the WAN to internal services on the LAN. Thus all incoming UDP and TCP packets will be blocked unless they are associated with a corresponding outgoing UDP packet or TCP connection.**

Table 10.1.1.1 describes the steps required on the laptop and desktop computers while **Table 10.1.1.2** describes the steps that are required on the Proxim Orinoco AP-2000. For an exact description of the AP-2000 configuration consult the Proxim Orinoco AP-2000 User Guide which is available at the following url:

http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/std_adp.php?p_faqid=1221&p_created=1075322819&p_sid=X*P1w73h&p_lva=&p_sp=cF9zcmNoPSZwX3NvcnRfYnk9JnBfZ3JpZHNvcnQ9JnBfcm93X2NudD05NDYmcF9wYWdlPTE*&p_li=

Step #	Implementation Guidance applicable to computers	Applies to		Motivation
		Laptops ?	Desktop ?	
1	On each computer select Start>Control Panel>System and go to the tab on the menu entitled "Computer Name". Select the change button next to the text "To rename this computer or join a domain, click Change". On the "Computer name changes" menu which appears, select the "Workgroup" radio button and enter the name of the workgroup to be used for this network.	yes	yes	This step configures the Windows workgroup name on each computer in the network.
2	**Install Proxim Orinoco a/b/g Combo Card Gold and Proxim driver version 2.4.2.17 or later which supports WPA.**	yes	no	WPA support is available in the October 31, 2003 version of the driver. If necessary obtain said driver from the Proxim www site at (http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/std_adp.php?p_faqid=1171&p_created=1073614125&p_sid=fWmVN63h&p_lva=1082&p_sp=cF9zcmNoPTEmcF9zb3J0X2J5PSZwX2dyaWRzb3J0PSZwX3Jvd19jbnQ9MjAmcF9zZWFyY2hfdGV4dD0mcF9zZWFyY2hfdHlwZT1zZWFyY2hfbmwmcF9wcm9kX2x2bDE9NTAmcF9wcm9kX2x2bDI9NTEmcF9jYXRfbHZsMT0xMDYmcF9jYXRfbHZsMj0mcF9wYWdlPTE*&p_li=)
3	On the Internet Protocol (TCP/IP) Properties sheet General Tab for the wireless or wired LAN interface select "Obtain an IP address automatically" and "Obtain DNS server address automatically". Make sure that "Client for Microsoft Networks" and "File and Print Sharing for Microsoft Networks are installed for this interface.	yes	yes	DHCP service is provided by the Linksys router which obtains the primary and secondary DNS addresses from the ISP. See **Figure 13.5.2** for a screenshot of these settings.
4	**Disable NetBIOS by opening the "Connection Properties" menu of the wired or wireless NIC,**	yes	yes	Since all computers on the network are running at a Windows

Step #	Implementation Guidance applicable to computers	Applies to		Motivation
		Laptops ?	Desktop ?	
	click on the "Advanced" button, navigate to and select the "WINS" tab, and once there, select the "Disable Netbios over TCP/IP" radio button			2000 level or later, it is not necessary to have Netbios enabled.
5	**On the Advanced tab of the Network Connection Properties menu, select the checkbox to enable the Internet Connection Firewall and click Settings. This will take you to the Advanced Settings menu from which you can enable the ports and services on the firewall that are necessary to support workgroup networking and Remote Desktop Connection (RDP). The transport layer ports and protocols include the following:** ➔ **Netbios Datagram Service: UDP Port 138** ➔ **Netbios Name Service UDP Port 137** ➔ **Netbios Session Service TCP Port 139** ➔ Remote Desktop Service TCP Port 3389 ➔ **DHCP/BOOTP Server=>Client UDP Port 68** The ports/protocols shown above which are shown in **bold blue typeface** must be added, since the standard ICF does not include these. The one in black is already configured in the standard ICF. **On the Security Logging Tab of the Advanced Settings Menu, select the "Log dropped packets" and "Log successful connections" checkboxes.** **On the ICMP Tab of the Advanced Settings Menu, select "Allow incoming echo request" checkbox.**	yes	yes	Because of the complexity of correctly setting up the Microsoft Windows ICF on a computer whose network interface is connected to a Microsoft network, the recommendation from Microsoft is to turn off this firewall. This author disagrees with that guidance and recommends that the firewall be enabled and properly configured to support the necessary protocols. It should be noted that the firewall is stateful and only inspects packets coming into the computer on which the firewall is activated. Thus it will not stop a Trojan from "dialing home" for orders if such Trojan manages to find its way onto the computer in question. Microsoft has stated that once Service Pack 2 for Windows XP is released, the ICF will be enabled by default however it STILL will not filter outgoing packets/connections. **Figure 13.5.3**, **Figure 13.5.4**, and **Figure 13.5.5** provide screenshots of the sequence of steps to configure the Microsoft Windows ICF. **Important Note:** **1. Depending upon what other applications are running on the desktops it may be necessary to open up additional protocol/port combinations on the ICF.**
6	Connect the Desktop PC to the Linksys router using a cat-5 patch cable.	no	yes	Having one computer attached to the network using a wired connection facilitates system initialization and troubleshooting of the wireless sub-segment.

Step #	Implementation Guidance applicable to computers	Applies to		Motivation
		Laptops ?	Desktop ?	
7	Install configure, and activate the AP-2000 Access Point	no	no	Activate the 802.11 Access Point (see **Table 10.1.1.2** below for details)

Step #	Implementation Guidance applicable to computers	Applies to		Motivation
		Laptops ?	Desktop ?	
8	On the Wireless Networks Tab of the Network Connection Properties Menu of the 802.11 wireless NIC card, configure the Wireless properties of the card as follows: ➔ Check the checkbook entitled “Use Windows to configure my wireless Settings” ➔ **Select “Advanced” in the lower right hand corner of the menu and then on the “Advanced” menu select the radio button, “Access point (infrastructure) networks only”.** ➔ **Leave unchecked the checkbox entitled “Automatically connect to non-preferred networks”** ➔ **Return to the Wireless Networks Tab of the Network Connection Properties Menu and in the “Available Networks” pane, highlight the network for configuration who’s SSID should be shown there and entitled “XYZ Enterprise Wireless LAN” and then select “Configure”.** **On the “association” tab for the Wireless network properties Menu of XYZ Enterprise Wireless LAN:** ➔ **select WPA-PSK from the pull down menu next to “Network Authentication”** ➔ **select TKIP from the pull down menu next to “Data Encryption”** ➔ **enter the 64 hexadecimal digit pre-shared key next to “Network Key”** ➔ **re-enter the 64 hexadecimal digit pre-shared key next to “Confirm Network Key”** Select “ok” on the Wireless network properties menu to close it out. **In the preferred networks pane, make sure that the network whose SSID is “XYZ Enterprise Wireless LAN” is at the top of the list if there is more than one preferred network. Make sure that there are not any preferred networks on the list that are not secured with at least WPA unless the user knows that it is safe to associate with such networks from a security perspective (e.g. in a home with no electronic eavesdroppers).**	yes	no	This is where the LAP PC wireless NIC is configured to associate with the AP-2000 using the WPA pre-shared key mode of operation. The NIC should also be configured to only associate with infrastructure networks so that accidental association with an ad-hoc (802.11 peer to peer) network cannot occur. Furthermore it should be configured to NOT associate with non-preferred networks. Once this step is completed the wireless NIC’s on the laptop PC’s should be properly associated with the Proxim Orinoco AP-2000. A quick test of Internet access and workgroup file sharing can be performed at this time. The screenshots that provide the sequence of steps to configure the wireless NIC and wireless network settings on the computers are shown in **Figure 13.5.6** and **Figure 13.5.7.** The Microsoft Wireless Zero Configuration (WZC) feature makes it very easy for a user to associate with a wireless network. Therefore it is important to configure this service so that association ONLY occurs with trusted networks that have the requisite level of security which should be at least WPA-PSK.

Step #	Implementation Guidance applicable to computers	Applies to		Motivation
		Laptops ?	Desktop ?	
9	**Check Windows Update Service history log on the computer to confirm that the wireless security rollup described in Microsoft Knowledge Article KB826942 is Installed. If the update has not already been installed then download and install this update using Windows Update Service**.	yes	no	This rollup corrects a number of security related flaws in Microsoft's implementation of WPA in Windows XP. The Microsoft KB article can be found at the following url: (http://support.microsoft.com/?kbid=826942)

WPA pre-Shard Key Implementation Steps on Windows XP Computers
Table 10.1.1.1

Step #	Implementation Guidance applicable to Proxim Orinoco AP-2000	Motivation
1	Install Proxim Orinoco b/g card that is shipped with the base unit into Radio slot A of the AP-2000. Connect the AP-2000 to the Linksys router via a category 5 Cable and power up the unit.	The unit is shipped disassembled and a one step assembly is required
2	Insert the Proxim AP-2000 Configuration CD into the desktop PC CD ROM drive, install the AP-2000 software and run the Scan Tool that is installed on the PC. The Scan Tool will detect AP 2000 by means of its MAC address at which point you can select the line in the display corresponding to that MAC address, click on the Change button and then enter the following items: ➔ Static IP address of the AP (192.168.1.99) ➔ Subnet Mask ➔ Gateway Address	Although the AP-2000 has a pre-configured IP address of 10.0.0.1, this address is incompatible with the Linksys router (without modification to its routing table, which, in turn requires disabling DHCP). The Scan Tool enables discovery of the AP-2000 on the basis of its MAC address and, once discovered, the tool permits the sysadmin to configure an IP address. See **Figure 13.5.1** for a screen shot of the GUI for the Scan Tool.
3	Using an http browser (e.g. Microsoft Internet Explorer or Netscape Navigator) on the desktop computer connect to the http interface of the AP-2000 at the aforementioned static IP address configured in step 2. The interface is protected with a password and the factory default password is, “password”. **Using the browser navigate to the “Management” TAB of the “Configure” www page to change the passwords for HTTP/Telent/SNMP to strong password values which must be in the range of 6-32 characters. Pick a long passphrase of 16 characters or greater**.	The remaining steps of configuring the AP-2000 can be accomplished via the http/html interface.
4	**Download the software/firmware update that supports WPA from the Proxim web site to the desktop computer. Then, on the desktop computer, run the Solarwinds TFTP software that is provided on the Proxim AP-2000 CD, in order to transfer the software/firmware update from the desktop computer to the AP-2000. The AP will reboot itself automatically upon successful completion of the download. The version number of this software/firmware is: v2.4.5**	The Proxim AP 2000 itself has to be updated with WPA support. The url to the required download is as follows: http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/std_adp.php?p_faqid=1221&p_created=1075322819&p_sid=X*P1w73h&p_lva=&p_sp=cF9zcmNoPSZwX3NvcnRfYnk9JnBfZ3JpZHNvcnQ9JnBfcm93X2NudD05NDYmcF9wYWdlPTE*&p_li= This release is designated v2.4.5, and dated Jan 19, 2004. It is an update from the version that was used in the testing that was documented in this paper. This is a maintenance release which contains corrections for 25 specific software faults including some pertaining to WPA.

Step #	Implementation Guidance applicable to Proxim Orinoco AP-2000	Motivation
5	After re-initialization of the AP-2000 with its updated software, again navigate to the AP-2000 http interface and re-enter the configuration management www site. At this point you will configure the following essential items on different tabs/sub tabs of the configuration www page: On the Tab: System, configure: ➔ APName ➔ Location ➔ Contact Name ➔ Contact Email ➔ Contact Phone On the Tab: Interfaces, Sub tab: Operational Mode ➔ Set Wireless A operational mode to "802.11 b/g" On the Tab: Interfaces, Sub tab: Wireless-A ➔ Set SSID = "XYZ Enterprise Wireless LAN" ➔ Check Enable Auto Channel Select ➔ Set Transmit Rate to Auto Fallback On the Tab: Network, Sub tab: Link Integrity ➔ Select the checkbox "Enable Link Integrity" ➔ In the Target IP address Table, create an entry for the IP address of the Cisco/Linksys Router and insert the IP address of the router, 192.168.1.1 into the table. **On the Tab: Management, Sub tab: IP Access Table** ➔ **Configure the IP Access Table to limit the permitted IP source addresses from which the AP http interface will accept incoming connections to the scope of the DHCP address range (i.e. 192.168.1.100-192.168.1.105)** **On the Tab: Management, Sub tab: Services** ➔ **Enable HTTPS (Secure WEB)** ➔ **In the "HTTP Interface Bitmask" pull down menu, select "Ethernet"** ➔ **Select the checkbox entitled "Enable HTTPS (Secure Web)"** **On the Tab: Security, Sub tab: Authentication** ➔ **In the Authentication Mode Pull-down menu for Slot A Select "WPA-PSK"** ➔ **Enter the 64 hexadecimal digit pre-shared key value for Slot A** **On the Tab: Security, Sub tab: MAC Access** ➔ **Select "Enable MAC Access Control" check box**	This step configures all of the essential parameters of the Proxim Orinoco AP-2000 that will enable communications with the 802.11 b/g NIC cards using WPA-PSK. The link integrity feature provides a means for the AP to quickly determine that its connection to the LAN has failed and thereby force the wireless connections to the AP to disassociate. Through this means, wireless users will be informed quickly if the wired segment of the LAN or router has a serious malfunction. Although it is always possible for an attacker to spoof a MAC address and defeat the MAC filtering defense, it is nonetheless recommended by this author to provide another layer of defense by this means. The HTTP interface to the AP-2000 will be secured with SSL and only devices on the wired segment of the LAN will be permitted to have access to this interface.

Step #	Implementation Guidance applicable to Proxim Orinoco AP-2000	Motivation
	➔ **Select "Passthru" for Operation Type** ➔ **Enter a MAC access Control Table consisting of the MAC address of each of the 4 wireless NIC's in the network configuration.**	
6	**Obtain and install an http web server digital certificate and download this to the AP-2000 using the Solarwinds TFP software running on the desktop computer.**	This step provides an additional level of security for the http access to the AP-2000 administrative interface by replacing the Proxim supplied default server digital certificate with one that is specific to the user's organization.
7	Return to LAPTOP PC Implementation Guidance table to complete network activation	See **Table 10.1.1.1** for details.

WPA pre-Shard Key Implementation Steps on Proxim Orinoco AP-2000
Table 10.1.1.2

10.2 Windows Active Directory Domain Network Scenario

Figure 10.2.1.1 below depicts a simple Windows Active Directory Domain Network such as one might find in a small business. The primary differences between this configuration and the one in section **10.1** are as follows:

- ➔ it has a larger quantity of user computers (laptops + desktops)
- ➔ it uses a higher port capacity SOHO router (8 switched ports)
- ➔ it includes a server computer to provide centralized authentication, file sharing, and other services for the wired and wireless computers on the LAN.

The most significant difference is that this configuration makes use of many of the advanced features of the Microsoft Windows Server 2003 operating system including:

- ➔ Active Directory
- ➔ Certificate Services
- ➔ Internet Information Service (IIS)
- ➔ Internet Authentication Service (IAS)
- ➔ Domain Name Service (DNS)
- ➔ Dynamic Host Control Protocol Service (DHCP)

These functions are in addition to the standard file server capabilities generally available on a server based network.

10.2.1 Windows Active Directory Domain Network Scenario

Below is a bulleted description of the network configuration.

- The network consists of 11 computers (objects numbered 5-15 in the figure). The server computer (object number 5 in the figure) is running Microsoft Windows Server 2003 Standard Edition. The server is connected to the LAN using a wired connection (100bT) to the Cisco/Linksys router. While it is technically feasible using WPA to connect servers securely to the wireless LAN, it is not recommended to connect this particular server using 802.11 for performance reasons.

- The 5 laptops (objects numbered 6-10 in the figure) and 5 desktops (objects numbered 11-15 in the figure) are each running Windows XP Pro SP1.

- The 5 laptops are networked using a single Proxim Orinoco AP-2000 (object number 4 in the figure) running in 802.11 b/g mode.

- The AP-2000 is connected in turn to a SOHO router, in this case, the Cisco/Linksys RV802 (object number 3 in the figure) and the router is connected to a DSL or Cable Modem (object number 2 in the figure) and the Internet (object number 1 in the figure).

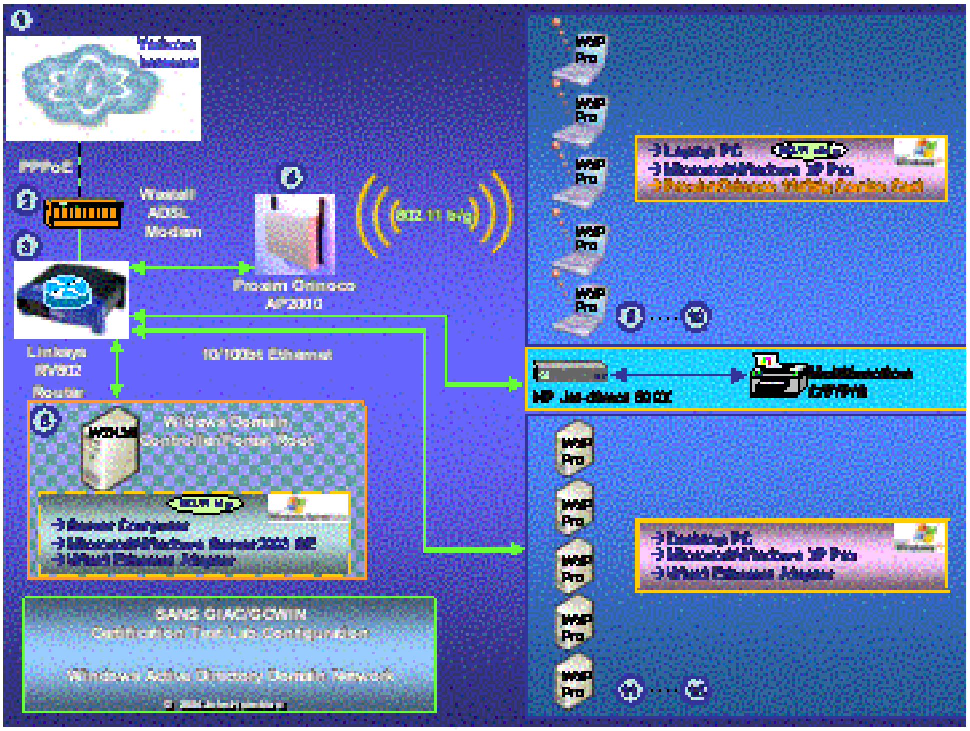
- The desktop computers and the server are each connected to the network with a wired (100bT) connection to the Linksys router.

- In addition there is a shared multifunction (print/copy/fax/scan) printer, connected to a HP Jetdirect print server and the print server joins the network via a wired connection to the Cisco/Linksys router. Since the printer is shared via the stand alone print server, each computer can have its own instance of the printer installed with a TCP/IP printer port connection to the Jetdirect print server. Consequently, the Windows XP printer sharing feature is not required. The Jetdirect print server is configured with a static IP address.

- Domain Name Service (DNS) for domains other than those for which the Windows 2003 server is authoritative is assumed to be provided by the Internet Service Provider that also delivers the cable modem or DSL service.

- The router supports Domain Host Control Protocol (DHCP) service, however in this configuration, in contrast to that of section **10.1.1** of this paper, the DHCP service is provided by the Windows 2003 Server. This provides for improved management including event logging of the usage of the DHCP service considerably beyond what is available from the CISCO router GUI.

- ➔ The domain name for the Active Directory Domain is **sb.local** and the computer name of the domain controller is **sbserver**



Windows Active Directory Domain Network Configuration
Figure 10.2.1.1

Table 10.2.1.1
, **Table 10.2.1.2**, and **Table 10.2.1.3** below provide a high level step by step summary of implementing WPA in this environment. The explanation provided in these tables assumes that the Linksys router has already been configured and is operating with the following parameter settings:

- ➔ a non-routable IP address range of 192.161.1.1/24 on the LAN.
- ➔ the necessary configuration parameters from the WAN side of the network including the ISP's primary and secondary DNS addresses and the encapsulation protocol if any (e.g. Point to Point Protocol over Ethernet – PPPoE)
- ➔ **Stateful firewall enabled**
- ➔ **NO mappings of incoming IP address/port combinations from the WAN to internal services on the LAN. Thus all incoming UDP and TCP**

packets will be blocked unless they are associated with a corresponding outgoing UDP packet or TCP connection.

Table 10.2.1.1
describes the steps required to configure and activate the server, **Table 10.2.1.2** describes the steps required to configure the laptop and desktop computers, and **Table 10.2.1.3** describes the steps that are required on the Proxim Orinoco AP-2000.

For the sake of ease of readability for the reader of this paper, all of the steps pertaining to the laptop and desktop computers and the Proxim Orinoco AP-2000 are included here even though many of those steps are exactly the same as in the configuration described in section **10.1.1.** Differences in these tables from the corresponding steps in the corresponding table entry in section **10.1.1** will be highlighted in **yellow background**.

Because this network is configured with Microsoft Windows Active Directory, it should be possible to "push out" the configurations of the wireless clients using Group Policy. This is because, starting with the Server 2003 family of operating systems, Microsoft is supporting a new sub-container of the Group Policy security container, called "Wireless Network (802.11) Policies". This new sub-container is shown in **Figure 13.5.8**. Unfortunately, Microsoft does not yet have GP support for the new WPA Wireless Client Update features that need to be associated with this new policy sub-container. The author checked this by using the Group Policy Editor snap in to navigate this section of a group policy template and noted that there is no way to specify WPA in the network properties for the wireless client. Therefore, for the purpose of this paper it is assumed that the wireless clients on the 5 laptop computers will be individually configured by means of the GUI as was done in the WW network configuration described in section **10.1.1** of this paper.

Group policy can be used to push out the computer and user certificates that are required for the wireless clients, however, this must be accomplished by first connecting each laptop computer up to the LAN using a wired Ethernet connection and joining the computers and users to the domain. At that point an update of the GPO's for those laptop computers and users will be loaded onto the laptop computers and the certificates will be put into the appropriate certificate stores (computer and user respectively) where they can then be accessed when the computer next attempts to associate with the 802.11 network. This approach solves the "chicken and egg" dilemma of how do you download the credentials to a wireless client that are also used to authenticate that client to the wireless network in the first place! Another alternative would be to temporarily operate the wireless LAN with no encryption, or better still with WPA-PSK to enable this first instance of AD authentication and authorization so the certificates can be downloaded to the client notebook computers.

Manual deployment of the computer certificates can be accomplished by exporting the certificate and private key from the AD domain controller to each laptop computer in turn and installing the certificate in that computer's computer certificate store. The user certificates can be manually deployed by means of the certificate services web enrollment interface (//systemname/certsrv) which will also place the newly generated user certificate into the computer's user certificate store for that user. Unfortunately there is no way to use this web interface to easily generate computer certificates. For large numbers of computers and users it is recommended to use GP to perform the distribution of at least the computer certificates. This can be done when a new laptop is first configured for enrollment into the domain using the procedure mentioned above of temporarily connecting the computer to the wired LAN.

For an exact description of the AP-2000 configuration consult the Proxim Orinoco AP-2000 User Guide which is available at the following url:

http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/std_adp.php?p_faqid=1221&p_created=1075322819&p_sid=X*P1w73h&p_lva=&p_sp=cF9zcmNoPSZwX3NvcnRfYnk9JnBfZ3JpZHNvcnQ9JnBfcm93X2NudD05NDYmcF9wYWdlPTE*&p_li=

Step #	Implementation Guidance applicable Microsoft Windows Server 2003 Standard Edition	Motivation
1	Install and configure DNS	Active Directory integrated DNS offers a number of advantages including ease of replication of zone information and the ability to tightly control zone transfers.
2	Install and configure DHCP	The Microsoft DHCP server provides much better logging and monitoring capability than the Cisco/Linksys DHCP server provided on the router.
3	Install and configure IIS	IIS is required in order to support certificate services as well as remote administration of Windows Server 2003.
4	In accordance with the Microsoft article "Enterprise Deployment of Secure 802.11 Networks Using Microsoft Windows"[41] ➔ Configure the laptop computer, desktop computer, and user accounts in Active Directory ➔ Install and configure Certificate Services and Certificate WWW Enrollment Services ➔ Install computer certificates and user certificates for each laptop computer and user that require access	Although the implementation steps in this section do not provide the details to do so, Microsoft best practice recommends: ➔ for highest DNS service availability, that both a primary and a backup DNS server be configured.

Step #	Implementation Guidance applicable Microsoft Windows Server 2003 Standard Edition	Motivation
	to the wireless LAN infrastructure. The installation of these certificates can be accomplished by using Group Policy to update the laptops while each one is temporarily connected, in turn, to the wired LAN. If Group Policy is NOT used then the computer certificates will have to be manually exported from the server, one at a time, with their private keys since they cannot be deployed using the www enrollment services capability. The user certificates can manually deployed using the web certificate enrollment services interface installed in the step above. → Install and activate Internet Authentication Services including the RADIUS shared secret which will also be installed on the Proxim-AP2000 in a later step. → In the Properties of the IAS Server enable logging of both successful and unsuccessful logging attempts. → In Active Directory Users and Computers create a group called "Users and Computers Authorized to access the 802.11 Wireless LAN" and put the laptop computers and laptop users in this group. → Define a Remote Access Policy in IAS for 802.11 Wireless Access Users and specify "Users and Computers Authorized to access the 802.11 Wireless LAN" as a "Remote Access Policy" policy matching condition along with "NAS Port Type Matches 802.11" → Define a Connection Request Policy to specify Windows Integrated Authentication and to restrict, as required, the days and hours during which the policy applies.	→ for highest IAS service availability, that a primary and backup RADIUS server be configured. → for the highest level of security of the certificate services infrastructure, that the Enterprise Root Certificate Services provider be disconnected from any and all live networks (i.e. kept off line and in a highly secured location).

Windows 2003 Server Implementation Steps
Table 10.2.1.1

Step #	Implementation Guidance applicable to computers	Applies to		Motivation
		Laptops ?	Desktop ?	
1	On each computer select Start>Control Panel>System and go to the tab on the menu entitled "Computer Name". Select the change	yes	yes	This step configures the AD domain membership on each computer in the network.

Step #	Implementation Guidance applicable to computers	Applies to		Motivation
		Laptops ?	Desktop ?	
	button next to the text "To rename this computer or join a domain, click Change". On the "Computer name changes" menu which appears, select the "Domain" radio button and enter the name of the Domain "sb.local" for this network.			
2	**Install Proxim Orinoco a/b/g Combo Card Gold and Proxim driver version 2.4.2.17 or later which supports WPA.**	yes	no	WPA support is available in the October 31, 2003 version of the driver. If necessary obtain said driver from the Proxim www site at (http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/std_adp.php?p_faqid=1171&p_created=1073614125&p_sid=fWmVN63h&p_lva=1082&p_sp=cF9zcmNoPTEmcF9zb3J0X2J5PSZwX2dyaWRzb3J0PSZwX3Jvd19jbnQ9MjAmcF9zZWFyY2hfdGV4dD0mcF9zZWFyY2hfdHlwZT1zZWFyY2hfbmwmcF9wcm9kX2x2bDE9NTAmcF9wcm9kX2x2bDI9NTEmcF9jYXRfbHZsMT0xMDYmcF9jYXRfbHZsMj0mcF9wYWdlPTE*&p_li=)
3	On the Internet Protocol (TCP/IP) Properties sheet General Tab for the wireless or wired LAN interface select "Obtain an IP address automatically" and "Obtain DNS server address automatically". Make sure that "Client for Microsoft Networks" and "File and Print Sharing for Microsoft Networks are installed for this interface.	yes	yes	DHCP service is provided by Microsoft 2003 server which obtains the primary and secondary DNS addresses from the ISP. See **Figure 13.5.2** for a screenshot of these settings.
4	**Disable NetBIOS by opening the "Connection Properties" menu of the wired or wireless NIC, click on the "Advanced" button, navigate to and select the "WINS" tab, and once there, select the "Disable Netbios over TCP/IP" radio button**	yes	yes	Since all computers on the network are running at a Windows 2000 level or later, it is not necessary to have Netbios enabled.
5	**On the Advanced tab of the Network Connection Properties menu, select the checkbox to enable the Internet Connection Firewall and click Settings. This will take you to the Advanced Settings menu from which you can enable the ports and services on the firewall that are necessary to support workgroup networking and Remote Desktop Connection (RDP). The transport layer ports and protocols include the following:** ➔ Remote Desktop Service TCP Port 3389 ➔ **DHCP/BOOTP Server=>Client UDP Port 68** ➔ **Kerberos KSHELL TCP Port 544** ➔ **Kerberos Passwords TCP Port 464** ➔ **Kerberos Passwords UDP Port 464** ➔ **Kerberos Secure Auth. TCP Port 88** ➔ **Kerberos Secure Auth. UDP Port 88**	yes	yes	Because of the complexity of correctly setting up the Microsoft Windows ICF on a computer whose network interface is connected to a Microsoft network, the recommendation from Microsoft is to turn off this firewall. This author disagrees with that guidance and recommends that the firewall be enabled and properly configured to support the necessary protocols. It should be noted that the firewall is stateful and only inspects packets coming into the computer on which the firewall is activated. Thus it will not stop a Trojan from "dialing home" for orders if such Trojan manages

Step #	Implementation Guidance applicable to computers	Applies to		Motivation
		Laptops ?	Desktop ?	
	➔ LDAP TCP Port 389 ➔ LDAP UDP Port 389 ➔ LDAP SSL UDP Port 636 ➔ RPC Mapper TCP Port 135 The ports/protocols shown above which are shown in **bold blue typeface** must be added, since the standard ICF does not include these. The one in black is already configured in the standard ICF. **On the Security Logging Tab of the Advanced Settings Menu, select the "Log dropped packets" and "Log successful connections" checkboxes.** **On the ICMP Tab of the Advanced Settings Menu, select "Allow incoming echo request" checkbox.**			to find its way onto the computer in question. Microsoft has stated that once Service Pack 2 for Windows XP is released, the ICF will be enabled by default however it STILL will not filter outgoing packets/connections. **Figure 13.5.3**, **Figure 13.5.4**, and **Figure 13.5.5** provide screenshots of the sequence of steps to configure the Microsoft Windows ICF. **Important Notes:** **1. Depending upon what other applications are running on the desktops it may be necessary to open up additional protocol/port combinations on the ICF.** **2. Guidance provided in this section is provisional and has not been confirmed in a test lab. Further research is required to confirm that the protocols and ports recommended here are sufficient for proper operating of the computers with the Domain Controller. The protocol/port recommendations were derived from the table in the text, "5.1 Windows 2000/XP/2003 Active Directory"[42] Try these ICF settings on one computer with a wired connection to the network first to confirm that they are acceptable.**
6	Connect the Desktop PC's to the Linksys router using a cat-5 patch cable.	no	yes	Having at least one computer attached to the network using a wired connection facilitates system initialization and troubleshooting of the wireless sub-segment.
7	Install configure, and activate the AP-2000 Access Point	no	no	Activate the 802.11 Access Point (see **Table 10.2.1.3** below for details)

Step #	Implementation Guidance applicable to computers	Applies to		Motivation
		Laptops ?	Desktop ?	
8	On the Wireless Networks Tab of the Network Connection Properties Menu of the 802.11 wireless NIC card, configure the Wireless properties of the card as follows: ➔ Check the checkbox entitled "Use Windows to configure my wireless Settings" ➔ **Select "Advanced" in the lower right hand corner of the menu and then on the "Advanced" menu select the radio button, "Access point (infrastructure) networks only".** ➔ **Leave unchecked the checkbox entitled "Automatically connect to non-preferred networks"** ➔ **Return to the Wireless Networks Tab of the Network Connection Properties Menu and in the "Available Networks" pane, highlight the network for configuration who's SSID should be shown there and entitled "XYZ Enterprise Wireless LAN" and then select "Configure:** **On the "association" tab for the Wireless network properties Menu of XYZ Enterprise Wireless LAN** ➔ **select TKIP from the pull down menu next to "Data Encryption"** ➔ **select "WPA" from the pull down menu next to "Network Authentication"** **On the "authentication" tab for the Wireless network properties Menu of XYZ Enterprise Wireless LAN** ➔ **select "Smart Card of other certificate" from the pull down menu next to "EAP Type"** ➔ **Select the checkbox "Authenticate as computer when computer information is available"** ➔ **Click on the Properties button**	yes	no	This is where the LAP PC wireless NIC is configured to associate with the AP-2000 using the WPA mode of operation. The NIC should also be configured to only associate with infrastructure networks so that accidental association with an ad-hoc (802.11 peer to peer) network cannot occur. Furthermore it should be configured to NOT associate with non-preferred networks. Once this step is completed the wireless NIC's on the laptop PC's should be properly associated with the Proxim Orinoco AP-2000. A quick test of Internet access and workgroup file sharing, and access to the server can be performed at this time. The screenshots that provide the sequence of steps to configure the wireless NIC and wireless network settings on the computers are shown in **Figure 13.5.9** and **Figure 13.5.10** The Microsoft Wireless Zero Configuration (WZC) feature makes it very easy for a user to associate with a wireless network. Therefore it is important to configure this service so that association ONLY occurs with trusted networks that have the requisite level of security which should be at lease WPA-PSK.

Step #	Implementation Guidance applicable to computers	Applies to		Motivation
		Laptops ?	Desktop ?	
	On the Smart Card or other Certificate Properties Menu → Select the radio button "Use a certificate on this computer" → Select the checkbox "Use simple certificate selection [Recommended]" → Select the checkbox "Validate server certificate" Select "ok" on the Smart Card or other Certificate properties menu to close it out. Select "ok" on the Wireless network properties menu to close it out. In the preferred networks pane, make sure that the network whose SSID is "XYZ Enterprise Wireless LAN" is at the top of the list if there is more than one preferred network. Make sure that there are not any preferred networks on the list that are not secured with at least WPA unless the user knows that it is safe to associate with such networks from a security perspective (e.g. in a home with no electronic eavesdroppers).			
9	Check Windows Update Service history log on the computer to confirm that the wireless security rollup described in Microsoft Knowledge Article KB826942 is Installed. If the update has not already been installed then download and install this update using Windows Update Service.	yes	no	This rollup corrects a number of security related flaws in Microsoft's implementation of WPA in Windows XP. The Microsoft KB article can be found at the following url: (http://support.microsoft.com/?kbid=826942)

WPA Implementation Steps on Windows XP Computers
Table 10.2.1.2

Step #	Implementation Guidance applicable to Proxim Orinoco AP-2000	Motivation
1	Install Proxim Orinoco b/g card that is shipped with the base unit into Radio slot A of the AP-2000. Connect the AP-2000 to the Linksys router via a category 5 Cable and power up the unit.	The unit is shipped disassembled and a one step assembly is required
2	Insert the Proxim AP-2000 Configuration CD into the desktop PC CD ROM drive, install the AP-2000 software and run the Scan Tool that is installed on the PC. The Scan Tool will detect AP 2000 by means of its MAC address at which point you can select the line in the display corresponding to that MAC address, click on the Change button and then enter the following items: ➔ Static IP address of the AP (192.168.1.99) ➔ Subnet Mask ➔ Gateway Address	Although the AP-2000 has a pre-configured IP address of 10.0.0.1, this address is incompatible with the Linksys router (without modification to its routing table, which, in turn requires disabling DHCP). The Scan Tool enables discovery of the AP-2000 on the basis of its MAC address and once discovered, the tool permits the sysadmin to configure an IP address. See **Figure 13.5.1** for a screen shot of GUI for the Scan Tool.
3	Using an http browser (e.g. Microsoft Internet Explorer or Netscape Navigator) on the desktop computer connect to the http interface of the AP-2000 at the aforementioned static IP address configured in step 2. The interface is protected with a password and the factory default password is, "password". **Using the browser navigate to the "Management" TAB of the "Configure" www page to change the passwords for HTTP/Telent/SNMP to strong password values which must be in the range of 6-32 characters. Pick a long passphrase of 16 characters or greater**.	The remaining steps of configuring the AP-2000 can be accomplished via the http/html interface.
4	**Download the software/firmware update that supports WPA from the Proxim web site to the desktop computer that serves as the sysadmin computer. Then, on that computer, run the Solarwinds TFTP software that is provided on the Proxim AP-2000 CD, in order to transfer the software/firmware update from the desktop computer to the AP-2000. The AP will reboot itself automatically upon successful completion of the download. The version number of this software/firmware is: v2.4.5**	The Proxim AP 2000 itself has to be updated with WPA support. The url to the required download is as follows: http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/std_adp.php?p_faqid=1221&p_created=1075322819&p_sid=X*P1w73h&p_lva=&p_sp=cF9zcmNoPSZwX3NvcnRfYnk9JnBfZ3JpZHNvcnQ9JnBfcm93X2NudD05NDYmcF9wYWdlPTE*&p_li= This release is designated v2.4.5, and dated Jan 19, 2004. It is an update from the version that was used in the testing that was documented in this paper. This is a maintenance release which contains corrections for 25 specific software faults including some pertaining to WPA.

Step #	Implementation Guidance applicable to Proxim Orinoco AP-2000	Motivation
5	After re-initialization of the AP-2000 with its updated software, again navigate to the AP-2000 http interface and re-enter the configuration management www site. At this point you will configure the following essential items on different tabs/sub tabs of the configuration www page: On the Tab: System, configure: ➔ APName ➔ Location ➔ Contact Name ➔ Contact Email ➔ Contact Phone On the Tab: Interfaces, Sub tab: Operational Mode ➔ Set Wireless A operational mode to "802.11 b/g" On the Tab: Interfaces, Sub tab: Wireless-A ➔ Set SSID = "XYZ Enterprise Wireless LAN" ➔ Select the checkbox "Enable Auto Channel Select" ➔ Set Transmit Rate to "Auto Fallback" On the Tab: Network, Sub tab: Link Integrity ➔ Select the checkbox "Enable Link Integrity" ➔ In the Target IP address Table, create an entry for the IP address of the Cisco/Linksys Router and insert the IP address of the router, 192.168.1.1 into the table. On the Tab: Network, Sub tab: IP Configuration ➔ Select the checkbox "Enable DNS Client " ➔ In the address field "DNS Primary Server IP Address" insert the IP address of the Primary DNS server as configured on the Windows Server 2003 System ➔ In the address field "DNS Secondary Server IP Address" insert the IP address of the Secondary DNS server as configured on the Windows Server 2003 System ➔ In the text field "DNS Client Default Domain Name" insert the Domain Name for the AD domain for this network, sb.local **On the Tab: Management, Sub tab: IP Access Table** ➔ **Configure the IP Access Table to limit the permitted IP source addresses from which the AP http interface will accept incoming connections to the scope of the DHCP address range (i.e. 192.168.1.100-192.168.1.105)** **On the Tab: Management, Sub tab: Services**	This step configures all of the essential parameters of the Proxim Orinoco AP-2000 that will enable communications with the 802.11 b/g NIC cards using WPA. The link integrity feature provides a means for the AP to quickly determine that its connection to the LAN has failed and thereby force the wireless connections to the AP to disassociate. Through this means, wireless users will be informed quickly if the wired segment of the LAN or router has a serious malfunction. Although it is always possible for an attacker to spoof a MAC address and defeat the MAC filtering defense, it is nonetheless recommended by this author to provide another layer of defense by this means. The HTTP interface to the AP-2000 will be secured with SSL and only devices on the wired segment of the LAN will be permitted to have access to this interface.

Step #	Implementation Guidance applicable to Proxim Orinoco AP-2000	Motivation
	➔ Enable HTTPS (Secure WEB) ➔ In the “HTTP Interface Bitmask” pull down menu, select “Ethernet” ➔ Select the checkbox entitled “Enable HTTPS (Secure Web)” On the Tab: Security, Sub tab: Authentication ➔ In the Authentication Mode Pull-down menu for Slot A Select “WPA” On the Tab: Security, Sub tab: MAC Access ➔ Select “Enable MAC Access Control” check box ➔ Select “Passthru” for Operation Type ➔ Enter a MAC access Control Table consisting of the MAC address of each of the 4 wireless NIC’s in the network configuration. On the Tab: Radius, Sub tab: EAP/802.1X Auth ➔ Select the checkbox “Enable Primary EAP/802.1x Authentication Server” ➔ If a backup EAP/802.1x Authentication Server is configured in the network then select the checkbox “Enable Backup EAP/802.1x Authentication Server” ➔ For the Primary EAP/802.1X Authentication Server ➔ Next to the Server Addressing Format in the pull down menu, select “Name” ➔ In the field entitled Server Name/IP Address, insert the FQDN of the IAS server, “sbserver.sb.local” ➔ In the field entitled Shared Secret, insert the Radius shared secret that was referred to in step 4 of Figure 10.2.1.1 ➔ In the field entitled Confirm Shared Secret, insert the Radius shared secret that was referred to in step 4 of Figure 10.2.1.1 ➔ For the Backup EAP/802.1X Authentication Server (if configured) ➔ Next to the Server Addressing Format in the pull down menu, select “Name” ➔ In the field entitled Server Name/IP Address, insert the FQDN of the IAS server, “sbserver.sb.local” ➔ In the field entitled Shared Secret, insert the Radius shared secret that was referred to in step 4 of Figure 10.2.1.1 ➔ In the field entitled Confirm Shared Secret, insert the Radius shared secret that was	

Step #	Implementation Guidance applicable to Proxim Orinoco AP-2000	Motivation
	referred to in step 4 of Figure 10.2.1.1	
6	**Obtain and install an http web server digital certificate and download this to the AP-2000 using the Solarwinds TFP software running on one of the sysadmin computer that is connected to the wired LAN.**	This step provides an additional level of security for the http access to the AP-2000 administrative interface by replacing the Proxim supplied default server digital certificate with one that is specific to the user's organization.
7	Return to LAPTOP PC Implementation Guidance table to complete network activation	See **Table 10.1.1.1** for details.

WPA Implementation Steps on Proxim Orinoco AP-2000
Table 10.2.1.3

10.3 Providing Guest Access to the 802.11 Wireless LAN

In some instances in may be desirable to provide guest users access to a separate 802.11 Wireless LAN so that those users can access the Internet while they are visiting the enterprise or government agency which also has a wireless LAN for its internal users. Because the Proxim Orinoco AP-2000 supports the IEEE 802.1Q Virtual LAN (VLAN) protocol, it is possible to establish such a separate wireless network for guest users. This can be accomplished in one of two ways with the AP-2000:

a) with the use of a radio in the second radio slot in the Proxim Orinoco AP-2000 configured on a separate radio channel and a separate VLAN with its own Service Set Identifier (e.g. "guest wireless network")

or

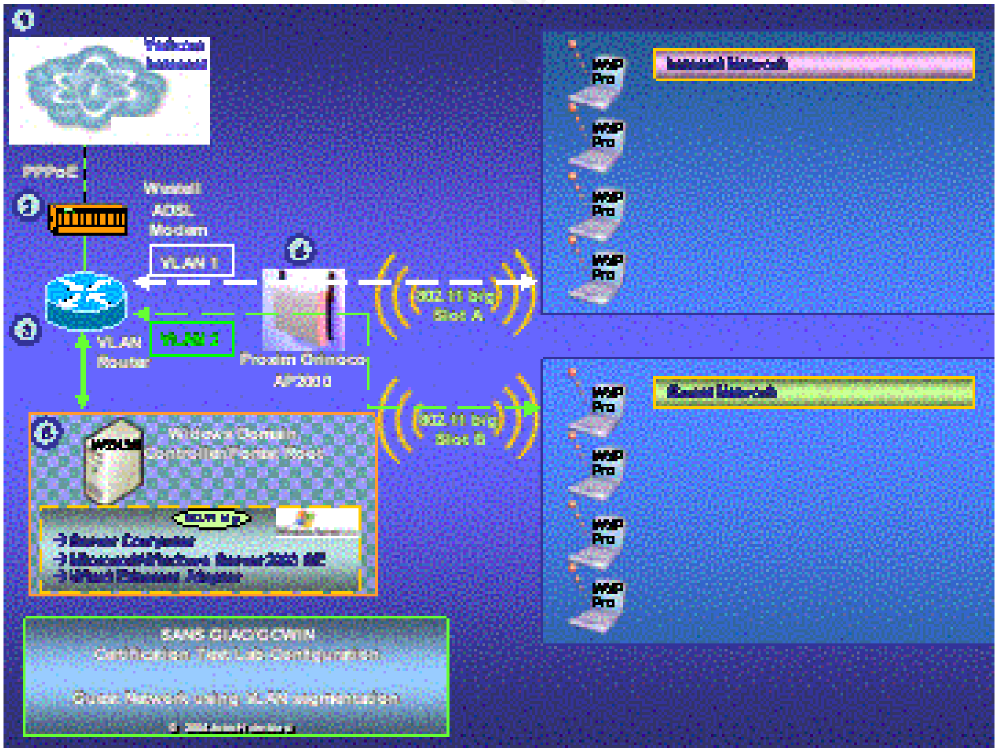
b) with the use of the same radio but a different VLAN with its own Service Set Identifier (e.g. "guest wireless network").

With either approach, and because of the VLAN protocol, it is feasible to provide guest user access while denying these guest users access to the company's internal LAN. With either approach, of course, the router would also have to support the IEEE 802.1Q Virtual LAN (VLAN) protocol and a DHCP server would have to be configured on this VLAN to serve IP addresses to the guest computers. The router must also be capable of preventing traffic from the guest network from being routed to the enterprise or government agency internal LAN unless such traffic flows are properly managed through additional filtering rules.

Approach a) above has a significant security benefit over approach b) and is also more practical to implement because with approach b) it would be necessary for the guest users to either have access to the same WPA Preshared Key if the WPA-PSK method is being used on the internal 802.11 network or, if WPA is being used on the internal

802.11 network, then the guest users would have to have computer and user accounts and digital certificates acceptable to the RADIUS server and Kerberos authentication and authorization service in order to be successfully authenticated by the RADIUS infrastructure.

Also with a second radio, this radio can be configured to utilize WPA-PSK **with its own** Pre-shared key **that is different** from the one used for the internal network in order to provider privacy and authentication for the guest users. The Pre-shared key can be provided to each guest as they request service. Of course, in this scenario, since each guest has the same pre-shared key it is possible that one guest could attempt to eavesdrop on the authentication session of another guest so this solution is not 100% safe for the user. Nonetheless, it is certainly much more secure than if such guests were to go to the nearest coffee shop for wireless Internet access. An additional security measure would be to change the pre-shared key whenever a user leaves the premises. This would not affect guests whose laptop computers or PDA's were still associated with and authenticated to the guest network but the next time such remaining guests tried to associate with the 802.11 guest network, they would have to install the new pre-shared key. **Figure 10.3.1** below depicts an 802.11 wireless network configured with dual b/g radios.



Proxim 802.11 Wireless LAN with Dual Radios for Guest Network Support
Figure 10.3.1

It should also be pointed out that concern has been raised by some security experts about flaws in the VLAN protocol that could lead to security vulnerabilities so this kind of configuration would not be recommended for very high security situations. However, in those situations the use of 802.11 wirelesses is less likely in any case.

The time available to the author to conduct the testing of 802.11 proved insufficient to conduct a test of the VLAN functionality of the Proxim AP-2000. Also, VLAN capable routers are typically much more expensive than their non-VLAN capable SOHO counterparts.

10.4 Additional Security Measures Applicable to Enterprise Wireless Access

Although this paper demonstrates that WPA provides a very robust solution to the weaknesses and consequent vulnerabilities which can lead to the compromise of user authentication, message privacy, and message integrity inherent in the original WEP standard, it may be desirable in some situations to provide additional security measures with respect to 802.11 wireless access. Despite the robust authentication afforded by WPA using EAP-TLS that derives from the use of the methods and technologies of asymmetric encryption and so-called Public Key Infrastructure, the use of these technologies should not be viewed as a security panacea. In their paper, "The Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure"[43] authors Carl Ellison and Bruce Schneier point out the potential weaknesses of PKI, not so much in the technology itself but in the processes and people that are necessary to support it properly. The premise of this paper serves as an argument in favor of using a defense in depth strategy to mitigate the risks of a weakness in any one layer of defense.

Table 10.4 below highlights only a few of the measures that could be taken and which could be easily applied to one or both of the network configurations described in this section **10** of the paper. Because these additional practices will each have their own economic and performance impacts on the system in question, the reader is advised to fully understand their consequences and costs before implementing them.

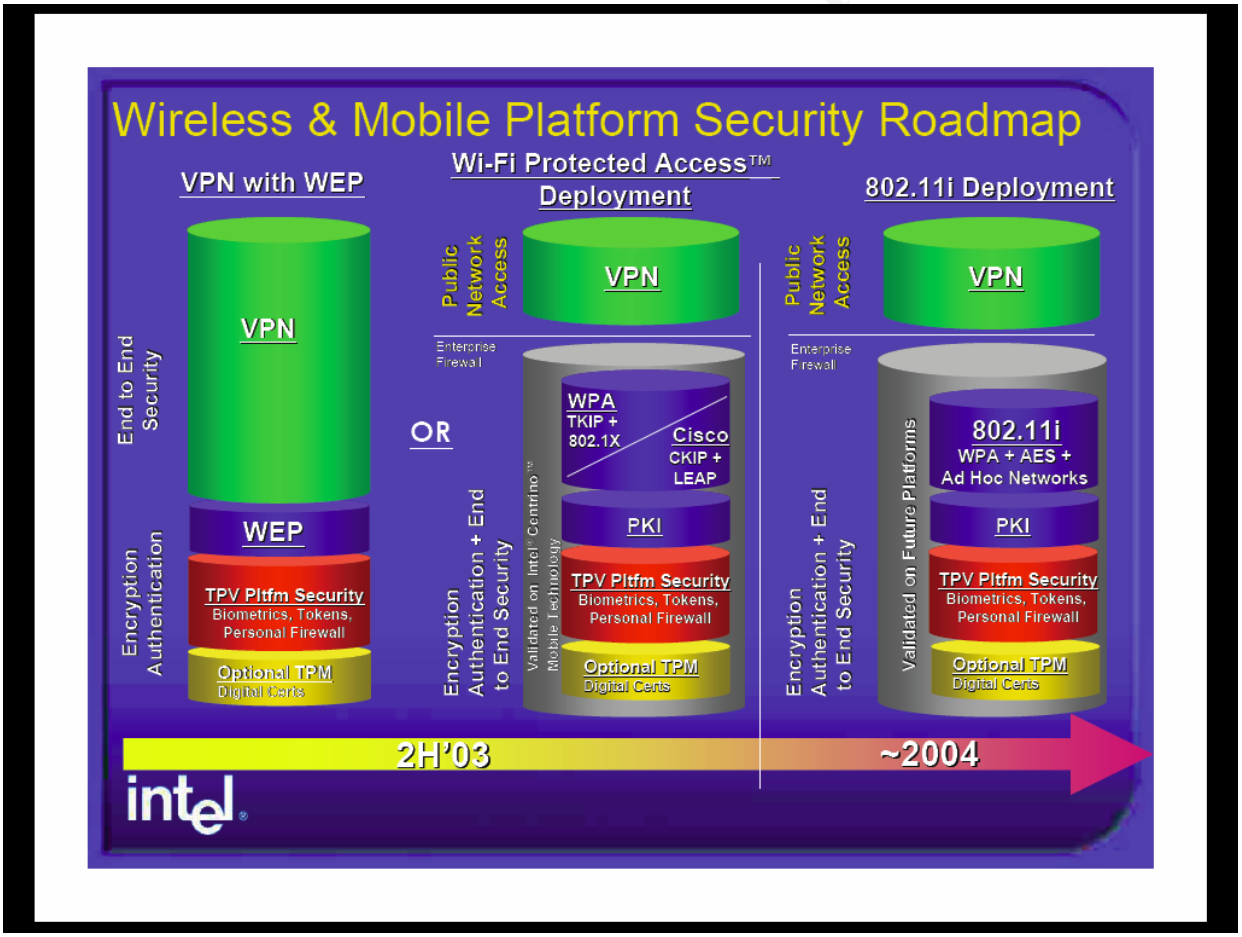
Guidance	Explanation	Applies to	
		WW Network	AD Domain Network
Use Microsoft Encrypting File System	As a part of the wireless user policy, mandate the use of the Microsoft Windows Encrypting File System (EFS) to protect sensitive information stored on the computers which are connected via the 802.11 LAN segment. When deploying EFS, make certain that a Backup EFS recover agent is created using Certificate Services and Group Policy in the case of the AD domain network, and using the windows tool, cipher.exe in the case of Windows XP computers in a WW network.	✓	✓
Use IPSEC	Some might argue that adding a second layer of encryption to that provided by the Temporal Key Integrity Protocol (TKIP) of WPA is overkill. Nonetheless there	✓	✓

	are situations where such a "belts and suspenders" solution may be warranted. Define and implement a common Microsoft Windows IPSEC policy for all of the computers that are connected via the 802.11 LAN segment. This policy should require that ALL communications must be encrypted using the Encapsulating Security Payload (ESP) method of IPSEC. This policy can be deployed manually in the case of a WW network and via Group Policy in the case of an AD domain network. To mitigate the negative performance impact of encrypting/decrypting all communications to/from the systems using IPSEC it is possible to purchase outboard crypto hardware to perform the bulk encryption. Such devices are available for laptop computers as PCMCIA crypto accelerators (e.g. http://www.3com.com/products/en_US/detail.jsp?tab=features&pathtype=purchase&sku=3CRFW102)for approximately $200.		
Use a Firewall to isolate the 802.11 LAN segment	Place a firewall between the wireless LAN segment and the wired LAN segment and open only the protocol/port pairs that are required to allow effective operation of the Windows XP systems on the wireless segment on the rest of the network. Guidance on the required protocol/port pairings that must be opened on this firewall can be found in step 5 of Table 10.1.1.1 and Table 10.2.1.1 for the WW network and the AD domain network respectively.	✓	✓
Limit Hours of Access for Wireless Users	One of the features of Microsoft IAS is the ability as a part of the Connection Request Policy that is defined as a part of the Connection Request Processing for each IAS Server to implement day and time of day restrictions on access. Implement this policy to restrict the times and days of access for the Windows XP systems on the wireless segment of the network	NO	✓
Regularly Inspect Security and Event Logs	The Microsoft based WPA solution in this paper provides integrated Windows computer and user authentication as screenshots in section **13.2** to **13.4** demonstrate. The Windows Security Event log and System Event log can provide information about successful and unsuccessful attempts to log on to the domain in the case of the AD domain network configuration. Daily, or more frequent inspection of these logs can ferret out such suspicious events for further analysis.	NO	✓
MAP Sensitive Folders to Server on the wired LAN	Using Microsoft Windows Group Policy it is possible to redirect (map) folders to another server. This feature can be used then to map the user folders (Application Data, Desktop, My Documents, and Start Menu to a server which is located on the wired segment of the network.	NO	✓
Use Terminal Services for Sensitive apps	Rather than risk the exposure of sensitive data that might be subject to surveillance on a Windows XP system that is connected via an 802.11 wireless LAN segment, the applications which manipulate such data can be housed on a server that is on the wired LAN segment and use terminal services/Remote Desktop Protocol to reach those services from such Windows XP Systems.	✓	✓

Additional Security Guidance for 802.11 LANS
Table 10.4

10.5 Additional Security Measures Applicable to Public Wireless Access

Although the focus of this paper has been on the use Wireless Protected Access^TM behind the firewall in enterprise and government networks based on the Microsoft operating system, it is worth taking a brief look at how WPA fits in to the market for public wireless access services (so-called wireless hot-spot services). In recent years, Intel Corporation has made major investments in wireless technologies as a core component of its Centrino^TM mobile product strategy and has itself recognized the unique requirements for security that derive from use of the wireless medium. At the Intel communications summit in October, 2003 Anthony Andrews[44] articulated Intel's view, shown in **Figure 10.5.1** below, on how 802.11 wireless network security would evolve for both enterprise and public network access.


Wireless & Mobile Platform Security Roadmap
VPN with WEP
Wi-Fi Protected Access™ Deployment
802.11i Deployment
End to End Security
Encryption Authentication
VPN
WEP
TPV Pltfm Security
Biometrics, Tokens, Personal Firewall
Optional TPM
Digital Certs
OR
Public Network Access
Enterprise Firewall
Encryption Authentication + End to End Security
Validated on Intel® Centrino™ Mobile Technology
WPA
TKIP + 802.1X
Cisco
CKIP + LEAP
PKI
802.11i
WPA + AES + Ad Hoc Networks
Validated on Future Platforms
2H'03
~2004
intel

Intel Vision for the Near Term Evolution of 802.11 Security
Figure 10.5.1

As this roadmap indicates, the deployment of first, WPA with TKIP, and then, the full 802.11i standard with the AES, each based on the underpinning of a Public Key

Infrastructure (PKI), will occur during the 2003-2004 timeframe. It should also be noted in this roadmap that Intel advocates the continued use of an end to end Virtual Private network (VPN) overlay for public network access even after the deployment of WPA and 802.11i. This advice is no doubt based on the reality that, it will be quite some time, and years perhaps, before WPA, let alone 802.11i is fully deployed in the world's public network hot-spots. While the use of an IPSEC VPN does not totally eliminate the possibility of a man in the middle attack during the association of the user's 802.11 device with the intended hot-spot access point, VPN technology does provide privacy for the user's traffic once association with the (hopefully) correct access point has been achieved using 802.11 with WEP. In addition, even in the case where the hot-spot service provider can secure the 802.11 wireless link, VPN technology should be applied since the wireless user's traffic will traverse the Internet on its way to and from the enterprise network gateway. Of course these end-to-end VPN's will need to be administered by the enterprise sysadmins even if those same enterprises do not have 802.11 wireless networks of their own. Hence the deployment of Microsoft technologies including IPSEC VPN, Routing and Remote Access (RRAS) and Internet Authentication Service (IAS) are destined to experience robust growth in coming years as an increasing proportion of enterprise network users access their networks using 802.11 wireless communications from both inside the firewall as well as from public hot-spots that are on the open Internet.

11 Conclusions

Wireless Protected AccessTM with EAP/802.1X based authentication represents a vital step forward in the development of wireless LAN infrastructures in both enterprise and government environments. Fortunately, WPA is able to make use of a significant amount of already extant 802.11 wireless infrastructures. Barring any unforeseen cryptographic flaws in WPA the technology will undergo rapid absorption into the market while the IEEE finishes work during 2004 on the even more robust 802.11i standard. CIO's/CTO's and CISO's need to develop a plan of action to get this technology deployed in their wireless infrastructures during the next 12-18 months. While the focus in this paper has been on technical implementation measures for 802.11 wireless network security, perhaps as important, is the need for a sound policy for the use of wireless technologies within the enterprise or government agency. Jamil Farschei has written a two part article entitled "Wireless Network Policy Development[45] and this is a good starting point for the development of such a policy in your own organization. CIO's, CTO's, and CISO's would be well advised to have a robust policy in place which includes the policy with respect to so-called "road warrior", guest users, and home users prior to beginning the deployment of wireless network technology in the firm.

12 Appendix A1 – Test Project Costs and Level of Effort

Table 12.1

provides a very rough estimate of the costs of the major components that were utilized in this test. The Proxim equipment was procured from Wincomm Technologies Corp. (http://www.winncom.com) and the most of the IBM ThinkPad equipment was procured via auction on Ebay and upgraded as necessary with additional RAM/Disk memory. The Microsoft software was procured from Microsoft under the terms of the Action Pack subscription agreement that the author has with Microsoft.

Supplier	Component	Approximate Acquisition Cost ($)
Proxim	AP-2000	495
Proxim	Orinoco Gold a/b/g card	60
Lucent	AP-1000	500
Lucent	Orinoco Gold b card	0
Netgear	WAG511 Wireless Adapter	86
Microsoft	MN-500 Access Point	75
Microsoft	MN-620 Wireless Adapter	
Linksys	WPC54G Wireless Adapter	63
Linksys	BEFSX41 Firewall/Router/Switch	71
IBM	Thinkpad 570 Computers (5)	1,750
Westell	ADSL Modem	50
	Total	3,149

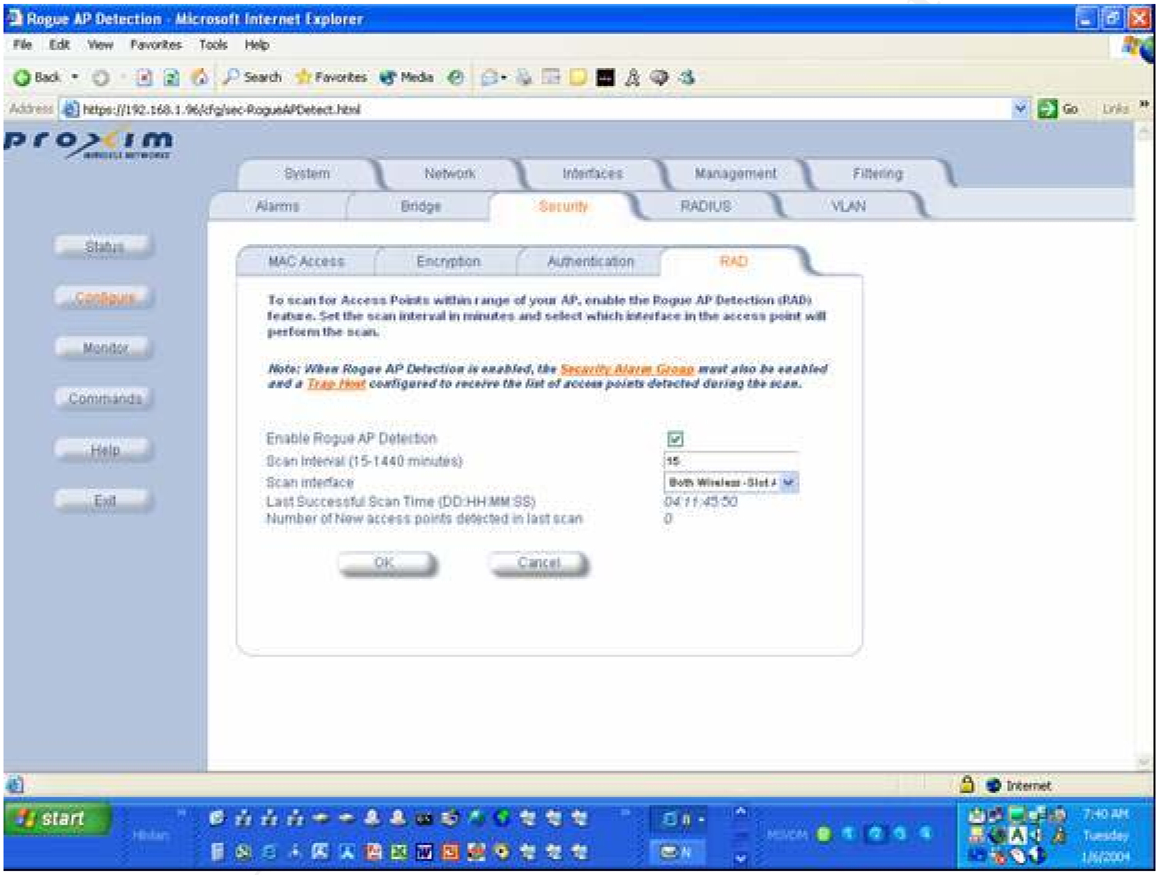
Approximate Project Cost
Table 12.1

The author estimates that the total level of effort in the research, procurement, installation, test execution, and production of this report was of the order of 400 hours including the spent reading the several texts on the subject of 802.11 networks.

13 Appendix A2 – Screen Shots

13.1 Screen Shots of Proxim AP-2000 HTTP Admin Interface

This section provides a sample of screen shots of the Proxim-AP-2000 HTTP Admin interface.

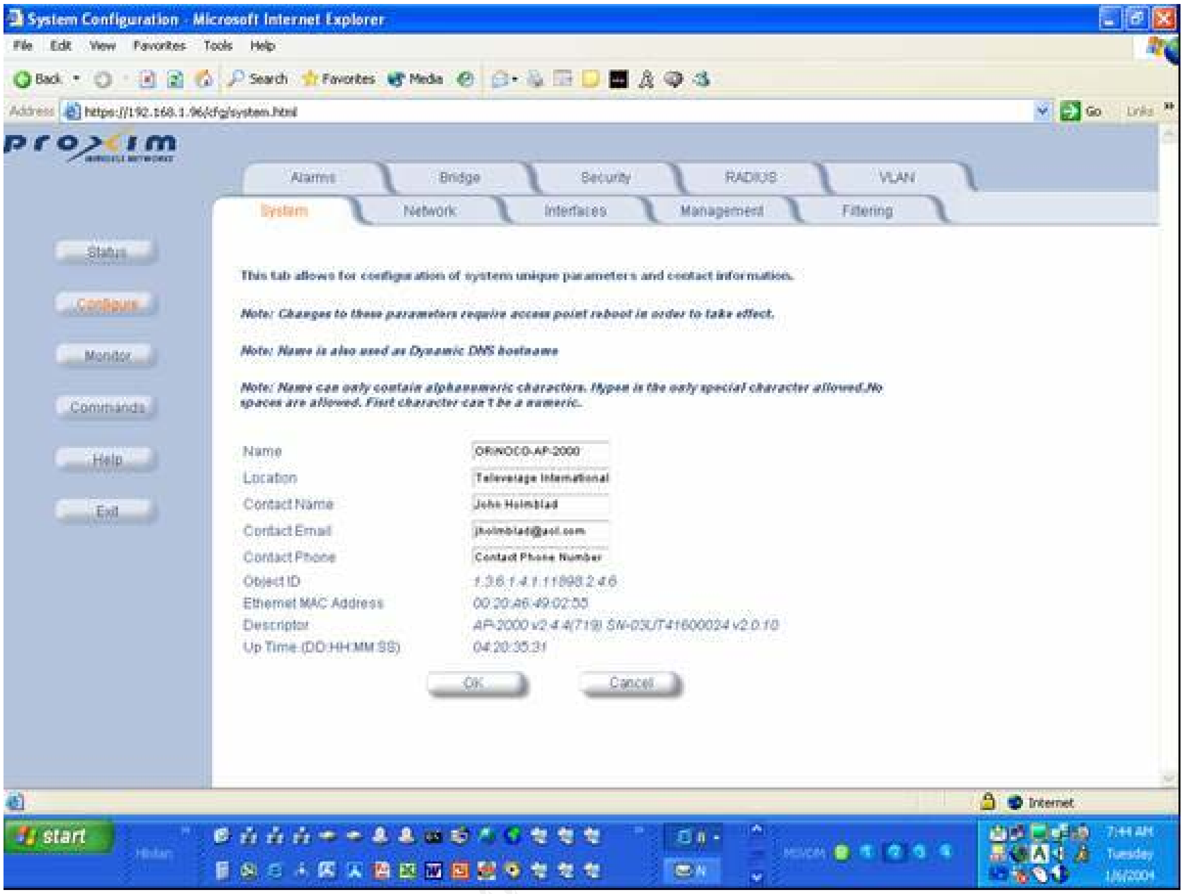

Rogue AP Detection - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.168.1.96/cfg/sec-RogueAPDetect.html
Go Links
proxim
System Network Interfaces Management Filtering
Alarms Bridge Security RADIUS VLAN
Status
Configure
Monitor
Commands
Help
Exit
MAC Access Encryption Authentication RAD
OK Cancel
start
Internet
7:40 AM
Tuesday
1/6/2004

To scan for Access Points within range of your AP, enable the Rogue AP Detection (RAD) feature. Set the scan interval in minutes and select which interface in the access point will perform the scan.

Note: When Rogue AP Detection is enabled, the Security Alarm Group must also be enabled and a Trap Host configured to receive the list of access points detected during the scan.

Enable Rogue AP Detection ☑
Scan Interval (15-1440 minutes) 15
Scan interface Both Wireless - Slot A
Last Successful Scan Time (DD:HH:MM:SS) 04:11:45:50
Number of New access points detected in last scan 0

Proxim AP-2000 Screen Shot #1 – Rogue Activity Detection Tab
Figure 13.1.1



This tab allows for configuration of system unique parameters and contact information.

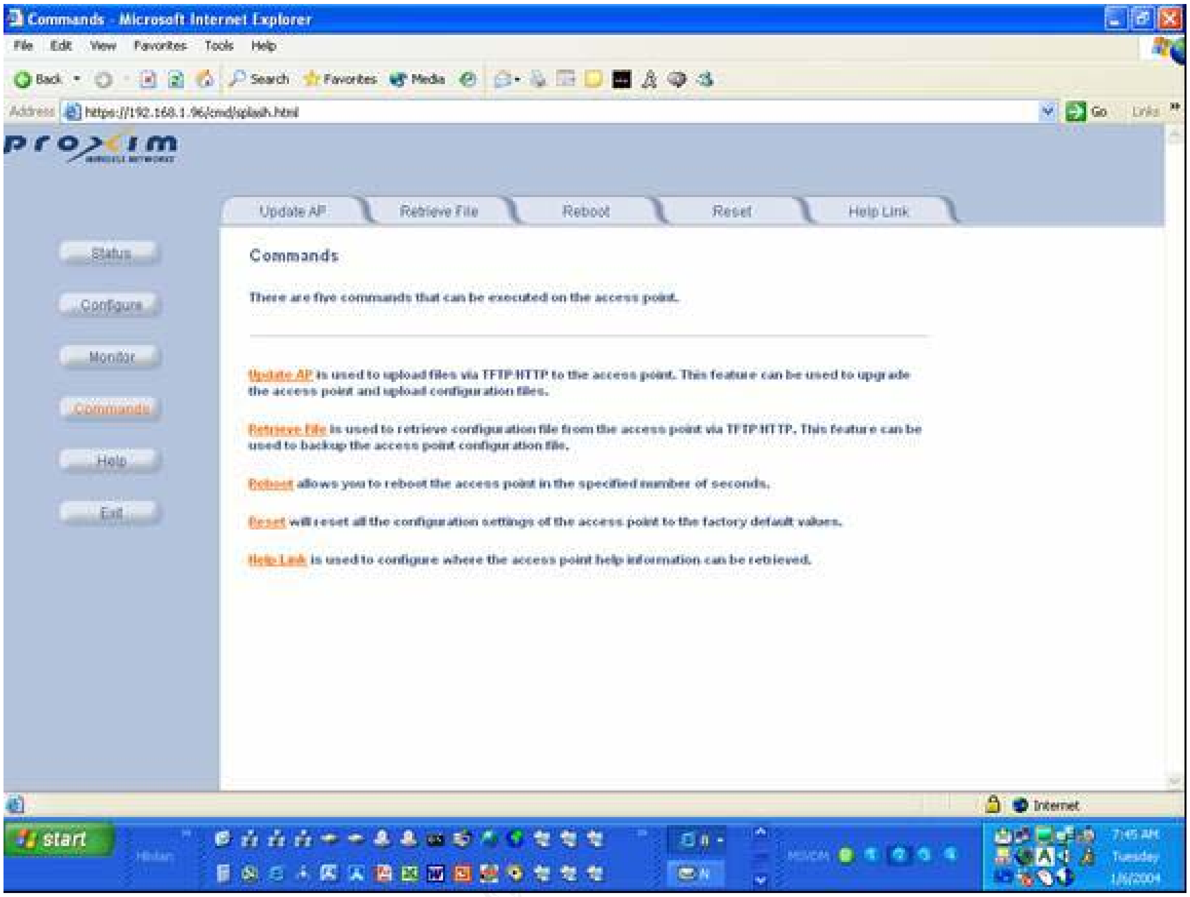
Note: Changes to these parameters require access point reboot in order to take effect.

Note: Name is also used as Dynamic DNS hostname

Note: Name can only contain alphanumeric characters. Hypen is the only special character allowed.No spaces are allowed. First character can't be a numeric.

Name	ORINOCO-AP-2000
Location	Televerage International
Contact Name	John Holmblad
Contact Email	jholmblad@aol.com
Contact Phone	Contact Phone Number
Object ID	1.3.6.1.4.1.11898.2.4.6
Ethernet MAC Address	00:20:A6:49:02:55
Descriptor	AP-2000 v2.4.4(719) SN-03UT41600024 v2.0.10
Up Time (DD:HH:MM:SS)	04:20:35:31

Proxim AP-2000 Screen Shot #2 – System Status Tab
Figure 13.1.2



Commands

There are five commands that can be executed on the access point.

Update AP is used to upload files via TFTP/HTTP to the access point. This feature can be used to upgrade the access point and upload configuration files.

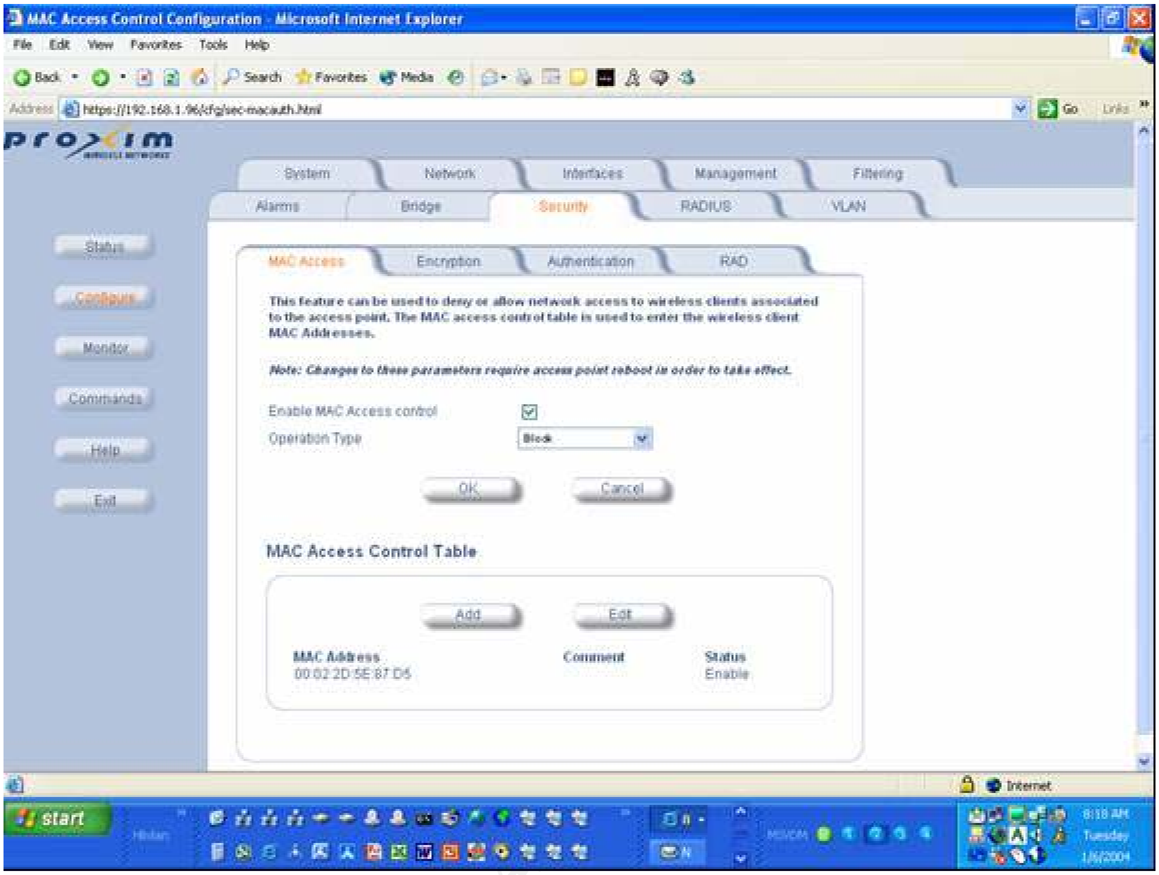
Retrieve File is used to retrieve configuration file from the access point via TFTP/HTTP. This feature can be used to backup the access point configuration file.

Reboot allows you to reboot the access point in the specified number of seconds.

Reset will reset all the configuration settings of the access point to the factory default values.

Help Link is used to configure where the access point help information can be retrieved.

Proxim AP-2000 Screen Shot #3 – Rogue Commands Tab
Figure 13.1.3



This feature can be used to deny or allow network access to wireless clients associated to the access point. The MAC access control table is used to enter the wireless client MAC Addresses.

Note: Changes to these parameters require access point reboot in order to take effect.

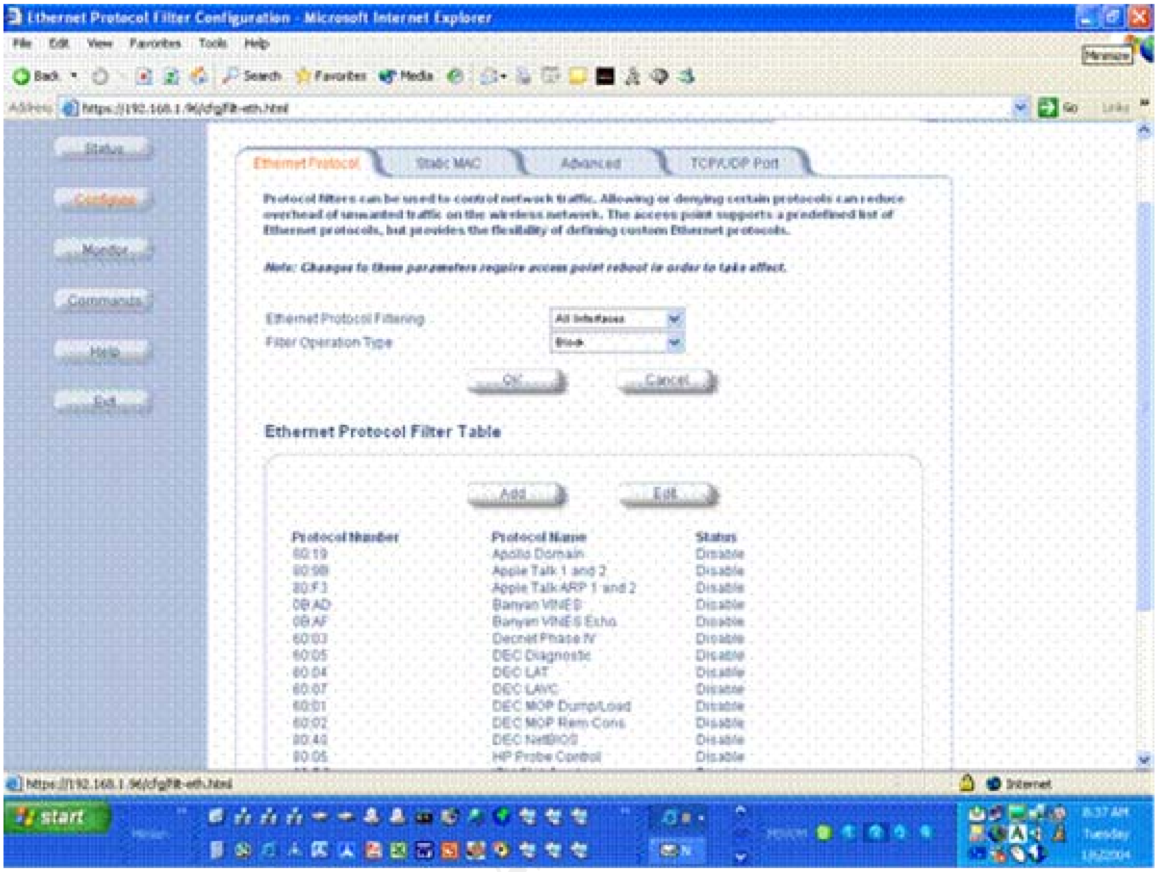
Enable MAC Access control ☑

Operation Type: Block

MAC Access Control Table

MAC Address	Comment	Status
00:02:2D:5E:87:D5		Enable

Proxim AP-2000 Screen Shot #4 – MAC Access TAB
Figure 13.1.4


Ethernet Protocol Filter Configuration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://192.168.1.96/cfgfilt-eth.html
Status
Configure
Monitor
Commands
Help
Exit
Ethernet Protocol
Static MAC
Advanced
TCP/UDP Port
OK
Cancel
Add
Edit
Internet
start

Protocol filters can be used to control network traffic. Allowing or denying certain protocols can reduce overhead of unwanted traffic on the wireless network. The access point supports a predefined list of Ethernet protocols, but provides the flexibility of defining custom Ethernet protocols.

Note: Changes to these parameters require access point reboot in order to take affect.

Ethernet Protocol Filtering: All Interfaces

Filter Operation Type: Block

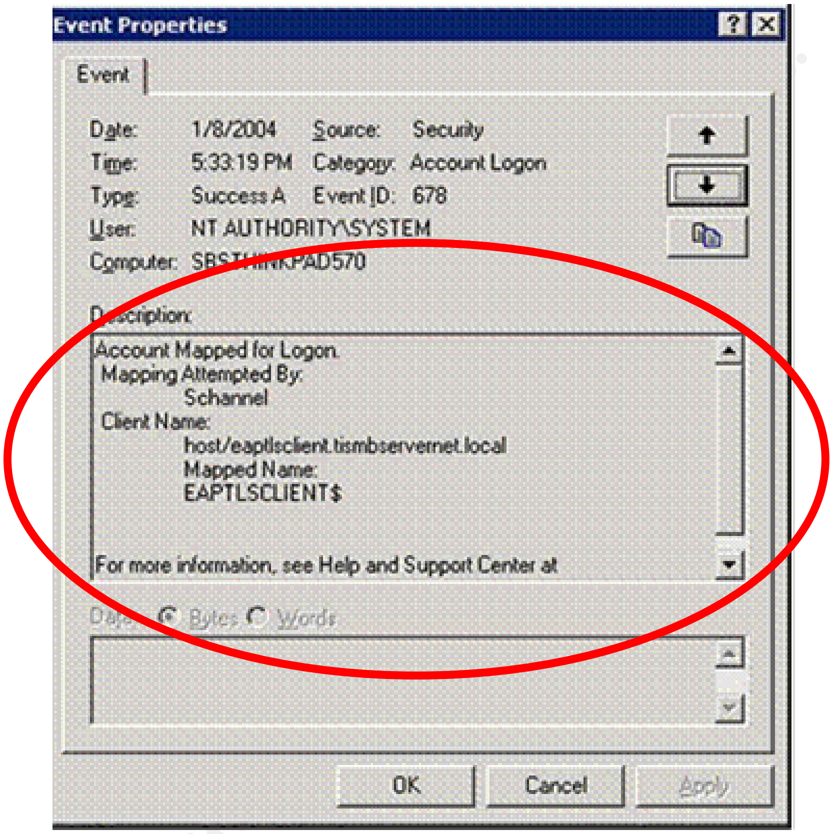
Ethernet Protocol Filter Table

Protocol Number	Protocol Name	Status
80:19	Apollo Domain	Disable
80:9B	Apple Talk 1 and 2	Disable
80:F3	Apple Talk ARP 1 and 2	Disable
0B:AD	Banyan VINES	Disable
0B:AF	Banyan VINES Echo	Disable
60:03	Decnet Phase IV	Disable
60:05	DEC Diagnostic	Disable
60:04	DEC LAT	Disable
60:07	DEC LAVC	Disable
60:01	DEC MOP Dump/Load	Disable
60:02	DEC MOP Rem Cons	Disable
80:40	DEC NetBIOS	Disable
80:05	HP Probe Control	Disable

Proxim AP-2000 Screen Shot #5 – Filtering Tabs
Figure 13.1.5

13.2 Screen Shots of EAP-TLS Authentication Results

This section provides the previously referenced screen shots of the Windows SBS 2003 Premium Edition System Event and Security Event logs which pertain to the EAP-TLS authentication process.

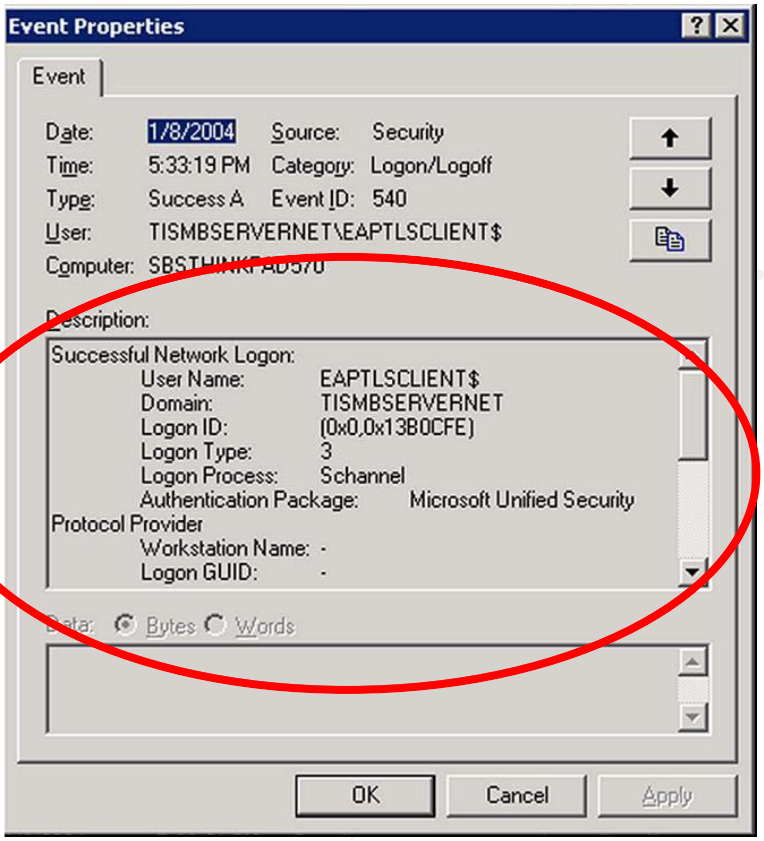


Date: 1/8/2004 Source: Security
Time: 5:33:19 PM Category: Account Logon
Type: Success A Event ID: 678
User: NT AUTHORITY\SYSTEM
Computer: SBSTHINKPAD570

Description:

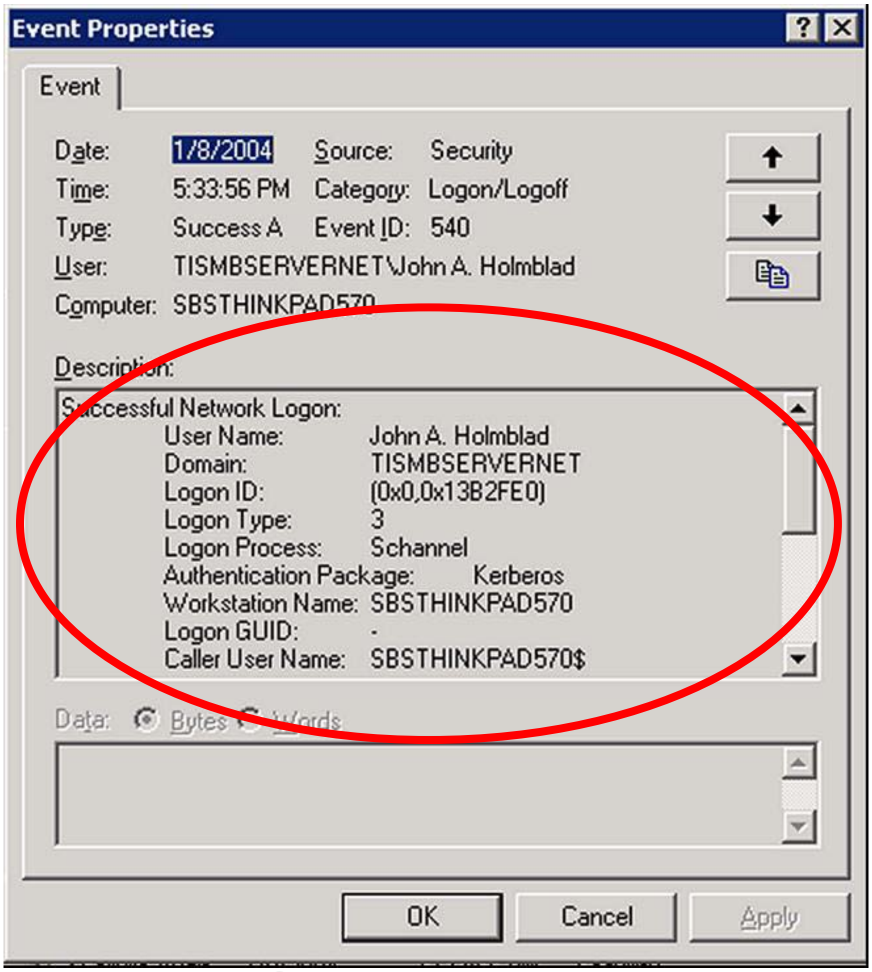
```
Account Mapped for Logon.
 Mapping Attempted By:
          Schannel
 Client Name:
          host/eaptlsclient.tismbservernet.local
          Mapped Name:
          EAPTLSCLIENT$


For more information, see Help and Support Center at
```

EAP-TLS Screen Shot #1– Successful Account Logon Security Event for COMPUTER eaptlsclient.tismbservernet.local
Figure 13.2.1



```
Date:      1/8/2004         Source:    Security
Time:      5:33:19 PM       Category:  Logon/Logoff
Type:      Success A        Event ID:  540
User:      TISMBSERVERNET\EAPTLSCLIENT$
Computer:  SBSTHINKPAD570

Description:
Successful Network Logon:
        User Name:          EAPTLSCLIENT$
        Domain:             TISMBSERVERNET
        Logon ID:           (0x0,0x13B0CFE)
        Logon Type:         3
        Logon Process:      Schannel
        Authentication Package:     Microsoft Unified Security
Protocol Provider
        Workstation Name:   -
        Logon GUID:         -
```

EAP-TLS Screen Shot #2 – Successful Logon/Logoff Security Event for COMPUTER eaptlsclient.tismbservernet.local
Figure 13.2.2



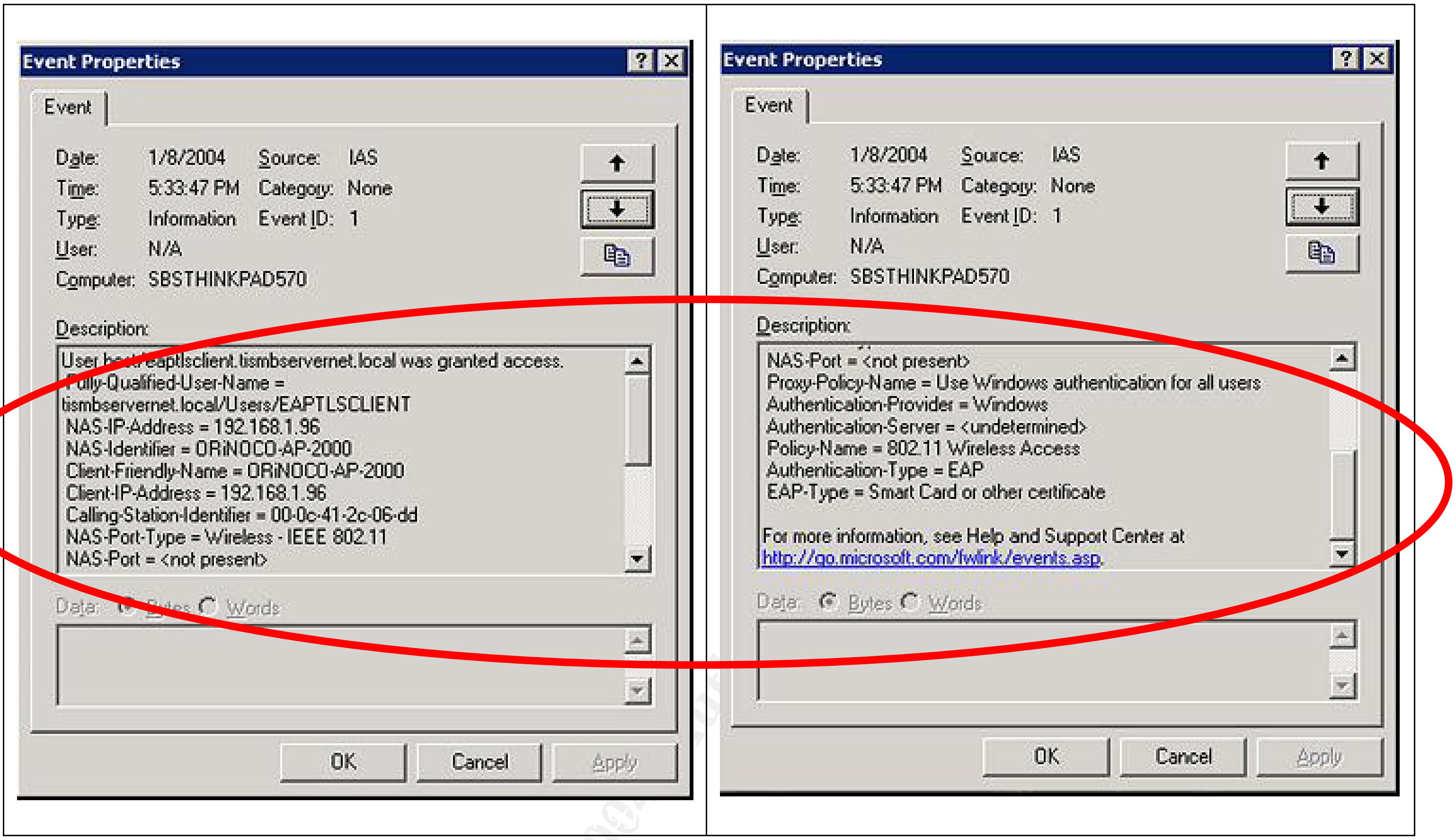
Date: 1/8/2004 Source: Security
Time: 5:33:56 PM Category: Logon/Logoff
Type: Success A Event ID: 540
User: TISMBSERVERNET\John A. Holmblad
Computer: SBSTHINKPAD570

Description:

```
Successful Network Logon:
        User Name:            John A. Holmblad
        Domain:               TISMBSERVERNET
        Logon ID:             (0x0,0x13B2FE0)
        Logon Type:           3
        Logon Process:        Schannel
        Authentication Package:       Kerberos
        Workstation Name:     SBSTHINKPAD570
        Logon GUID:           -
        Caller User Name:     SBSTHINKPAD570$
```

Data: ● Bytes ○ Words

EAP-TLS Screen Shot #3 – Successful Logon/Logoff Security Event for USER John A. Holmblad@tismbservernet.local
Figure 13.2.3



Date: 1/8/2004 Source: IAS
Time: 5:33:47 PM Category: None
Type: Information Event ID: 1
User: N/A
Computer: SBSTHINKPAD570

Description:

```
User host/eaptlsclient.tismbservernet.local was granted access.
 Fully-Qualified-User-Name =
tismbservernet.local/Users/EAPTLSCLIENT
 NAS-IP-Address = 192.168.1.96
 NAS-Identifier = ORiNOCO-AP-2000
 Client-Friendly-Name = ORiNOCO-AP-2000
 Client-IP-Address = 192.168.1.96
 Calling-Station-Identifier = 00-0c-41-2c-06-dd
 NAS-Port-Type = Wireless - IEEE 802.11
 NAS-Port = <not present>
```

Data: ● Bytes ○ Words

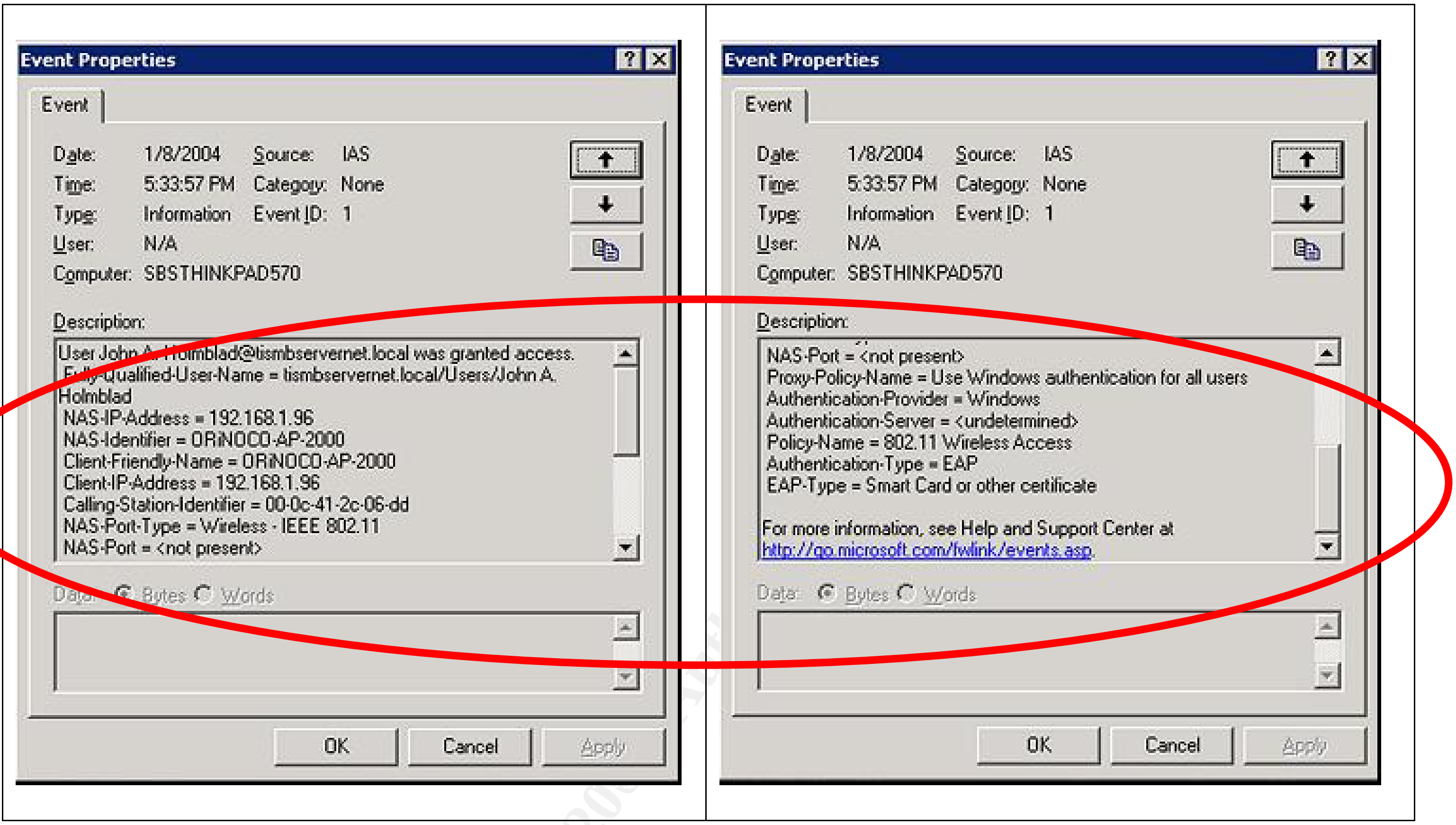
Date: 1/8/2004 Source: IAS
Time: 5:33:47 PM Category: None
Type: Information Event ID: 1
User: N/A
Computer: SBSTHINKPAD570

Description:

```
 NAS-Port = <not present>
 Proxy-Policy-Name = Use Windows authentication for all users
 Authentication-Provider = Windows
 Authentication-Server = <undetermined>
 Policy-Name = 802.11 Wireless Access
 Authentication-Type = EAP
 EAP-Type = Smart Card or other certificate

For more information, see Help and Support Center at
http://go.microsoft.com/fwlink/events.asp.
```

Data: ● Bytes ○ Words

EAP-TLS Screen Shot #4 – Successful IAS Access Grant System Event for COMPUTER eaptlsclient.tismbservernet.local
Figure 13.2.4



Date: 1/8/2004 Source: IAS
Time: 5:33:57 PM Category: None
Type: Information Event ID: 1
User: N/A
Computer: SBSTHINKPAD570

Description:

```
User John A. Holmblad@tismbservernet.local was granted access.
 Fully-Qualified-User-Name = tismbservernet.local/Users/John A.
Holmblad
 NAS-IP-Address = 192.168.1.96
 NAS-Identifier = ORiNOCO-AP-2000
 Client-Friendly-Name = ORiNOCO-AP-2000
 Client-IP-Address = 192.168.1.96
 Calling-Station-Identifier = 00-0c-41-2c-06-dd
 NAS-Port-Type = Wireless - IEEE 802.11
 NAS-Port = <not present>
```

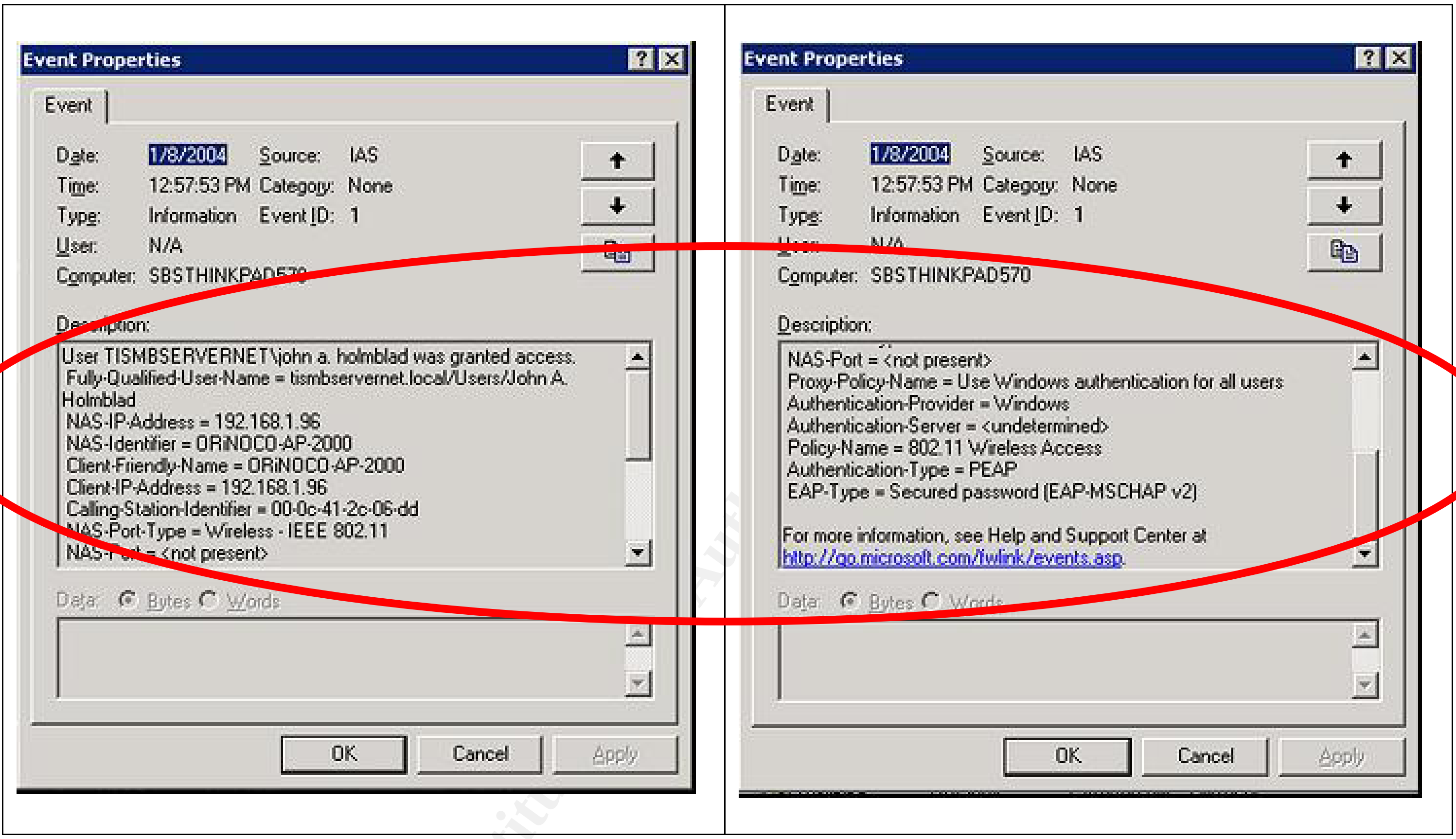
```
 NAS-Port = <not present>
 Proxy-Policy-Name = Use Windows authentication for all users
 Authentication-Provider = Windows
 Authentication-Server = <undetermined>
 Policy-Name = 802.11 Wireless Access
 Authentication-Type = EAP
 EAP-Type = Smart Card or other certificate

For more information, see Help and Support Center at
http://go.microsoft.com/fwlink/events.asp.
```

Data: ● Bytes ○ Words

EAP-TLS Screen Shot #5 – Successful IAS Access Grant System Event for USER John A. Holmblad.tismbservernet.local
Figure 13.2.5

13.3 Screen Shots of PEAP- MS CHAP V.2 Authentication Results with WPA

This section provides the previously referenced screen shots of the Windows SBS 2003 Premium Edition System Event and Security Event logs which pertain to the PEAP-MS CHAP V.2 authentication process when used with WPA encryption.



Date: 1/8/2004 Source: IAS
Time: 12:57:53 PM Category: None
Type: Information Event ID: 1
User: N/A
Computer: SBSTHINKPAD570

Description:

User TISMBSERVERNET\john a. holmblad was granted access.
Fully-Qualified-User-Name = tismbservernet.local/Users/John A. Holmblad
NAS-IP-Address = 192.168.1.96
NAS-Identifier = ORiNOCO-AP-2000
Client-Friendly-Name = ORiNOCO-AP-2000
Client-IP-Address = 192.168.1.96
Calling-Station-Identifier = 00-0c-41-2c-06-dd
NAS-Port-Type = Wireless - IEEE 802.11
NAS-Port = <not present>

Date: 1/8/2004 Source: IAS
Time: 12:57:53 PM Category: None
Type: Information Event ID: 1
User: N/A
Computer: SBSTHINKPAD570

Description:

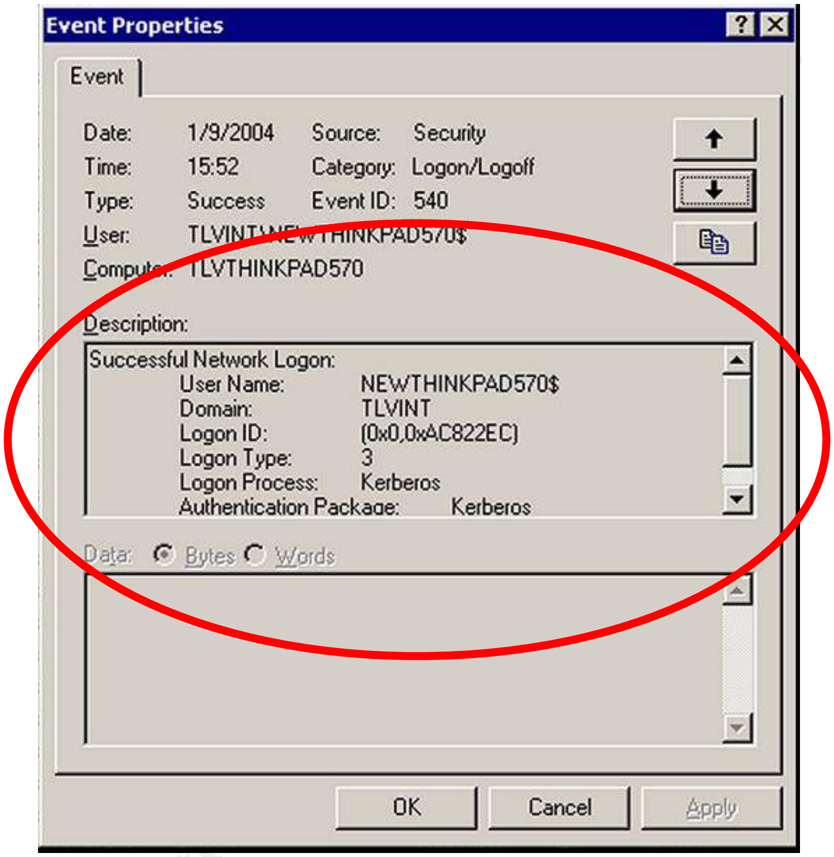
NAS-Port = <not present>
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = 802.11 Wireless Access
Authentication-Type = PEAP
EAP-Type = Secured password (EAP-MSCHAP v2)

For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.

PEAP MS CHAP V.2 with WPA Screen Shot #1 – Successful IAS Access Grant for user TISMBSERVERNET\John A. Holmblad
Figure 13.3.1

13.4 Screen Shots of PEAP- MS CHAP V.2 Authentication Results with WEP

This section provides the previously referenced screen shots of the Windows 2000 Advanced Server System Event and Security Event logs which pertain to the PEAP-MS CHAP V.2 authentication process with WEP encryption.

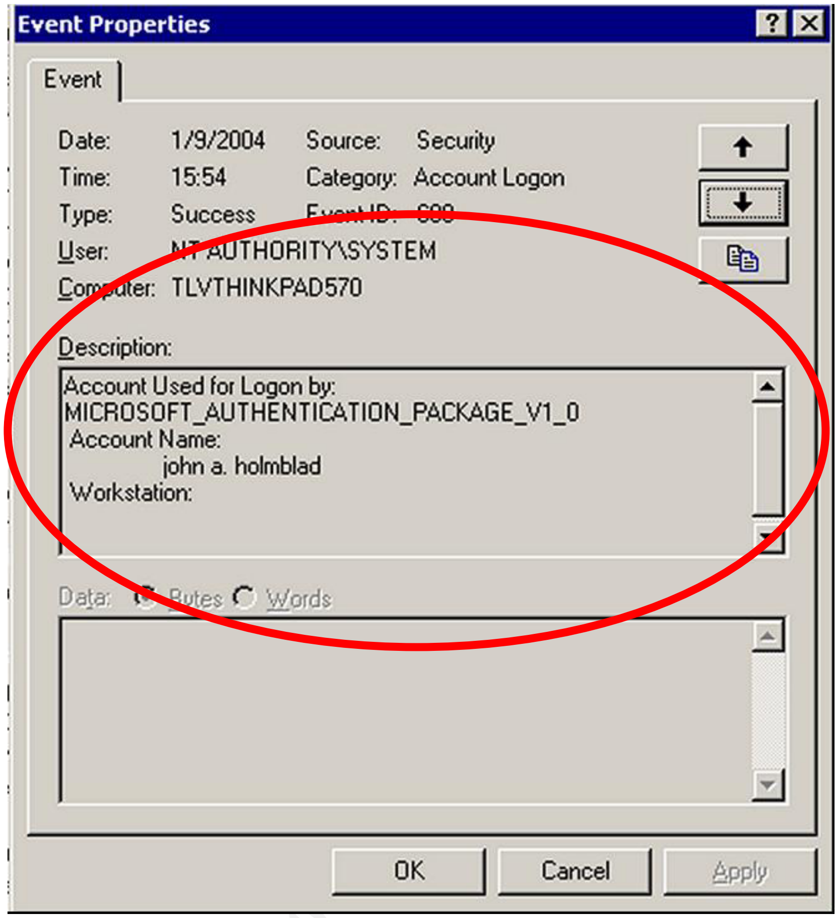


Date: 1/9/2004 Source: Security
Time: 15:52 Category: Logon/Logoff
Type: Success Event ID: 540
User: TLVINT\NEWTHINKPAD570$
Computer: TLVTHINKPAD570

Description:

```
Successful Network Logon:
        User Name:              NEWTHINKPAD570$
        Domain:                 TLVINT
        Logon ID:               (0x0,0xAC822EC)
        Logon Type:             3
        Logon Process:          Kerberos
        Authentication Package:         Kerberos
```

PEAP MS CHAP V.2 with WEP Screen Shot #1 – Successful Logon/Logoff Security Event for COMPUTER newthinkpad570@tlvint.net
Figure 13.4.1



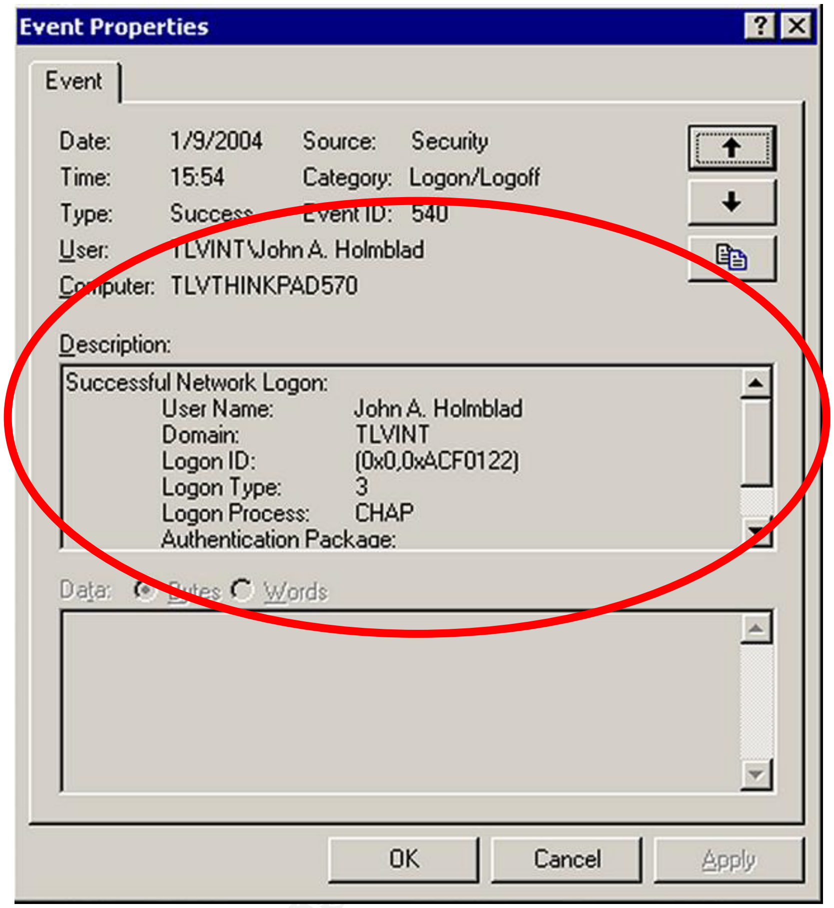
Date: 1/9/2004 Source: Security
Time: 15:54 Category: Account Logon
Type: Success Event ID: 680
User: NT AUTHORITY\SYSTEM
Computer: TLVTHINKPAD570

Description:

```
Account Used for Logon by:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
 Account Name:
              john a. holmblad
 Workstation:
```

Data: ● Bytes ○ Words

PEAP MS CHAP V.2 with WEP Screen Shot #2 – Account Logon Security Event for USER john a. holmblad@tlvint.net Figure 13.4.2



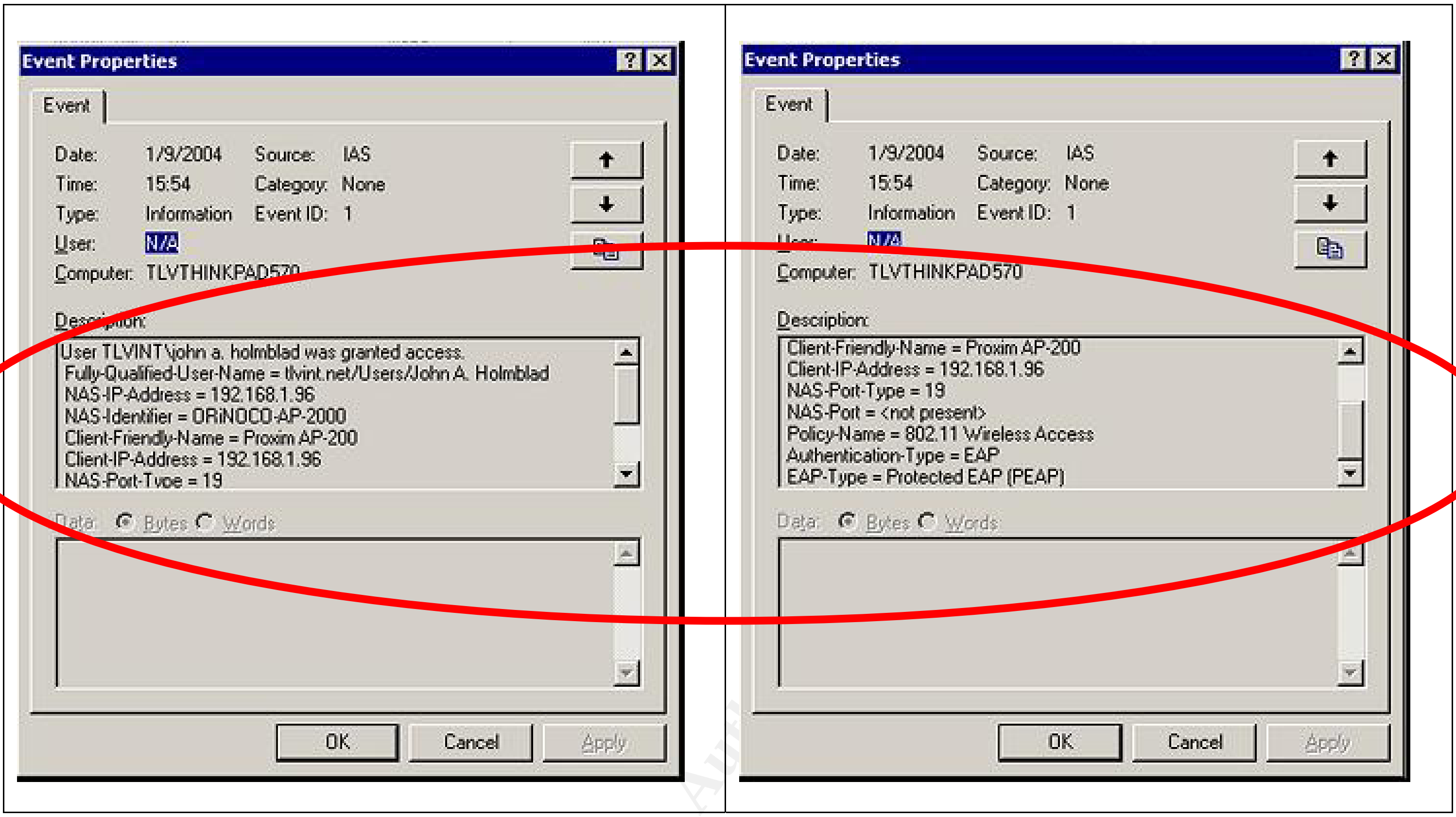
Date: 1/9/2004 Source: Security
Time: 15:54 Category: Logon/Logoff
Type: Success Event ID: 540
User: TLVINT\John A. Holmblad
Computer: TLVTHINKPAD570

Description:

```
Successful Network Logon:
        User Name:              John A. Holmblad
        Domain:                 TLVINT
        Logon ID:               (0x0,0xACF0122)
        Logon Type:             3
        Logon Process:          CHAP
        Authentication Package:
```

Data: ● Bytes ○ Words

PEAP MS CHAP V.2 with WEP Screen Shot #3 – Account Logon/Logoff Security Event for USER john a. holmblad@tlvint.net Figure 13.4.3



Date: 1/9/2004 Source: IAS
Time: 15:54 Category: None
Type: Information Event ID: 1
User: N/A
Computer: TLVTHINKPAD570

Description:

```
User TLVINT\john a. holmblad was granted access.
Fully-Qualified-User-Name = tlvint.net/Users/John A. Holmblad
NAS-IP-Address = 192.168.1.96
NAS-Identifier = ORiNOCO-AP-2000
Client-Friendly-Name = Proxim AP-200
Client-IP-Address = 192.168.1.96
NAS-Port-Type = 19
```

Data: ● Bytes ○ Words

Date: 1/9/2004 Source: IAS
Time: 15:54 Category: None
Type: Information Event ID: 1
User: N/A
Computer: TLVTHINKPAD570

Description:

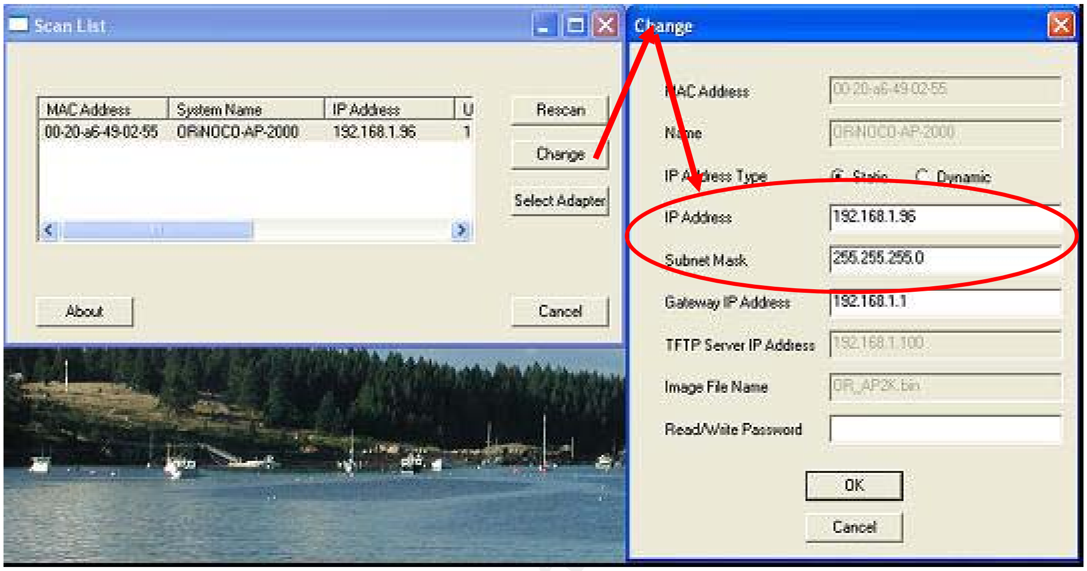
```
Client-Friendly-Name = Proxim AP-200
Client-IP-Address = 192.168.1.96
NAS-Port-Type = 19
NAS-Port = <not present>
Policy-Name = 802.11 Wireless Access
Authentication-Type = EAP
EAP-Type = Protected EAP (PEAP)
```

Data: ● Bytes ○ Words

PEAP MS CHAP V.2 with WEP Screen Shot #4 – Successful IAS Access Grant for user TLVINT\john a. Holmblad
Figure 13.4.4

13.5 Screen Shots Pertaining to Windows Workgroup Network Configuration

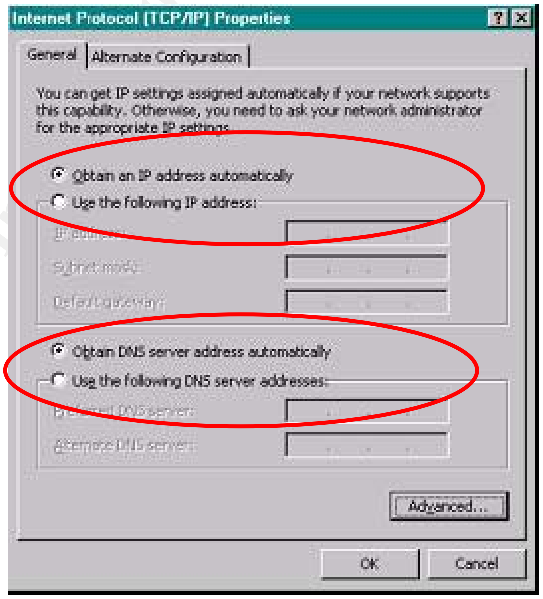
This section provides the previously referenced screen shots that pertain to the Windows Workgroup network design presented in section **10.1.**



MAC Address	System Name	IP Address	U
00-20-a6-49-02-55	ORiNOCO-AP-2000	192.168.1.96	1

MAC Address: 00-20-a6-49-02-55
Name: ORINOCO-AP-2000
IP Address Type: ● Static ○ Dynamic
IP Address: 192.168.1.96
Subnet Mask: 255.255.255.0
Gateway IP Address: 192.168.1.1
TFTP Server IP Address: 192.168.1.100
Image File Name: OR_AP2K.bin
Read/Write Password:

Proxim Orinoco AP-2000 Scan Tool – IP Address Configuration
Figure 13.5.1

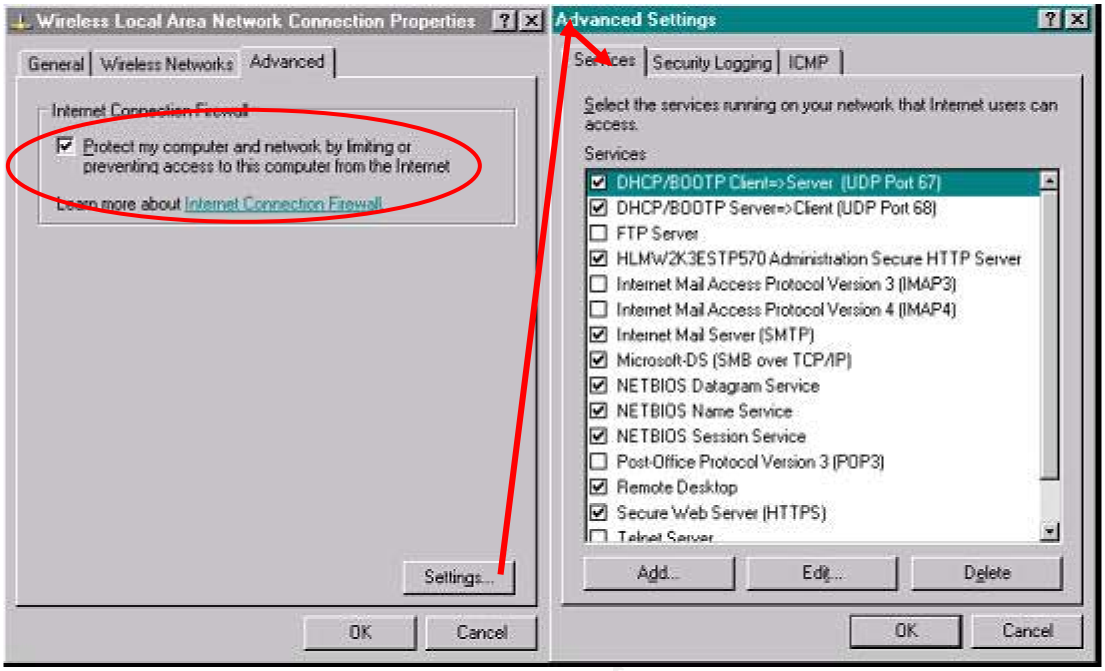


You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:
IP address:
Subnet mask:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

Internet Protocol (TCP/IP) Properties Settings
Figure 13.5.2



Wireless Local Area Network Connection Properties

General | Wireless Networks | Advanced

Internet Connection Firewall

☑ Protect my computer and network by limiting or preventing access to this computer from the Internet

Learn more about Internet Connection Firewall

Advanced Settings

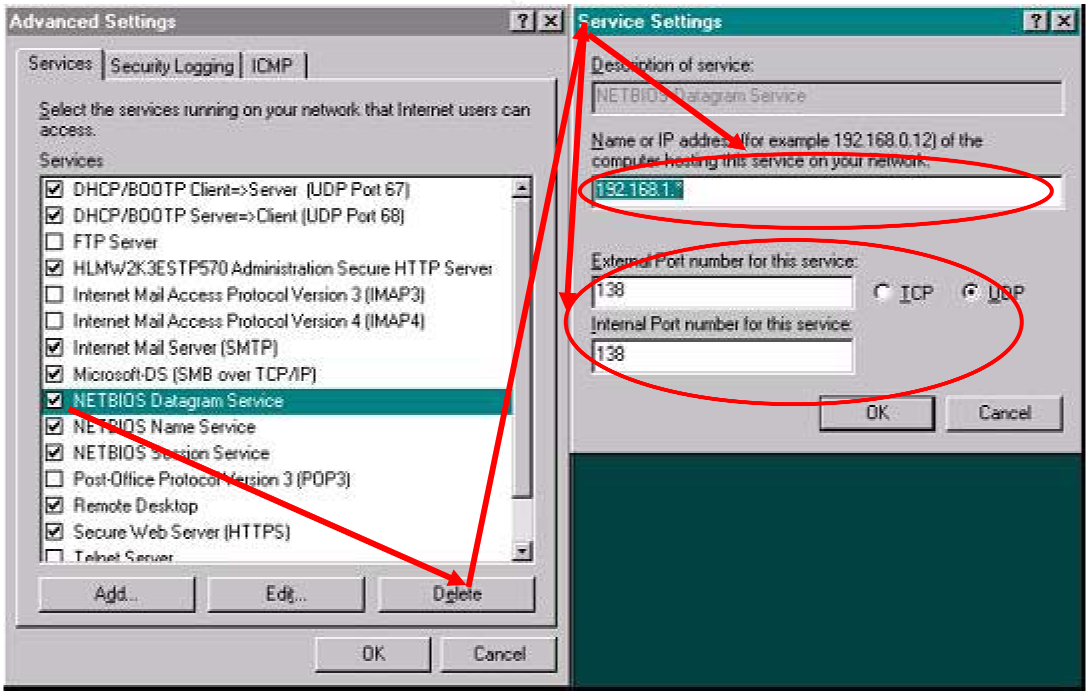
Services | Security Logging | ICMP

Select the services running on your network that Internet users can access.

Services

☑ DHCP/BOOTP Client=>Server (UDP Port 67)
☑ DHCP/BOOTP Server=>Client (UDP Port 68)
□ FTP Server
☑ HLMW2K3ESTP570 Administration Secure HTTP Server
□ Internet Mail Access Protocol Version 3 (IMAP3)
□ Internet Mail Access Protocol Version 4 (IMAP4)
☑ Internet Mail Server (SMTP)
☑ Microsoft-DS (SMB over TCP/IP)
☑ NETBIOS Datagram Service
☑ NETBIOS Name Service
☑ NETBIOS Session Service
□ Post-Office Protocol Version 3 (POP3)
☑ Remote Desktop
☑ Secure Web Server (HTTPS)
□ Telnet Server

Internet Connection Firewall Settings – Services
Figure 13.5.3



Advanced Settings

Services | Security Logging | ICMP

Select the services running on your network that Internet users can access.

Services

☑ DHCP/BOOTP Client=>Server (UDP Port 67)
☑ DHCP/BOOTP Server=>Client (UDP Port 68)
□ FTP Server
☑ HLMW2K3ESTP570 Administration Secure HTTP Server
□ Internet Mail Access Protocol Version 3 (IMAP3)
□ Internet Mail Access Protocol Version 4 (IMAP4)
☑ Internet Mail Server (SMTP)
☑ Microsoft-DS (SMB over TCP/IP)
☑ NETBIOS Datagram Service
☑ NETBIOS Name Service
☑ NETBIOS Session Service
□ Post-Office Protocol Version 3 (POP3)
☑ Remote Desktop
☑ Secure Web Server (HTTPS)
□ Telnet Server

Service Settings

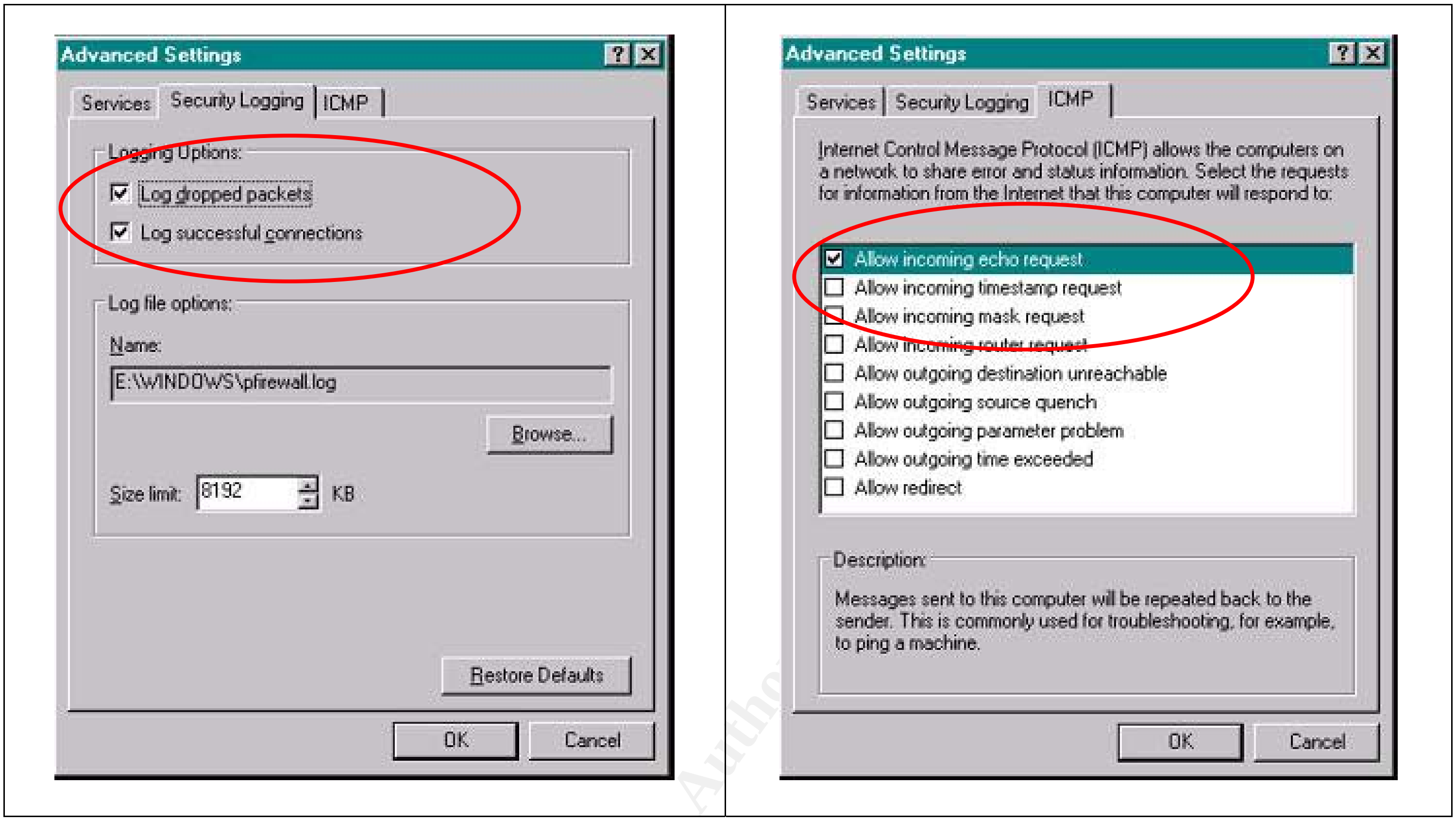
Description of service:
NETBIOS Datagram Service

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.*

External Port number for this service:
138 ○ TCP ● UDP

Internal Port number for this service:
138

Internet Connection Firewall Settings – Services>Service Settings
Figure 13.5.4



Logging Options:

☑ Log dropped packets

☑ Log successful connections

Log file options:

Name: E:\WINDOWS\pfirewall.log

Size limit: 8192 KB

Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to:

☑ Allow incoming echo request

□ Allow incoming timestamp request

□ Allow incoming mask request

□ Allow incoming router request

□ Allow outgoing destination unreachable

□ Allow outgoing source quench

□ Allow outgoing parameter problem

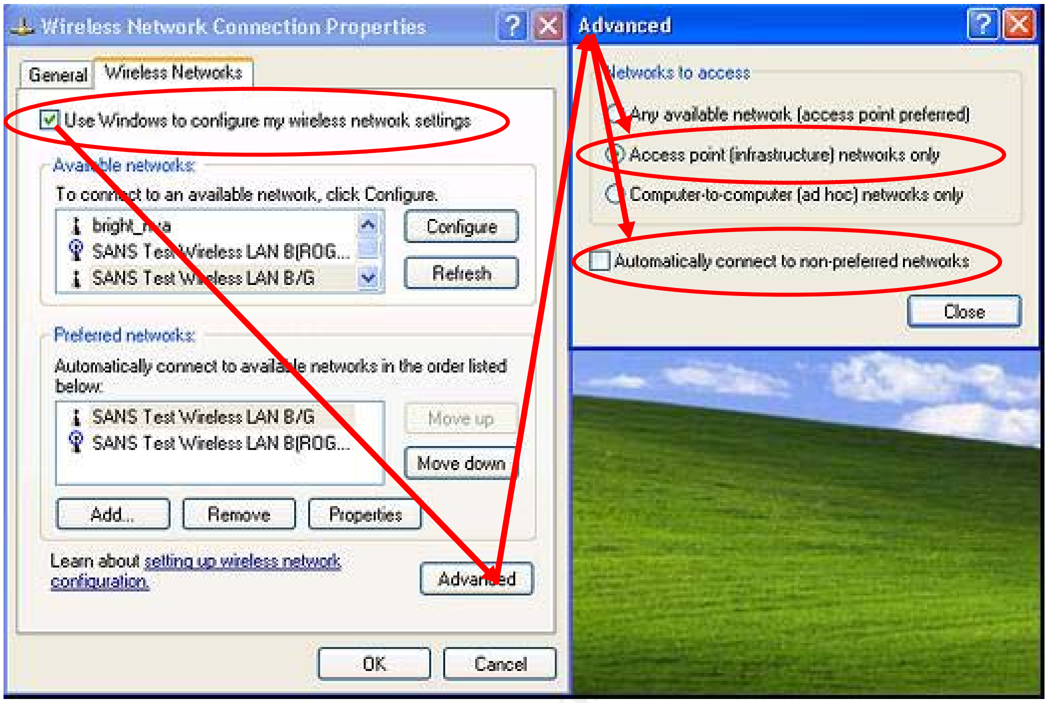
□ Allow outgoing time exceeded

□ Allow redirect

Description:

Messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting, for example, to ping a machine.

Internet Connection Firewall Settings – Security Logging and ICMP
Figure 13.5.5



Wireless Network Connection Properties

General | Wireless Networks

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

- bright_nva
- SANS Test Wireless LAN B|ROG...
- SANS Test Wireless LAN B/G

Preferred networks:

Automatically connect to available networks in the order listed below:

- SANS Test Wireless LAN B/G
- SANS Test Wireless LAN B|ROG...

Learn about setting up wireless network configuration.

Advanced

Networks to access

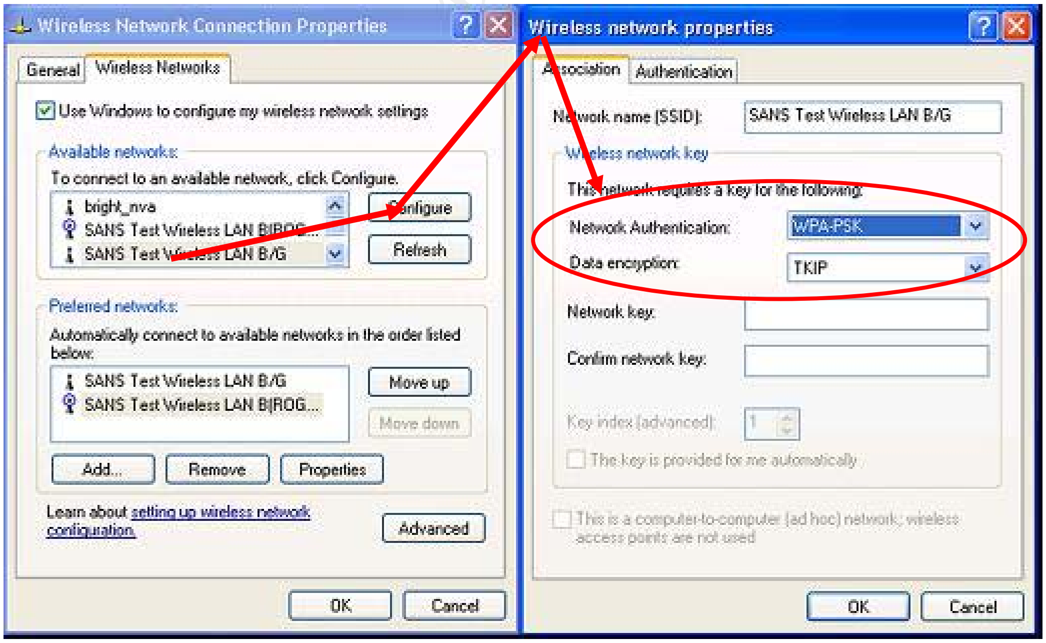
○ Any available network (access point preferred)

● Access point (infrastructure) networks only

○ Computer-to-computer (ad hoc) networks only

□ Automatically connect to non-preferred networks

Connection Properties>Wireless Networks Settings
Figure 13.5.6



Wireless Network Connection Properties

General | Wireless Networks

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

- bright_nva
- SANS Test Wireless LAN B|ROG...
- SANS Test Wireless LAN B/G

Preferred networks:

Automatically connect to available networks in the order listed below:

- SANS Test Wireless LAN B/G
- SANS Test Wireless LAN B|ROG...

Learn about setting up wireless network configuration.

Wireless network properties

Association | Authentication

Network name (SSID): SANS Test Wireless LAN B/G

Wireless network key

This network requires a key for the following:

Network Authentication: WPA-PSK

Data encryption: TKIP

Network key:

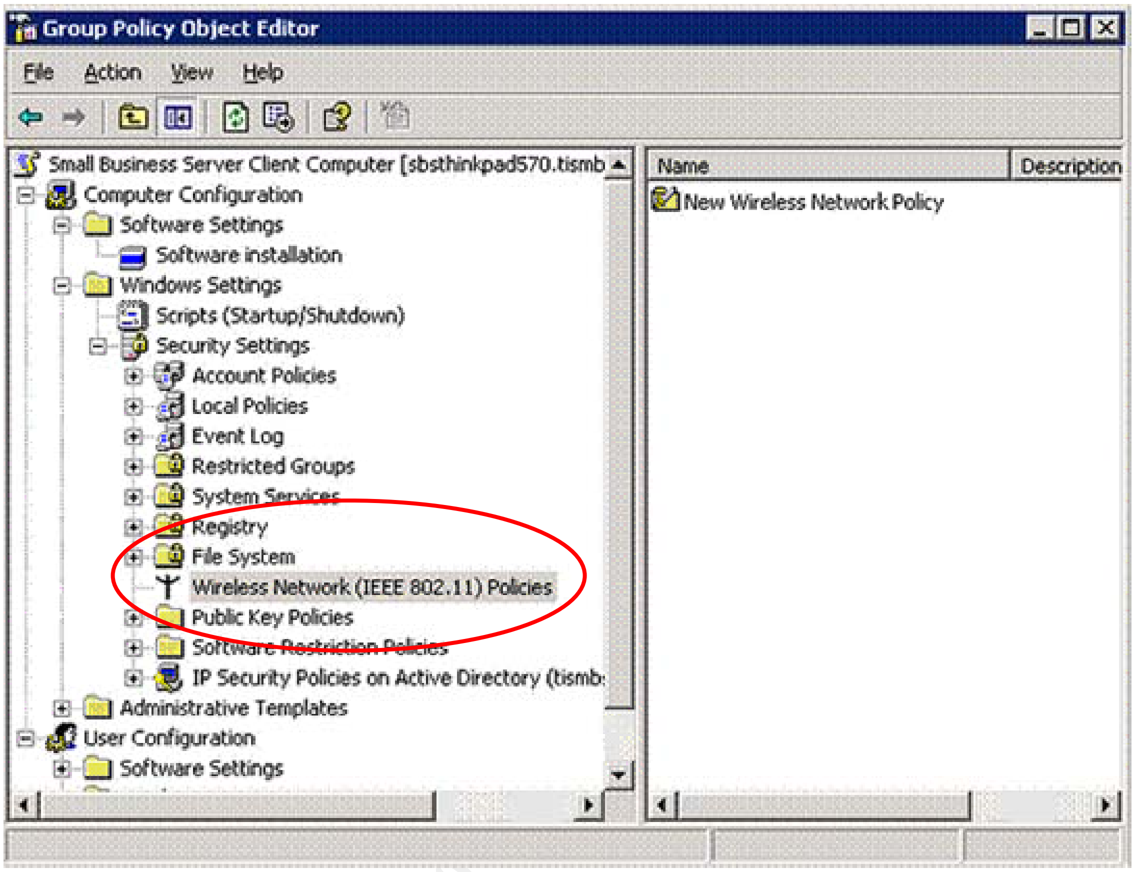
Confirm network key:

Key index (advanced): 1

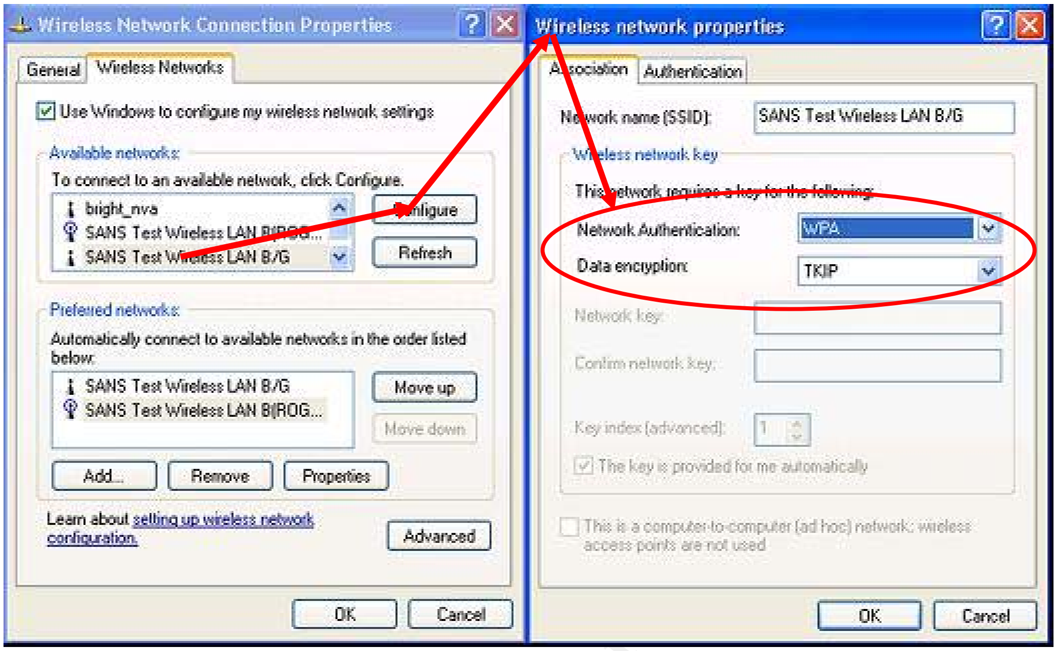
□ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Connection Properties>Wireless Network Properties>WPA-PSK+TKIP
Figure 13.5.7



Group Policy Component for Wireless Network (IEEE 802.11) Policies
Figure 13.5.8



☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

bright_nva
SANS Test Wireless LAN B/ROG...
SANS Test Wireless LAN B/G

Preferred networks:

Automatically connect to available networks in the order listed below:

SANS Test Wireless LAN B/G
SANS Test Wireless LAN B|ROG...

Learn about setting up wireless network configuration.

Network name (SSID): SANS Test Wireless LAN B/G

Wireless network key

This network requires a key for the following:

Network Authentication: WPA

Data encryption: TKIP

Network key:

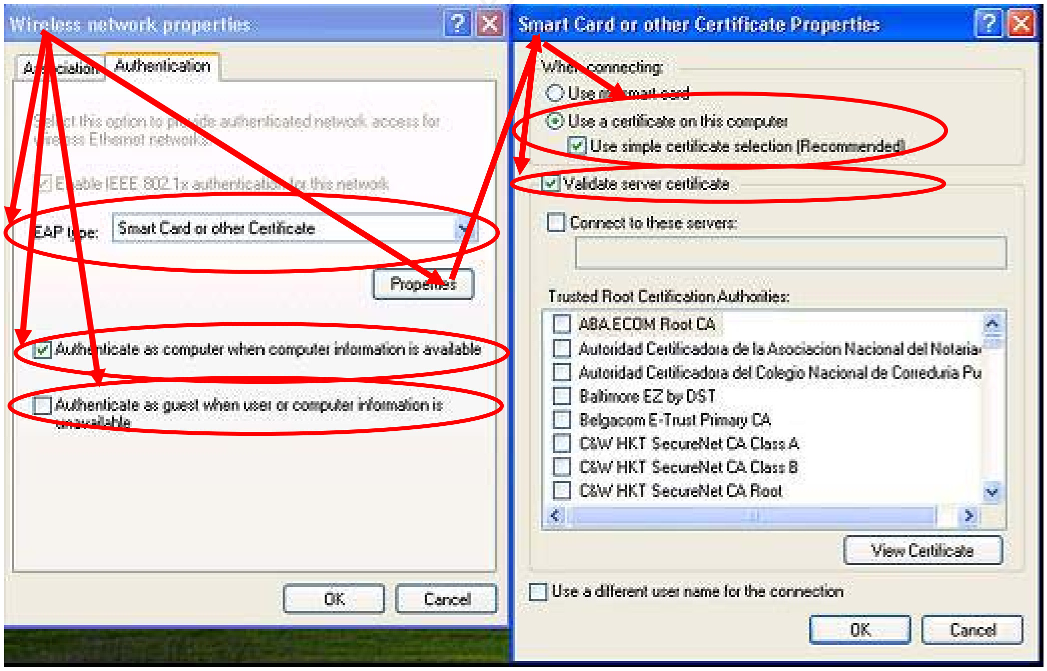
Confirm network key:

Key index (advanced): 1

☑ The key is provided for me automatically

□ This is a computer-to-computer (ad hoc) network; wireless access points are not used

Connection Properties>Wireless Network Properties>WPA +TKIP
Figure 13.5.9


Wireless network properties
Association
Authentication
Properties
OK
Cancel
Smart Card or other Certificate Properties
View Certificate
OK
Cancel

Select this option to provide authenticated network access for wireless Ethernet networks.

☑ Enable IEEE 802.1x authentication for this network

EAP type: Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ ABA.ECOM Root CA
□ Autoridad Certificadora de la Asociacion Nacional del Notaria
□ Autoridad Certificadora del Colegio Nacional de Correduria Pu
□ Baltimore EZ by DST
□ Belgacom E-Trust Primary CA
□ C&W HKT SecureNet CA Class A
□ C&W HKT SecureNet CA Class B
□ C&W HKT SecureNet CA Root

□ Use a different user name for the connection

Connection Properties>Wireless Network Properties>WPA +TKIP
Figure 13.5.10

14 References

[1] Bob O'Hara and Al Petrick. IEEE 802.11 Handbook. IEEE Press. 2001. pp 1-18.

[2] Washington Post, Sunday October 19, 2003.

[3] Gordon Moore. Cramming More Components onto Integrated Circuits. Electronics, Vol. 38, number 8, April 19, 1965.

[4] George Gilder, Metcalfe's Law and Legacy, *Forbes ASAP,* September 13, 1993.

[5] IEEE, Standards for Wireless LANs: Wireless LAN medium access control (mac) and physical layer (phy) specifications, IEEE Standard 802.11,1997.

[6] Wi-Fi Alliance, Wireless Protected Access, Version 2.0, April 29, 2003.

[7] IEEE, Standards for LAN/MAN Bridging & Management: Standard for port based network access control, IEEE Standard 802.x, March 2001.

[8] IEEE, Standards for Wireless LANs: Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security Draft 3.0.

[9] ITU, The Directory: Public-key and attribute certificate frameworks.

[10] ISOC/IETF, RFC 2284, PPP Extensible Authentication Protocol.

[11] ISOC/IETF, RFC 2246, Transport Layer Security.

[12] ISOC/IETF, RFC 2716, EAP - Transport Layer Security.

[13] Ashwin Palekar, Dan Simon, Glen Zorn, Joe Salowey , Hao Zhou, S. Josefsson, Internet DRAFT Protected EAP Protocol (PEAP) Version 2, draft-josefsson-pppext-eap-tls-eap-07.txt.October 26, 2003.

[14] ISOC/IETF, RFC 2138, Remote Authentication Dial-in User Service.

[15] http://www.alpcom.it/hamradio/marconi.html.

[16] John Edney, William A. Arbaugh, Real 802.11 Security, Wi-Fi Protected Access and 802.11i, Addison-Wesley, 2004.

[17] R.L. Rivest, the RC4 Encryption Algorithm, RSA, Data Security Inc., March 12, 1992. (Proprietary).

[18] Bruce Schneier, Applied Cryptography, Second Edition, Wiley, 1996. pp 397-398.

[19] Bruce Schneier, IBI,. p 398.

[20] John Edney. IBID, pp 67-103.

[21] Nikita Borisov, Ian Goldberg, David Wagner. Intercepting Mobile Communications: The Insecurity of 802.11, Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, July 16-21, 2001.

[22] S, Fluhrer, I. Martin, and A. Shamir, Weaknesses in the key scheduling algorithm of RC4, Eighth Annual workshop on Selected Areas in Cryptography, August 2001.

[23] Peter Judge, Wi-Fi hacks are getting more serious, Techworld, December 19, 2003.

[24] Agere Systems, Principles of 802.1x security Orinoco Technical Bulletin 048/B, Agere Systems Inc. April 2002.

.

[25] John Edney, IBID, pp 122-128.

[26] Department of Commerce National Institute of Standards and Technology, Standard: FIPS Publication 197: Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES).

[27] IBID, John Edney, pp 231-259,

[28].Agere Systems IBID, P2

[29] IEEE, Standards for Wireless LANs: Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security Draft 3.0, IBID, pp 87-129.

[30] Microsoft, Step-by-Step Guide for Setting Up Secure Wireless Access in a Test Lab, Microsoft document, May, 2003

[31] Microsoft, Enterprise Deployment of Secure 802.11 Networks Using Microsoft Windows, Microsoft document, February, 2003.

[32] Joseph Davies, Deploying Secure 802.11 Networks with Microsoft Windows, Microsoft Press. 2003, pp 165-235.

[33] Jahanzeb Khan and Anis KHwaja, Building Secure Wireless Networks with 802.11, Wiley. 2003, pp 231-238.

[34] Warwick Ford, Michael S. Baum, Secure Electronic Commerce Second Edition, Prentice Hall PTR, 2001, PP 152-157.

[35] IEEE, Standards for Wireless LANs: Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security Draft 3.0, IBID, pp 4-6.

[36] Microsoft, Windows XP Wireless Deployment Technology and Components Overview. Microsoft document - Wi-Fi.doc, October, 2003.

[37] ISOC/IEFT RFC 2284, IBID.

[38] Wavelink. Wavelink Mobile Manager How it Works Whitepaper. Wavelink. October 2002.

[39] Carol Bailey and Dr. Thomas W. Shinder. Configuring Windows 2000 Without Active Directory. Syngress Publishing, Inc.2001.

[40] Christopher Hertel. Implementing CIFS: The Common Internet File System. Prentice Hall PTR; 1st edition. August 14, 2003.

[41] IBID. Microsoft, Enterprise Deployment of Secure 802.11 Networks Using Microsoft Windows, Microsoft document

[42] Jason Fossen. Track 5 – Securing Windows. 5.1 Windows 2000/XP/2003 Active Directory. The SANS Institute. 2003. pp 18-19.

[43] Carl Ellison and Bruce Schneier. Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure. Computer Security Journal, Volume XVI, November 1, 2000. pp1-8.

[44] Anthony Ambrose. Impact of Wireless Communications. Intel Communications Summit 2003. p12.

[45] Jamil Farshehi. Wireless Network Policy Development (Part I and Part II). http://www.securityfocus.com/infocus/1732 and http://www.securityfocus.com/infocus/1735