



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Auditing Systems, Applications, and the Cloud (Audit 507)"  
at <http://www.giac.org/registration/gсна>

**An Audit of a Wireless Demonstration Network Implementing Cisco Aironet 1200**

**An Auditor's Perspective**



Oliver Viitamaki

GSNA Practical V2.1 - San Francisco - December 2002

<b>Table of Contents</b>	<b>Page Number</b>
<b>Abstract/Summary</b>	<b>6</b>
<b>GSNA Assignment 1 – Research in Audit, Measurement Practice and Control</b>	<b>6</b>
Identify the System to be Audited	6
Risk Evaluation	10
Current State of Auditing, with respect to a Wireless Access Point	14
<b>GSNA Assignment 2 – Create an Audit Checklist</b>	<b>19</b>
Audit Checklist	19
Scope	19
A. ADMINISTRATIVE SECTION	23
B. ORGANIZATIONAL STRUCTURE / SYSTEM OVERVIEW, DOCUMENTATION, & TRAINING	28
C. Fieldwork Cisco Aironet 1200, Installation	34
D. Fieldwork Cisco Aironet 1200, Configuration	37
E. Fieldwork Cisco Aironet 1200, Management	57
F. Fieldwork Cisco Aironet 1200, Unauthorized Wireless Access Point Detection	61
G. Fieldwork Cisco Aironet 1200, 802.11b wireless card installation and Configuration	64
H. Fieldwork Cisco Aironet 1200, Laptop System vulnerability assessment with 802.11 b card installed.	66
<b>GSNA Assignment 3 – Audit Evidence</b>	<b>71</b>

<b>Conduct the Audit</b>	<b>71</b>
<b>A. ADMINISTRATIVE SECTION</b>	<b>73</b>
<b>B. ORGANIZATIONAL STRUCTURE / SYSTEM OVERVIEW, DOCUMENTATION, &amp; TRAINING</b>	<b>73</b>
<b>C. Fieldwork Cisco Aironet 1200, Installation</b>	<b>74</b>
<b>D. Fieldwork Cisco Aironet 1200, Configuration</b>	<b>75</b>
<b>E. Fieldwork Cisco Aironet 1200, Management</b>	<b>115</b>
<b>F. Fieldwork Cisco Aironet 1200, Unauthorized Wireless Access Point Detection</b>	<b>116</b>
<b>G. Fieldwork Cisco Aironet 1200, 802.11b wireless card installation and Configuration</b>	<b>120</b>
<b>H. Fieldwork Cisco Aironet 1200, Laptop System vulnerability assessment with 802.11 b card installed.</b>	<b>120</b>
<b>Overview Residual Risk</b>	<b>122</b>
<b>Measure the Residual Risk</b>	<b>124</b>
<b>Evaluate the Audit</b>	<b>125</b>
<b>GSNA ASSIGNMENT 4 – Audit Report</b>	<b>126</b>
<b>Audit Report</b>	<b>126</b>
<b>Executive Summary</b>	<b>126</b>
<b>Audit Findings</b>	<b>128</b>

<b>A. ADMINISTRATIVE SECTION</b>	<b>128</b>
<b>B. ORGANIZATIONAL STRUCTURE / SYSTEM OVERVIEW, DOCUMENTATION, &amp; TRAINING</b>	<b>128</b>
<b>C. Fieldwork Cisco Aironet 1200, Installation</b>	<b>129</b>
<b>D. Fieldwork Cisco Aironet 1200, Configuration</b>	<b>130</b>
<b>E. Fieldwork Cisco Aironet 1200, Management</b>	<b>131</b>
<b>F. Fieldwork Cisco Aironet 1200, Unauthorized Wireless Access Point Detection</b>	<b>132</b>
<b>G. Fieldwork Cisco Aironet 1200, 802.11b wireless card installation and Configuration</b>	<b>132</b>
<b>H. Fieldwork Cisco Aironet 1200, Laptop System vulnerability assessment with 802.11 b card installed</b>	<b>133</b>
<b>Background/Risk</b>	<b>133</b>
<b>    All Items marked as Fail during the Audit</b>	<b>133</b>
<b>Audit Recommendations</b>	<b>139</b>
<b>Costs</b>	<b>139</b>
<b>Compensating Controls</b>	<b>140</b>
<b>Appendix A</b>	<b>141</b>
<b>Appendix B</b>	<b>145</b>
<b>Appendix C</b>	<b>148</b>
<b>REFERENCES</b>	<b>156</b>
<b>Figures</b>	
<b>    Figure 1: Acme Development Wireless Demo Network</b>	<b>6</b>
<b>    Figure 2: Cisco Default (from the Factory) settings</b>	<b>7</b>
<b>    Figure 3: Acme Development Wireless Demo Network</b>	<b>10</b>
<b>    Figure 4: Risk Areas</b>	<b>19</b>
<b>    Figure 5: Acme Development Wireless Demo Network with Monitoring Equipment</b>	<b>20</b>
<b>    Figure 6: Risk Avoidance Matrix.</b>	<b>22</b>
<b>    Figure 7: Wireless LAN Security Levels</b>	<b>39</b>
<b>    Figure 8: Acme Development Wireless Demo Network with Monitoring Equipment</b>	<b>71</b>

Figure 9: Base Access Point Hardware Version Revision Information	76
Figure 10: 802.11b Card inserted in Base Station Revision Information	77
Figure 11: 802.11b Antenna Hardware Information	78
Figure 12: Password Screen	79
Figure 13: Access Point Summary Status Screen, after Log On	80
Figure 14: Access Point Software Versions Screen	81
Figure 15: 802.11b Card Software Versions Screen	82
Figure 16: Captured Beacon Frames	83
Figure 17: Screen Shot of Media Disconnected Status	87
Figure 18: Broadcast SSID Details	88
Figure 19: WEP Details Before Filtering	89
Figure 20: Non WEP Encrypted Packets	90
Figure 21: Additional Link Layer Security Features Disabled	92
Figure 22: MAC based Access and Association Screen Shot (Association)	93
Figure 23: MAC based Access and Association Screen Shot (Disassociation)	94
Figure 24: MAC based Access and Association Screen Shot Summary Status	95
Figure 25: No MAC based Address Filters on Access Point	96
Figure 26: Authenticator Configuration	97
Figure 27: Remote Authentication Dial-in User Service (RADIUS) based Access control	100
Figure 28: RADIUS with Extensible Authentication Protocol (EAP)	102
Figure 29: DHCP IP addressing	108
Figure 30: DHCP IP addressing packet Capture	109
Figure 31: "Special Use IP Address Assignment"	111
Figure 32: SNMP Disabled	112
Figure 33: Password Screen	114
Figure 34: Unauthorized Wireless Networks Sample 1	117
Figure 35: Unauthorized Wireless Networks Sample 2	118
Figure 36: Unauthorized Wireless Networks Sample 3	119
Figure 37: Acme Development Wireless Demo Network	126

## Abstract/Summary

The following paper is an Audit of a Product Demonstration Network in a DMZ environment, implemented with a Wireless, Cisco Access Point, mixed vendor end devices, a Radius server, and Firewall. The audit Checklist developed is tailored to this environment, and current as of January 2003, but can be adapted to other implementations.

## GSNA Assignment 1 –Research in Audit, Measurement Practice and Control

### Identify the System to be Audited

The focus of the audit (performed by Audit Co.) is a Cisco Aironet 1200 Series Wireless Access Point, and how it is integrated into the network at Acme Development Company, to provide access for a customer demonstration facility. The audit is written from an Auditor's perspective, for the purpose of insuring that the Wireless network is compliant with company policy, and that the IT manager can sign off the implementation as an acceptable risk. Thus, this is a technical audit of the system. The Cisco Aironet 1200 access point supports both 802.11a and 802.11b radio and Antenna units. The 802.11a unit will be outside the scope of the audit, as it will not be placed into service for another 6 months. The network being audited is depicted in Figure 1 below.

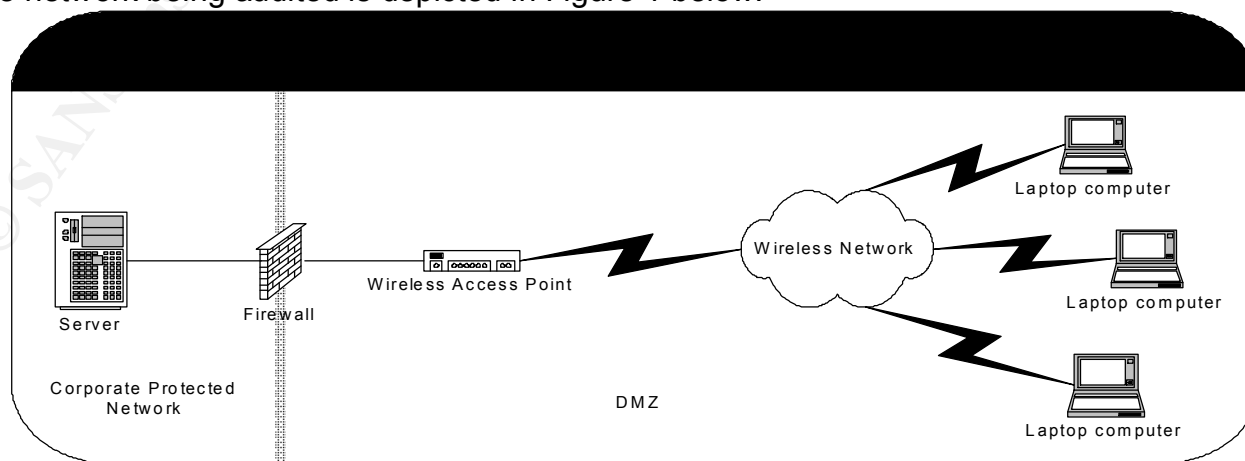


Figure 1

Aironet 1200 Wireless Network Access Point

Model: AIR – AP1200

Serial Number: VDF0641Q2M3

System Software Versions: System Firmware version: 12.01a

System Web pages Version 12.01

Hardware Version: Revision F0

Consisting of

AIR-MP20B Wireless LAN Module 2.4 GHz 11Mbps: Revision A0

Serial Number: VMS06330HL9

Radio Software Version: 5.02.12

Antenna Hardware Version B0

**Figure 2: Cisco Default (from the Factory) settings**

Parameter	Default Value
System Name	AP1200-xxxxxx (the last six characters of the unit's MAC address)
Terminal Type (on serial interface only)	Teletype
Config Server Protocol	DHCP
IP address	10.0.0.1
IP Subnet Mask	255.255.255.0



Default Gateway	255.255.255.255
AP Radio: Internal (2.4-GHz radio)	
SSID	tsunami
Role in Radio Network	Root Access Point
Optimize Radio Network For	Throughput
AP Radio: Module (5-GHz radio)	
SSID	tsunami
Role in Radio Network	Root Access Point
Optimize Radio Network For	Throughput
Ensure Compatibility With	(none selected)
SNMP Admin. Community	(blank)

A typical wireless client system will be used as a representative example of any other clients, which could be connected as part of the Demonstration facility. It is beyond the scope of this Audit to sample all of the configurations of any of the other wireless clients, which may be connected to this facility.

Toshiba 6100 Laptop Serial Number: Y2062765Q

Operating System: Windows XP

Built in Wireless Card MAC Address: 00:02:2D:6B:28:00

Cisco 2.4 GHz Aironet Wireless Card Information used for monitoring

Cisco Aironet Wireless card Model AIR-PCM350 Serial Number: VEM064207W1

Cisco Aironet Wireless card Hardware Version: Revision K0

Cisco Aironet Wireless card Software Version: Windows NDIS Driver: 8.2.3

802.11b Radio Firmware: 4.25.30

Boot Block version: 1.50

Additional Software

Cisco Aironet Wireless Client Utilities: Version 5.05.001 for Windows

Cisco Secure ACS Version 3.1

The Laptop used for auditing Toshiba 6100 Laptop Serial Number: Y2063981P

Operating Systems: Windows XP and Redhat Linux 2.4.18-24.8.0

Built in Wireless Card MAC Address: 00:02:2D:6F:77:BC

Etherpeek version 5.0.0

Airopeek NX version: 1.2.0

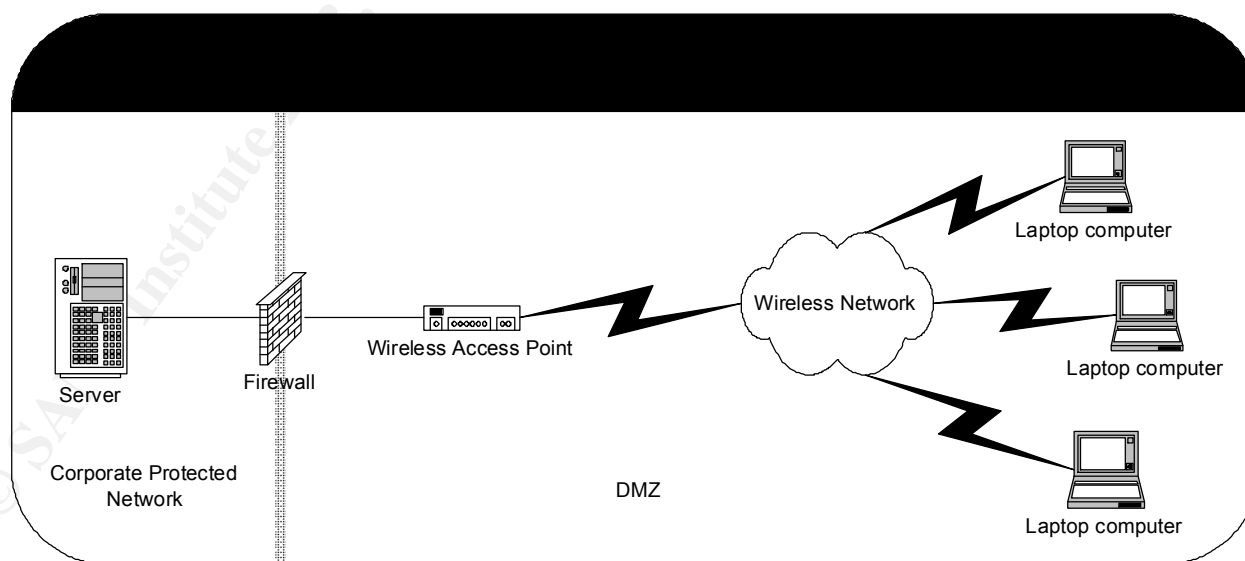
Nessus version 1.2.6 with Plugins 1.2.6

The Laptop used for monitoring the wired network Toshiba 4300 Laptop Serial Number 80012869J

Operating System: Windows XP

The Laptop used for running various scenarios Toshiba 6100 Laptop Serial Number: Y2063543Q  
Operating System: Windows XP  
Built in Wireless Card MAC Address: 00:02:2D:59:E2:BF

## Risk Evaluation



**Figure 3**

The Network diagram, Figure 3, provided by Acme Development Company demonstrates that there is a basic understanding of the developing exposures related to wireless networks. This is indicated by the design, which effectively places the wireless network outside of the network protected by the Firewall. This design starts to implement "defence in depth" architecture. It can, if the hardware and software features are configured appropriately,

fully implement the “defence in depth” methodology. It is up to the audit to validate whether or not, the laptops, access point, Firewall and Access Server, are used to the best advantage in this situation. Thus the audit will focus primarily on Access point settings, the Laptop Wireless Card settings, the Laptop Software configuration, and authentication mechanisms used. Acme has stated that it is outside of the scope of the Audit to evaluate the Firewall beyond providing a connection to the network.

A wireless network is prone to all of the familiar vulnerabilities of a wired network plus all of the vulnerabilities common to a shared open media network, without, physical cabling, for signal transmission. Thus OSI layer 1 and 2 (Physical and Link Layer) form the areas where new exposures will be discovered. OSI layer 3 and above still have the same exposures that exist today, and will have any that are discovered into the future. The Physical and Link Layers are where the newest standards for Wireless communication are being developed and implemented. As these standards are implemented various parties, developers, implementers, Whitehats, Greyhats and Blackhats alike, are busy discovering the implementation exposures, thus forcing the standards to be modified to correct the discovered issues, thereby limiting security exposures. This activity, the new and developing standards, the discovered implementation issues and exposures, make this area of auditing a very dynamic one, thus, audit lists that are made for this version of hardware and software implementation, will only provide a starting point for audits of tomorrow. It is noted that the new standard 802.11i, is expected to provide yet another solution to Wireless LAN security flaws by year-end (2003). This will require an update to any audit checklist produced before that date.

Wireless access points introduce threats presented by internal vulnerabilities such as Rogue access points, unsecured network configurations, and accidental associations. There are also external vulnerabilities such as eavesdropping, corporate espionage, identity theft, Denial of Service and Man-in-the Middle attacks, all of which are still evolving.

The issue of how likely is an exposure to be discovered is a matter of some conjecture, is also location specific, and corporate profile specific. As an example, if the company was known to be developing armaments for the military, and the office was located next to a coffee shop with wireless access, we can safely deduce it would be a matter of minutes, before the existence of the network was discovered. In today’s environment, with the heightened interest in wireless network exposures, well known, freely available exposure evaluation tools, it would be safe to say within hours of the discovery of the network; it would be mapped for exposures. These exposures would then be further probed, to discover what could be accessed. The announcement of the exposures, including their magnitude, would soon follow, with corresponding levels of media coverage. All of this activity is more than likely to occur within a week. As a second example, if the wireless network was installed at a motor home dealer at the edge of a small town, the

existence of the network could be well known, to the local inhabitants, but there would be little interest in exploiting it for nefarious purposes. The net result being that a small exposure in the first example would be widely broadcast, while a very large exposure in the second example could go unnoticed.

In summary one can safely say that Wireless Networks are subject to a heightened level of risk than wired networks. This situation will remain true for a few years as exposures are uncovered, standards developed and implemented, and best practices are written and applied.

In [Topics in Auditing- High Level Review of WLAN](#) Review of WLAN – Philip J. Coran presents a good overview of the associated “Risks and Vulnerabilities of Wireless Networks and 802.11B” in sections 1.3 through 1.5

Four “Top Ten” lists are mentioned below, which I have used to assist in developing an audit checklist. They could also be used to start development of a Best Practices document.

3com manager Bruce Comeau's widely copied and circulated top-ten list of ways to secure a wireless network can be found at [ca.3com.com/landing\\_page/top10.html](http://ca.3com.com/landing_page/top10.html).

Exploiting and Protecting 802.11b Wireless Networks <http://www.extremetech.com/article2/0,3973,31255,00.asp>

And Securing your Wireless Network [http://www.practicallynetworked.com/support/wireless\\_secure.htm](http://www.practicallynetworked.com/support/wireless_secure.htm)

Ten Steps to a Secure Wireless Network (pc Magazine)

<http://www.pcmag.com/article2/0%2C4149%2C844020%2C00.asp>

#### Risk Mitigation Methods For Your Wireless Network

- Attempt to locate the access points toward the center of the building, away from the windows, & exterior walls
- Attempt to use a protocol other than TCP/IP for File and Printer Sharing.
- Follow secure file-sharing practices
  - This means:
    - Minimize what is shared. Limit as much as possible to specific Files, not drives
    - Protect any shared item, with a password, preferably the shared item is encrypted
- Do not use the default password on your access point/router; change it, to a strong one.
- Purchase access points which support 128 bit or better WEP

- Enable WEP Encryption
- Use WEP for data and Authentication
- Use non-obvious WEP keys and periodically change them
- Disallow router/ AP administration via wireless
- Use MAC address based Access and Association control.
- Don't send the SSID
- Don't accept "ANY" SSID
- Change the default SSID of your product.
- Don't change the SSID to reflect your company's main names, divisions, or products
- Don't change the SSID to your street address.
- Disable "broadcast SSID" whenever possible.
- Purchase access points that have flashable/upgradable firmware
- When possible consider using static IP addresses for your wireless NICs and disable DHCP.
- If you're using a wireless router, consider changing the IP subnet to a private addressing scheme.
- Periodically survey your site using a tool like NetStumbler to discover when "rogue" access points appear.
- Take a notebook equipped with NetStumbler with an external antenna outside your building and survey what someone parked in your parking lot might "see".
- Consider using an additional level of authentication, such as RADIUS, before you permit an association with your access points
- Some products support additional security features that are either not defined by the 802.11b standard, or not mandated by the standard, evaluate the additional security and usefulness of each of these options
  - Specific to Cisco Aironet 1200 Series Wireless Access Point:
    - Disable Cisco Discovery Protocol

Many people believe that the best method to secure a wireless network is by using a combination of the suggestions above. However, the most effective strategy would be to put your wireless access points into a DMZ, and have your wireless users tunnel into your network using a VPN.

The consequences of a security breach in the wireless network can vary from a nuisance incident on a Laptop, to compromise of the Enterprise Network at Acme, with disclosure of proprietary company information. In order for the needs of a demonstration network to be met, the balance between usability and security needs to be carefully

evaluated, and may need multiple levels of security control objectives, and methods to be implemented in order for it to be a useable implementation

### **Current State of Auditing, with respect to a Wireless Access Point**

The vast array of information available on wireless networks demonstrates that there are well known and well exploited exposures, which creates media interest. The resources below were the most significant of the many articles available, which I used, to insure that my understanding of Wireless networks, the standards, the vulnerabilities, and the exposure limiting solutions, was current. There are many other pieces of information available, which may equally well suit the needs of other Auditors.

The following group of 3 articles parallels the Wireless Audit taken at Acme Development Company. The Audit requirements were different. The articles demonstrate a similar process, from start to finish.

“Comprehensive security audits unearth common wireless vulnerabilities”, Jul 15, 2002, John Verry, TechRepublic

“Penetration testing finds more holes in wireless network”, Aug 6, 2002, John Verry, TechRepublic

“Security audit's final steps: Break the bad news and fix the WLAN”, Sep 12, 2002, John Verry, TechRepublic

The following list of resources was used to develop the Audit checklist. Various pieces were drawn from various articles. The NIST standards, and previous GSNA Practicals were used as guidelines to develop major sections. The information in the news articles kept the audit current. Cisco information made the audit specific to the Cisco deployment at Acme Development Company.

#### **News Articles**

<http://www.nwfusion.com/news/2003/0310wirelessvpn.html> an article named “Securing WLANs still a hit or miss proposition” discusses some of the approaches currently available to address Wireless LAN Security.

<http://www.eweek.com/article2/0,3959,865802,00.asp> an article named “Wireless LAN Lockdown” dated February 3, 2003. It is a high level view of Wireless LAN issues, and includes a description of the standards.

<http://computerworld.com/newsletter/0%2C4902%2C78807%2C0.html?nlid=AM> The Wi-Fi Alliance plans to start certifications of 54M bit/sec. WLAN equipment this summer. Analysts and a major supplier are concerned that the new standard is not ready for prime time.

<http://www.nwfusion.com/news/2003/0221wlansecur.html> an article covering the IEEE 802.11i standard which plugs security holes in IEEE 802.11 wireless LANs The standard likely won't see final approval or shipping products until about a year from now.

<http://www.drizzle.com/~aboba/IEEE/> **The Unofficial 802.11 Security Web Page**

<http://www.networkmagazine.com/article/COM20030121S0002> 802.11's Maturity Propels WLAN Adoption The article describes how Wireless Networks are becoming popular

<http://www.networkmagazine.com/article/NMG20021203S0006/1> Roadblocks for War Drivers: Stop Wi-Fi from Making Private Networks Public The article describes protective measures for Wireless networks.

<http://www.blackhat.com/presentations/bh-usa-02/baird-lynn/bh-us-02-lynn-802.11attack.ppt> Advanced 802.11 Attack, Mike Lynn and Robert Baird, Black Hat 2002, Las Vegas NV, July 2002. The presentation describes advanced attack techniques

<http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-potter-802.1x.ppt> 802.1x What it is, How it's broken, and How to fix it. Bruce Potter The Schmoo Group Black Hat 2002, Las Vegas NV, July 2002 The presentation demonstrates problems and solutions with the latest current security improvements for Wireless Lans



[WaveLock](#) a free utility for blocking non administrative access to wireless network adapters in Windows 2000 and Windows XP.

[Wireless LAN Security News](#) is a list of News Articles covered by Cisco.

### **National Institute of Standards and Technology**

[SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices](#) (.PDF) The document provides recommendations of the National Institute of standards and Technology on configuration, and management of 802.11, Bluetooth and Handheld Network Devices.

[NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems."](#) (.PDF) is a document containing a questionnaire constructed from specific control objectives and techniques, which can be used to access the current risk status of their information security programs.

[NIST Security Assessment Tool, Automated Security Self-Evaluation Tool \(ASSET\) and accompanying documentation](#) "The purpose of ASSET is to automate the completion of the questionnaire contained in NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems."

[NIST Special Publication 800-37, "Guidelines for Security Certification and Accreditation of Federal Information Technology Systems, October 2002](#) (.PDF) is a document which can help to establish a standard process to be used to certify and accredit a system for specific needs.

[Draft NIST Special Publication 800-55, Security Metrics Guide for Information Technology Systems](#) (.PDF) "The document provides advice on how an organization, through the use of metrics, may assess the adequacy of in-place security controls, policies, and procedures. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments".

## **National Infrastructure Protection Center**

[Best Practices for Wireless Fidelity \(802.11b\) Network Vulnerabilities](#)

## **GCNA Practicals on Wireless Access Points**

[Auditing the Cisco Aironet 340 Wireless Access Point](#) - Mark Gryparis

[Auditing the Wireless Environment: A Mobile Wireless LAN Used for Training in Multiple Sites on a Corporate WAN- An Auditor's Perspective](#) - Angela Loomis

[Auditing a Wireless Access Point: The Orinoco Outdoor Router 1000 Configured as a Wireless Access Point](#) - Slawomir Marcinkowski

[Topics in Auditing- High Level Review of WLAN](#) Review of WLAN – Philip J. Coran

## **Cisco Specific Security Articles:**

[WLAN Security](#) 15 Cisco related Wireless Security articles some of which are noted below

Software: Protected Extensible Authentication Protocol Support 21/Oct/2002

Response to University of Maryland's Security Analysis 08/Sep/2002

Cisco Wireless LAN Security Bulletin on WEP Weaknesses 25/Sep/2001

Cisco Shares Findings From Recent WLAN Security Research 10/Aug/2001

Cisco Secure Access Control Server v2.6 - No. 1264

[Cisco Aironet Products Now Include Protected Extensible Authentication Protocol Support](#)

[Cisco Aironet Wireless LAN Security Overview](#)

[802.11 Wireless LAN Security White Paper](#)

[Configuring the Cisco Wireless Security Suite](#)

## **Cisco Aironet 1200 Series Access Point Firmware and Utilities**

[http://www.cisco.com/pcgi-bin/tablebuild.pl/aironet\\_1200\\_series\\_ap](http://www.cisco.com/pcgi-bin/tablebuild.pl/aironet_1200_series_ap)

## **Cisco Aironet 1200 Series Wireless Access Point Specific, Security Articles**

## **SECURITY ADVISORIES**

[http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_security\\_advisories\\_list.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_security_advisories_list.html)

## **FIELD NOTICES**

[http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_field\\_notices\\_list.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_field_notices_list.html)

Repeater Mode Denies Wireless Client Access

LEAP and Broadcast Key Rotation Requires VLAN Config on AP1200

Cisco Aironet 1200 Series Access Point Hangs under Bursts of Ethernet Traffic

## **Bulletins**

[http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_bulletins\\_list.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletins_list.html)

Cisco Aironet Regulatory Domain Options 08/Jul/2002

Cisco Aironet Response to Press - Flaws in 802.11 Security 06/Sep/2001

Cisco Aironet Security Solution Provides Dynamic WEP 06/Sep/2001

## GSNA Assignment 2 – Create an Audit Checklist

### Audit Checklist

The following audit checklist has been compiled using business appropriate input from Acme Development Company, and the above noted documents, tips, and practicals. It is intended to be used in auditing the Cisco Aironet 1200 Series, Wireless Access Point solution, implemented as an access point for a customer demonstration facility. See Figure 4 below.

Risk Area #2 is treated as a hostile environment. There are no printers permitted in the Wireless area. Acme made that decision in order to be able to disable File and Printer Sharing on the computers in the Wireless network.

### Scope

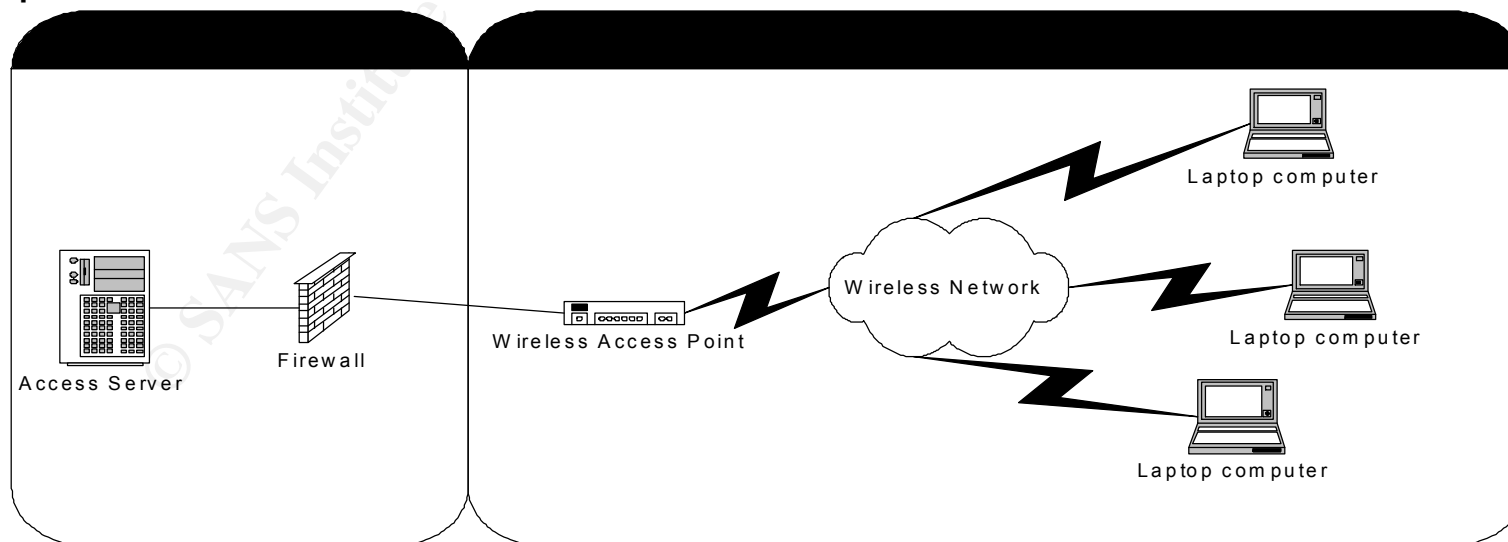
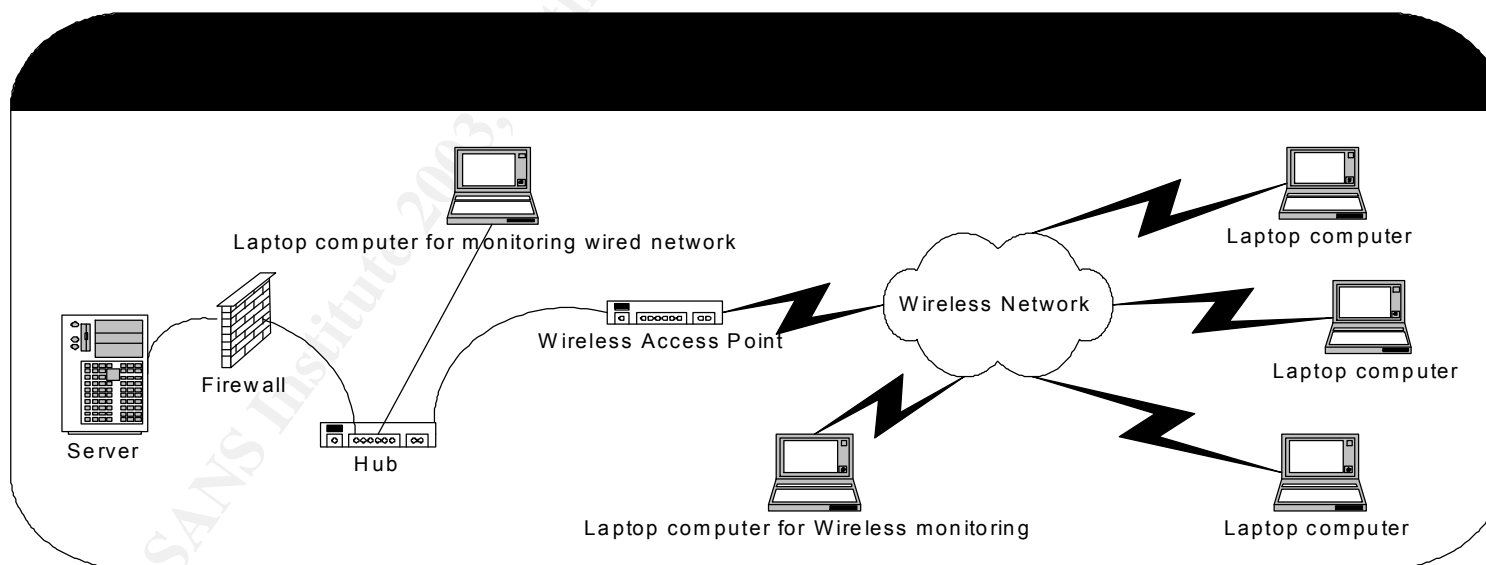


Figure 4

Risk Area 1 is outside the scope of this Audit; it requires a specific Audit of its own. It is acknowledged that vulnerabilities in Area 1 impact the functionality of the network as a whole.

This audit is concerned with Risk Area #2, the Cisco Aironet 1200 Series Wireless Access Point and associated Windows XP Professional laptops. The 802.11a section of the unit is outside the scope of this audit.



**Figure 5**

The monitoring environment is set up as depicted above in Figure 5. The Laptop monitoring the Wireless side is setup to run Wildpackets Airopeek NX, the Laptop monitoring the wired side is setup running Wildpackets Etherpeek. The two units are used in a combined manner, to record network activity. The advantage of this method of operation is that the machine on the Wireless side is able to produce a recording of the network activity taking place between end nodes and the Access Point, (AP) that may or may not be encoded in some manner, while the machine on the wired

side is able to record the same information, with some of that encoding, WEP as an example, removed. Naturally neither of the machines will be able to easily decrypt IPsec traffic, but the wired side will be able to identify it as such. The monitoring will occur in a minimum of 4 stages. Both the Laptop on the wired and wireless sides will be recording traffic through stages 2, 3, 4 and any others, which may be required. The first stage is required to establish average network loads, and develop filters, as required to discard traffic, to limit the amount of information being captured. The second stage is started after completing the first stage, and runs for approximately an hour, while the administrator, or his/her appointee boots a machine, on the wireless side and logs on to the network successfully several (minimum of 3 times). This is repeated with a machine that does not have the necessary credentials to make a network connection, and then stepping through the process of adding credentials until the log on is successful. Sections D and E of the audit are to be completed at this time as well. The recording of activity is stopped on both machines the collected packets are recorded, to disk, preferably a CDROM.

After the completion of stage 2 and the data recording, the Laptop on the wireless side is setup to record packets with the baseline filter as described in the "Security Audit Template" section of "Using the New AiroPeek Alarm and Template Features" it is included in Appendix B of this document. The Laptop on the wired side is set to record without any filters set, if it can handle the data volume. It may be appropriate to filter out some of the repetitive traffic, e.g. BPDU, VRRP, recognized Multicast (OSPF) etc, as identified in Stage one on the machine connected to the wired side. Both machines are set to record for a minimum of a 24-hour period. The data recorded is then written to disk, again preferably CDROM, for later analysis. Stage 4 has both Laptops recording information as stage 3, but the Laptop on the wireless is set to record all the information without any filters

Below, in Figure 6, is the Acme Development Company risk avoidance matrix. It attempts to consolidate the decision making around the Consequences of a Failure to meet the criteria of an audit, with the estimated probability that someone else will discover the issue of the consequence of the Audit item not being met; producing the estimated assumed Exposure (assumed risk) to the organization. During discussions with Acme Development Company it was discovered that Acme is willing to assume a medium level of risk.

The matrix is a modification of the one presented in NIST Special Publication 800-37, "Guidelines for Security Certification and Accreditation of Federal Information Technology Systems", October 2002, page 29

CONSEQUENCE	X	Probability	=	Exposure
High		High		High
Medium		High		High
Low		High		Medium
High		Medium		High
Medium		Medium		Medium
Low		Medium		Medium
High		Low		Medium
Medium		Low		Medium
Low		Low		Low

**Figure 6**

**Objective:** The purpose of the audit is to validate to the IT manager, that pertinent network design steps have been taken, and implemented, in the Wireless Network as it was built, to minimize the security risk to Acme Development Corp, and identify what risk remains present.

**Convention Used:** Areas in the Audit which require Auditor or Administrator to take action are indicated by [action to be taken]

## Section A, ADMINISTRATIVE SECTION

**Objective(s):** To allow the auditor necessary time and/or resources to research the system being audited and develop an effective audit plan.

**Source(s):** Ratliff, Richard L. Internal Auditing: Principles and Techniques. Altamonte Springs: The Institute of Internal Auditors, 1996. 187-193.

**Source(s):** GIAC Training, Security Basics, Minimum Best Practices

**Source(s):** Auditing a Distributed Intrusion Detection System: An Auditors Perspective Darrin Wassom July 2002

Pages 12 - 14

NOTE: The sources cited above refer to all of Section A unless otherwise noted

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
<b>A. ADMINISTRATIVE SECTION</b>						
1. Prepare a Strategic Audit Plan for the area(s) or function(s) to be reviewed.	The expected result is this plan.	O	Deficiencies may be overlooked if the audit plan is poorly designed, causing a poor, incomplete, audit.	L	H	M
2. Prepare a Detailed Audit Budget for the area(s) or function(s) to be	The expected result is an audit budget that identifies the time, labor	S	When the time, resources and scope needed to	H	L	M



AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
reviewed.	and resources needed to conduct a full assessment, and produces a time line, which can be used to monitor audit progress.		conduct a proper assessment are incorrectly identified, and communicated to the sponsor, an ineffective audit will be the result, therefore incorrectly assessing the associated risks.			
<p>3. Prepare Statement of Scope and Methods memorandum for the area(s) or function(s) to be reviewed. Address the memorandum to the appropriate level of management. Request copies or access to information necessary to begin work on the review. This information includes but is not limited to:</p> <p>Policies, procedures, and system user manuals.</p> <p>Reports concerning the audit activity,</p>	The expected result is to foster effective communication between the auditor and the entity being audited. Generally, an auditor will make personal contact and then send a formal memorandum requesting various pieces of information before the audit begins. At the start of the Technical audit, the auditor will have the necessary information, and individuals identified to perform an effective and timely audit, which	O	This is considered a common courtesy and the only real risk involved with not including this step is a possible delay in getting the information needed to conduct the audit, thereby delaying the audit schedule.	H	L	M

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	RISK	CONSEQUENCE	PROBABILITY	EXPOSURE
i.e. special projects, studies, other audit reports  Organizational charts from CEO down to area(s) being reviewed  Job descriptions  Flow charts  Applicable network and/or system documentation	remains on schedule.					
4. Review Audit Co. Information Security process, information storage and retrieval, and information destruction policy and procedures, relevant to this engagement with Acme Development Company (client).  Identify with the client which information and documentation will be returned to the client after the audit is complete and which information Audit Co will retain.	Procedure and process in place at Audit Co. are compliant with security process and procedures required by client	O	The Information made available to the Auditor from Audit Co, by the client (Acme Development Co.) would present improper information disclosure if not handled in a way that respects the expectations and requirements of the client.	H	L	M

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	RISK	CONSEQUENCE	PROBABILITY	EXPOSURE
Demonstrate to the client how the information once provided, is kept secure, how the information is being secured after the audit, how long the information is kept by Audit Co, and how the information is destroyed after it is no longer required.						
5. Review Statement of Scope and Methods, projected costing and obtain written authorization for Audit to take place	. Written authorization provided	O	Without authorization, agreement on scope and projected cost, the Audit cannot take place in its current form.	H	L	M
6. Document Opening Conference Notification Memo Meeting Agenda Management's Comments / Meeting Notes Schedule Exit Conference	The opening conference, called by the senior corporate sponsor, will outline the audit plan with management and will be the starting point to coordinate time and resources associated with the audit. This step also allows for appropriate response from management before a	O	The audit opening conference is the only opportunity to present a professional start to the audit, and demonstrate management's commitment to a proper audit.	H	L	M

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	RISK	CONSEQUENCE	PROBABILITY	EXPOSURE
	formal exit conference is scheduled.					
7. Comparison of Budgeted Hours to Actual Hours	This step is needed to ensure that initial estimates were correct and, if required, change the estimate for future audits being conducted on the same or similar systems, as well as insuring that the agreed to schedule is maintained.	S	This step is needed to ensure accurate estimates are made when developing audit plans. The difference between 50 and 100 hours is significant to an audit team trying to allocate time and resources to various audit plans.	H	L	M
8. Prepare audit issues. Provide audit findings to appropriate management before Exit Conference. Discuss audit issues and recommendations with appropriate management personnel during course of audit as appropriate and at Exit Conference.	It is likely that some issues or deficiencies will be noted during the course of the audit. Changes can be made during the actual audit but they must still be reported to maintain the integrity of the audit plan. This step is usually a joint effort between the auditor and the entity being audited to develop a corrective course of action to remedy any issues that may arise.	O	Integrity of the audit is extremely important. If an administrator makes on the spot changes during the course of an audit it needs to be entered into the final report, and documented, as appropriate, to reflect non-compliance with Change control procedures.	H	L	M

## B. ORGANIZATIONAL STRUCTURE / SYSTEM OVERVIEW, DOCUMENTATION, & TRAINING

**Objective(s):** Determine the reporting structure of the organization being audited. Determine if system documentation exists and if policies and procedures defining the usage or rational for the system being deployed are present. Determine if proper training has been attended. Determine if proper security and patch application notification and process are in place.

**Source(s):** Ratliff, Richard L. Internal Auditing: Principles and Techniques. Altamonte Springs: The Institute of Internal Auditors, 1996. 187-193.

**Source(s):** GIAC Training, Security Basics, Minimum Best Practices

**Source(s):** Auditing a Distributed Intrusion Detection System: An Auditors Perspective Darrin Wassom July 2002  
Pages 12 - 14

NOTE: The sources referenced above apply to all of Section B.

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	RISK	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
<b>B. ORGANIZATIONAL STRUCTURE / SYSTEM OVERVIEW, DOCUMENTATION, &amp; TRAINING</b>						
1. Determine the reporting structure from the area(s) to be reviewed up to the CEO. Initial memo should request a copy of	A copy of the organization chart should be available. This will be helpful in determining the reporting structure of the organization and	S	Knowing the reporting structure of the organization is beneficial. It will allow the auditor to	L	L	L

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
<p>the organization chart.</p> <p>If a formal chart is not available then interview the entity being audited to determine the reporting structure.</p>	<p>what areas of management need to be included in any meetings and/or published reports.</p>		<p>address reports appropriately but most importantly, it will establish boundaries of the organization, and give the auditor a good idea what parts of the system/network are owned by the organization being audited.</p>			
<p>2. Determine if policies and/or procedures exist that define the requirement for, intended usage of, and rational for the system(s) being audited.</p> <p>This information should form an integral part of the Site Security Policy Documents.</p>	<p>Ideally, written policies and procedures will be available for review. It is possible that informal policies exist. If that is the case then a subjective interview will be necessary. If there are no written policies, then best practices should apply, as in RFC 2196, Site Security Handbook  <a href="http://www.ietf.org/rfc/rfc2196.txt">http://www.ietf.org/rfc/rfc2196.txt</a>  or the article</p>	S	<p>A written policy establishes the expected responses to a set of stimuli. Without a written policy in place, each individual reacts to a stimulus, in a manner that is compliant with his or her personal experience. The personal experience may not accurately reflect the expected response</p>	H	M	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	RISK	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
	<a href="#">"Security in a box: It's not enough"</a> discusses the need for security policy		required of the company. A written, followed, formal procedure document will establish an expected response process thereby decreasing risk			
3. Determine if documentation exists for the system(s) being reviewed. This would include any system documentation, scripts, change control processes, and network diagrams.  Initial memo should request any available documentation.  If documentation does not exist then an interview of the organization being audited will be necessary	Copies of all system documentation, diagrams, etc should be made available for review. This is essential in understanding the system, why it is being used and if it is being properly maintained and administered.	S	In addition to policies, it is extremely helpful to have access to any and all system documentation outlining how the system is implemented and used. Without formal documentation, it is a challenge to conduct a timely effective, exhaustive audit.	H	M	H
4. Determine if Administrators and/or Security personal have been trained on the specific device or have other	Copies of certificates of training courses taken, valid certifications achieved are provided.	S	Without proper training or experience, the security and functionality of the	H	M	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
<p>equivalent documented suitable training and experience.</p> <p>Initial memo should request a copy of relevant training that has been attended, and/or current, relevant certifications.</p>			<p>subsystem may be impaired, thereby increasing risk</p>			
<p>5. Determine if Administrators and/or Security personal belong to device relevant mailing lists; and receive updates regularly from Wireless Standards Bodies.</p> <p>Initial memo should request a list of relevant device and security mailing lists to which each group belongs</p> <p>During the Interview determine how notifications of potential security exposures are handled, and how software updates are handled.</p> <p>Determine how the organization is kept up to date with developments in</p>	<p>An assigned individual is responsible for determining the applicability of potential security exposures, and tasked with their resolution. An assigned individual is responsible for determining the applicability of software updates, and applying them In this case, with the Cisco Aironet Access Point, membership in the <a href="#">Cisco TAC Newsletter</a>, access to the Aironet software selector, Cisco Bug toolkit, Cisco Specific Security Articles: Cisco Aironet Series Access Point Firmware and Utilities Cisco Aironet</p>	S	<p>Without specific individuals being tasked with monitoring the appropriate mailing lists, receiving timely update notifications, and applying appropriate changes, security and/or functionality will be impaired.</p>	H	M	H



AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	RISK	CONSEQUENCE	PROBABILITY	EXPOSURE
the Wireless Arena.	Series Wireless Access Point Specific, Security Articles, Security Advisories, Field Notices, and Bulletins					
6. Determine if there is a testing facility for testing security and updated software functionality, previous to implementation in a production environment. Determine how this forms a part of the Change Control process  Initial memo should request information about the change control processes, testing facility supporting the change control process, and supporting documentation.	An assigned group is responsible for determining the applicability of potential security exposures, and tasked with their resolution testing.  An assigned individual is responsible for determining the applicability of software updates, and testing them before whole scale application.	S	Without specific individuals being tasked with testing of functional changes, and the integration of those functional changes, the operability of the systems may be impaired.	H	M	H
7. Determine if there is a user security training program in place	Documented, scheduled, updated, user training program in place.	S	Without an effective, security training program in place, end users will remain unaware of the	H	M	H

full rights.

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	RISK	C O N S E Q U E N C E	P R O B A B I L I T Y	EX PO SU RE
			security issues presented, thereby increasing risk.			

© SANS Institute 2003,

## C: Fieldwork Cisco Aironet 1200, Installation

*Objective(s):* Determine how and where the base unit(s) are installed within the facility, what physical access controls are in place, and what signal propagation mitigation steps have been taken.

*Source(s):* GIAC Training, Security Basics, Minimum Best Practices

*Source(s):* [SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices](#)

Pages 3-11, 3-43

*Source(s):* [Defense In Depth: Preventing Going Hairless Over Wireless](#) Jonathon Berry April 17, 2002

NOTE: The sources referenced above apply to all of Section C

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	RISK	C O N S E Q U E N C E	P R O B A B I L I T Y	Ex PO SU RE
<b>C. Fieldwork Cisco Aironet 1200, Installation</b>						
1. Determine physically where in the facility the base unit(s) are located  Access to the base unit(s) require authentication, through a control mechanism such as a pass card, or key. [Check physical Access methods]	Locate the “known” units. Observe that reasonable steps have been undertaken to place the base units properly, to limit access, and limit signal leakage. [Assign a PASS when the AP is located in a locked	S	If the base unit is located in an unsecured area it can easily be moved, and easily change the signal strength outside of the facility.	M	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
<p>The base unit(s) should be located towards the center of the facility, away from windows, exterior walls, and direct openings to the exterior of the facility. This achieves 2 distinct goals; it helps to provide maximum coverage within the facility, while minimizing the signal strength outside the facility. [Check physical location.]</p> <p>The acceptable data rates, Radio setting, can be used to limit the radio association distance, by allowing only higher data rates to associate with the Access Point [Have administrator make a network connection to manage the AP (For 11.0 Mbps) -&gt; Setup -&gt; AP Radio: Internal -&gt; Hardware, check values set to yes and/or Basic.]</p>	<p>room with card key access or accessible only with key access, where access to key is restricted and access recorded otherwise FAIL]</p> <p>Discover the radio acceptable data rates, configured into the Access Point. The higher the minimum accepted connection rate, the shorter the distance from the AP the receiver will have to be located [Acceptable settings for 11.0 Mbps would be 1.0-no, 2.0-no, 5.5-no, 11.0-basic = PASS, otherwise FAIL]</p>		<p>The stronger the signal strength is to the exterior of the facility, the easier it is for an unauthorized machine to attempt to be connected to the private network.</p>			
<p>2. Determine signal strength at multiple sampling points.</p>	<p>The signal strength, as observed on the laptop with the Wireless NIC, with</p>	O	<p>An individual with a suitably equipped laptop</p>	M	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
Use the Cisco Aironet Client Setup Utility ( <a href="#">ACUv505001.exe</a> ) to assess the signal quality [Start-> Programs -> ACUv505001.exe -> Site survey]	the default antenna, outside of the facility is insufficient to allow communication. [Assign PASS when not associated and signal quality "Poor" at all of the identified sampling points, otherwise FAIL]		will be able to easily make a connection to the wireless network, without obvious auxiliary antennae attached to the laptop.			
3. Determine if there is a documented process in place to monitor when the base station is physically accessed. [Locate Log Book, Key sign out Log, or Card key access log inspect recorded entries]	[Assign a PASS if there is a documented process in place which records identity, dates, and times, of access and that there is a security policy compliant evaluation process of the access information, in place, otherwise FAIL.]	O	The base station's location, or settings could be modified without proper controls if the access logs are poorly monitored.	M	H	H
4. Determine if there is a documented process in place to actively monitor the wireless network signal strength outside of the facility, at known locations and intervals. [Locate Monitoring Log, and inspect recorded entries]	[Assign a PASS if there is a documented process in place, which has dates, times and locations of measurements taken that is reviewed at times specified by the Security Policy]	O	The base station's location, or settings could be modified without proper controls if the access logs are poorly monitored.	M	H	H

## D. Fieldwork Cisco Aironet 1200, Configuration

*Objective(s):* Determine the software configuration of the base station

*Source(s):* GIAC Training, Security Basics, Minimum Best Practices

[http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_configuration\\_guide\\_chapter09186a008010f63d.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_configuration_guide_chapter09186a008010f63d.html)

*Source(s):*

[SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices](#)

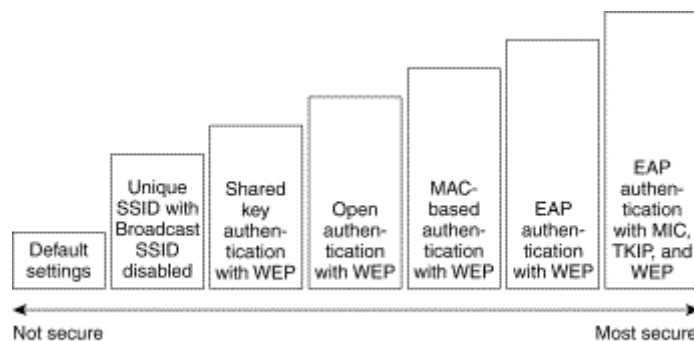
Pages 3-24 to 3-29 and 3-40 to 3-47

*Source(s):* [802.11, 802.1x, and Wireless Security](#), J. Philip Cagier June 23, 2002

NOTE: The sources referenced above apply to all of Section D

NOTE: The diagram below depicts increasing levels of security as defined by Cisco

### Wireless LAN Security Levels



[Cisco Aironet 1200 Series Access Point Software Configuration Guide](#)  
[Levels of Security](#)

[Security Overview](#)

Figure 7

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
<b>D. Fieldwork Cisco Aironet 1200, Configuration</b>						
<p>1. Determine hardware versions of installed Access Point, and 802.11b card installed in it, and associated antennae.</p> <p>[Inspect shipping/receiving/recorded documentation for Hardware Revision data]</p>	<p>Model: AIR – AP1200 System Firmware version: 12.01a System Web pages Version 12.01 Hardware Version: Revision F0</p> <p>AIR-MP20B Wireless LAN Module 2.4 GHz 11Mbps: Revision A0 Radio Firmware Version: 5.02.12 Boot Block Version 1.59 Antenna Hardware Version B0</p> <p>[Assign a PASS if the values are the same as above or Higher, otherwise FAIL]</p>	O	When hardware versions are not current, known issues affecting the operation of the access point will be likely to occur. This may create documented exposures resulting in a Denial of Service	L	L	L
<p>2. Determine that the default password has been changed to a Company security policy appropriate password. Test the base station by attempting to access it from the wireless, LAN and</p>	<p>Validate that the password that is provided by the administrator is Company security policy compliant. If there is no written policy, then best practices procedures apply, as</p>	O	If the password is poorly chosen, or remains at the manufacturer default, the wireless access point is easily compromised,	M	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
<p>console port using the default Cisco password. [Test the base station by attempting to access it from the wireless, LAN and console port using the default Cisco password. The default is "no password"]</p> <p>Have the administrator provide the current password, evaluate that it is within corporate security policy guidelines, for complexity, then have the administrator type it in. [Connect to the AP using the Web Console and observe that a connection is made when correctly typing the password provided]</p>	<p>indicated in <a href="#">Sans/FBI Top 20 Vulnerabilities</a>, items, Windows #7 Unix #10. The password should not be the default.</p> <p>[Assign a PASS if the supplied password is non default and Company security policy compliant, or is non default and compliant with best practices, otherwise FAIL]</p>		<p>therefore all other security would immediately be suspect.</p>			
<p>3. Determine firmware version of installed unit and associated cards</p> <p>12.01T1 is the latest early deployment release as of 31 Jan 2003. It is the Cisco recommended version.</p>	<p>Model: AIR – AP1200</p> <p>Software Version 11.56 is the most current stable release and has the following Cisco recorded bugs as of 31 Jan 2003 Of severity level 3 or higher.</p>	O	<p>When firmware versions are not current, known issues affecting the operation of the access point will be likely to occur, or a full security feature set</p>	M	H	H



AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
<p>[Have administrator make a network connection to manage the AP, once connected at the Summary status page go to -&gt;Setup -&gt;Cisco Services Setup -&gt; Distribute Firmware to other Cisco Devices. The information contained in the list is the current Access Point Software. Then go to -&gt;Setup -&gt; AP Radio: Internal -&gt;Internal Identification, check values Firmware and Boot Block for the Radio Firmware]</p>	<p><a href="#">CSCdz23591</a> AP stops sending multicast causing config distribution problems. <a href="#">CSCdz32270</a> DHCP client id and channel information distributed to all Access Points. <a href="#">CSCdz15816</a> Enabling MIC will cause PCOMM/SNA not to work</p> <p>12.01T1 is the latest early deployment release as of 31 Jan 2003. [Assign a PASS if the software is at 12.01T1, otherwise FAIL]</p>		<p>may not be available. This may create well-documented exposures. Operating at the latest early deployment release may introduce software features that have undiscovered problems.</p> <p>12.01T1 was released 24/Jan/2003. A new version of Software 12.2(8)JA. was released on 15/Feb/ 2003. This is a representation of how quickly wireless software becomes out of date.</p>			
<p>4. Determine that the interval between "Beacon Frames" has been made as long as possible. Cisco Aironet allows this value to be set to a maximum of 5 Sec (5000kmicrosec).</p>	<p>[Assign a PASS if the Beacon Frames are 5 seconds apart, otherwise FAIL]</p>	O	<p>Extending the time between Beacon Frames makes the Access Point quieter (less detectable). The Beacon Frames</p>	L	L	L

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	RISK	CONSEQUENCE	PROBABILITY	EXPOSURE
[Using the captured data created in stage 2 of network monitoring of the <b>Wireless side</b> , open the file using Wildpackets Airopeek, validate that the Beacon Packets are sent at a time interval of 5 seconds (current Cisco maximum) between packets. Start-> Programs -> Wildpackets AiroPeek NX -> Find a Beacon packet -> Edit -> Select Related Packets ->by Protocol ->Hide Unselected. The packets displayed are sequential Beacon packets only. Insure Delta Time is selected in the header, the time interval between Beacon packets is displayed]			announce the presence of the Wireless Network. If the Wireless network announcements are made less frequent, than the network is slightly harder to detect. It may also cause some manufacturers equipment to fail to interoperate.			
5. Determine that the default Service Set Identifier (SSID) has been changed to a Company security policy compliant value. The default SSID is "tsunami." [Using the Capture file, obtained in	[Assign a PASS if the SSID is not the default, is security policy compliant, and does not allow associations from stations implementing the broadcast SSID, otherwise FAIL]	O	When the SSID remains at the default, the product vendor is easily identified, and known vulnerabilities can be readily exploited.	M	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
<p>the capture in stage 2 of the <b>Wireless side</b>, select a 802.11 Probe a Response packet from this AP (Mac Address 00:0B:46:66:D2:24), open the packet, scroll down to the first Information Element value, observe the SSID value, insure that it is not "tsunami" 2) Have administrator make a network connection to manage the AP, once connected at the Summary status page go to -&gt;Setup -&gt;AP Radio Internal Hardware. View the entry for Allow Broadcast SSID to associate? 3) Using a Laptop with a wireless connection that has not been configured to access this network, assume DHCP address assignment, correctly configure the wireless card with WEP Key, enable the Broadcast SSID, and see whether it can associate. Go to-&gt; Start -&gt; Settings -&gt; Network Connections -&gt;Wireless</p>			<p>See the following list.  <a href="#">Default SSID's for several common 802.11 Access Point and PCMCIA card Products</a></p> <p>When the SSID is not security policy compliant, it exposes the network to compromise in addition to demonstrating non-policy compliance.</p> <p>When "any SSID" is accepted, by the AP then any wireless card can associate with the wireless network. Allowing associations to be formed using the broadcast SSID is rated as a "High Risk" by ISS in the notification  <a href="#">cisco-aironet-broadcast-</a></p>			

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
Network Connection -> Properties -> Wireless Network -> Add -> do not enter the SSID, adjust the Data Encryption, Network Authentication switches, and enter the Network Key as appropriate. Observe whether or not an IP address is assigned]			<a href="#">ssid (6287)</a> . Disabling the Broadcast SSID also makes the AP less visible to Netstumbler see "AiroPeekNX is a wireless security jack-of-all-trades" TechRepublic article.  Easily defeated by capturing wireless packets, from working machines, and therefore must be used in association with other security procedures.			
6. Wired-Equivalent Privacy (WEP) Encryption Validate that WEP encryption is enabled [1) Using the Capture file, obtained in the capture in stage 2, of the <b>Wireless side</b> select a 802.11 Probe Response packet from this AP (Mac Address 00:0B:46:66:D2:24),	Capture wireless network traffic to validate that it is encrypted. [Assign a PASS if it is WEP Encrypted, otherwise FAIL]  [Assign a PASS if it is 128 bits (physically 104 bits) or better, and complies with corporate policy, or if there is no corporate policy, then	O	With a properly chosen WEP key it is difficult to decrypt the data within a short time interval (matter of minutes at this time). It is discussed in the following paper from AT&T <a href="http://www.cs.rice.edu/~ast">http://www.cs.rice.edu/~ast</a>	H	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
<p>open the packet, scroll down to 802.11 Management - Probe Response, observe the Privacy: value, insure that it is set to "1" This indicates that WEP is enabled. Using the Capture file, perform an edit to select all the data that is not 802.11 WEP encrypted data, and hide it, look at the remaining data, for data that has not been encoded, and has meaningful information Select a packet e.g. Beacon packet Edit -&gt; select related packets -&gt; By protocol -&gt; Hide Selected Packets -&gt; select next packet to be hidden and repeat until the only packets remaining to be displayed are unencoded packets.]</p> <p>Examine the WEP key to validate that it is corporate policy compliant, and that it is 128 bits, or more in length [Have the administrator provide the</p>	<p>best practices, otherwise FAIL.]</p>		<p><a href="#">ubble/wep/wep_attack.htm</a>            Tools such as AirSnort and WEPCrack can be used to crack the WEP key. This requires that the WEP keys be changed frequently. It has to be changed at the Access point and each of the cards individually, thereby creating a management nightmare.</p> <p>Easily defeated by silently capturing wireless packets, from working machines, and therefore must be used in association with other security procedures.</p>			

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
encryption key, being used. Validate that it is 128 bits (physically 104 bits) or better, and complies with corporate policy, or if there is no corporate policy, then best practices.]						
<p>7. Additional link Layer Security Features available on the Unit. The settings are covered in a Cisco Document, <a href="#">Configuring the Cisco Wireless Security Suite</a></p> <ul style="list-style-type: none"> <li>• Message Integrity Check MIC. Needs WEP enabled with Full Encryption and Aironet Extensions enabled.</li> <li>• Temporal Key Integrity Protocol (WEP Key Hashing) Needs WEP enabled with Aironet Extensions enabled. (Cisco Proprietary)</li> <li>• Broadcast WEP Key Rotation. Requires WEP to be enabled,</li> </ul>	<p>The settings implemented in the 12.01T1 software are currently Cisco extensions to the Standard, and do not fully implement the 802.1x Link Layer Security standard for cross vendor compatibility. Not all vendors' hardware and software will function with, or make use of these settings. [PASS if implemented, or FAIL if not]</p>	O	<p>These settings enhance WEP security, and are to be implemented in conjunction with other security controls. Other than viewing the settings in the Access Point, it would be difficult to quickly, independently validate these settings. Two articles describing some of the 802.1x standards information can be found in <a href="#">What is 802.1x?</a> and <a href="#">802.1X provides user</a></p>	L	M	M

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
<p>LEAP or EAP-TLS authentication. [Have administrator make a network connection to manage the AP, once connected at the Summary status page go to -&gt;Setup -&gt;AP Radio Advanced. Look at the data contained in Enhanced MIC verification for WEP, Temporal Key Integrity Protocol (TKIP), and Broadcast WEP Key rotation interval.]</p>			<a href="#">authentication.</a>			
<p>8. Discover whether Media Access Control (MAC) address based Access and Association control has been implemented. [Using a Laptop with a wireless connection, correctly setup and configured, establish a connection to the network. Using a Laptop with a wireless connection that has not been configured to access this</p>	<p>[Assign a PASS if a Wireless card that should be able to authenticate, with the Access Point, is able to, and the card which should not be able to associate is unable to associate with the Access Point, otherwise FAIL If the list of MAC addresses is empty assign a FAIL]</p>	O	<p>This is a first level access control methodology. It provides limited control is easily defeated and should be implemented in association with other security procedures.</p> <p>A program named "Macof"  <a href="http://lists.insecure.org/lists/bugtraq/1999/May/0056.ht">http://lists.insecure.org/lists/bugtraq/1999/May/0056.ht</a> </p>	M	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
<p>network, assume DHCP address assignment, correctly configure the wireless card with WEP Key, SSID, and 802.1 X values as required, and see whether it can associate. Go to-&gt; Start -&gt; Settings -&gt; Network Connections -&gt;Wireless Network Connection -&gt; Properties -&gt; Wireless Network -&gt; Add -&gt; enter the SSID, adjust the Data Encryption, Network Authentication switches, and enter the Network Key as appropriate, then go to Authentication, and adjust Enable IEEE 802.1x, and EAP types as appropriate. Then perform the MAC based authentication test. Record If an IP address is assigned, Start -&gt; Programs -&gt; Accessories -&gt;Command Prompt -&gt; type Ipconfig /all, and observe and record the data presented, looking for IP address assignment, repeat as required,</p>			<p><a href="#">ml</a> can be used to feed Mac addresses to the Access point to see if it is vulnerable to MAC address table overflow issues. A sniffer can be used to capture a valid MAC address, which can then be substituted for the MAC address in use by an unregistered card, and if the original card, to which the MAC address belongs to is not accessing the Access Point, a connection which appears valid will be made by the card with the acquired, substitute MAC address.</p>			



AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
<p>observe the events that take place for 5 minutes and record as appropriate. To access data from the AP, Have administrator make a network connection to manage the AP, once connected at the Summary status page go to -&gt;Setup -&gt; Address Filters, observe and record the data. Go to Setup -&gt; Security Server -&gt;Authentication Server, observe and record the data.]</p>						
<p>9. Discover whether Remote Authentication Dial-in User Service (RADIUS) based Access control has been implemented.</p> <p>[Using the captured data created in stage2 of network monitoring on the <b>wired</b> side, open the file using Wildpackets Etherpeek, Start-&gt; Programs -&gt; Wildpackets EtherPeek -&gt; locate a successful logon sequence-</p>	<p>(Requires a RADIUS server) [Assign a PASS, if, RADIUS access control implemented, otherwise FAIL]</p>	O	<p>Radius is a reasonable access control methodology, when used appropriately. The limitation here is the user is authenticated, but RADIUS alone does not conceal the data transferred after the access to the network is</p>	M	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
> Edit -> identify the packets required for the logon ->select them ->Hide Unselected. The packets displayed are the logon sequence packets only. Evaluate the logon process. If packets are displayed with the protocol "Radius" then Radius authentication is being used. If no radius packets can be found in the Capture of the successful logon on sequence then Radius authentication is not being used]			granted.  Must be used in combination with other security methods.			
10. Discover whether RADIUS based Access control has been implemented, with Extensible Authentication Protocol (EAP), a protocol supporting 802.1x features.  There are 2 major types of working EAP, LEAP and PEAP. LEAP is Lightweight Extensible Authentication Protocol, and is Cisco proprietary,	(Requires a RADIUS server, EAP enabled)  [Assign a PASS, if, RADIUS access control, with EAP implemented, otherwise FAIL]	O	This solution attempts to overcome the limitation of WEP by enabling a more secure and optionally more frequent key exchange mechanism The AirSnort and WEPCrack attacks would also be slowed by these changes,	M	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
<p>PEAP is Protected Extensible Authentication Protocol, and is the IEEE 802.1x variation implementing server side EAP-TLS, EAP-SIM and EAP-MD5</p> <p>[Using the Capture file obtained in stage 2 for the <b>Wireless side</b>, find a successful log on sequence from this AP (Mac Address 00:0B:46:66:D2:24) and the test machine, open the packets, inspect contents, Locate EAP Success reply packet]</p>			<p>as keys should change often enough that the attacker might not be able to accumulate enough data to crack a key, before it changes. There are more processing (therefore performance) challenges associated with the key exchange/update issues. Two articles describing some of the 802.1x standards information can be found in <a href="#">What is 802.1x?</a> and <a href="#">802.1X provides user authentication.</a></p>			
<p>11. Discover whether VLAN based Networking has been implemented</p> <p>[1)Question the Administrator to</p>	<p>[Assign a pass if VLANs have been implemented, otherwise FAIL]</p>	O	<p>VLANs provide additional security by attempting to segregate network users.</p>	M	M	M

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
discover whether or not Acme has implemented VLANs in the Wireless Network. 2) Using the Capture file obtained in stage 2 for the <b>Wired side</b> , observe the Packets recorded for evidence of VLAN tagging]			In the implementation in use by Acme, this provides little additional security at this time.			
12. Discover whether IPSec (VPN) based Access control has been implemented [Using the captured data created in stage2 of network monitoring on the <b>Wired side</b> , open the file using Wildpackets Etherpeek, Start-> Programs -> Wildpackets EtherPeek -> locate a successful logon sequence-> inspect the packets following the successful logon for protocol IPSEC->select them ->Hide Unselected. The packets displayed are the IPSEC packets only. Evaluate the packet contents. It may be encrypted depending on whether Authentication	[Assign a PASS, if, IPSec protocol 50 Encapsulation Security Payload is implemented otherwise FAIL]	O	Currently offers the most secure method available for establishing a wireless network connection, as the connection is encrypted from the client all the way to the Firewall (decryption point).	M	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
Header, (IP protocol 51) or Encapsulation Security Payload (IP protocol 50) is being used]						
<p>13. Is there a Static IP addressing scheme in place?</p> <p>[Using a Laptop with a wireless connection, correctly setup and configured, establish a connection to the network then Start -&gt; Programs -&gt; Accessories -&gt;Command Prompt -&gt; type Ipconfig /all, and observe and record the data presented. Check for DHCP Enabled set to YES. Using the captured data created in stage2 of network monitoring on the <b>wired</b> side, open the file using Wildpackets Etherpeek, Start-&gt; Programs -&gt; Wildpackets EtherPeek -&gt; locate a successful logon sequence-&gt; Edit -&gt; identify the packets just previous to the logon we are looking for packets</p>	<p>[Assign a PASS, if, no IP address assigned on boot up.</p> <p>Assign a FAIL, if, IP address assigned on boot up is not a part of Acme's wireless network.</p> <p>Assign a PASS, if, the IP address assigned on boot up is not a part of Acme's wireless network, but is a part of 169.254.aaa.bbb, where a and b are numerical values, and the machine performing the evaluation is running a Microsoft Operating System.</p> <p>Assign a FAIL, if, IP address assigned, is a part of Acme's wireless network, and DHCP is enabled]</p>	O	<p>By manually assigning IP addresses, it requires more effort to successfully communicate with other machines on Acme's network. . A sniffer can be used to capture an IP address, which can then be used to determine the network-addressing scheme for this network.</p> <p>Easily defeated by silently capturing wireless packets, from working machines, and therefore must be used in association with other security procedures.</p>	L	H	M

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
that would occur as the DHCP address assignment occurs ->select them ->Hide Unselected. The packets displayed are the logon sequence packets, and activity just previous. Evaluate the packets for DHCP activity. If packets are displayed with the protocol "DHCP" then DHCP address assignment is being used. If no DHCP packets can be found in the Capture then DHCP is not being used]	For further information regarding the 169.254.aaa.bbb address refer to the RFC defining special IPV4 address assignment, <a href="http://www.rfc-editor.org/rfc/rfc3330.txt">http://www.rfc-editor.org/rfc/rfc3330.txt</a>					
14. Has the wireless network been assigned a part of the "Special-Use IP address" space? [Using a Laptop with a wireless connection, correctly setup and configured, establish a connection to the network then Start -> Programs -> Accessories ->Command Prompt -> type Ipconfig /all, and observe and record the data presented. Evaluate	[Assign a PASS, if the address is a part of a known "Special-Use address space" in use by Acme Development Company otherwise FAIL.] For further information regarding the public address refer to the RFC defining special IPV4 address assignment, <a href="http://www.rfc-editor.org/rfc/rfc3330.txt">http://www.rfc-editor.org/rfc/rfc3330.txt</a>	O	When the IP addresses for the wireless network are not allocated from a "Special-Use address pool" then a registered address must be in use. Using a freely available tool such as "SamSpade" can then discover the assigned owner of the address this	L	L	L

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
the value assigned for IP Address]			ownership can then be associated with the company, thereby increasing risk.			
15. Determine that the wireless access point has SNMP disabled [To access data from the AP, Have administrator make a network connection to manage the AP, once connected at the Summary status page go to ->Setup ->SNMP, observe and record the data. For independent assurance, using the captured data created in stage 2 of network monitoring on the <b>wired side</b> , open the file using Wildpackets Etherpeek, Start-> Programs -> Wildpackets EtherPeek -> visibly search the packets looking for protocol SNMP select them ->Hide Unselected. The packets displayed are the SNMP	[Assign a PASS, if, SNMP disabled, otherwise FAIL]	O	Incorrectly implemented SNMP monitoring will allow unauthorized users to quickly determine, and possibly adjust the security settings of the Wireless access point	H	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	RISK	CONSEQUENCE	PROBABILITY	EXPOSURE
packets only. Evaluate the packet contents. If the data can be read then SNMP version 3 is not being used (this AP at this software version does not support SNMPv3)]						
<p>16. Determine that the administrator has entered a new administrative password</p> <p>[Have the administrator obtain and enter a new company valid password into the Access Point and then validate that it cannot be accessed using the default password or the password used in step 3. To access data from the AP, Have administrator make a network connection to manage the AP, once connected at the Summary status page go to -&gt;Setup -&gt; Security Setup -&gt; Change Current User Password -&gt; enter Old User Password, New User Password,</p>	[Assign a PASS, if you the Auditor cannot log in with the password provided in step 3, or the default, otherwise FAIL]	O	The administrator password to the wireless Access Point was disclosed to the Auditor, in step 3. It now needs to be changed, in accordance with company guidelines.	M	L	M



full rights.

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	RISK	C O N S E Q U E N C E	P R O B A B I L I T Y	EX PO SU RE
Confirm Password and Apply, then exit from the Access Point. Attempt to connect to the AP.]						

© SANS Institute 2003,

## E. Fieldwork Cisco Aironet 1200, Management

*Objective(s):* Determine how the base station is managed

*Source(s):* GIAC Training, Security Basics, Minimum Best Practices

*Source(s):*

[SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices](#)

Pages 3-23 to 3-29 and 3-40 to 3-47

*Source(s):* [Penetration Testing on 802.11b Networks](#) Benjamin Huey

February 24, 2002

NOTE: The sources referenced above apply to all of Section E

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	Ex PO SU RE
<b>E. Fieldwork Cisco Aironet 1200, Management</b>						
1. Determine access methods used to manage the base station from the <b>wired</b> side.  Attempt telnet access to base station Attempt SSH access to base station Attempt http access to base station	[Assign a PASS if administrative access to the Wireless Access point, is obtained using SSH, or Https, otherwise FAIL.]	O	Access to manage the Wireless Access Point needs to be carefully controlled. Should the access be unsecured due to an exposure then the security settings are	H	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	RISK	CONSEQUENCE	PROBABILITY	EXPOSURE
<p>Attempt https access to base station</p> <p>Scan access point with Nessus looking for open ports.</p>			<p>suspect, and risk is increased. It is possible for SSH (and many other protocols) to be hijacked by a man-in-the-middle attacks. For example <a href="http://www.monkey.org/~dugsong/dsniff/">http://www.monkey.org/~dugsong/dsniff/</a> could be used to facilitate this exposure</p>			
<p>2. Determine access methods used to manage the base station from the <b>Wireless</b> side using 802.11b access.</p> <p>Attempt telnet access to base station</p> <p>Attempt SSH access to base station</p> <p>Attempt http access to base station</p> <p>Attempt https access to base station</p> <p>Scan access point with Nessus looking for open ports</p>	<p>[Assign a PASS if there is no administrative access to the Wireless Access point, from the <b>Wireless</b> Side, otherwise FAIL.]</p>	O	<p>The wireless access point should not be managed from the Wireless side. If it can be this will increase risk.</p>	H	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	RISK	C O N S E Q U E N C E	P R O B A B I L I T Y	EX PO SU RE
3. Discover that Cisco Discovery Protocol (CDP) has been disabled [1]Have administrator make a network connection to manage the AP -> Setup -> Services -> Cisco Services -> Cisco Discovery Protocol (Evaluate that Cisco Discover Protocol is Disabled) 2) Using the Capture file, obtained in the capture in stage 2 of the <b>Wireless side</b> , locate a CDP packet from this AP (Mac Address 00:0B:46:66:D2:24) If CDP is enabled a packet should be found within the first 5 minutes of monitoring]	[Assign a PASS if CDP is disabled otherwise FAIL]	O	Cisco Discovery Packets are used by Cisco manufactured products to discover other Cisco products. The packets carry neighbor information. Once captured they can be used to produce network maps. The Wireless network is an unsecured area, therefore announcing networking equipment neighbor information presents an increase in risk.	H	M	H
4. Discover that Network Monitoring has been implemented on the Wireless Network. [Have administrator demonstrate what information the network Monitoring equipment is	[Assign a PASS if there is Network Monitoring in place, otherwise FAIL]	O	Network Monitoring is required for tracking authorized/unauthorized network usage, and would be beneficial in measuring	H	M	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	EX PO SU RE
recording.]			performance during customer Demos.			

## F. Fieldwork Cisco Aironet 1200, Unauthorized Wireless Access Point Detection

**Objective(s):** Determine if there are any “Rogue” wireless access points in/around the facility.

**Source(s):** GIAC Training, Security Basics, Minimum Best Practices

**Source(s):**

[SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices](#) Pages 3-40 to 3-47

**Source(s):** [How to Avoid Ethical and Legal Issues In Wireless Network Discovery](#) Erik Montcalm November 13, 2002  
Sections 5 & 6.

NOTE: The sources referenced above apply to all of Section F

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	RISK	C O N S E Q U E N C E	P R O B A B I L I T Y	EX PO SU RE
<b>F. Fieldwork Cisco Aironet 1200, Unauthorized Wireless Access Point Detection</b>						
1. Walk around the perimeter, parking lot, and streets adjacent to the facility of Acme Development Company, looking for evidence of Warchalking. <a href="http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf">http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf</a> provides an initial list of Warchalking Symbols, <a href="http://wlana.net/warchalking.htm">http://wlana.net/warchalking.htm</a> has	[Assign a PASS if no marks indicating WarChalking activity has taken place, otherwise FAIL]	O	If the facility has been identified as having a world accessible Wireless Access Point, then security has been compromised. Risk has been increased substantially.	H	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	RISK	C O N S E Q U E N C E	P R O B A B I L I T Y	EX PO SU RE
additions.						
2. Using Wildpackets Airopeek, wireless network analyzer, investigate the facility for unauthorized Wireless networks. [Using the Capture file obtained in stage 4 for the <b>Wireless side</b> at the start of the audit, investigate the facility for unauthorized Wireless networks, Start-> Programs -> Wildpackets EtherPeek-> Open the capture file-> click on Peer Map tab.]	[Assign a PASS if no unauthorized networks are identified as being detected within the Acme Development Company Facility otherwise FAIL]	O	Detecting unauthorized networks within the facility indicates security policy has not been followed. This increases risk.	H	H	H
3. Check known Wardriving sites for entries describing the location of the facility and characteristics of the Wireless network that is in use by Acme Development Company <a href="http://wirelessanarchy.com/">http://wirelessanarchy.com/</a> <a href="http://www.80211hotspots.com/">http://www.80211hotspots.com/</a> <a href="http://www.wigle.net">http://www.wigle.net</a>	[Assign a PASS if the site is not identified on any Wardriving sites, otherwise FAIL]	O	If the facility has been identified as having a world accessible Wireless Access Point, then security has been compromised. Risk has been increased substantially	H	H	H

full rights.

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	RISK	C O N S E Q U E N C E	P R O B A B I L I T Y	EX PO SU RE
<a href="http://mapserver.zhrodaque.net">http://mapserver.zhrodaque.net</a> <a href="http://worldwidewardrive.org/">http://worldwidewardrive.org/</a> [If there are entries for Acme, have the Administrator, ask that the entries be removed.]						

© SANS Institute 2003,



## G. Fieldwork Cisco Aironet 1200, 802.11b wireless card installation and configuration.

*Objective(s):* Determine what the Hardware, Firmware and Software Versions of the 802.11b card installed

*Source(s):* Determine the status of the 802.11b Wireless card installation

*Source(s):* GIAC Training, Security Basics, Minimum Best Practices

*Source(s):* [SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices](#)

Pages 3-40 to 3-47

NOTE: The sources referenced above apply to all of Section H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	RISK	C O N S E Q U E N C E	P R O B A B I L I T Y	EX PO SU RE
<b>G. Fieldwork Cisco Aironet 1200, 802.11b wireless card installation and configuration.</b>						
1. Determine hardware version of installed 802.11b card and associated antenna.  [Inspect recorded documentation. It is almost impossible to tell from the Hardware itself]	[Assign a PASS if Revision K0 or higher, otherwise FAIL]	O	When hardware versions are not current, known issues affecting the operation of the access point will be likely to occur. This may create well-documented exposures thereby increasing risk.	L	M	M

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	Ex PO SU RE
2. Determine firmware version of installed 802.11b card  [Use the Cisco Aironet Client Setup Utility ( <a href="#">ACUv505001.exe</a> ) to display the settings that the client node has been provided at authentication ACU -> Status (Evaluate Firmware Version, Boot Block Version, and NDIS Driver Version)]	[Assign a PASS if Windows NDIS Driver: 8.2.3 802.11b Radio Firmware: 4.25.30 Boot Block version: 1.50 or higher, otherwise FAIL.]	O	When firmware versions are not current, known issues affecting the operation of the access point will be likely to occur, or a full security feature set may not be available. This may create well-documented exposures. Operating at the latest early deployment release may introduce software features that have undiscovered problems, thereby increasing risk.	L	M	M

## H. Fieldwork Cisco Aironet 1200, Laptop System vulnerability assessment with 802.11 b card installed.

*Objective(s):* Determine what wireless Laptop vulnerabilities there are with the 802.11b card installed

*Source(s):* GIAC Training, Security Basics, Minimum Best Practices

*Source(s):* [SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices](#) Pages 3-40 to 3-47

*Source(s):* [Securing Desktop Workstations](#) (A practice from the CERT® Security Improvement Modules)

*Source(s):* [Develop a computer deployment plan that includes security issues](#) (A practice from the CERT® Security Improvement Modules)

NOTE: The sources referenced above apply to all of Section H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	RISK	C	P	Ex
				O	R	P
H. Fieldwork Cisco Aironet 1200 Laptop System vulnerability assessment with 802.11b Card Installed						
1. Determine patch level of Windows XP Professional Laptop [Start -> Windows Update -> Scan for Updates (Evaluate that there are no entries in "Critical Updates and Service Packs) if there are, discover from the administrator,	[Assign a PASS if the system is at the most current Windows XP patch level, otherwise FAIL, if a Fail make a note of the reasoning provided by the administrator]	O	Microsoft has released a number of critical Windows XP patches. If the patches have not been installed the system has known vulnerabilities. Risk has	H	M	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
why the installation of the updates has not been undertaken)]			been increased			
2. Determine that File Sharing and remote Printing services are removed from the Networking control panel and are uninstalled, and shutdown. [Start -> Settings -> Network Connections -> (choose the correct wireless card) -> properties -> IP -> properties. (Evaluate that only Internet Protocol (TCP/IP) is displayed in the Window)]	[Assign a PASS if TCP/IP is the only component in the Networking Control Panel, otherwise FAIL]	O	File Sharing and remote Printing represent a known increase in risk. See <a href="#">CERT Advisory CA-2003-08 Increased Activity Targeting Windows Shares</a> , which specifically discusses issues with Windows XP, as well as Windows 2000. Wireless configurations store the WEP key, either in clear text on the local file system or in a weakly encrypted form, generally in the registry. When remote registry editing is allowed, file sharing is enabled, the WEP key can	H	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
			easily be copied from the Laptop, and decrypted.			
3. Determine that all network services not required for Customer Demonstration purposes are shutdown. At this time Acme Development Company has determined that only TCP/IP is required. [Start -> Settings -> Network Connections -> (choose the correct wireless card) -> properties -> IP -> properties. (Evaluate that only Internet Protocol (TCP/IP) is displayed in the Window)]	[Assign a PASS if only the identified services, required for Customer Demo purposes are running, otherwise FAIL]	S	Unknown services running open additional points of access to the Laptop, thereby increasing risk.	M	M	M
4. Determine that an Antivirus program is installed, up to-date, and running [Start -> Programs -> Network Associates -> Virus Scan Console -> (Evaluate that VShield is set to start at Startup) -> auto update -> Run Now	[Assign a PASS if the Antivirus program is installed, up to-date, and running, otherwise FAIL]	O	Choosing not to run an up to-date Virus detection program substantially compromises the Laptop and the network, thereby increasing risk	H	H	H

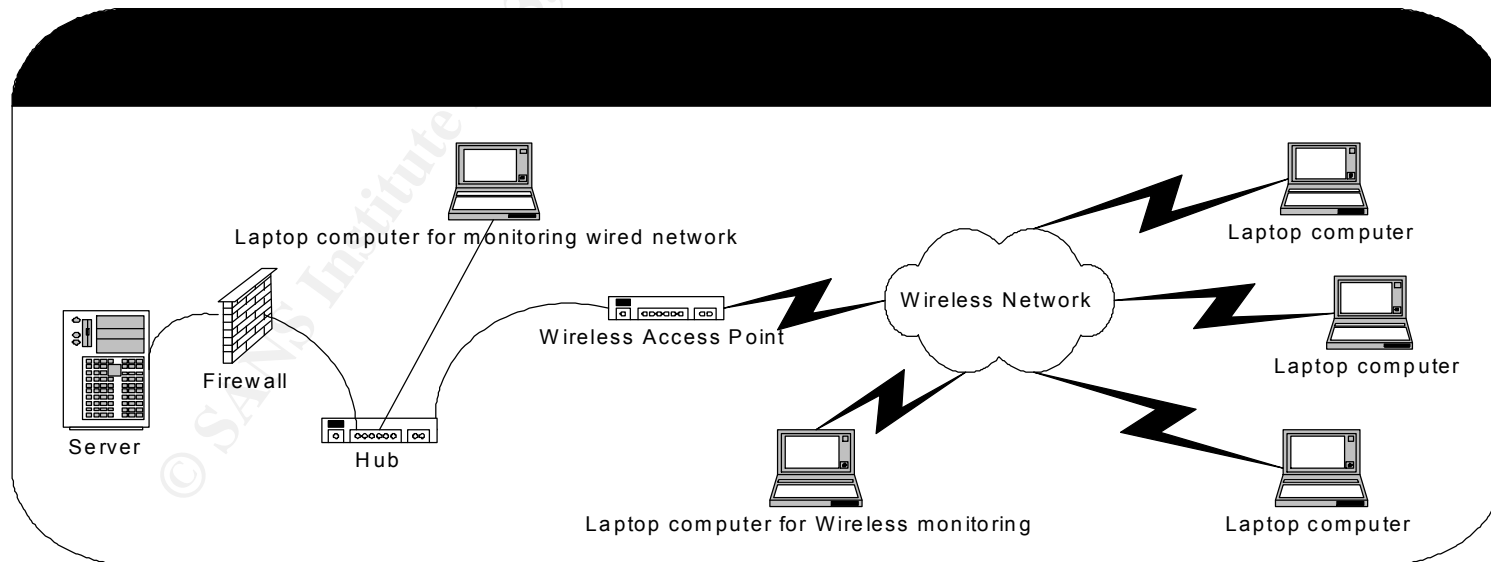
AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TYPE	Risk	CONSEQUENCE	PROBABILITY	EXPOSURE
(Evaluate that the message received after the update completes is "The new .DAT files are the same version as the installed .DAT files")]						
5. Determine that a personal Firewall is installed, up to-date, and running. [If using the Windows XP built in Filtering program then Start -> Settings -> Network Connections -> (choose the correct wireless card) -> properties -> IP -> properties -> Advanced TCP/IP Settings -> TCP/IP Filtering (Evaluate for TCP/IP Filtering being enabled on all adapters, and specified ports required for demonstration purposes to have been identified and set to enable those ports only)]	[Assign a PASS if the personal Firewall is installed, up to-date, and running, otherwise FAIL]	O	Choosing not to run an up to-date Firewall program substantially compromises the Laptop and the network, thereby increasing risk	H	H	H
6. Using Nessus a vulnerability assessment tool, determine the	[Assign a PASS if the ports detected open are those indicated in the	O	Failing to limit the vulnerability of the Laptop	H	H	H

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	COMPLIANCE/EXPECTED RESULTS	TY PE	Risk	C O N S E Q U E N C E	P R O B A B I L I T Y	E X P O S U R E
current vulnerabilities of the Laptop.	customer supplied documentation, otherwise FAIL]		to network intrusions, will compromise the Laptop as well as the network, thereby increasing risk			
7. Determine that the default passwords on the Laptop have been changed to Company security policy appropriate password, or disabled. [Start -. Settings -> Control Panel -> Administrative Tools -> Computer Management ->Local Users and Groups -> Users (Evaluate Local users accounts for Policy Compliance, Evaluate Local Groups for Policy Compliance)]	[Assign a PASS if the default accounts have been disabled or assigned Company Security Policy Compliant Values, otherwise FAIL]	O	If the Laptop is easily compromised due to lax security settings or configuration, it is only a matter of time before the network will be compromised	H	H	H

## GSNA Assignment 3 – Audit Evidence

**Supplementary information for Graders:** In this section there is a lot of data, Sections A, B, C, E, G and H are presented as a summary, of the data found. Section D and F contain the information presented for Grading. Section F contains unexpected information discovered during the audit

### Conduct the Audit



**Figure 8**

During discussions with Acme representatives, it was agreed that this audit, is a Baseline audit, therefore, indicating that vulnerability is present, will be considered to be enough proof of its existence. An exploit will not be



required to demonstrate the existence of the vulnerability.

The monitoring environment is set up as depicted above, in Figure 8. The Laptop monitoring the Wireless side is setup to run Wildpackets Airopeek NX, the Laptop monitoring the wired side is setup running Wildpackets Etherpeek. The two units are used in a combined manner, to record network activity. The advantage of this method of operation is that the machine on the Wireless side is able to produce a recording of the network activity taking place between end nodes and the Access Point, (AP) that may or may not be encoded in some manner, while the machine on the wired side is able to record the same information, with some of that encoding, WEP as an example, removed. Naturally neither of the machines will be able to easily decrypt IPsec traffic, but the wired side will be able to identify it as such.

The monitoring will occur in a minimum of 4 stages. Both the Laptop on the wired and wireless sides will be recording traffic through stages 2, 3, 4 and any others, which may be required. The first stage is required to establish average network loads, and develop filters, as required to discard traffic to limit the amount of information being captured.

Stage 2 is started after completing the first stage, and runs for approximately an hour, while the administrator, or his/her appointee boots a machine, on the wireless side and logs on to the network successfully several (minimum of 3) times. This is repeated with a machine that does not have the necessary credentials to make a network connection, and then stepping through the process of adding credentials until the log on is successful. Sections D and E of the audit are completed at this time as well. The recording of activity is stopped on both machines, the collected packets are recorded, to disk, preferably a CDROM.

In Stage 3, the Laptop on the wireless side is setup to record packets with the baseline filter as described in the "Security Audit Template" section of "Using the New AiroPeek Alarm and Template Features" it is included in Appendix B of this document. The Laptop on the wired side is set to record without any filters set, if it can handle the data volume. It may be appropriate to filter out some of the repetitive traffic, e.g. BPDU, VRRP, recognized Multicast (OSPF) etc, as identified in Stage one, on the machine connected to the wired side. Both machines are set to record for a minimum of a 24-hour period. The data recorded is then written to disk, again preferably CDROM, for later analysis.

Stage 4 has both Laptops recording information as stage 3, but the Laptop on the wireless is set to record all the information without any filters.

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>A. ADMINISTRATIVE SECTION</b>	
1. Prepare a Strategic Audit Plan for the area(s) or function(s) to be reviewed.	Complete
2. Prepare a Detailed Audit Budget for the area(s) or function(s) to be reviewed.	Complete
3. Prepare Statement of Scope and Methods memorandum for the area(s) or function(s) to be reviewed.	Complete
4. Review Audit Co. Information Security process, information storage and retrieval, and information destruction policy and procedures, relevant to this engagement with Acme Development Company (client).	Complete
5. Review Statement of Scope and Methods, projected costing and obtain written authorization for Audit to take place	Complete
6. Document Opening Conference	Complete
7. Comparison of Budgeted Hours to Actual Hours	Complete
8. Prepare audit issues.	Complete

AUDIT STEPS: ORGANIZATIONAL STRUCTURE, SYSTEM OVERVIEW	STATUS
<b>B. ORGANIZATIONAL STRUCTURE / SYSTEM OVERVIEW, DOCUMENTATION, &amp; TRAINING</b>	
1. Determine the reporting structure from the area(s) to be reviewed up to the CEO.	Complete
2. Determine if policies and/or procedures exist that define the requirement for, intended usage of, and rational for the system(s) being audited.	<b>FAIL/no written Wireless policy and Procedures</b>
3. Determine if documentation exists for the system(s) being reviewed. This would include any system documentation, scripts, change control processes, and network diagrams.	Complete

AUDIT STEPS: ORGANIZATIONAL STRUCTURE, SYSTEM OVERVIEW	STATUS
4. Determine if Administrators and/or Security personal have been trained on the specific device or have other equivalent documented suitable training	<u>PASS</u>
5. Determine if Administrators and/or Security personal belong to device relevant mailing lists; and receive updates regularly from Wireless Standards Bodies.	<u>PASS</u>
6. Determine if there is a testing facility for testing security and updated software functionality, previous to implementation, in a production environment. Determine how this forms a part of the Change Control process	<b>FAIL/no testing facility</b>
7. Determine if there is a user security training program in place	<b>FAIL/no User training Program</b>

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>C. Fieldwork Cisco Aironet 1200, Installation</b>	
1.Determine physically where in the facility the base unit(s) are located.	<b>FAIL/located near external wall</b>
2.Determine signal strength at multiple sampling points.	<b>FAIL/ strong signal external to facility, due to AP location</b>
3.Determine if there is a documented process in place to monitor when the base station is physically accessed.	<b>FAIL/ recording but no monitoring</b>
4.Determine if there is a documented process in place to actively monitor the wireless network signal strength, outside of the facility, at known locations and intervals.	<b>FAIL/ process, but no historical monitoring log</b>

## D. Fieldwork Cisco Aironet 1200, Configuration

### D1. Determine hardware versions of installed Access Point, 802.11a card installed in it, and associated antennae.

**Action:** [Inspect shipping/receiving/recorded documentation for Hardware Revision data]

**Expected Results:** Model: AIR – AP1200 System Firmware version: 12.01a System Web pages Version 12.01

Hardware Version: Revision F0

Consisting of

AIR-MP20B Wireless LAN Module 2.4 GHz 11Mbps: Revision A0

Radio Firmware Version: 5.02.12

Boot Block Version 1.59

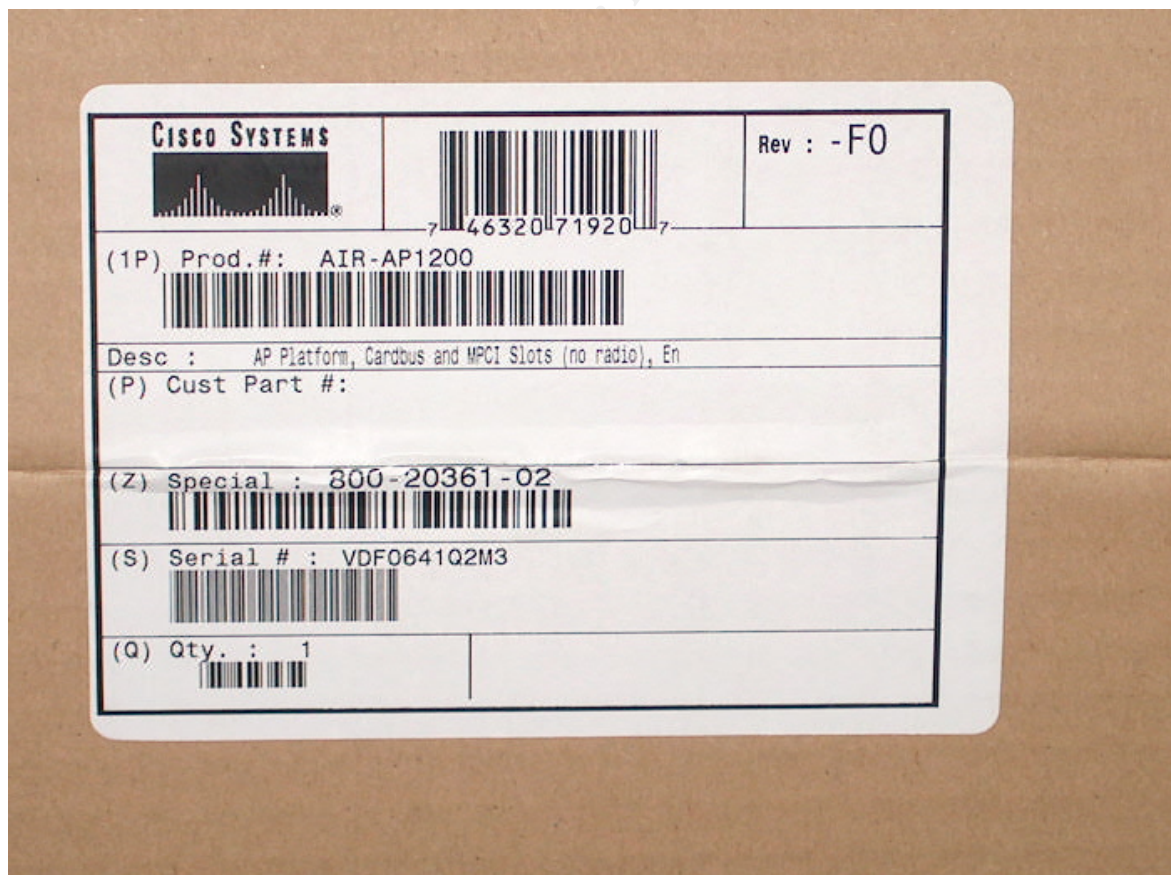
Serial Number: VMS06330HL9

Antenna Hardware Version B0

[Assign a PASS if the values are the same as above or higher, otherwise FAIL]

**Actual Results:** PASS Figures 9, 10, and 11

Base Access Point:  
AIR- AP1200 Wireless Network Access Point Model: AIR – AP1200  
Serial Number: VDF0641Q2M3  
Hardware Version: Revision F0



**Figure 9**

Card inserted into Base Station:  
AIR-MP20B Wireless LAN Module 2.4 GHz 11Mbps: Revision A0  
Serial Number: VMS06330HL9  
Hardware Revision: A0



Figure 10



# Antenna Hardware Version B0



Figure 11

## D2 Determine that the default password has been changed to a Company security policy appropriate password

**Action:** Determine that the default password has been changed to a Company security policy appropriate password. Test the base station by attempting to access it from the wireless, LAN and console port using the default Cisco password. The default is "no password"

**Expected Results:** Observe that a password is required to access the AP, in each of the 3 cases. Have the administrator provide the current password, evaluate that it is within corporate security policy guidelines, for complexity, then have the administrator type it in. [Connect to the AP using the Web Console and observe that a connection is made when correctly typing the password provided]

**Actual Results:** PASS (the access point actually is known by another name which has been disguised) See Figures 12 & 13

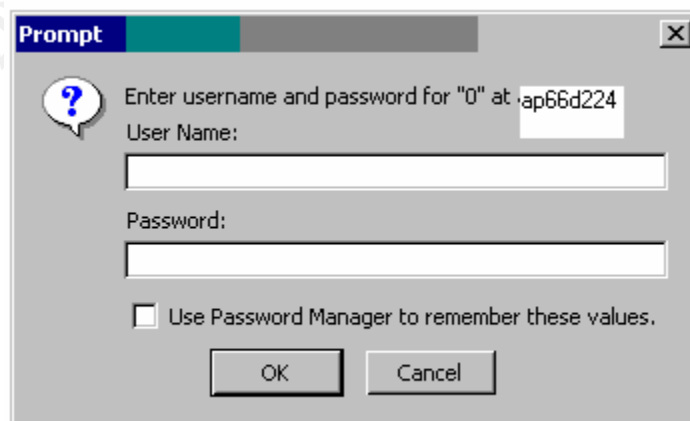


Figure 12

An incorrectly typed password cycled back to the "Prompt" screen each time, in each of the 3 cases.



Below, Figure 13 is the response from a correctly typed password. It is the default successful logged in screen.

**AP66d224 Summary Status**

Cisco 1200 Series AP 12.01T1

2003/02/26 14:09:34

**Current Associations**

<b>Clients:</b> 0 of 1	<b>Repeaters:</b> 0 of 0	<b>Bridges:</b> 0 of 0	<b>APs:</b> 1
------------------------	--------------------------	------------------------	---------------

**Recent Events**

Time	Severity	Description
2003/02/26 14:08:55	Warning	Station 00022d6b2800 Failed Authentication, status "Authentication Transaction Sequence Number Out-of-Order"
2003/02/26 14:08:31	Info	Deauthenticating 000b4691e806, reason "Previous Authentication No Longer Valid"
2003/02/26 14:08:31	Warning	No EAP-Authentication response for Station 000b4691e806 from server 10.100.10.1
2003/02/26 14:08:00	Info	Station 000b4691e806 Associated
2003/02/26 14:08:00	Info	Station 000b4691e806 Authenticated

**Network Ports**

Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	10.0	10.200.20.240	000b4666d224
AP Radio: Internal	Up	11.0	10.200.20.240	000b4666d224

[Home][Map][Login][Network][Associations][Setup][Logs][Help]

Cisco 1200 Series AP 12.01T1 © Copyright 2002 Cisco Systems, Inc. credits

Document: Done (4.515 secs)

Figure 13

### D3. Determine firmware version of installed unit and associated cards

**Action:** [Have administrator make a network connection to manage the AP, once connected at the Summary status page go to ->Setup ->Cisco Services Setup -> Distribute Firmware to other Cisco Devices. The information contained in the list is the current Access Point Software. Then go to ->Setup -> AP Radio: Internal ->Internal Identification, check values Firmware and Boot Block for the Radio Firmware]

**Expected Results:** [Assign a PASS if the software is at 12.01T1, otherwise FAIL]. The information is valid as of 31 Jan 2003

**Actual Results:** PASS (12.01A, 12.01, 5.0212 are all components of 12.01T1) Figure 14 displays the base system unit, Figure 15 displays the 802.11b card information.

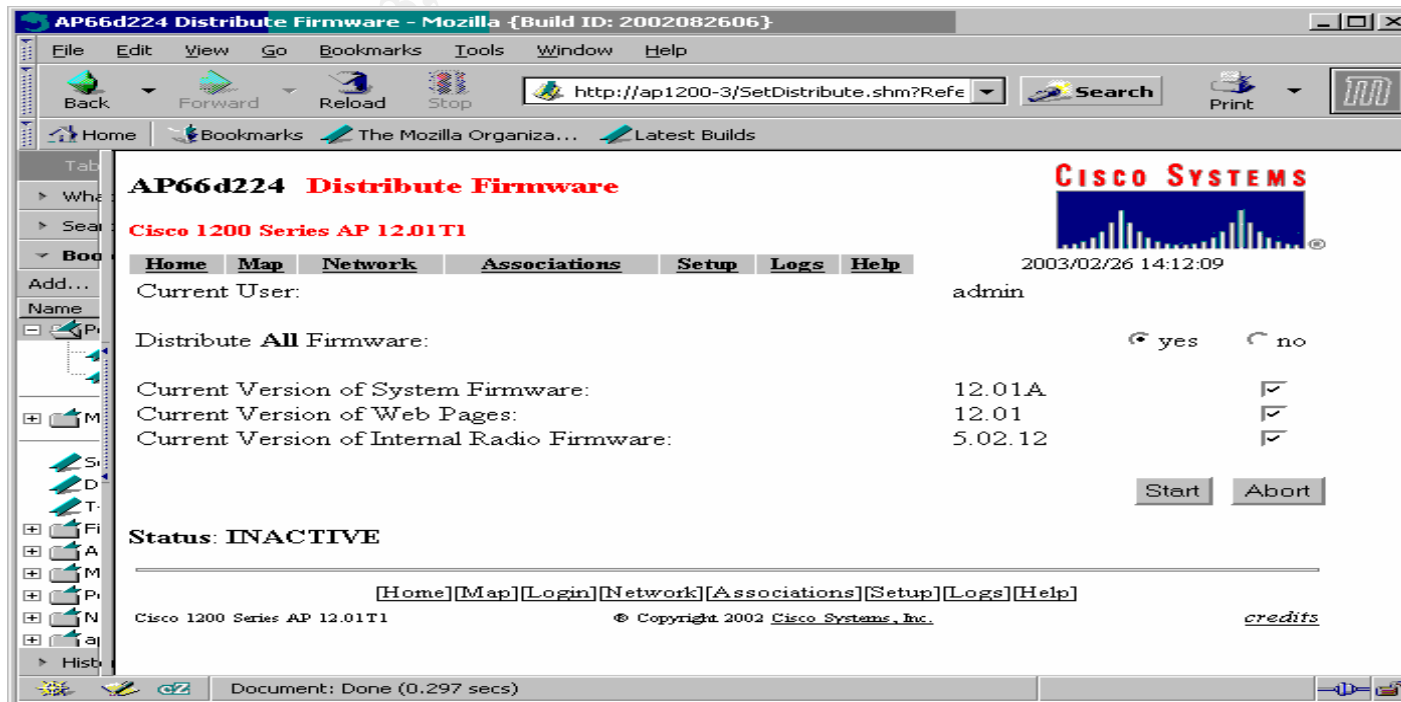


Figure 14

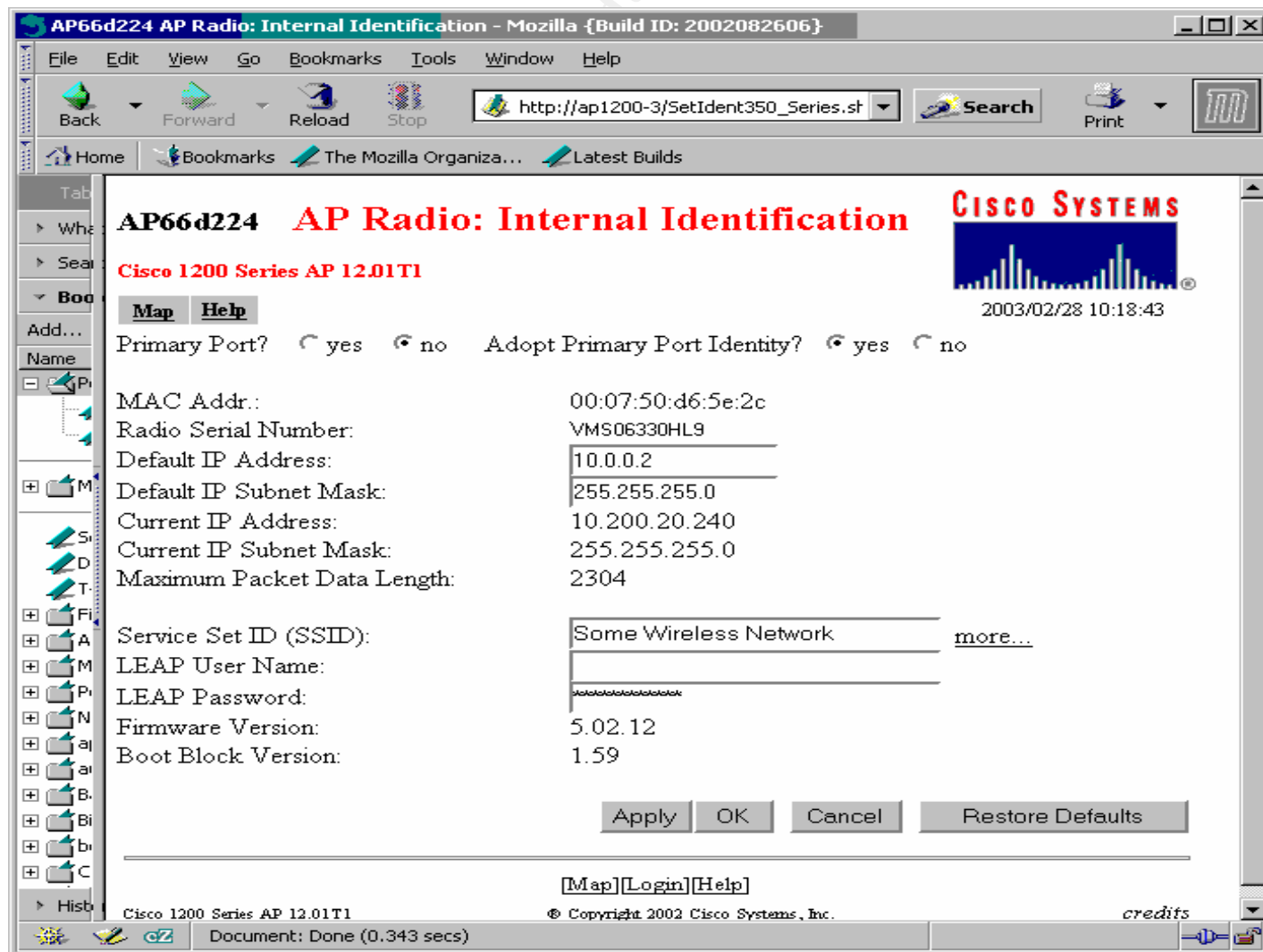


Figure 15

#### D4 Determine that the interval between “Beacon Frames” has been made as long as possible

**Action:** [Using the captured data created in stage 2 of network monitoring of the *Wireless side*, open the file using Wildpackets Airopeek, validate that the Beacon Packets are sent at a time interval of 5 seconds (current Cisco maximum) between packets. Start-> Programs -> Wildpackets AiroPeek NX -> Find a Beacon packet -> Edit -> Select Related Packets ->by Protocol ->Hide Unselected. The packets displayed are sequential Beacon packets only. Insure Delta Time is selected in the header, the time interval between Beacon packets is displayed]

**Expected Results:** [Assign a PASS if the Beacon packets are 5 or more seconds apart, otherwise FAIL]

**Actual Results:** PASS Figure 16 displaying only Beacon packets, and the time between them is approximately 5.12 seconds

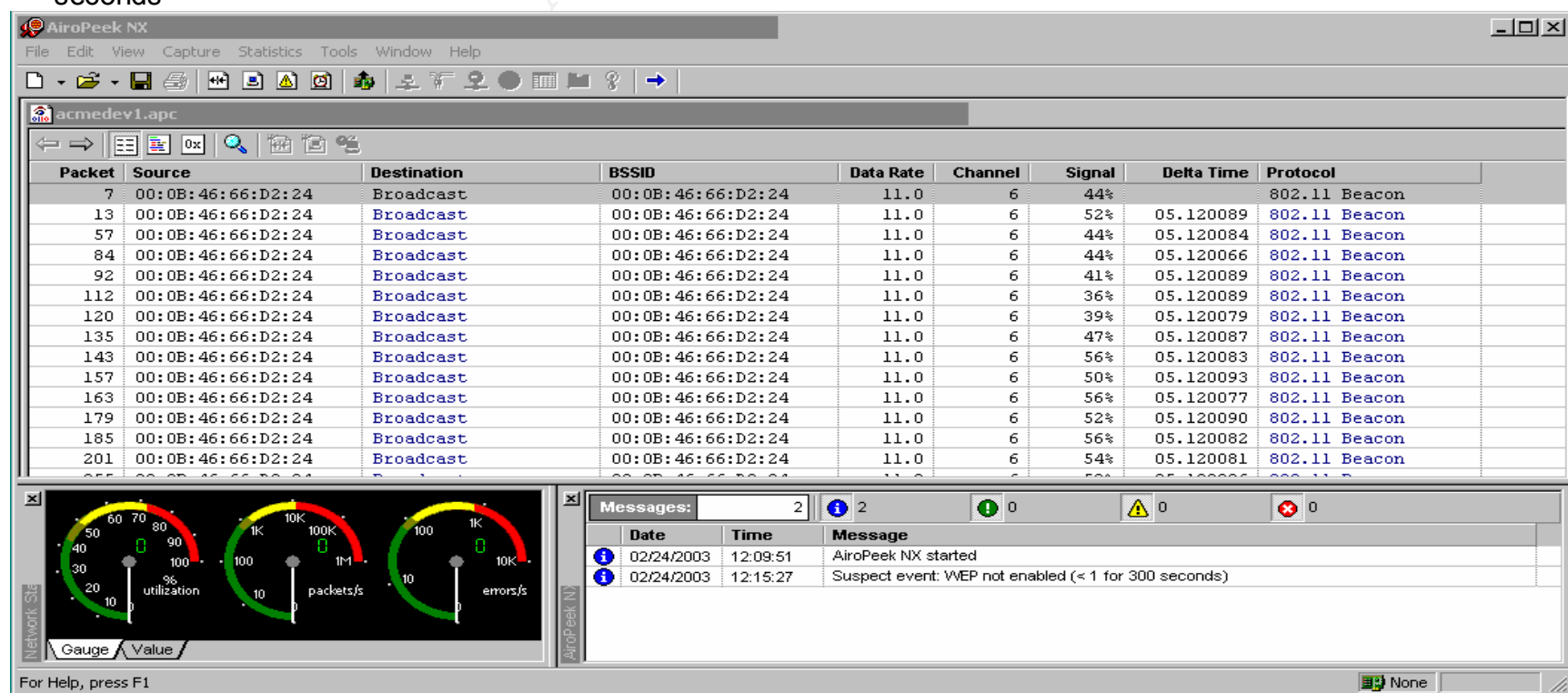


Figure 16

## D5 Determine that the default Service Set Identifier (SSID) has been changed to a Company security policy compliant value

**Action:** [1) Using the Capture file, obtained in the capture in stage 2 of the *Wireless side*, select a 802.11 Probe a Response packet from this AP (Mac Address 00:0B:46:66:D2:24), open the packet, scroll down to the first Information Element value, observe the SSID value, insure that it is not "tsunami". 2) Have administrator make a network connection to manage the AP, once connected at the Summary status page go to -> Setup -> AP Radio Internal Hardware. View the entry for Allow Broadcast SSID to associate 3) Using a Laptop with a wireless connection that has not been configured to access this network, assume DHCP address assignment, correctly configure the wireless card with WEP Key, enable the Broadcast SSID, and see whether it can associate. Go to -> Start -> Settings -> Network Connections -> Wireless Network Connection -> Properties -> Wireless Network -> Add -> do not enter the SSID, adjust the Data Encryption, Network Authentication switches, and enter the Network Key as appropriate. Observe whether or not an IP address is assigned]

**Expected Results:** [Assign a PASS if the SSID is not the default, is security policy compliant, if used, and does not allow associations from stations implementing the broadcast SSID, otherwise FAIL]

**Actual Results:** PASS Broadcast SSID disabled, in AP settings, (Figure 18) Packet capture below demonstrates the SSID is not the default, and is WEP enabled. Figure 17 demonstrates that the media is disconnected, and no IP address is assigned

### Packet Info

Flags: 0x00  
Status: 0x00  
Packet Length: 101  
Timestamp: 07:23:05.560065 02/24/2003  
Data Rate: 22 11.0 Mbps  
Channel: 6 2437 MHz  
Signal Level: 54%

### 802.11 MAC Header

Version: 0  
Type: %00 Management  
Subtype: %0101 Probe Response  
To DS: 0  
From DS: 0  
More Frag.: 0

Retry: 0  
 Power Mgmt: 0  
 More Data: 0  
 WEP: 0  
 Order: 0  
 Duration: 213 Microseconds  
 Destination: 00:02:2D:59:E2:BF  
 Source: 00:0B:46:66:D2:24 ← Access point  
 BSSID: 00:0B:46:66:D2:24  
 Seq. Number: 1698  
 Frag. Number: 0  
 802.11 Management - Probe Response  
 Timestamp: 325632748366 Microseconds  
 Beacon Interval: 5000  
 ESS: 1  
 IBSS: 0  
 CF Pollable: 0  
 CF Poll Req.: 0  
**Privacy: 1** ← When Privacy =1 WEP is enabled  
 Short Preamble: 1  
 PBCC: 0  
 Chan. Agility: 0  
 Reserved: 0

#### Information Element

Element ID: 0 SSID  
 Length: 21  
**SSID: Some Wireless Network** ← SSID has been changed from "tsunami"

#### Information Element

Element ID: 1 Supported Rates  
 Length: 1  
 Supported Rate: 0x96 11.0 Mbps (BSS Basic Rate)

#### Information Element

Element ID: 3 Direct Sequence Parameter Set  
 Length: 1  
 Channel: 6

Information Element

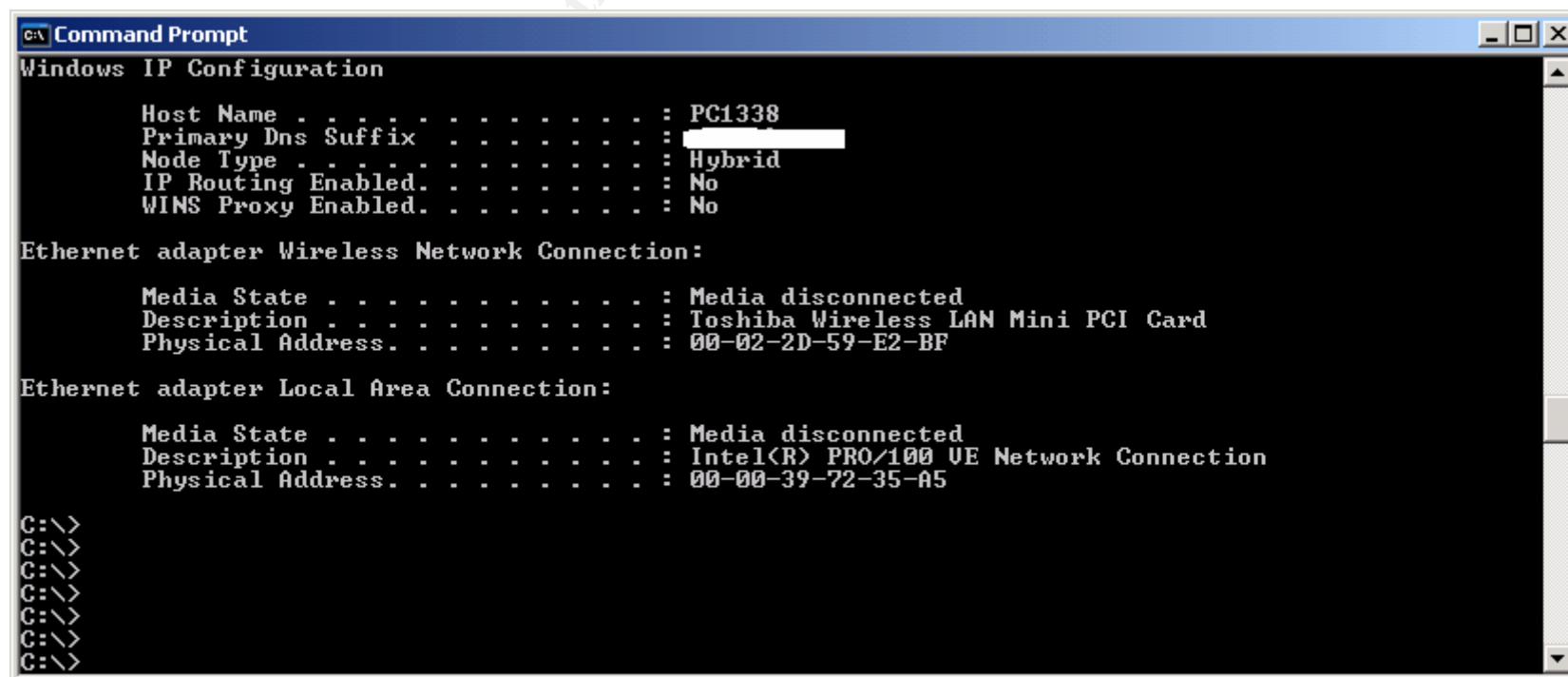
Element ID: 133

Length: 30

Value: 0x00004C0D0700FF001100415036366432323400000000000000001000022

FCS - Frame Check Sequence

FCS (Calculated): 0x3A6A94A4



```
C:\ Command Prompt
Windows IP Configuration

Host Name . . . . . : PC1338
Primary Dns Suffix . . . . . : 
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Wireless Network Connection:

Media State . . . . . : Media disconnected
Description . . . . . : Toshiba Wireless LAN Mini PCI Card
Physical Address. . . . . : 00-02-2D-59-E2-BF

Ethernet adapter Local Area Connection:

Media State . . . . . : Media disconnected
Description . . . . . : Intel(R) PRO/100 VE Network Connection
Physical Address. . . . . : 00-00-39-72-35-A5

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

Figure 17

## AP66d224 AP Radio: Internal Hardware

Cisco 1200 Series AP 12.01T1

CISCO SYSTEMS



2003/03/17 14:37:26

[Map](#) [Help](#)

Service Set ID (SSID):  [more...](#)

Allow "Broadcast" SSID to Associate?: ☐ yes ☒ no

Enable "World Mode" multi-domain operation?:

Data Rates (Mb/sec):

1.0  2.0  5.5  11.0

Transmit Power:

Frag. Threshold (256-2338):

RTS Threshold (0-2339):

Max. RTS Retries (1-255):

Max. Data Retries (1-255):

Beacon Period (19-5000 Kusec):

Data Beacon Rate (DTIM):

Default Radio Channel:

In Use: 6

Search for less-congested Radio Channel?:

[Restrict Searched Channels](#)

Receive Antenna:

Transmit Antenna:

If VLANs are *not* enabled, set Radio Data Encryption through the link below. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

[Radio Data Encryption \(WEP\)](#)

[Map](#) [Login](#) [Help](#)

Cisco 1200 Series AP 12.01T1

© Copyright 2002 Cisco Systems, Inc.

[credits](#)

Figure 18



## D6 Wired-Equivalent Privacy (WEP) Encryption

**Action:** [1) Using the Capture file, obtained in the capture in stage 2, of the **Wireless side** select a 802.11 Probe Response packet from this AP (Mac Address 00:0B:46:66:D2:24), open the packet, scroll down to 802.11 Management - Probe Response, observe the Privacy: value, insure that it is set to "1" This indicates that WEP is enabled. A typical entry is shown in D5 above, in the packet capture. 2) Using the Capture file, perform an edit, to select all the data that is not 802.11 WEP encrypted data, and hide it, look at the remaining data, for data that has not been encoded, and has meaningful information Select a packet e.g. Beacon packet Edit -> select related packets -> By protocol -> Hide Selected Packets -> select next packet to be hidden and repeat until the only packets remaining to be displayed are unencoded packets. In this case the only ones remaining are Null Function packets. 3) Examine the WEP key to validate that it is corporate policy compliant, and that it is 128 bits, or more in length [Have the administrator provide the encryption key, being used. Validate that it is 128 bits (physically 104 bits) or better, and complies with corporate policy, or if there is no corporate policy, then best practices.]

**Expected Results:** Capture wireless network traffic to validate that it is encrypted. [Assign a PASS if it is WEP Encrypted, otherwise FAIL]

[Assign a PASS if it is 128 bits (physically 104 bits) or better, and complies with corporate policy, or if there is no corporate policy, then best practices otherwise FAIL.] Inspected WEP key is physically 104 bits.

**Actual Results:** **PASS** Figure 19 shows the data, before the start of filtering, as indicated by the action above. After filtering out all of the data that is not WEP encoded one is left with Null Function packets. These are depicted in Figure 20. The data contained in the remaining packets for the time being is considered to provide little additional information.

Typical Packet data in the file (below) before initial filtering.

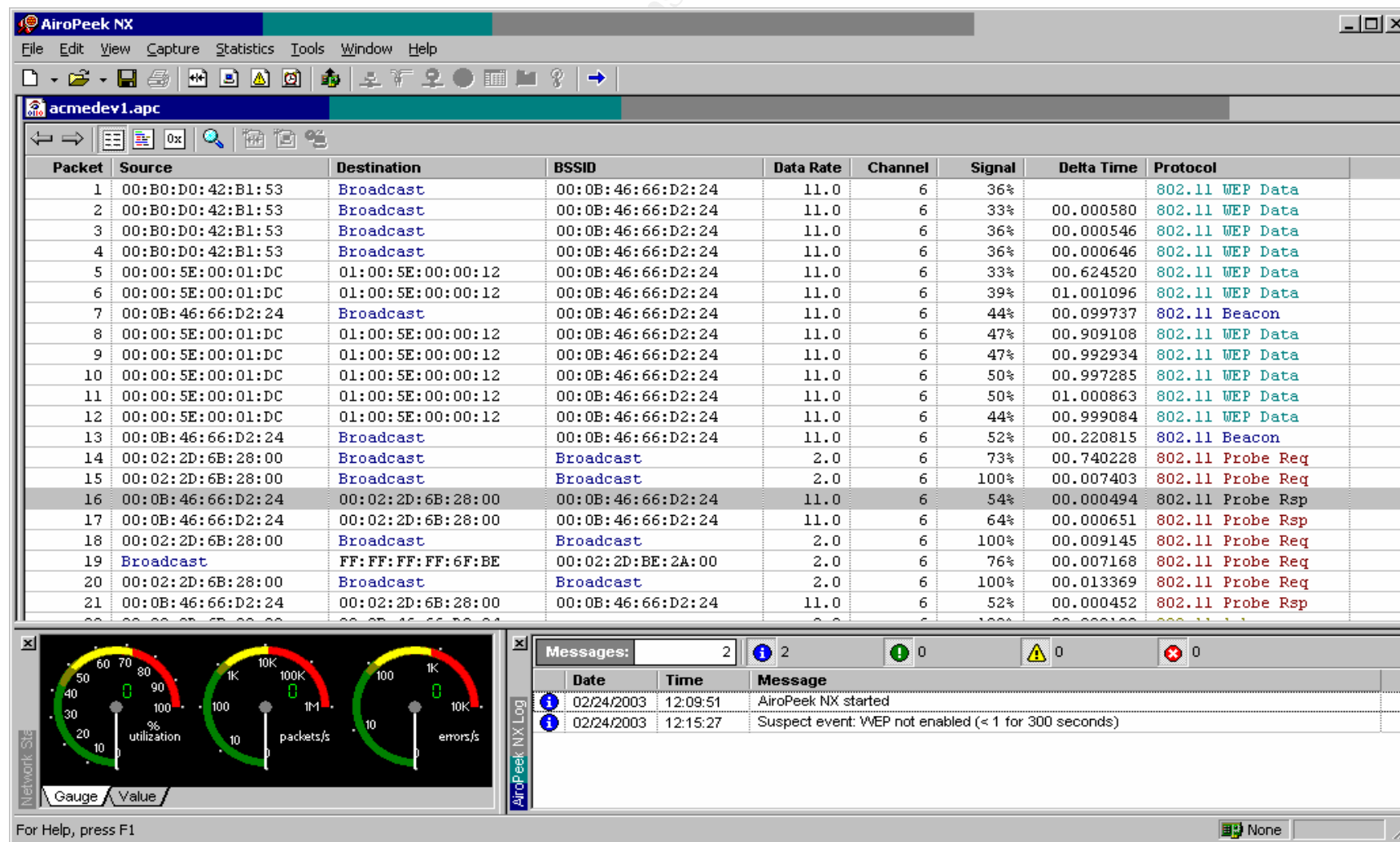


Figure 19

Typical data not WEP encoded after repeat filtering (below) it is a Null Function Packet, and contains no data of any merit.

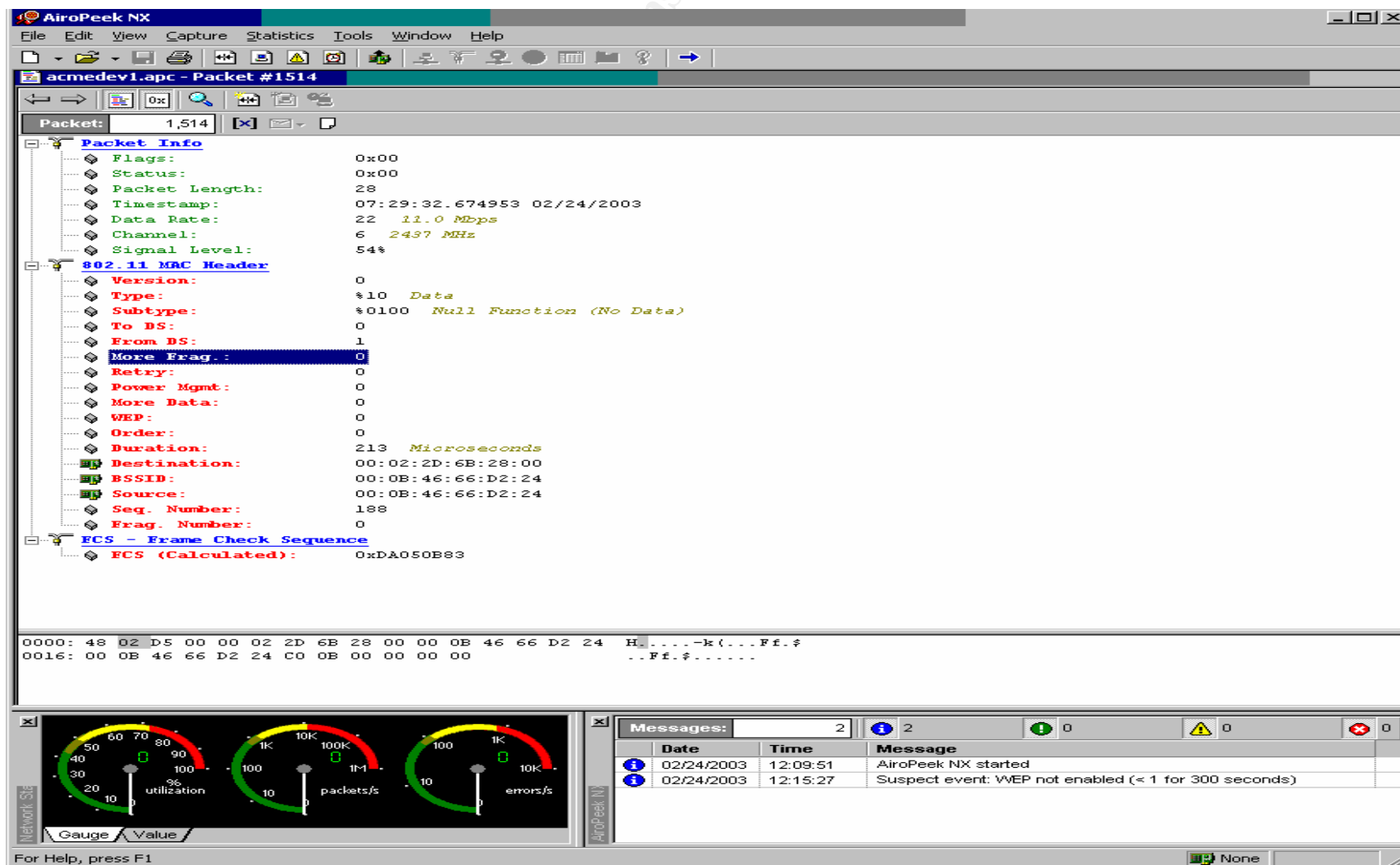


Figure 20

### **D7 Additional Link Layer Security Features available on the Unit**

**Action:** [Have administrator make a network connection to manage the AP, once connected at the Summary status page go to ->Setup ->AP Radio Advanced. Look at the data contained in Enhanced MIC verification for WEP, Temporal Key Integrity Protocol (TKIP), and Broadcast WEP Key rotation interval.]

**Expected Results:** The settings implemented in the 12.01T1 software are currently Cisco extensions to the Standard, and do not fully implement the 802.1x standard for cross vendor compatibility. Not all vendors' hardware and software will function with, or make use of these settings.

[PASS if implemented, otherwise FAIL]

**Actual Results: FAIL**

Enhanced MIC verification for WEP "None", Temporal Key Integrity Protocol (TKIP) "None", Broadcast WEP Key rotation interval (sec) 0, as demonstrated in Figure 21 below, in approximately the middle of the figure.

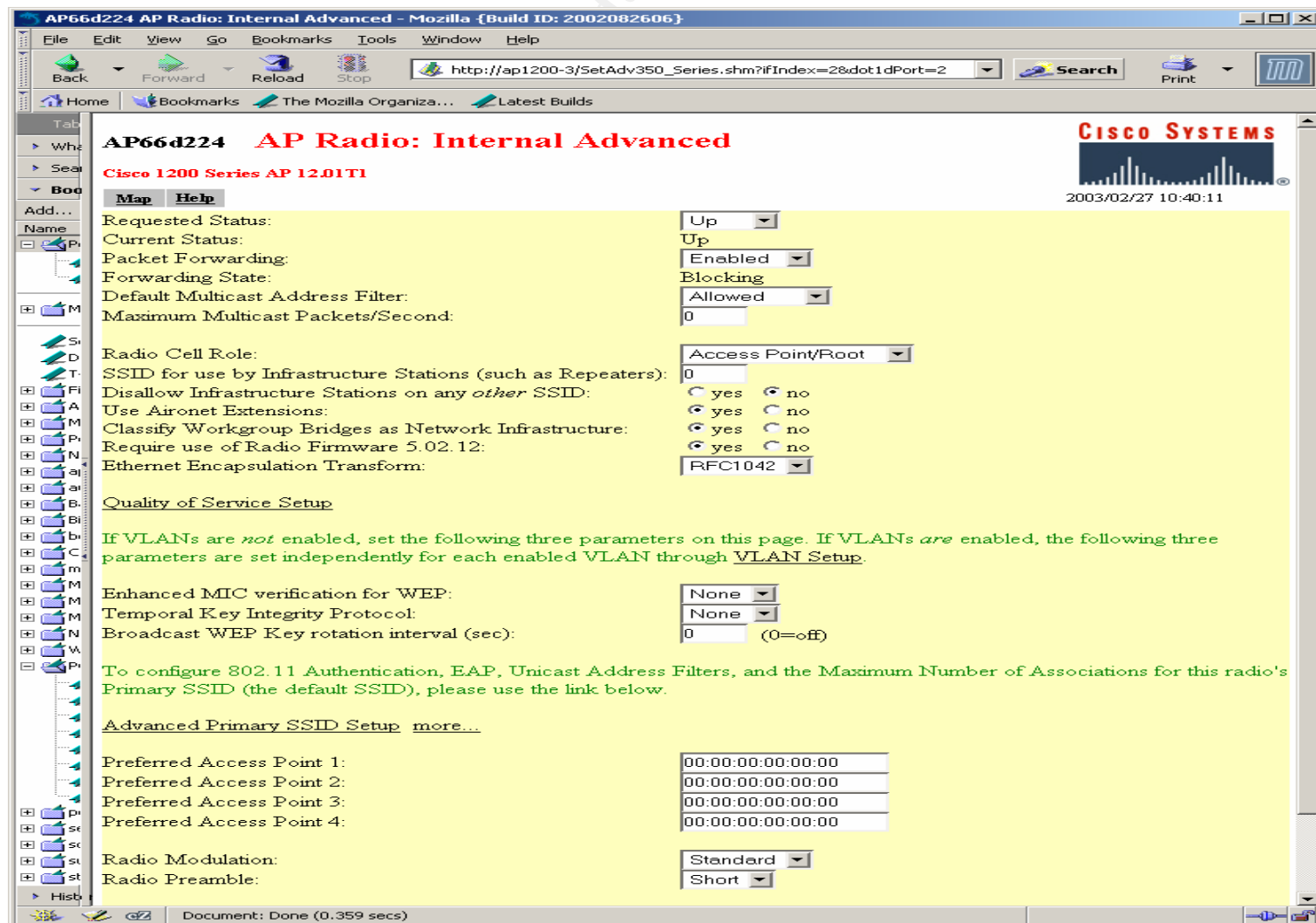


Figure 21

### **D8 Discover whether Media Access Control (MAC) address based Access and Association control has been implemented.**

**Action:** [Using a Laptop with a wireless connection, correctly setup and configured, establish a connection to the network. This tests successful association. Then using a Laptop with a wireless connection that has not been configured to access this network, assume DHCP address assignment, correctly configure the wireless card with WEP Key, SSID, and 802.1 X values as required, and see whether it can associate. Go to-> Start -> Settings -> Network Connections ->Wireless Network Connection -> Properties -> Wireless Network -> Add -> enter the SSID, adjust the Data Encryption, Network Authentication switches, and enter the Network Key as appropriate, then go to Authentication, and adjust Enable IEEE 802.1x, and EAP types as appropriate. Then perform the MAC based authentication test. Record If an IP address is assigned, Start -> Programs -> Accessories ->Command Prompt -> type Ipconfig /all, and observe and record the data presented, looking for IP address assignment, repeat as required, observe the events that take place for 5 minutes and record as appropriate. To access data from the AP, Have administrator make a network connection to manage the AP, once connected at the Summary status page go to ->Setup -> Address Filters, observe and record the data. Go to Setup -> Security Server ->Authentication Server, observe and record the data.]

**Expected Results:** Assign a PASS if a Wireless card that should be able to authenticate, with the Access Point, is able to, and the card, which should not be able to associate, is unable to remain associated with the Access Point, otherwise FAIL.

**Actual Results:** PASS although the Access point is not performing MAC authentication, there appears to be another device further in performing a similar function, as the information below indicates.

The first 3 frames below, Figures 22,23, and 24 have been recorded for a station that has not been entered into any access database, as the auditor brought it along for this test. Looking at the first 3 frames below, Figures 22,23, and 24, there is an association formed, see Figure 24 at 14:52:33 with the AP, it lasts for approximately 30 seconds and then is de-authenticated Figure 24 at 14:53:03 (media disconnected). This action repeats every few minutes. It is demonstrated in the first 2 pictures below, Figures 22 & 23. The Access point indicates that the disassociation is due to NO EAP Authentication from the server, this is in Figure 24 The Figure 25 demonstrates that there are no MAC addresses entered in the Access point. Figure 26 also confirms that MAC authentication is not used in the Access point, it is using Radius and EAP authentication instead.

```

C:\>
C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : PC1338
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . : 
    Description . . . . . : Toshiba Wireless LAN Mini PCI Card
    Physical Address. . . . . : 00-02-2D-59-E2-BF
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 
    DHCP Server . . . . . : 255.255.255.255

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Description . . . . . : Intel(R) PRO/100 VE Network Connecti
    Physical Address. . . . . : 00-00-39-72-35-A5

C:\>
```

Figure 22

```
C:\ Command Prompt
Windows IP Configuration

    Host Name . . . . . : PC1338
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Wireless Network Connection:

    Media State . . . . . : Media disconnected
    Description . . . . . : Toshiba Wireless LAN Mini PCI Card
    Physical Address. . . . . : 00-02-2D-59-E2-BF

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Description . . . . . : Intel(R) PRO/100 VE Network Connection
    Physical Address. . . . . : 00-00-39-72-35-A5

C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
```

Figure 23



AP66d224 Summary Status - Mozilla {Build ID: 2002082606}

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop http://ap1200-3/ Search Print

Home Bookmarks The Mozilla Organiza... Latest Builds

**AP66d224 Summary Status**

Cisco 1200 Series AP 12.01T1

CISCO SYSTEMS

2003/02/26 15:00:54

Home Map Network Associations Setup Logs Help

**Current Associations**

Clients: 1 of 2	Repeaters: 0 of 0	Bridges: 0 of 0	APs: 1
-----------------	-------------------	-----------------	--------

**Recent Events**

Time	Severity	Description
2003/02/26 14:57:32	Info	Station=[10.200.20.150]00022d6b2800 User="" EAP-Authenticated
2003/02/26 14:53:03	Info	Deauthenticating 00022d59e2bf, reason "Previous Authentication No Longer Valid"
2003/02/26 14:53:03	Warning	No EAP-Authentication response for Station 00022d59e2bf from server 10.100.10.1
2003/02/26 14:52:33	Info	Station 00022d59e2bf Associated
2003/02/26 14:52:33	Info	Station 00022d59e2bf Authenticated

**Network Ports**

Device	Status	Mb/s	IP Addr.	MAC Addr.
Ethernet	Up	10.0	10.200.20.240	000b4666d224
AP Radio: Internal	Up	11.0	10.200.20.240	000b4666d224

**Diagnostics**

[Home][Map][Login][Network][Associations][Setup][Logs][Help]

Cisco 1200 Series AP 12.01T1 © Copyright 2002 Cisco Systems, Inc. credits

Document: Done (0.266 secs)

Figure 24

## No MAC Address Filters Entered

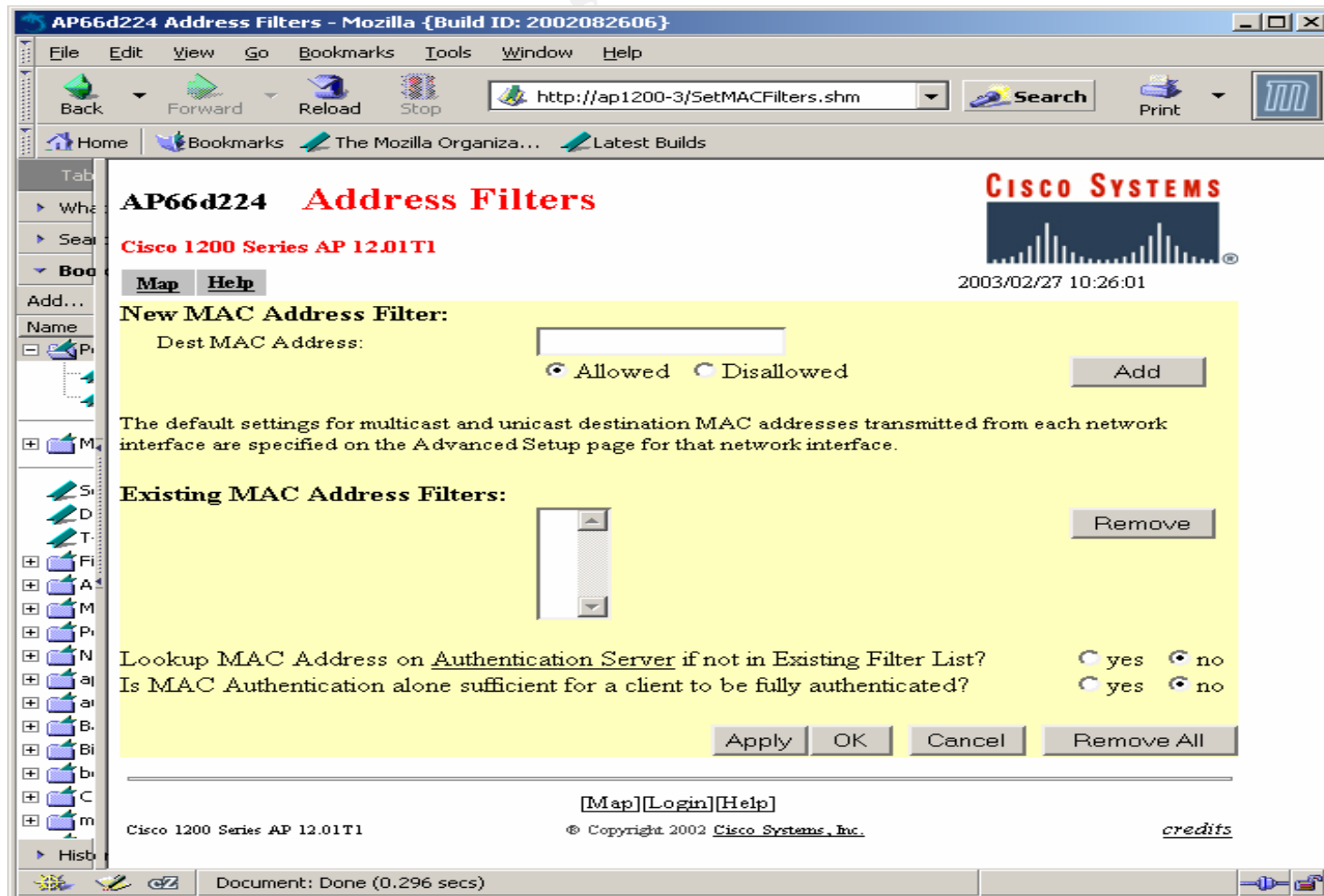


Figure 25

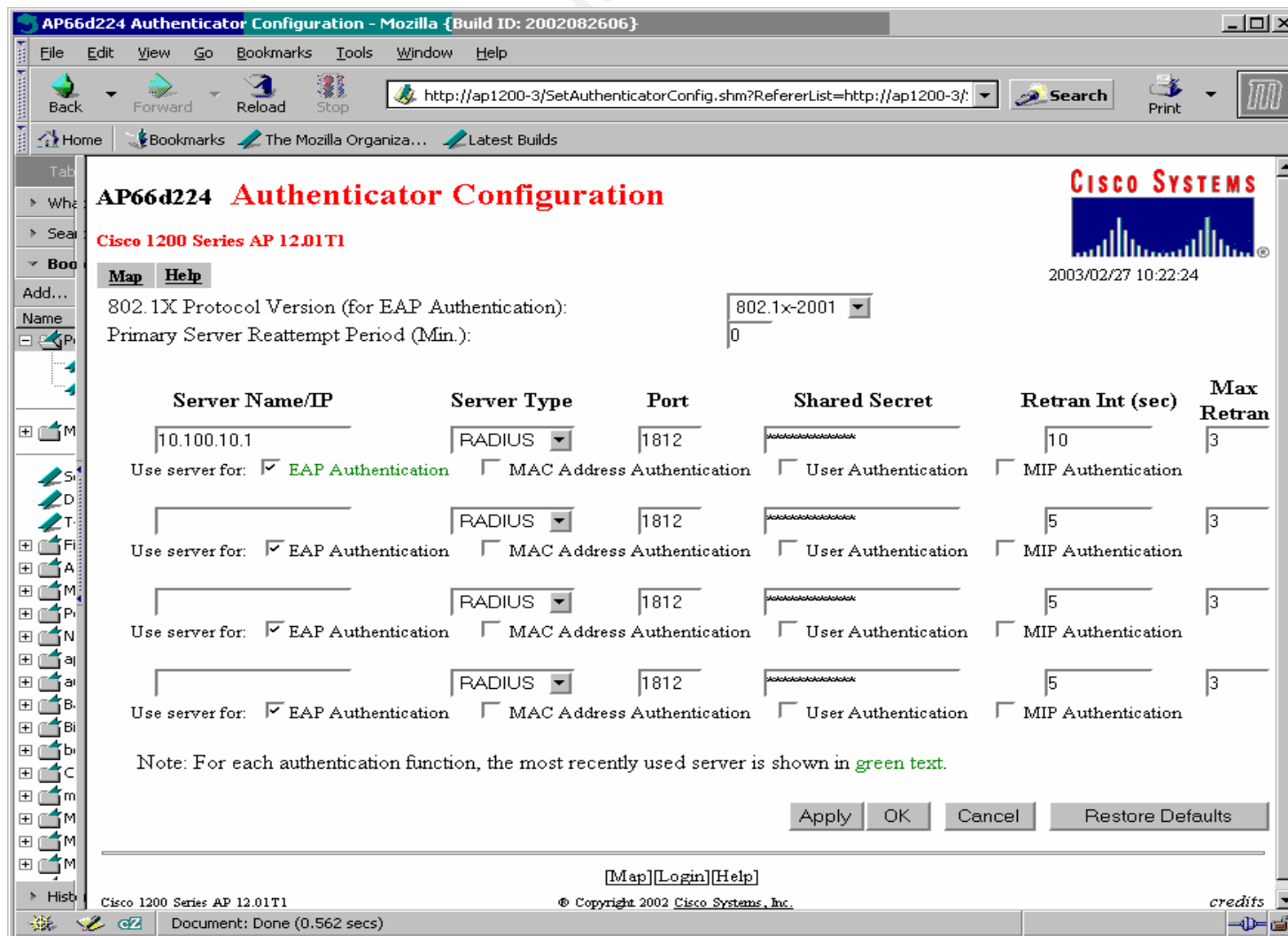


Figure 26

**D9 Discover whether Remote Authentication Dial-in User Service (RADIUS) based Access control has been implemented.**

**Action:** [Using the captured data created in stage 2 of network monitoring on the *wired* side, open the file using Wildpackets Etherpeek, Start-> Programs -> Wildpackets EtherPeek -> locate a successful logon sequence-> Edit -> identify the packets required for the logon ->select them ->Hide Unselected. The packets displayed are the logon sequence packets only. Evaluate the logon process. If packets are displayed with the protocol "Radius" then Radius authentication is being used. If no radius packets can be found in the Capture of the successful logon on sequence then Radius authentication is not being used]

**Expected Results:** (Requires a RADIUS server) [Assign a PASS, if, RADIUS access control implemented, otherwise FAIL]

**Actual Results:** PASS Figure 26 establishes the expectation that server 10.100.10.1 is providing Radius authentication, the packet trace in Figure 27 confirms that Radius authentication is being provided by Node "Viking". The administrator confirmed that Node "Viking" and 10.100.10.1 are the same, this was substantiated by the packet decode, not included for brevity.

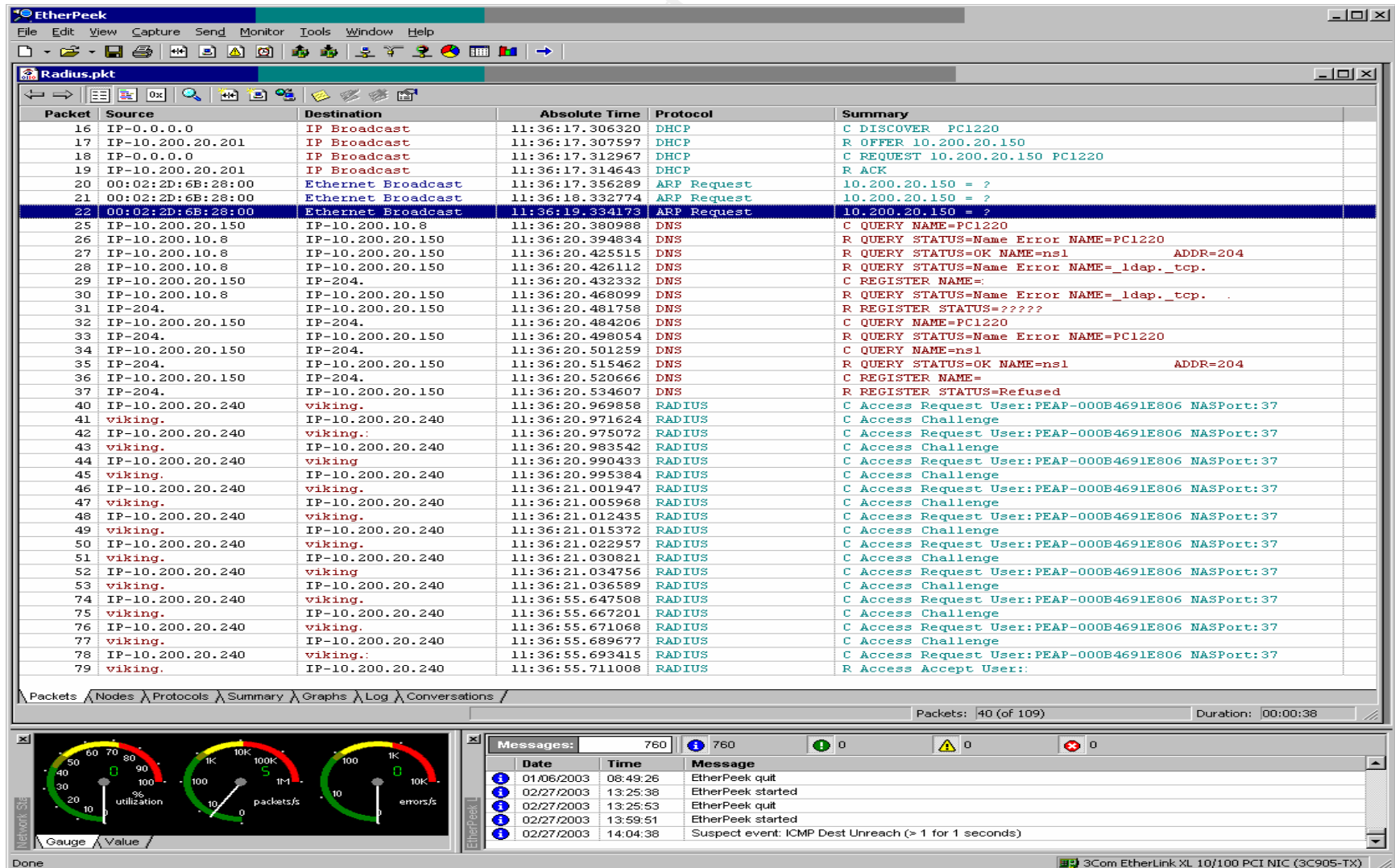


Figure 27

**D10 Discover whether RADIUS based Access control has been implemented, with Extensible Authentication Protocol (EAP), a protocol supporting 802.1x features.**

**Action:** [Using the Capture file obtained in stage 2 for the *Wireless side*, find a successful log on sequence from this AP (Mac Address 00:0B:46:66:D2:24) and the test machine, open the packets, inspect contents, Locate EAP Success reply packet]

**Expected Results:** (Requires a RADIUS server, EAP enabled)[Assign a PASS, if, RADIUS access control, with EAP implemented, otherwise FAIL]

**Actual Results:** PASS Figure 28 demonstrates the capture data we are looking for, the EAP start and request packets are 1166 and 1168 respectively, the EAP Success reply packet is 1363.

The first packet capture displayed after Figure 28 is the EAP start Request packet 1166. The second displayed capture is the contents of the EAP Success packet 1363

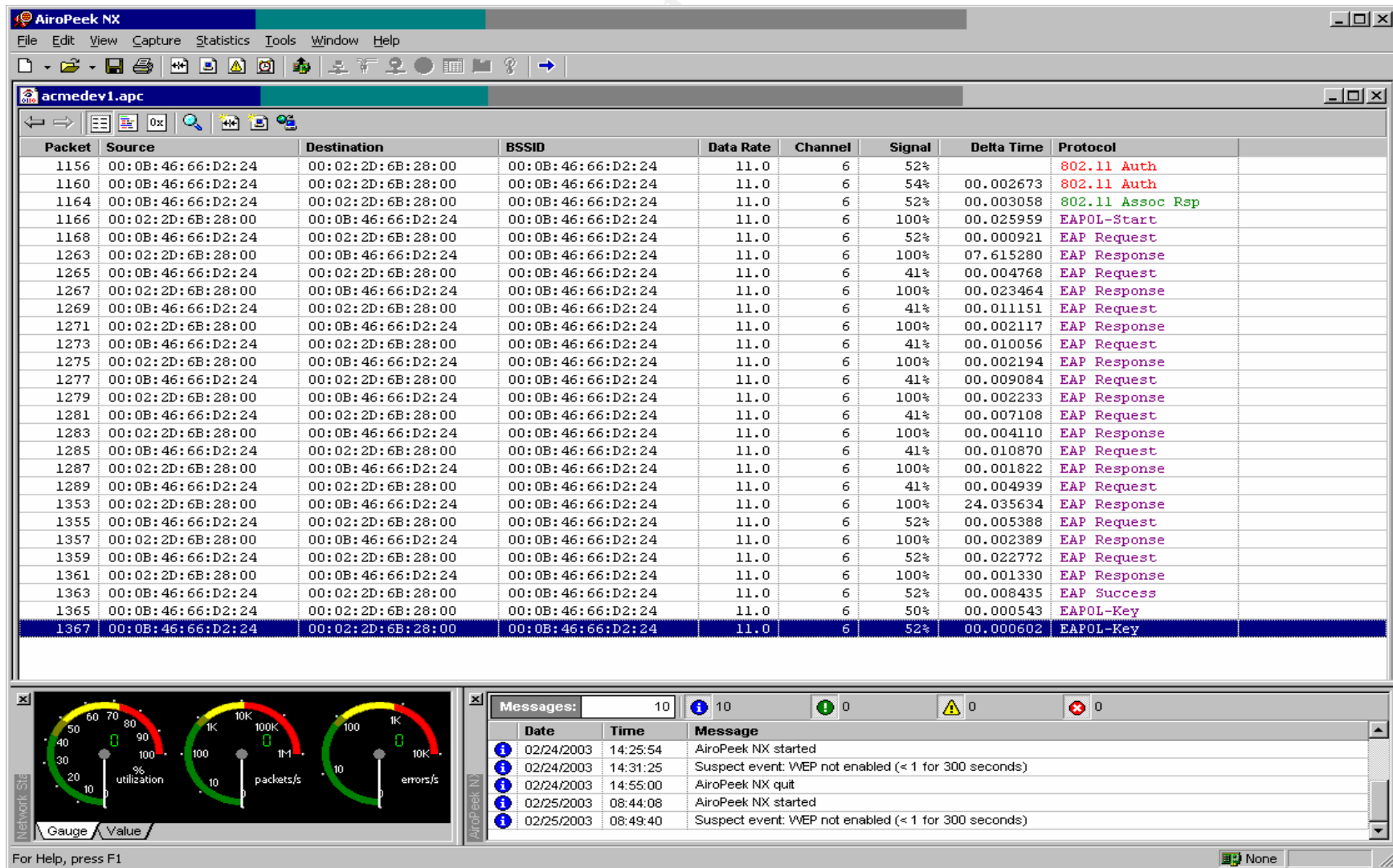


Figure 28

## EAP start Request

### Packet Info

Flags: 0x00  
Status: 0x00  
Packet Length: 41  
Timestamp: 07:28:32.530628 02/24/2003  
Data Rate: 22 11.0 Mbps  
Channel: 6 2437 MHz  
Signal Level: 100%

### 802.11 MAC Header

Version: 0  
Type: %10 Data  
Subtype: %0000 Data Only  
To DS: 1  
From DS: 0  
More Frag.: 0  
Retry: 0  
Power Mgmt: 0  
More Data: 0  
WEP: 0  
Order: 0  
Duration: 213 Microseconds  
BSSID: 00:0B:46:66:D2:24  
**Source:** 00:02:2D:6B:28:00 ← Toshiba Network Adapter  
**Destination:** 00:0B:46:66:D2:24 ← Cisco Access Point  
Seq. Number: 14  
Frag. Number: 0

### 802.2 Logical Link Control (LLC) Header

Dest. SAP: 0xAA SNAP  
Source SAP: 0xAA SNAP  
Command: 0x03 Unnumbered Information  
**Protocol:** 0x000000888E 802.1x Authentication

### 802.1x Authentication

Protocol Version: 1  
**Packet Type:** 1 EAPOL – Start ← Extensible Authentication Protocol over LAN  
Body Length: 0



Packet Data:  
00  
FCS - Frame Check Sequence  
FCS (Calculated): 0xDAB2AE54

## EAP Reply

### Packet Info

Flags: 0x00  
Status: 0x00  
Packet Length: 101  
Timestamp: 07:28:32.531549 02/24/2003  
Data Rate: 22 11.0 Mbps  
Channel: 6 2437 MHz  
Signal Level: 52%

### 802.11 MAC Header

Version: 0  
Type: %10 Data  
Subtype: %0000 Data Only  
To DS: 0  
From DS: 1  
More Frag.: 0  
Retry: 0  
Power Mgmt: 0  
More Data: 0  
WEP: 0  
Order: 0  
Duration: 213 Microseconds  
**Destination: 00:02:2D:6B:28:00** ← Toshiba Network Adapter  
BSSID: 00:0B:46:66:D2:24  
**Source: 00:0B:46:66:D2:24** ← Cisco Access Point  
Seq. Number: 42  
Frag. Number: 0

### 802.2 Logical Link Control (LLC) Header

Dest. SAP: 0xAA SNAP  
Source SAP: 0xAA SNAP  
Command: 0x03 Unnumbered Information

**Protocol:** 0x000000888E 802.1x Authentication

802.1x Authentication

Protocol Version: 1

**Packet Type:** 0 EAP - Packet

Body Length: 61

EAP - Packet

**Code:** 1 Request

Identifier: 46

Length: 61

**Type:** 1 Identity

**Type-Data:** .networkid=Some Wireless Network,nasid=AP66d224,portid=0 ← The network being audited.

FCS - Frame Check Sequence

FCS (Calculated): 0x45A05F48

## EAP Success

Packet Info

Flags: 0x00

Status: 0x00

Packet Length: 44

Timestamp: 07:29:04.316693 02/24/2003

Data Rate: 22 11.0 Mbps

Channel: 6 2437 MHz

Signal Level: 52%

802.11 MAC Header

Version: 0

Type: %10 Data

Subtype: %0000 Data Only

To DS: 0

From DS: 1

More Frag.: 0

Retry: 0

Power Mgmt: 0

More Data: 0

WEP: 0

Order: 0

Duration: 213 Microseconds  
**Destination:** 00:02:2D:6B:28:00 ← Toshiba Network Adapter  
BSSID: 00:0B:46:66:D2:24  
**Source:** 00:0B:46:66:D2:24 ← Cisco Access Point  
Seq. Number: 126  
Frag. Number: 0  
802.2 Logical Link Control (LLC) Header  
Dest. SAP: 0xAA SNAP  
Source SAP: 0xAA SNAP  
Command: 0x03 Unnumbered Information  
**Protocol:** 0x00000088E 802.1x Authentication  
802.1x Authentication  
Protocol Version: 1  
**Packet Type:** 0 EAP - Packet  
Body Length: 4  
**EAP - Packet**  
**Code:** 3 Success  
Identifier: 91  
Length: 4  
  
FCS - Frame Check Sequence  
FCS (Calculated): 0xD0EF9035

---

### D11 Discover whether VLAN based Networking has been implemented

**Action:** [1) Question the Administrator to discover whether or not Acme has implemented VLANs in the Wireless Network. 2) Using the Capture file obtained in stage 2 for the *wired side*, observe the Packets recorded for evidence of VLAN tagging]

**Expected Results:** [Assign a pass if VLANs have been implemented, otherwise FAIL]

**Actual Results:** **FAIL** No VLANs implemented The Administrator admitted VLANs are not implemented. The Network trace on the *wired* side showed no evidence of packets having VLAN Tagging implemented.

## D12 Discover whether IPSec (VPN) based Access control has been implemented

**Action:** [Using the captured data created in stage2 of network monitoring on the **wired** side, open the file using Wildpackets Etherpeek, Start-> Programs -> Wildpackets EtherPeek -> locate a successful logon sequence-> inspect the packets following the successful logon for protocol IPSEC->select them ->Hide Unselected. The packets displayed are the IPSEC packets only. Evaluate the packet contents. It may be encrypted depending on whether Authentication Header, (IP protocol 51) or Encapsulation Security Payload (IP protocol 50) is being used]

**Expected Results:** [Assign a PASS, if, IPSec Encapsulation Security Payload (IP protocol 50) implemented, otherwise FAIL]

**Actual Results:** **FAIL** No IPSEC packets recorded

## D13 is there a Static IP addressing scheme in place?

**Action:** [Using a Laptop with a wireless connection, correctly setup and configured, establish a connection to the network then Start -> Programs -> Accessories ->Command Prompt -> type Ipconfig /all, and observe and record the data presented. Check for DHCP Enabled set to YES. Using the captured data created in stage 2 of network monitoring on the **wired** side, open the file using Wildpackets Etherpeek, Start-> Programs -> Wildpackets EtherPeek -> locate a successful logon sequence-> Edit -> identify the packets just previous to the logon we are looking for packets that would occur as the DHCP address assignment occurs ->select them ->Hide Unselected. The packets displayed are the logon sequence packets, and activity just previous. Evaluate the packets for DHCP activity. If packets are displayed with the protocol "DHCP" then DHCP address assignment is being used. If no DHCP packets can be found in the Capture then DHCP is not being used]

**Expected Results:** [Assign a PASS, if, no IP address assigned on boot up followed by association.

Assign a FAIL, if, IP address assigned on boot up, followed by association, is not a part of Acme's wireless network.

Assign a PASS, if, the IP address assigned on boot up, followed by association, is not a part of Acme's wireless network, but is a part of 169.254.aaa.bbb, and the machine performing the evaluation is running a Microsoft Operating System. Assign a FAIL, if, IP address assigned, is a part of Acme's wireless network, and DHCP is enabled]

**Actual Results:** **FAIL** (Ethernet adapter Wireless Network Connection, DHCP Enabled, yes DHCP Server 10.200.20.201 as demonstrated in Figure 29, and in the network trace Figure 30)

```

C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : PC1220
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : 

Ethernet adapter Wireless Network Connection 2:

    Media State . . . . . : Media disconnected
    Description . . . . . : Cisco Systems 350 Series PCMCIA Wireless LAN Adapter
    Physical Address. . . . . : 00-0B-46-91-E8-06

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . . . . : 
    Description . . . . . : Toshiba Wireless LAN Mini PCI Card
    Physical Address. . . . . : 00-02-2D-6B-28-00
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IP Address. . . . . : 10.200.20.150
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.200.20.1
    DHCP Server . . . . . : 10.200.20.201
    DNS Servers . . . . . : 10.200.10.8
                           10.200.10.9
    Lease Obtained. . . . . : Thursday, February 27, 2003 10:44:39 AM
    Lease Expires . . . . . : Thursday, February 27, 2003 12:44:39 PM

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Description . . . . . : Intel(R) PRO/100 VE Network Connection
    Physical Address. . . . . : 00-00-39-D5-D6-92

C:\>
C:\>
```

Figure 29

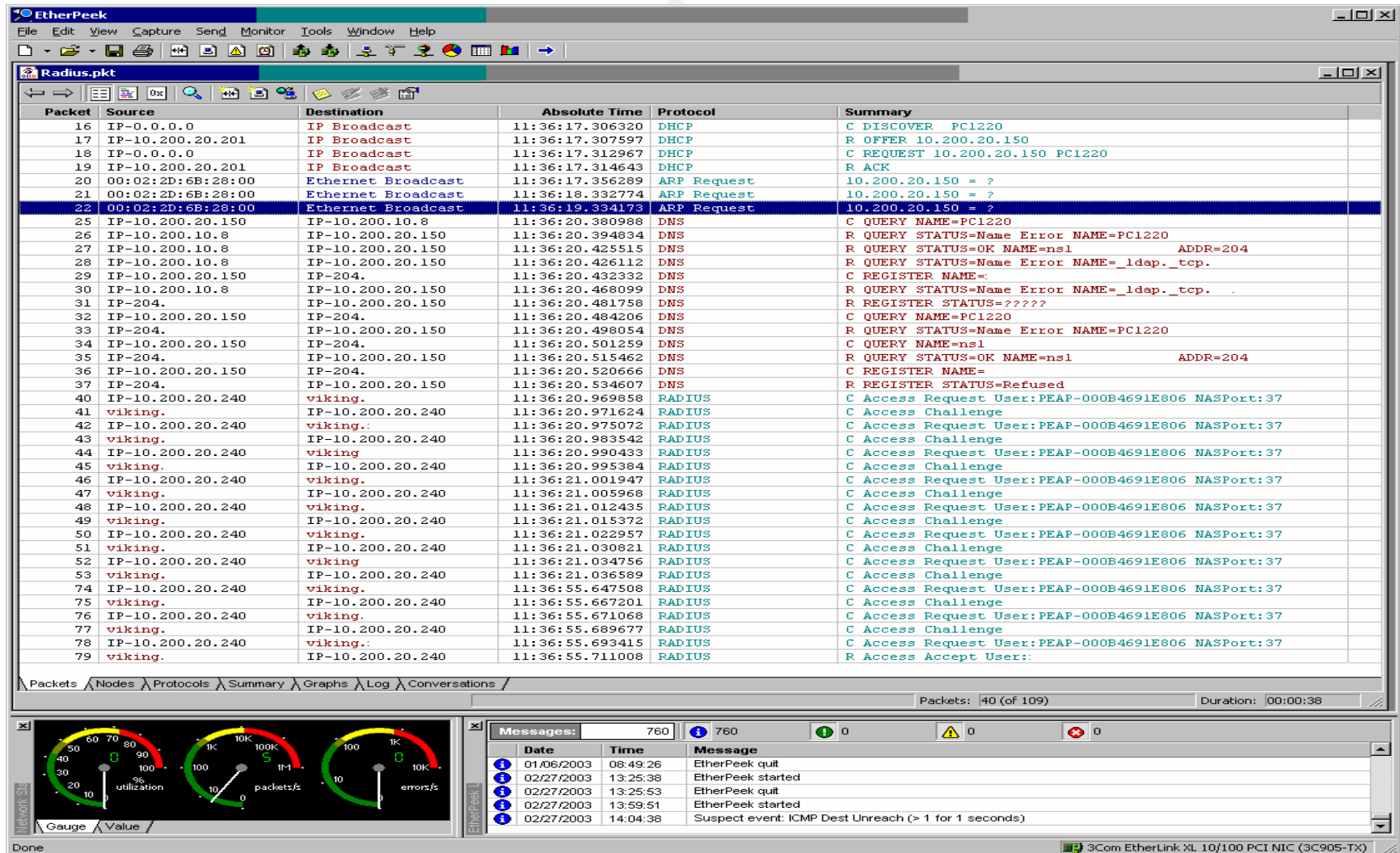


Figure 30

#### **D14 Has the wireless network been assigned a part of the “Special-Use IP address” space?**

**Action:** Using a Laptop with a wireless connection, correctly setup and configured, establish a connection to the network then Start -> Programs -> Accessories -> Command Prompt -> type Ipconfig /all, and observe and record the data presented. Evaluate the value assigned for IP Address]

**Expected Results:** [Assign a PASS, if the address is a part of a known “Special-Use” address space 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255 or 192.168.0.0 – 192.168.255.255 ” in use by Acme Development Company otherwise FAIL.]

**Actual Results:** PASS Address assigned is part of 10.0.0.0 “Special-Use” address space in use by Acme, see Figure 31.

```

C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : PC1220
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : 

Ethernet adapter Wireless Network Connection 2:

    Media State . . . . . : Media disconnected
    Description . . . . . : Cisco Systems 350 Series PCMCIA Wireless LAN Adapter
    Physical Address. . . . . : 00-0B-46-91-E8-06

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . . . . : 
    Description . . . . . : Toshiba Wireless LAN Mini PCI Card
    Physical Address. . . . . : 00-02-2D-6B-28-00
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IP Address. . . . . : 10.200.20.150
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.200.20.1
    DHCP Server . . . . . : 10.200.20.201
    DNS Servers . . . . . : 10.200.10.8
                           10.200.10.9
    Lease Obtained. . . . . : Thursday, February 27, 2003 10:44:39 AM
    Lease Expires . . . . . : Thursday, February 27, 2003 12:44:39 PM

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Description . . . . . : Intel(R) PRO/100 VE Network Connection
    Physical Address. . . . . : 00-00-39-D5-D6-92

C:\>
C:\>
```

Figure 31



### **D15 Determine that the wireless access point has SNMP disabled**

**Action:** [To access data from the AP, Have administrator make a network connection to manage the AP, once connected at the Summary status page go to ->Setup ->SNMP, observe and record the data. For independent assurance, using the captured data created in stage 2 of network monitoring on the **wired side**, open the file using Wildpackets Etherpeek, Start-> Programs -> Wildpackets EtherPeek -> visibly search the packets looking for protocol SNMP select them ->Hide Unselected. The packets displayed are the SNMP packets only. Evaluate the packet contents. If the data can be read then SNMP version 3 is not being used (this AP at this software version does not support SNMPv3)

**Expected Results:** [Assign a PASS, if, SNMP disabled, otherwise FAIL]

**Actual Results:** PASS SNMP setup is disabled, no SNMP packets recorded in the network traffic recording made in stage 2, see Figure 32, a few lines from the top, SNMP Disabled.

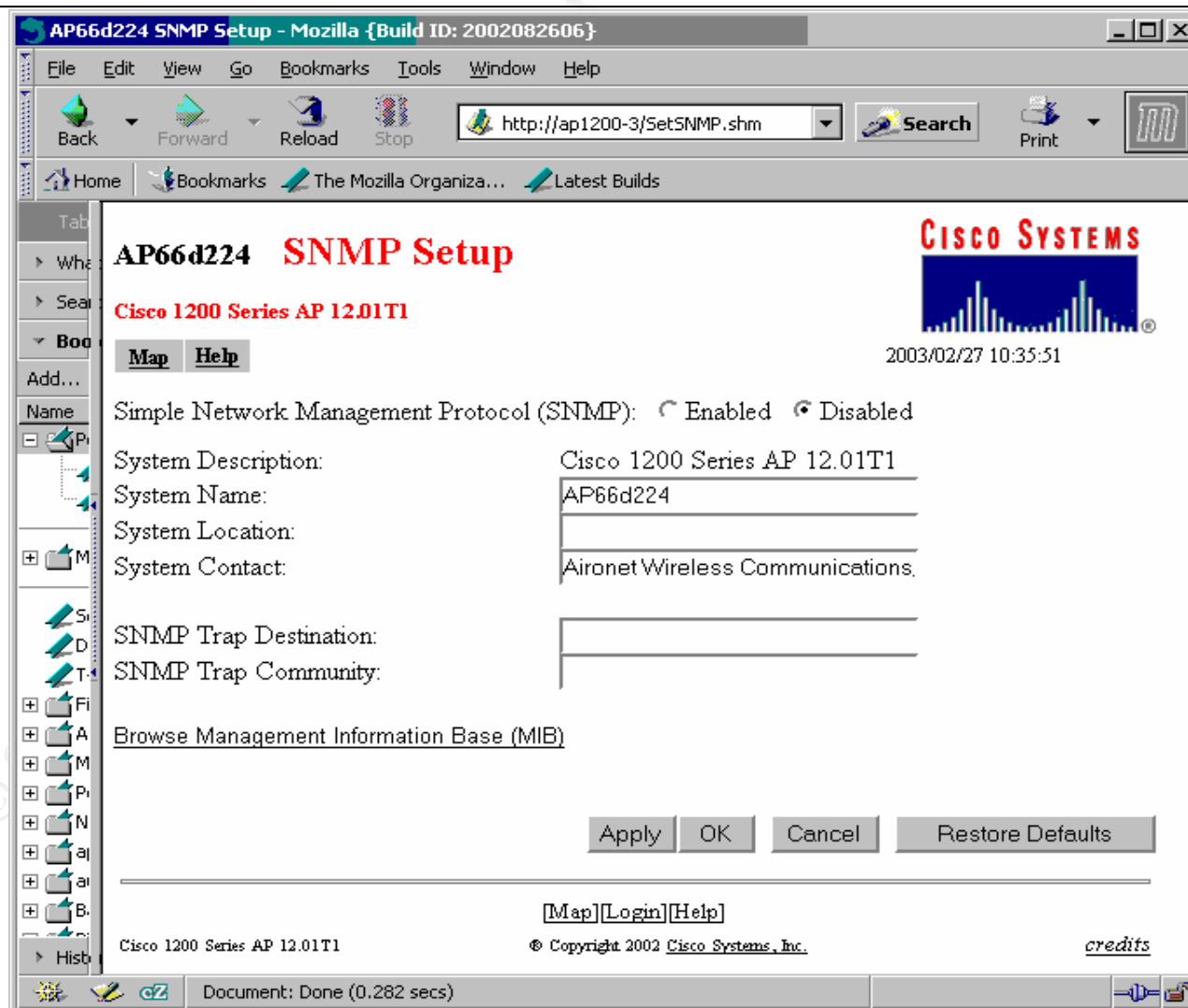


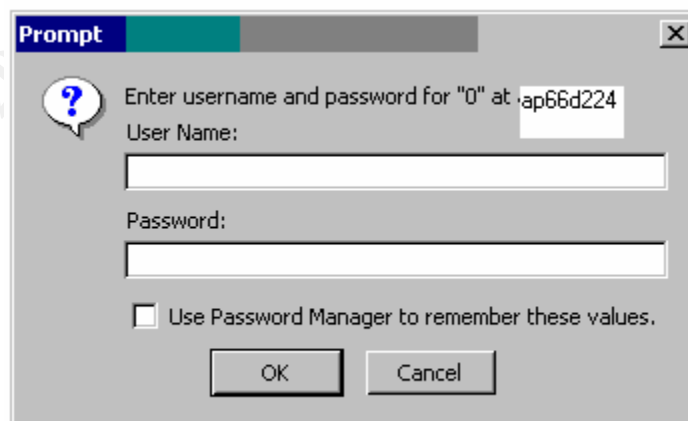
Figure 32

**D16 Determine that the administrator has entered a new administrative password**

**Action:** [Have the administrator obtain and enter a new company valid password into the Access Point and then validate that it cannot be accessed using the default password or the password used in step 3. To access data from the AP, Have administrator make a network connection to manage the AP, once connected at the Summary status page go to ->Setup -> Security Setup -> Change Current User Password -> enter Old User Password, New User Password, Confirm Password and Apply, then exit from the Access Point. Attempt to connect to the AP.]

**Expected Results:** [Assign a PASS, if you the Auditor cannot log in with the password provided in step 3, or the default password, otherwise FAIL]

**Actual Results:** PASS Figure 33



**Figure 33**

**An incorrectly typed password cycled back to the “Prompt” screen each time.**

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>E. Fieldwork Cisco Aironet 1200</b>	
<b>Management</b>	
1. Determine access methods used to manage the base station from the wired side. <ul style="list-style-type: none"> <li>• Attempt telnet access to base station</li> <li>• Attempt SSH access to base station</li> <li>• Attempt http access to base station</li> <li>• Attempt https access to base station</li> <li>• Scan access point with Nessus looking for open ports.</li> </ul>	<u>PASS</u> No Connection Connection Connection No connection Ports 22,23,80 &ICMP message
2. Determine access methods used to manage the base station from the <b>Wireless</b> side using 802.11b access. <ul style="list-style-type: none"> <li>• Attempt telnet access to base station</li> <li>• Attempt SSH access to base station</li> <li>• Attempt http access to base station</li> <li>• Attempt https access to base station</li> <li>• Scan access point with Nessus looking for open ports</li> </ul>	<u>FAIL/</u> Can be managed from Wireless side  No Connection Connection Connection No connection Ports 22,23,80 &ICMP message
3. Discover that Cisco Discovery Protocol (CDP) has been disabled	<u>PASS</u>
4. Discover what type of Network monitoring has been implemented	<b>FAIL/ No Monitoring implemented</b>

## F. Fieldwork Cisco Aironet 1200, Unauthorized Wireless Access Point Detection

### F1 Walk around the perimeter, parking lot, and streets adjacent to the facility or parking lot of Acme Development Company, looking for evidence of Warchalking

**Action:** [Walk around the facility, using the sidewalks, while observing the city street, the sidewalk, and the external street facing sides of the building for chalk marks as noted in <http://www.blackbeltjones.com/warchalking/warchalking09.pdf> or <http://wlana.net/warchalking.htm> for Warchalking Symbols. Take pictures as appropriate.]

**Expected Results:** [Assign a PASS if no marks indicating WarChalking activity has taken place, otherwise FAIL]

**Actual Results:** PASS no warchalking symbols noted

### F2 Using Wildpackets Airopoek, wireless network analyzer investigate the perimeter of the facility for unauthorized Wireless networks

**Action:** [Using the Capture file obtained in stage 4 for the **Wireless side** at the start of the audit, investigate the facility for unauthorized Wireless networks, Start-> Programs -> Wildpackets EtherPeek-> Open the capture file-> click on Peer Map tab. For Netstumbler Start -> Programs-> Netstumbler, it automatically starts capturing]

**Expected Results:** [Assign a PASS if no unauthorized networks are identified as being detected within the Acme Development Company Facility otherwise FAIL]

**Actual Results:** **FAIL** the results suggest that there are many other networks operating, as shown below, in the separate pictures, obtained over 3 sampling periods and using 2 different products, Wildpackets Airopoek and Netstumbler version 0.3.23. The situation has improved between Sample 1 (Figure 34) and Sample 3 (Figure 36), but there still is a problem here. Figure 35 provides Netstumbler's view of the problem.

Figure 34: Sample 1 - on day one.

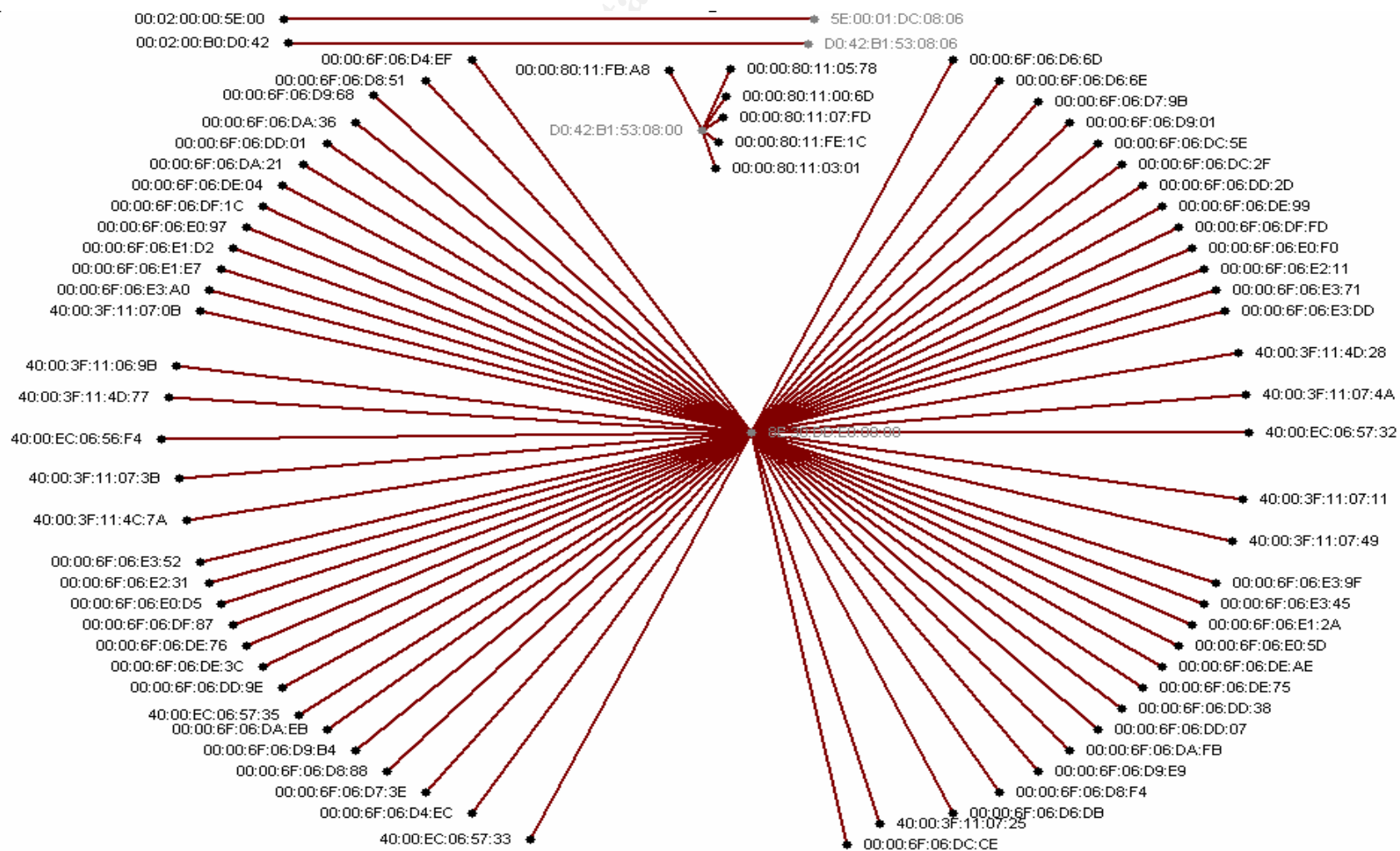
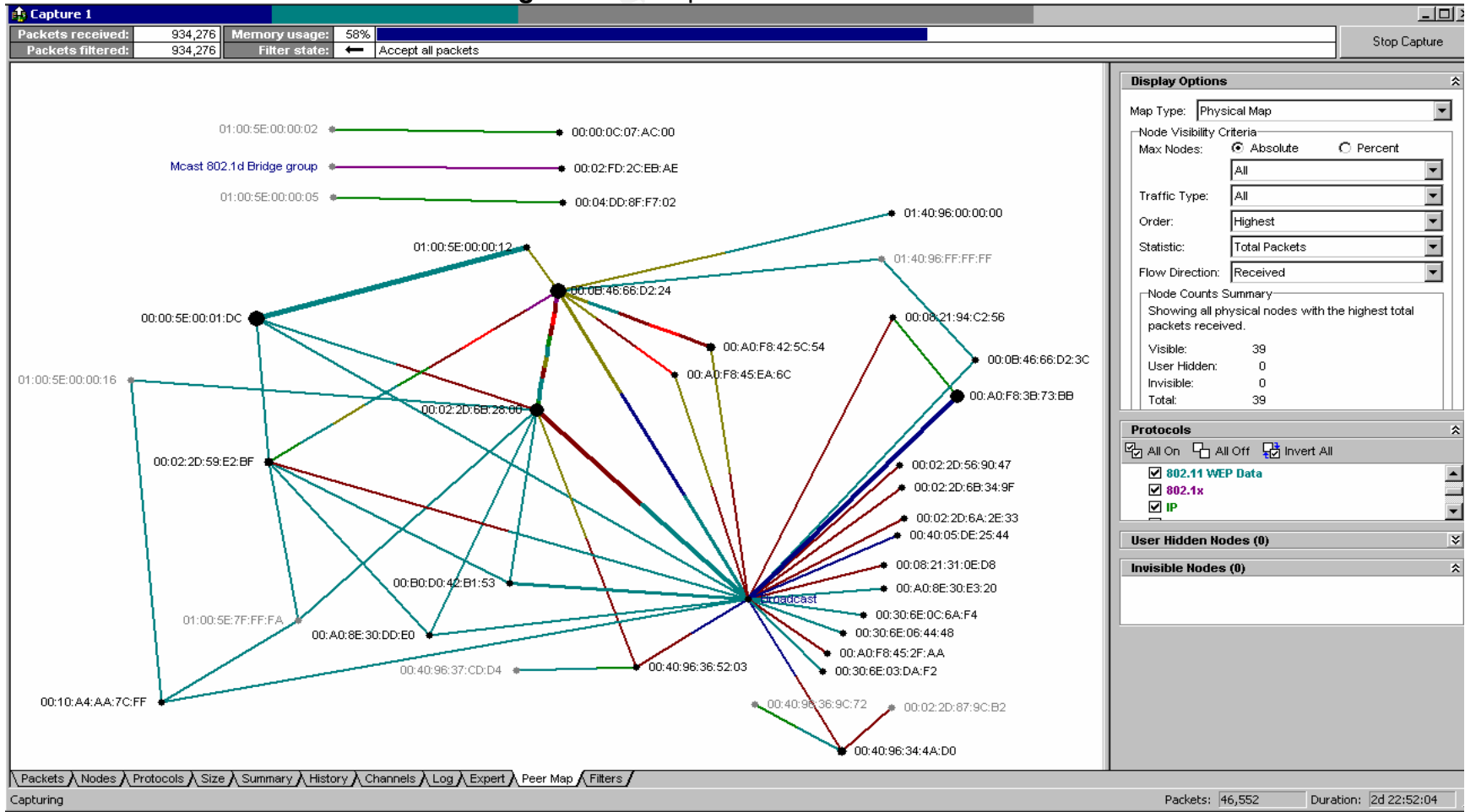


Figure 35: Sample 2 - the next day

The screenshot shows the Network Stumbler application window titled "Network Stumbler - 20030218115815.ns1". The interface includes a menu bar (File, Edit, View, Options, Window, Help), a toolbar with icons for file operations and scanning, and a left sidebar with expandable sections: Channels, SSIDs, and Filters. The main display area contains a table of detected wireless networks. The status bar at the bottom indicates "Ready", "Not scanning", "GPS: Disabled", and a page indicator "2 / 2".

MAC	SSID	Name	Ch...	V...	Type	W...	S...	Sign...	Noi...	SN...	L...	L...	First Seen	Last Seen	S...	N...	Fla...	Bea...
000B4666D2...	Some Wireless Network		6		AP	Yes	-70	-87	17				1:02:29 PM	1:02:29 PM			0031	5000
7203FA017F01	BABCDBE		3		Peer		-80	-93	12				12:00:34 PM	12:17:57 PM			0002	100





### F3 Check known Wardriving sites for entries describing the location of the facility and characteristics of the Wireless network that is in use by Acme Development Company

**Action:** Check known Wardriving sites for entries describing the location of the facility and characteristics of the Wireless network that is in use by Acme Development Company <http://wirelessanarchy.com/> and <http://www.80211hotspots.com/> and <http://www.wigle.net> and <http://mapserver.zhrodaque.net> and <http://worldwidewardrive.org/>  
If there are entries for Acme, have the administrator, ask that the entries be removed.]

**Expected Results:** [Assign a PASS if the site is not identified on any Wardriving sites, otherwise FAIL]

**Actual Results:** PASS No entries found

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>G. Fieldwork Cisco Aironet 1200, 802.11b wireless card installation and configuration.</b>	
1. Determine hardware version of installed 802.11b card and associated antenna.	<u>PASS</u>
2. Determine firmware version of installed 802.11b card	<u>PASS</u>

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>H. Fieldwork Cisco Aironet 1200, Laptop System vulnerability assessment with 802.11 b card installed.</b>	
1. Determine patch level of Windows XP Professional Laptop	<u>PASS</u>
2. Determine that File Sharing and remote Printing services are removed from the Networking control panel.	<b>FAIL/ file sharing and printing installed</b>
3. Determine that all network services not required for Customer Demonstration purposes are shutdown. At this time Acme Development Company has determined that only TCP/IP is required.	<u>PASS</u>

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
4. Determine that an Antivirus program is installed, up to-date, and running	<u>PASS</u>
5. Determine that a personal Firewall is installed, up to-date, and running.	<b>FAIL/not installed</b>
6. Using Nessus a network vulnerability assessment tool, determine the current vulnerabilities of the Laptop.	<b>FAIL/ports open due to File &amp; printer sharing, no Firewall</b>
7. Determine that the default passwords on the Laptop have been changed to a Company security policy appropriate password, or disabled	<u>PASS</u>

## Overview Residual Risk

### Summary review of All Items marked as Fail during the Audit

#### B. Organizational Structure / System Overview, Documentation, & Training

- |  |                    |
|--|--------------------|
| 2. Determine if policies and/or procedures exist that define the requirement for, intended usage of, and rational for the system(s) being audited.   | <b>Risk - High</b> |
| 6. Determine if there is a testing facility for testing security and updated software functionality, previous to implementation in a production environment.<br>Determine how this forms a part of the Change Control process. | <b>Risk - High</b> |
| 7. Determine if there is a user security training program in place.  | <b>Risk - High</b> |

#### C. Fieldwork Cisco Aironet 1200, Installation

- |  |                    |
|--|--------------------|
| 1. Determine physically where in the facility the base unit(s) are located.  | <b>Risk - High</b> |
| 2. Determine signal strength at multiple sampling points.  | <b>Risk - High</b> |
| 3. Determine if there is a documented process in place to monitor when the base station is physically accessed.  | <b>Risk - High</b> |
| 4. Determine if there is a documented process in place to actively monitor the wireless network signal strength outside of the facility, at known locations and intervals. | <b>Risk - High</b> |

#### D. Fieldwork Cisco Aironet 1200, Configuration

- |  |                      |
|--|----------------------|
| 7 Additional Link Layer Security Features available on the Unit.           | <b>Risk – Medium</b> |
| 11 Discover whether VLAN based Networking has been implemented             | <b>Risk - Medium</b> |
| 12 Discover whether IPSec (VPN) based Access control has been implemented. | <b>Risk - High</b>   |
| 13 Is there a Static IP addressing scheme in place?                        | <b>Risk – Low</b>    |

### **E. Fieldwork Cisco Aironet 1200 Management**

- 2. Determine access methods used to manage the base station from the **Wireless** side using 802.11b access. **Risk - High**
- 4. Discover what type of Network monitoring has been implemented **Risk – High**

### **F. Fieldwork Cisco Aironet 1200, Unauthorized Wireless Access Point Detection**

- 2 Using Wildpackets Airopeek, wireless network analyzer investigate the perimeter of the facility for unauthorized Wireless networks. **Risk - High**

### **H. Fieldwork Cisco Aironet 1200, Laptop System vulnerability assessment with 802.11 b card installed.**

- 2. Determine that File Sharing and remote Printing services are removed from the Networking control panel and are uninstalled, and shutdown. **Risk - High**
- 5. Determine that a personal Firewall is installed, up to-date, and running. **Risk - High**
- 6. Using Nessus a network vulnerability assessment tool, determine the current vulnerabilities of the Laptop. **Risk - High**

## Measure the Residual Risk

The audit has discovered 4 distinct areas of residual risk, a lack of Policy and Procedures, Laptop vulnerabilities, installation and configuration issues and no user security training. Out of the 4 areas the lack of policy and procedures, and lack of user training will create the largest, long term issues, as the policy would make clear what can or cannot be done, while the procedures will determine how these activities are undertaken, the user training will demonstrate the how and the reasoning for the need to resolve security issues. Items missing in this one area allow the other areas to exist.

To mitigate this first risk (Areas B2, B6, B7 and F2) require writing the Corporate Wireless Policy and Procedures, implementing the wireless network according to those requirements, and training the users. Writing the Policy would require approximately 5 man-days, approvals, possibly, 1 man-day. Writing the procedures would require approximately 5 man-days. Developing the training would require approximately 5 man-days. Total 16 man-days of effort. The Corporate Wireless Policy and Procedures Document (a control mechanism) would establish a baseline that would set the expectation of what is required. It would not, in and of itself make the wireless network more secure. The audit has successfully identified that currently there is no control mechanism present in this area.

The second identified risk area, H2, H5, H6, are the group of Laptop vulnerabilities. This is an exposure. It could be mitigated to a large degree by correctly implementing a personal firewall on each laptop, limiting printing and file sharing access, and encrypting the data on the Laptop. The capital outlay would be in the range of \$1.0k to \$5.5k depending on the choice of product and no more than 4 man-days in implementation. The audit has successfully identified that currently there is no mechanism in place to limit this exposure, without further action.

The third identified risk area (C1 through C4, and D7, D11, and D12, E2 and E4) is installation and configuration of the Access Point. This is an exposure. Relocating the access point further into the core of the facility could minimize the installation issue, at most a one half-man day activity. The configuration issues may not be able to be minimized at this time as all devices connected to the Access point may not support a VPN client, or the additional WEP features supported in this version of Cisco software. The audit has successfully identified that currently there is no mechanism in place to limit this exposure.

## Evaluate the Audit

Performing the audit has demonstrated that the system is auditable, and cost effective control mechanisms can be put into place to minimize risk. This audit has also produced a baseline, which Acme Development Company can use to measure progress in better securing the network, keeping it secure, or measuring how risk is increased.

The audit has been successful in identifying several issues that, with some effort can be overcome, to implement a more secure Wireless Networking environment within Acme Development Company. These areas would not have been apparent pre audit.

The audit checklist developed during the audit is an extension of work that has preceded me. It can be readily used to audit other Wireless installations, as it focuses less on what the settings in a particular device may be, but more on the method of looking at the events, which occur on the network, due to those settings. It can be used to externally validate that the software settings actually perform the function that the manufacturer has intended.

Reviewing written policy, then auditing its implementation is challenging and subjective. When there is no written policy in place and one is required to use "Best Practices" the challenge increases by at least an order of magnitude.

The audit process has demonstrated to me that the first audit of a technology or system, that an auditor performs himself or herself is a very involved process. A large amount of time is consumed in correctly building the contents and order of the audit checklist. If one fails to dedicate sufficient time to this activity, much more time is wasted during the audit, in revisiting areas incompletely covered in the first pass. The example here is that through correct definition of the items one wishes to cover in the audit, it can, in this case be segregated into at a minimum of 2 separate parallel activities, one checking the logon, passwords, software settings of the access point, while, the network sniffers are recording data to support or deny what one is being told or demonstrated, all in the course of normal operation. If this area was poorly defined in the beginning, work would have to be done twice, once to see that controls work as intended, a second time to record the network information.

An area (D7) was identified, during the audit that would be difficult to independently validate. This area is Additional WEP Security Features that are available on the Unit. The settings are covered in a Cisco Document, [Configuring the Cisco Wireless Security Suite](#). This would be very time consuming if one is to be successful, as the WEP key has to be captured and cracked, numerous times as it is automatically changed, when some of these options are enabled.

## GSNA ASSIGNMENT 4 – Audit Report

### Audit Report

#### Executive Summary

Audit Co. audited the Wireless Demonstration Network installed at Acme Development Company during the month of February 2003. It is a post implementation Audit. The network audited is depicted in the drawing Figure 37, below.

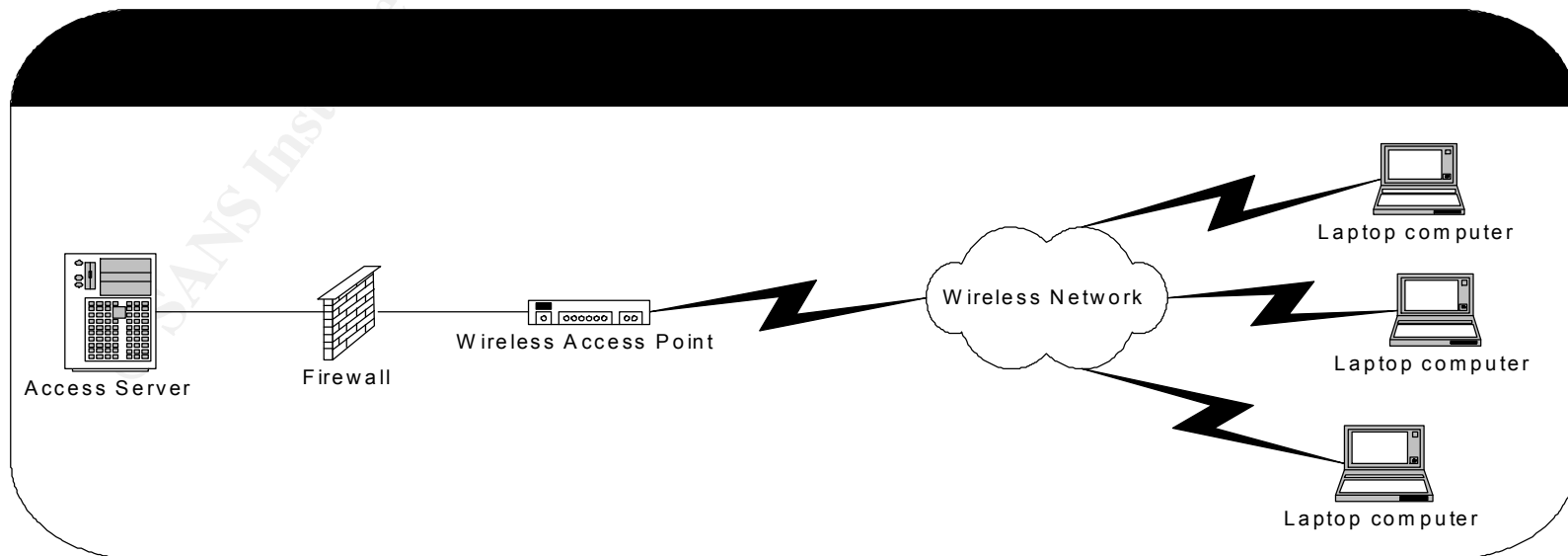


Figure 37

The audit has revealed 3 areas of increased security risk that can be mitigated with limited additional expenditure of time and funds.

The areas are as follows:

- 1) Acme Development Company does not have a written Corporate Policy and Procedure, covering Wireless networks, nor a User Security Training program. In Total it is estimated to take 16 man-days to develop, and approve. Implementation would require additional time. The exposure is large in this area as a number of unofficial networks were discovered at Acme. Without written corporate policy it will be virtually impossible to remove and prevent the installation of these rogue networks. Without user training on security matters, the insecure networks will be incorrectly reestablished almost as soon as they are removed, as users will not be familiar with the settings required and reasons to secure the network.
- 2) A group of Laptop vulnerabilities. Acme Development Company does not require that Laptops, which are normally in use, outside of the Firewall, in essence, outside of the secured network perimeter, have to have a working up to date Firewall installed. Seriously consider having printing and file sharing disabled, and consider installing data encryption software on each Laptop. The capital outlay would be in the range of \$1.0k to \$5.5k depending on the choice of product and require no more than a 3 man-days in implementation at this time.
- 3) The third identified major risk area is installation and configuration of the Access Point. The Access Point is located near an exterior wall of the Acme Development Company facility. Moving it to an interior area would decrease the Wireless signal available outside of the building. The configuration issues may have to remain as they are, as all equipment used in the Demo area do not support the installation of a VPN client, or do not implement all of the features made available with the latest Cisco software installed in the Access Point. Moving the Access Point is estimated to take a maximum of one half-man day, once a more suitable location is identified. The administrator has completed this action, just as the audit was completed.

Other major areas investigated during the audit received a pass. This would confirm that the Wireless Network as implemented is generally secure, but with a limited additional focus of 28 man-days, Hardware/Software \$3.5k to \$7.5K, and On-going -2 man-days per week the security risk could be mitigated greatly, and most of the items that failed could be turned into a pass.



## Audit Findings

The following is a summary of the evaluation and its outcome.

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>A. ADMINISTRATIVE SECTION</b>	
1. Prepare a Strategic Audit Plan for the area(s) or function(s) to be reviewed.	Complete
2. Prepare a Detailed Audit Budget for the area(s) or function(s) to be reviewed.	Complete
3. Prepare Statement of Scope and Methods memorandum for the area(s) or function(s) to be reviewed.	Complete
4. Review Audit Co. Information Security process, information storage and retrieval, and information destruction policy and procedures, relevant to this engagement with Acme Development Company (client).	Complete
5. Review Statement of Scope and Methods, projected costing and obtain written authorization for Audit to take place	Complete
6. Document Opening Conference	Complete
7. Comparison of Budgeted Hours to Actual Hours	Complete
8. Prepare audit issues.	Complete

AUDIT STEPS: ORGANIZATIONAL STRUCTURE, SYSTEM OVERVIEW	STATUS
<b>B. ORGANIZATIONAL STRUCTURE / SYSTEM OVERVIEW, DOCUMENTATION, &amp; TRAINING</b>	
1. Determine the reporting structure from the area(s) to be reviewed up to the CEO.	Complete
2. Determine if policies and/or procedures exist that define the requirement for, intended usage of, and rational for the system(s) being audited.	<b>FAIL/no written Wireless policy and Procedures</b>

AUDIT STEPS: ORGANIZATIONAL STRUCTURE, SYSTEM OVERVIEW	STATUS
3. Determine if documentation exists for the system(s) being reviewed. This would include any system documentation, scripts, change control processes, and network diagrams.	Complete
4. Determine if Administrators and/or Security personal have been trained on the specific device or have other equivalent documented suitable training	<u>PASS</u>
5. Determine if Administrators and/or Security personal belong to device relevant mailing lists; receive updates regularly from Wireless Standards Bodies.	<u>PASS</u>
6. Determine if there is a testing facility for testing security and updated software functionality, previous to implementation in a production environment. Determine how this forms a part of the Change Control process	<b>FAIL/no testing facility</b>
7. Determine if there is a user security training program in place	<b>FAIL/no User training Program</b>

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>C. Fieldwork Cisco Aironet 1200, Installation</b>	
1. Determine physically where in the facility the base unit(s) are located.	<b>FAIL/located near external wall</b>
2. Determine signal strength at multiple sampling points.	<b>FAIL/ strong signal external to facility, due to AP location</b>
3. Determine if there is a documented process in place to monitor when the base station is physically accessed.	<b>FAIL/ recording but no monitoring</b>
4. Determine if there is a documented process in place to actively monitor the wireless network signal strength outside of the facility, at known locations and intervals.	<b>FAIL/ process, but no historical monitoring log</b>

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>D. Fieldwork Cisco Aironet 1200, Configuration</b>	
1. Determine hardware versions of installed Access Point, and 802.11b card installed in it, and associated antennae.	<u>PASS</u>
2 Determine that the default password has been changed to a Company security policy appropriate password	<u>PASS</u>
3. Determine firmware version of installed unit and associated cards	<u>PASS</u>
4 Determine that the interval between "Beacon Frames" has been made as long as possible	<u>PASS</u>
5 Determine that the default Service Set Identifier (SSID) has been changed to a Company security policy compliant value	<u>PASS</u>
6 Wired-Equivalent Privacy (WEP) Encryption	<u>PASS</u>
7 Additional Link Layer Security Features available on the Unit	<b>FAIL/Not Implemented</b>
8 Discover whether Media Access Control (MAC) address based Access and Association control has been implemented	<u>PASS</u>
9 Discover whether Remote Authentication Dial-in User Service (RADIUS) based Access control has been implemented.	<u>PASS</u>
10 Discover whether RADIUS based Access control has been implemented, with Extensible Authentication Protocol (EAP), a protocol supporting 802.1x features.	<u>PASS</u>
11 Discover whether VLAN based Networking has been implemented	<b>FAIL / No VLANs implemented</b>
12. Discover whether IPsec (VPN) based Access control has been implemented	<b>FAIL/ Not Implemented</b>
13 Is there a Static IP addressing scheme in place?	<b>FAIL/DHCP Implemented</b>

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
14 Has the wireless network been assigned a part of the “Special-Use address” space?	<u>PASS</u>
15 Determine that the wireless access point has SNMP disabled	<u>PASS</u>
16 Determine that the administrator has entered a new administrative password	<u>PASS</u>

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>E. Fieldwork Cisco Aironet 1200, Management</b>	
1. Determine access methods used to manage the base station from the wired side. <ul style="list-style-type: none"> <li>• Attempt telnet access to base station</li> <li>• Attempt SSH access to base station</li> <li>• Attempt http access to base station</li> <li>• Attempt https access to base station</li> <li>• Scan access point with Nessus looking for open ports.</li> </ul>	<u>PASS</u> No Connection Connection Connection No connection Ports 22,23,80 &ICMP message
2. Determine access methods used to manage the base station from the <b>Wireless</b> side using 802.11b access. <ul style="list-style-type: none"> <li>• Attempt telnet access to base station</li> <li>• Attempt SSH access to base station</li> <li>• Attempt http access to base station</li> <li>• Attempt https access to base station</li> <li>• Scan access point with Nessus looking for open ports</li> </ul>	<b><u>FAIL/</u> Can be managed from Wireless side</b> No Connection Connection Connection No connection Ports 22,23,80 &ICMP

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
	message
3. Discover that Cisco Discovery Protocol (CDP) has been disabled	<u>PASS</u>
4. Discover what type of Network monitoring has been implemented	<b>FAIL/ No Monitoring implemented</b>

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>F. Fieldwork Cisco Aironet 1200, Unauthorized Wireless Access Point Detection</b>	
1. Walk around the perimeter, parking lot, and streets adjacent to the facility or parking lot of Acme Development Company, looking for evidence of Warchalking	<u>PASS</u>
2. Using Wildpackets AiropEEK, wireless network analyzer investigate the perimeter of the facility for unauthorized Wireless networks	<b>FAIL/ other rogue networks within Acme facility found</b>
3 Check known Wardriving sites for entries describing the location of the facility and characteristics of the Wireless network that is in use by Acme Development Company	<u>PASS</u>

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>G. Fieldwork Cisco Aironet 1200, 802.11b wireless card installation and configuration.</b>	
1. Determine hardware version of installed 802.11b card and associated antenna.	<u>PASS</u>
2. Determine firmware version of installed 802.11b card	<u>PASS</u>

AUDIT STEPS: OBJECTIVE, TESTING AND REFERENCE	STATUS
<b>H. Fieldwork Cisco Aironet 1200, Laptop System vulnerability assessment with 802.11 b card installed.</b>	
1. Determine patch level of Windows XP Professional Laptop	<u>PASS</u>
2. Determine that File Sharing and remote Printing services are removed from the Networking control panel and are uninstalled, and shutdown.	<b>FAIL/</b> file sharing and printing installed
3. Determine that all network services not required for Customer Demonstration purposes are shutdown. At this time Acme Development Company has determined that only TCP/IP is required.	<u>PASS</u>
4. Determine that an Antivirus program is installed, up to-date, and running	<u>PASS</u>
5. Determine that a personal Firewall is installed, up to-date, and running.	<b>FAIL/</b> not installed
6. Using Nessus a network vulnerability assessment tool, determine the current vulnerabilities of the Laptop.	<b>FAIL/</b> ports open due to File& printer sharing, no Firewall
7. Determine that the default passwords on the Laptop have been changed to a Company security policy appropriate password, or disabled	<u>PASS</u>

## Background/Risk

### All Items marked as Fail during the Audit

#### B. Organizational Structure / System Overview, Documentation, & Training

- Determine if policies and/or procedures exist that define the requirement for, intended usage of, and rational for the system(s) being audited.

**Risk – High**

Without a written, published Wireless Security Policy in place other individuals within Acme Development Company have the opportunity to establish Wireless Networks as they see fit. This has already occurred, as shown in section F2. These networks will be established with the manufacturer, default settings. The settings support ease of use, and

have all security or performance impacting settings turned off. This will allow non-employees outside of Acme to directly associate with the network, access the corporate network, and confidential information distributed on it without anyone knowing. This access is also able to deliver virus infections to any machine on the corporate network.

6. Determine if there is a testing facility for testing security and updated software functionality, previous to implementation in a production environment.  
Determine how this forms a part of the Change Control process.

**Risk - High**

There was no identified facility available for evaluating security changes or software updates. This forces the situation where untested security changes, or untested by Acme, software is placed into a production environment. It opens the opportunity for either the security changes or the new software to change or invalidate the security settings currently implemented. This change in security posture would not be known until another audit took place. The untested software may also negatively impact a portion of a demo, as the full suite of demo tests would not be performed until the first live customer demo.

7. Determine if there is a User Security Training program in place.

**Risk – High**

Without a User Security Training program in place users generally will not understand the exposures involved with running a Wireless network. This will allow the individuals involved to attempt to perform tasks in the most expedient way, without concern for security matters, they will generally be seen as a hindrance, and therefore bypassed. This increases risk substantially

### **C. Fieldwork Cisco Aironet 1200, Installation**

1. Determine physically where in the facility the base unit(s) are located.

**Risk – High**

The Access Point is located next to an external wall. This allows almost as much wireless signal to be transmitted outside of the wall as is transmitted inside. Re-locating the wireless access point can easily mitigate the issue. The Administrator has taken the recommended action to move the Access point to a better location.

2. Determine signal strength at multiple sampling points.

**Risk – High**

The issue here is the same as in C1 above. In moving the access point the administrator has now decreased the relative signal strength from 100% measured outside the back door of the facility to less than 40% at the same location.

3. Determine if there is a documented process in place to monitor when the base station is physically accessed.

**Risk – High**

Access to the location where the Wireless Access Point is located, is card key controlled. As part of performing the audit it was discovered that the access logs are not evaluated until there is a physical security breach of some nature. Therefore it is reasonable to assume the Wireless Access Point could be accessed and configuration changed without anyone noticing. A process should be put in place to monitor and evaluate the access logs to this area on a daily basis.

4. Determine if there is a documented process in place to actively monitor the wireless network signal strength outside of the facility, at known locations and intervals.

**Risk – High**

There is no documented process in place for actively monitoring Wireless signal strength. A wireless policy should be written, a process implemented to allow for weekly monitoring of the signal strength at various identified locations within and without the facility. The process should take into the account to not only measure signal strength but also the opportunity to locate and identify rogue access points as discovered in F2 below.

#### **D. Fieldwork Cisco Aironet 1200, Configuration**

- 7 Additional Link Layer Security Features available on the Unit.

**Risk – Medium**

Cisco has implemented several pre 802.11i Robust Security Network standard amendments. These additional features, being pre-standard, are not available on all other manufactured devices. They may be available at some future date. After discussions it became apparent that Acme requires the demo network to support more than one vendor's (Cisco) equipment, therefore the pre-standard features cannot be implemented, until the standard is issued, software written, and implemented on all of the devices used in the demo network. The mitigation for this issue is to



remain current with the software releases produced by the equipment manufacturers, that are used in the demo environment, test the software to validate the features it adds, and incorporate as appropriate.

**11 Discover whether IPSec (VPN) based Access control has been implemented. Risk – Medium**

After discussions it became apparent that IPSec couldn't be implemented in the demo network at this time, because not all of the equipment required supports IPSEC with the current version of available software. The mitigation for this issue is to remain current with the software releases produced by the equipment manufacturers, that are used in the demo environment, test the software to validate the features it adds, and incorporate as appropriate. The risk, although high, for this issue alone, taken in isolation, is mitigated to some degree by the 802.1X implementation that Acme has put in place, which is a port-level access control protocol which requires mutual authentication, WEP encryption, and maximizing the time between Beacon packets. These actions insure that the access point is fairly quiet on its own, requires authentication on the part of the Access Point and the wireless device, and carries encrypted data. These steps reduce the risk to a medium level, at this time.

**12 Is there a Static IP addressing scheme in place? Risk – Low**

Acme Development Company chooses to use dynamically assigned IP addressing, instead of statically assigned IP addressing for nodes attached to the demo network. The risk is mitigated by having IP addresses assigned after mutual authentication is successful and the media access layer address is authenticated with a server inside of the firewall as indicated in audit section D8.

**E. Fieldwork Cisco Aironet 1200 Management**

**2. Determine access methods used to manage the base station from the Wireless side using 802.11b access. Risk - High**

The ability to access and manage the Wireless Access Point from the Wireless side presents a high Risk situation, as the only authentication method in place on the Access Point is password based. Once the password to the Access Point is acquired, then the security settings can be adjusted to a less secure setting. There is no facility for failed logon lockout on the Access point. In order to limit this exposure the password should be changed frequently, and a monitoring program should be implemented to check that the settings have not been altered.

4. Discover what type of Network monitoring has been implemented

**Risk – High**

Acme Development Company needs to implement wireless network monitoring. At this time there are no performance recording devices present on the Wireless network. Therefore Acme is unable to assess the performance of the network. As this network is being implemented for customer demonstration purposes, it would be beneficial for Acme to understand performance bottlenecks (Benchmarking) during Customer Demonstrations, in order to be able to understand if a performance issue is due to product issues or to an exposure or attack taking place during the demo. This would be in addition to being able to track authorized/unauthorized network usage.

**F. Fieldwork Cisco Aironet 1200, Unauthorized Wireless Access Point Detection**

2 Using Wildpackets Airopeek, wireless network analyzer investigate the perimeter of the facility for unauthorized Wireless networks.

**Risk - High**

Acme Development Company needs to further investigate the rogue networks discovered in this section. It would appear that there are several nodes forming unauthorized local networks, as well as at least 1 other distinct Wireless Network. This is a large risk. This issue is made an even larger exposure, with the exposures presented by sections H2, H5, H6, B2 and C4.

**H. Fieldwork Cisco Aironet 1200, Laptop System vulnerability assessment with 802.11 b card installed.**

2. Determine that File Sharing and remote Printing services are removed from the Networking control panel and are uninstalled, and shutdown.

**Risk – High**

After discussions to discover the need for and use of the Demo network, it has become apparent that Acme Development Company requires to have File sharing and Printing services enabled on the Laptops in the Demo network. This is a high-risk activity with Laptops running Windows XP, as the operating system will attempt to associate with any available Access Point, as soon as the operating system is running and the Wireless card/Antenna is activated. The demo network is outside of the Security perimeter of Acme. This would immediately enable file sharing with other nodes. It is likely that the end user would not be aware of this association. The other node would then be able to remove, copy, or place files on that laptop, without the user easily being aware of this activity. See [Remote registry access A practical implementation](#) Copying the WEP key from the Laptop Registry

would be a simple operation in this configuration. This risk could be mitigated by having Wireless policies, and/or procedures in place (B2 above), implementing a personal Firewall (H5 below), and enabling IPSec communication (D11) on at least the laptops. Encryption software could also be purchased to encrypt the Laptop data. This would have an additional cost of \$100 to \$500 per laptop, and require less than ½ man-day per Laptop to install and configure.

5. Determine that a personal Firewall is installed, up to-date, and running.

**Risk – High**

The Laptops, in use do not have a personal Firewall installed. This over site, in combination with file and Printer sharing, enabled, the exposures identified in the Nessus scan, a lack of a Wireless Policy and the Demo network being outside the security perimeter make these machines especially vulnerable to tampering. To mitigate this risk, one could enable the built in Windows XP firewall as outlined in [Introduction to the Microsoft Windows XP Firewall](#). It could require the purchase of personal Firewall software at an additional cost of \$50 to \$150 per Laptop, if the XP Firewall was found to be lacking.

6. Using Nessus a network vulnerability assessment tool, determine the current vulnerabilities of the Laptop.

**Risk - High**

The Nessus scan of a typical Laptop was performed. It is included as Appendix C. This has confirmed that the Wireless Laptops have the standard Windows XP exposures. These exposures represent well-known vulnerabilities, which are enumerated in the scan, indicating the laptop can be readily compromised. To mitigate this risk, which is large, at a bare minimum a personal Firewall as noted above, should be configured, then file and printer sharing should be disabled or very carefully controlled by the firewall. This may require Acme to implement static IP addressing scheme.

## Audit Recommendations

The following recommendations are listed in order of priority, items 1 and 2 can be performed in parallel with the other items, and item 5 has been completed, as this audit was being written.

1. Develop a written, approved, published Wireless Security Policy, and implement it. Identified in section B2
2. Develop a User Security Training Program identified in section B7
3. Secure the laptops used in the Wireless Network, as identified in section H2 and H5, then retest with Nessus.
4. Search out and secure the Rogue networks discovered in section F2. Secure the machines participating in the rogue networks.
5. Move the Wireless Access Point to a location away from the exterior wall, section C1. The Administrator already undertook this action.
6. The following items require an implementation of, or improvement in, process. B6 (facility for testing security and updated software functionality), C2 (sample signal strength at multiple sampling points), C3 (documented process in place to monitor when the base station is physically accessed), C4, E2 (documented process in place to actively monitor the wireless network signal strength outside of the facility, at known locations and intervals) E4 implement Network Monitoring, D11 Implement VLANs as appropriate, E2 change passwords frequently.
7. Remain up to date with software introduced by the manufacturers, which supports more security features. Implement them as soon as they are tested, to increase security, or enable additional security features. This will allow the issues in sections D7 and D12 to be resolved.

## Costs

The following are estimations of costs to be incurred by Acme to implement the audit recommendations.

**Item 1** 11 man days      \$0 for software

**Item 2** 5 man-days      \$0 for software 1man day on going

**Item 3** 3 man days      \$1.5k to \$5.5k for software

**Item 4** 5 man days      \$0 for software

**Item 5** completed

**Item 6** 4 man days to set up, 0.5 man day per week, on going, initial software and hardware costs for Access Point \$2K, recycle a used PC for Network Monitoring, install and harden Linux, Ethereal and/or Snort, and/or MRTG.

**Item 7** 0.5 man-day per week on going, software cost is part of maintenance cost.

**Total Initial-setup** 28 man-days, Hardware/Software \$3.5k to \$7.5K

**On-going** -1 man-day per week associated annual maintenance costs.

### **Compensating Controls**

The concept of implementing a Wireless Demo Network is a new idea to Acme Development Company. It was thought that because the wireless concept had not been officially sanctioned that there would not be any deployment within Acme. The Audit evidence would strongly indicate otherwise. This demonstrates that what ever existing compensating controls were thought to have been in place did not exist or were ineffective.

© SANS Institute 2003, Author retains full rights.

## Appendix A

### Nessus Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

#### Scan Details

Hosts which were alive and responding during test	1
Number of security holes found	5
Number of security warnings found	2

#### Host List

Host(s)	Possible Issue
<a href="#">10.200.20.240</a>	Security hole(s) found

#### Analysis of Host

Address of Host	Port/Service	Issue regarding Port
10.200.20.240	<a href="#">ssh (22/tcp)</a>	Security warning(s) found
10.200.20.240	<a href="#">telnet (23/tcp)</a>	Security notes found
10.200.20.240	<a href="#">http (80/tcp)</a>	Security hole found
10.200.20.240	<a href="#">general/icmp</a>	Security warning(s) found
10.200.20.240	<a href="#">general/udp</a>	Security notes found

#### Security Issues and Fixes: 10.200.20.240

Type	Port	Issue and Fix
Warning	ssh (22/tcp)	<p>The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.</p> <p>These protocols are not completely cryptographically safe so they should not be used.</p> <p>Solution: If you use OpenSSH, set the option 'Protocol' to '2' If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'</p> <p>Risk factor: Low</p>
Informational	ssh (22/tcp)	An ssh server is running on this port
Informational	ssh (22/tcp)	Remote SSH version: SSH-1.5-Cisco-1.25
Informational	ssh (22/tcp)	<p>The remote SSH daemon supports the following versions of the SSH protocol:</p> <ul style="list-style-type: none"> <li>. 1.33</li> <li>. 1.5</li> <li>. 1.99</li> </ul>
Informational	telnet (23/tcp)	<p>The service closed the connection after 0 seconds without sending any data</p> <p>It might be protected by some TCP wrapper</p>
Vulnerability	http (80/tcp)	<p>The dll '_vti_bin/_vti_aut/dwssr.dll' seems to be present.</p> <p>This dll contains a bug which allows anyone with authoring web permissions on this system to alter the files of other users.</p> <p>In addition to this, this file is subject to a buffer overflow which allows anyone to execute arbitrary commands on the server and/or disable it</p> <p>Solution: delete /_vti_bin/_vti_aut/dwssr.dll</p> <p>Risk factor: High</p> <p>See also: <a href="http://www.wiretrip.net/rfp/p/doc.asp?id=45&amp;iface=1">http://www.wiretrip.net/rfp/p/doc.asp?id=45&amp;iface=1</a></p> <p><a href="#">CVE: CVE-2000-0260</a></p>
Vulnerability	http (80/tcp)	<p>There is a buffer overflow in the remote htimage.exe cgi when it is given the request:</p>

/cgi-bin/htimage.exe/AAAA[....]AAA?0,0

An attacker may use it to execute arbitrary code on this host.

Solution: delete it  
Risk factor: High  
[CVE: CAN-2000-0256](#)

**Vulnerability** http (80/tcp)

There is a buffer overflow in the remote htimage.exe cgi when it is given the request :

/cgi-bin/htimage.exe/AAAA[....]AAA?0,0

An attacker may use it to execute arbitrary code on this host.

Solution: delete it  
Risk factor: High  
[CVE: CAN-2000-0256](#)

**Vulnerability** http (80/tcp)

It may be possible to make a web server execute arbitrary code by sending it a too long url after /jsp.

Ie:  
GET /jsp/AAAA.....AAAAA

Risk factor: High  
Solution: Contact your vendor for the latest software release.  
[CVE: CAN-2001-0419](#)

**Vulnerability** http (80/tcp)

New Atlanta's ServletExec 4.1 is a servlet Engine for IIS implemented via an ISAPI filter. By making an overly long request for a .jsp file it is possible to crash IIS.

Solution:

Download patch #9 from [ftp://ftp.newatlanta.com/public/4\\_1/patches/](ftp://ftp.newatlanta.com/public/4_1/patches/)

References: [www.westpoint.ltd.uk/advisories/wp-02-0006.txt](http://www.westpoint.ltd.uk/advisories/wp-02-0006.txt)

Risk factor: High



Informational http (80/tcp) A web server is running on this port  
Informational http (80/tcp) The remote web server type is:  
thttpd/2.03 11jul98  
Solution: We recommend that you configure (if possible) your web server to return a bogus Server header in order to not leak information.

Warning general/icmp  
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.  
This may help him to defeat all your time based authentication protocols.  
Solution: filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).  
Risk factor: Low  
[CVE: CAN-1999-0524](#)

Informational general/udp For your information, here is the traceroute to 10.200.20.240 :  
10.100.40.253  
10.151.10.3  
10.200.20.240

---

This file was generated by [Nessus](#), the open-sourced security scanner.

## Appendix B

### Security Audit Template

#### Using the New AiroPeek Alarm and Template Features

The [Security Audit Template](#), located where you installed the program in the "Security Audit Template" folder, creates a capture window that triggers a notification when a packet matches any of the filters described below. Before using the template, you must load the [Security Audit Filters](#) file. By default, a "severe" notification is used. You can change the severity used in the Start Trigger action and use Notification options to email when the event occurs. Since the Security Audit Template has set filters to allow ONLY the security-related issues, the presence of one packet in the buffer indicates that an event has occurred. It may be helpful to display the "Filter" column in the packet list to determine which filter caused the template to trigger. Right-click on the packet list header to enable this column.

The alarm features are loaded and active by default when AiroPeek starts. They are contained in the default alarm file. Individual alarms can be deactivated from the View|Alarms menu command.

The Security Audit Template is a good example of what you can accomplish with the standard filter, trigger, and alarm features of AiroPeek. The template should be tailored to fit your network. Some of the filters may refer to traffic that is normal on your wireless LAN, so they should be disabled. You may know of other applications, however, that should not appear on your wireless LAN. It is easy to add a filter to look for such packets and configure AiroPeek notify you if they appear.

Please visit <http://www.wildpackets.com/wireless> for up-do-date information regarding the use of AiroPeek in conducting security audits on your wireless LAN.

### Security Audit Filters

- **Contention Free mode is in use on the network**

When the 802.11 Contention Free Mode (CFM) is implemented (through device configuration), the Access Point becomes the master controller of the WLAN BSSID and stations must specifically request permission to transmit. This mode is not commonly implemented and, if it were inadvertently active in a WLAN, then stations not using CFM would be unable to communicate. CFM should only be used when excessive Retries or CRC errors are being caused by a large number (over 30) of WLAN stations conflicting with each other in the same location.

- **Packets with default ESSID**

Access Points are pre-configured with vendor-selected default ESSID's. These include the text strings, "intel", "linksys", and many others. AiroPeek looks for the presence of these various default ESSID's. If the default ESSID was not reconfigured by the local site administrator then the door is wide open for an intruder to access the WLAN without authorization.

- **An unfamiliar host is requesting a DHCP address assignment**

Most host computers have an IP address that they were using prior to entering the WLAN. When a station appears in the WLAN and it has never had an IP address assigned to it, it is considered "unfamiliar." This could be a normal, non-threatening situation or it could indicate an unauthorized attempt to access the WLAN.

- **Cisco HSRP is operating across the WLAN**

Cisco's Hot Swap Router Protocol is sent between routers in a Cisco HSRP group to provide a redundant, fault-tolerant default gateway on the Ethernet. The presence of HSRP on the WLAN is incongruous and may indicate that the network configuration and topology is inappropriately allowing these packets to enter an Access Point for broadcast.

- **Cisco IGRP is operating across the WLAN**  
Typically, routers exchange their table information across the Ethernet LAN. It is unusual to see this behavior on the WLAN. The packets should be assessed to confirm that the network topology is configured in the desired manner.
- **Non-WEP (unencrypted) data is present on the WLAN**  
This filter looks for the existence of non-WEP encrypted traffic.
- **OSPF is operating across the WLAN**  
Typically, routers exchange their table information across the Ethernet LAN. It is unusual to see this behavior on the WLAN. The packets should be assessed to confirm that the network topology is configured in the desired manner.
- **The Request To Send mechanism is implemented on this network**  
A station sends a Request To Send packet and expects a Clear To Send reply before transmitting. Many 802.11 WLAN communicators do not use RTS/CTS. The packets should be assessed to confirm proper operation.
- **SNMP is operating across the WLAN**  
Simple Network Management Protocol, though a common protocol, is not commonly seen on Wireless LANs and can be inappropriately used in an attempt to break into an Access Point and change its configuration. The presence of SNMP on the WLAN may be an indication of a security breach. The packets should be assessed to determine why they are present on the WLAN. You can tailor this filter by including the IP addresses of your Access Points.
- **Spanning Tree Algorithm is operating across the WLAN**  
Spanning Tree Algorithm (802.1d) Bridge Protocol Data Unit (BPDU) packets are used by switches to establish a non-looping network topology. The presence of these packets on the WLAN means that one or more switches are trying to use the WLAN as an inter-switch path. This is atypical and if a rogue switch is present, it may cause connectivity problems in the WLAN and the Ethernet LAN as well. The packets should be assessed to determine the location of the switches.
- **TELNET is operating across the WLAN**  
The presence of TELNET on the WLAN may indicate an attempt to break into an Access Point and change its configuration. The packets should be assessed to determine why they are present on the WLAN.

## Security-Related Alarms

- **Wireless distribution system in use**  
Most WLAN Extended Service Set implementations interconnect Access Points through the Ethernet LAN. While there is nothing inherently wrong with a wireless link between Access Points, it may indicate the presence of a rogue Access Point that should not be participating in the network. Check to see if any individual computers are set up as a software-based Access Point.
- **Excessive 1 Mbit/s packets**  
The 1 Mbit/s data rate is normally used for various 802.11 management and control functions. There is a small amount of 1 Mbit/s traffic in any WLAN. When this Alarm is triggered, it indicates that an excessive amount of 1 Mbit/s traffic is present. This could be the result of environmental noise or conflicts between a large number of wireless communicators in the environment.
- **Excessive 802.11 Management traffic**  
There is a normal amount of background management traffic in any 802.11 WLAN. When an excessive amount is present, it may indicate that stations are being required to reassociate because of poor signal strength or quality, or that too many Access Points are present.

- **WEP not enabled**

If corporate policy is to use WEP on your Wireless LAN, then you should see WEP data. This alarm is activated if no WEP traffic is seen for a period of 5 minutes.

---

WildPackets, Inc.

<http://www.wildpackets.com/>

Copyright © 2002 WildPackets, Inc.  
All rights

© SANS Institute 2003, Author retains full rights.

## Appendix C

### Nessus Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

#### Scan Details

Hosts which were alive and responding during test	1
Number of security holes found	1
Number of security warnings found	6

#### Host List

Host(s)	Possible Issue
<a href="#">10.100.45.13</a>	Security hole(s) found

#### Analysis of Host

Address of Host	Port/Service	Issue regarding Port
10.100.45.13	<a href="#">unknown (135/tcp)</a>	Security warning(s) found
10.100.45.13	<a href="#">netbios-ssn (139/tcp)</a>	Security hole found
10.100.45.13	microsoft-ds (445/tcp)	No Information
10.100.45.13	<a href="#">unknown (1025/tcp)</a>	Security notes found
10.100.45.13	unknown (2701/tcp)	No Information
10.100.45.13	unknown (2702/tcp)	No Information
10.100.45.13	<a href="#">unknown (5000/tcp)</a>	Security notes found
10.100.45.13	<a href="#">general/tcp</a>	Security notes found
10.100.45.13	<a href="#">netbios-ns (137/udp)</a>	Security warning(s) found

10.100.45.13	<a href="#">general/icmp</a>	Security warning(s) found
10.100.45.13	<a href="#">unknown (1040/udp)</a>	Security notes found
10.100.45.13	<a href="#">general/udp</a>	Security notes found

Security Issues and Fixes: 10.100.45.13		
Type	Port	Issue and Fix
Warning	unknown (135/tcp)	<p>DCE services running on the remote can be enumerated by connecting on port 135 and doing the appropriate queries.</p> <p>An attacker may use this fact to gain more knowledge about the remote host.</p> <p>Solution : filter incoming traffic to this port. Risk factor: Low</p>
Informational	unknown (135/tcp)	<p>A DCE service is listening on this host UUID: 4b112204-0e19-11d3-b42b-0000f81abcff, version 1 Endpoint: ncalrpc[LRPC0000052c.00000001]</p>
Informational	unknown (135/tcp)	<p>A DCE service is listening on this host UUID: 1ff70682-0a51-30e8-076d-740be8abcfff, version 1 Endpoint: ncalrpc[Infrared Transfer Send]</p>
Informational	unknown (135/tcp)	<p>A DCE service is listening on this host UUID: 1ff70682-0a51-30e8-076d-740be8abcfff, version 1 Endpoint: ncalrpc[Wireless Link Notification]</p>
Informational	unknown (135/tcp)	<p>A DCE service is listening on this host UUID: 1ff70682-0a51-30e8-076d-740be8abcfff, version 1 Endpoint: ncalrpc[IcaApi]</p>
Informational	unknown (135/tcp)	<p>A DCE service is listening on this host UUID: 1ff70682-0a51-30e8-076d-740be8abcfff, version 1 Endpoint: ncacn_np:\\PC1339[\\pipe\\Ctx_WinStation_API_service]</p>
Informational	unknown (135/tcp)	<p>A DCE service is listening on this host UUID: 1ff70682-0a51-30e8-076d-740be8abcfff, version 1 Endpoint: ncalrpc[wzcsvc]</p>

Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 1ff70682-0a51-30e8-076d-740be8abcfff, version 1 Endpoint: ncalrpc[OLE3]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 1ff70682-0a51-30e8-076d-740be8abcfff, version 1 Endpoint: ncacn_np:\\PC1339[\\PIPE\\atsvc]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 378e52b0-c0a9-11cf-822d-00aa00abcfff, version 1 Endpoint: ncalrpc[Infrared Transfer Send]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 378e52b0-c0a9-11cf-822d-00aa00abcfff, version 1 Endpoint: ncalrpc[Wireless Link Notification]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 378e52b0-c0a9-11cf-822d-00aa00abcfff, version 1 Endpoint: ncalrpc[IcaApi]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 378e52b0-c0a9-11cf-822d-00aa00abcfff, version 1 Endpoint: ncacn_np:\\PC1339[\\pipe\\Ctx_WinStation_API_service]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 378e52b0-c0a9-11cf-822d-00aa00abcfff, version 1 Endpoint: ncalrpc[wzcsvc]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 378e52b0-c0a9-11cf-822d-00aa00abcfff, version 1 Endpoint: ncalrpc[OLE3]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 378e52b0-c0a9-11cf-822d-00aa00abcfff, version 1 Endpoint: ncacn_np:\\PC1339[\\PIPE\\atsvc]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 0a74ef1c-41a4-4e06-83ae-dc74fbabcfff, version 1 Endpoint: ncalrpc[Infrared Transfer Send]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 0a74ef1c-41a4-4e06-83ae-dc74fbabcfff, version 1 Endpoint: ncalrpc[Wireless Link Notification]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 0a74ef1c-41a4-4e06-83ae-dc74fbabcfff, version 1 Endpoint: ncalrpc[IcaApi]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 0a74ef1c-41a4-4e06-83ae-dc74fbabcfff, version 1 Endpoint: ncacn_np:\\PC1339[\\pipe\\Ctx_WinStation_API_service]

Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 0a74ef1c-41a4-4e06-83ae-dc74fbabcfff, version 1 Endpoint: ncalrpc[wzcsvc]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 0a74ef1c-41a4-4e06-83ae-dc74fbabcfff, version 1 Endpoint: ncalrpc[OLE3]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 0a74ef1c-41a4-4e06-83ae-dc74fbabcfff, version 1 Endpoint: ncacn_np:\\PC1339[\\PIPE\\atsvc]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcbfff, version 1 Endpoint: ncalrpc[Infrared Transfer Send] Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcbfff, version 1 Endpoint: ncalrpc[Wireless Link Notification] Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcbfff, version 1 Endpoint: ncalrpc[IcaApi] Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcbfff, version 1 Endpoint: ncacn_np:\\PC1339[\\pipe\\Ctx_WinStation_API_service] Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcbfff, version 1 Endpoint: ncalrpc[wzcsvc] Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcbfff, version 1 Endpoint: ncalrpc[OLE3] Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcbfff, version 1 Endpoint: ncacn_np:\\PC1339[\\PIPE\\atsvc] Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcbfff, version 1 Endpoint: ncalrpc[AudioSrv]



		Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcfff, version 1 Endpoint: ncacn_np:\PC1339[\PIPE\wkssvc] Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcfff, version 1 Endpoint: ncacn_np:\PC1339[\pipe\keysvc] Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcfff, version 1 Endpoint: ncalrpc[keysvc] Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fabcfff, version 1 Endpoint: ncacn_np:\PC1339[\PIPE\msgsvc] Annotation: Messenger Service
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 4b112204-0e19-11d3-b42b-0000f8abcfff, version 1 Endpoint: ncacn_np:\PC1339[\PIPE\DAV RPC SERVICE]
Informational	unknown (135/tcp)	A DCE service is listening on this host UUID: 4b112204-0e19-11d3-b42b-0000f8abcfff, version 1 Endpoint: ncacn_np:\PC1339[\PIPE\winreg]
Vulnerability	netbios-ssn (139/tcp)	. It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access  To prevent null sessions, see MS KB Article Q143474 (NT 4.0) and Q246261 (Windows 2000). Note that this won't completely disable null sessions, but will prevent them from connecting to IPC\$  . All the smb tests will be done as "/" in domain <a href="#">CVE : CVE-2000-0222</a>
Warning	netbios-ssn (139/tcp)	The domain SID can be obtained remotely. Its value is :  ABC : 5-21-3568188853-3288828060-38537ABCFFF  An attacker can use it to obtain the list of the local users of this host Solution : filter the ports 137 to 139 and 445

		Risk factor : Low
		<a href="#">CVE : CVE-2000-1200</a>
Warning	netbios-ssn (139/tcp)	<p>The host SID can be obtained remotely. Its value is : PC1339 : 5-21-971929597-3646181656-3495abcf</p> <p>An attacker can use it to obtain the list of the local users of this host Solution : filter the ports 137 to 139 and 445 Risk factor : Low</p>
		<a href="#">CVE : CVE-2000-1200</a>
Warning	netbios-ssn (139/tcp)	<p>A 'rfpoison' packet has been sent to the remote host. This packet is supposed to crash the 'services.exe' process, rendering the system instable. If you see that this attack was successful, have a look at this page : <a href="http://www.wiretrip.net/rfp/p/doc.asp?id=23&amp;iface=2">http://www.wiretrip.net/rfp/p/doc.asp?id=23&amp;iface=2</a></p>
		<a href="#">CVE : CVE-1999-0721</a>
Informational	netbios-ssn (139/tcp)	<p>The remote native lan manager is : Windows 2000 LAN Manager The remote Operating System is : Windows 5.1 The remote SMB Domain Name is : ABC</p>
Informational	unknown (1025/tcp)	<p>A DCE service is listening on this port UUID: 1ff70682-0a51-30e8-076d-740be8abcf, version 1 Endpoint: ncacn_ip_tcp:10.100.45.13[1025]</p>
Informational	unknown (1025/tcp)	<p>A DCE service is listening on this port UUID: 378e52b0-c0a9-11cf-822d-00aa00abcf, version 1 Endpoint: ncacn_ip_tcp:10.100.45.13[1025]</p>
Informational	unknown (1025/tcp)	<p>A DCE service is listening on this port UUID: 0a74ef1c-41a4-4e06-83ae-dc74fb1abcf, version 1 Endpoint: ncacn_ip_tcp:10.100.45.13[1025]</p>
Informational	unknown (1025/tcp)	<p>A DCE service is listening on this port UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fbabcf, version 1 Endpoint: ncacn_ip_tcp:10.100.45.13[1025] Annotation: Messenger Service</p>
Informational	unknown (5000/tcp)	A web server is running on this port
Informational	general/tcp	Nmap found that this host is running Windows 2000/XP/ME
Warning	netbios-ns (137/udp)	<p>. The following 6 NetBIOS names have been gathered : PC1339</p>

		ABC PC1339 PC1339 ABC ADMINISTRATOR . The remote host has the following MAC address on its adapter : 0x00 0x00 0x39 0x2e 0x6f 0xa2  If you do not want to allow everyone to find the NetBios name of your computer, you should filter incoming traffic to this port.  Risk factor : Medium
Warning	general/icmp	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.  This may help him to defeat all your time based authentication protocols.  Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).  Risk factor : Low <a href="#">CVE : CAN-1999-0524</a>
Informational	unknown (1040/udp)	A DCE service is listening on this port UUID: 5a7b91f8-ff00-11d0-a9b2-00c04fbabcfff, version 1 Endpoint: ncadg_ip_udp:10.100.45.13[1040] Annotation: Messenger Service
Informational	general/udp	For your information, here is the traceroute to 10.100.45.13 : 10.100.45.13

---

This file was generated by [Nessus](#), the open-sourced security scanner.

## REFERENCES

- Comeau, Bruce. "3Com's Top Ten Ways to Spoil a Wireless Hacker's Day", 2003  
URL: [ca.3com.com/landing\\_page/top10.html](http://ca.3com.com/landing_page/top10.html)
- Ellison, Craig. "Exploiting and Protecting 802.11b Wireless Networks" PC Magazine, September 4th 2001  
URL: <http://www.extremetech.com/article2/0,3973,31255,00.asp>
- "Securing your Wireless Network", URL: [http://www.practicallynetworked.com/support/wireless\\_secure.htm](http://www.practicallynetworked.com/support/wireless_secure.htm)
- Karagiannis, Konstantinos. "Ten Steps to a Secure Wireless Network" PC Magazine, 25 Feb 2003  
URL: <http://www.pcmag.com/article2/0%2C4149%2C844020%2C00.asp>
- Verry, John. "Comprehensive security audits unearth common wireless vulnerabilities", TechRepublic Jul 15, 2002
- Verry, John. "Penetration testing finds more holes in wireless network", TechRepublic, Aug 6, 2002
- Verry, John. "Security audit's final steps: Break the bad news and fix the WLAN", TechRepublic Sep 12, 2002
- Lynn, Mike and Baird, Robert "Advanced 802.11 Attack", Black Hat 2002, Las Vegas NV, July 2002  
URL: <http://www.blackhat.com/presentations/bh-usa-02/baird-lynn/bh-us-02-lynn-802.11attack.ppt>
- Potter, Bruce The Schmoo Group, "802.1x What it is, How it's broken, and How to fix it" Black Hat 2002, Las Vegas NV, July 2002 URL: <http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-potter-802.1x.ppt>

## News Articles

- Greene, Tim and Cox, John "Securing WLANs still a hit or miss proposition" NetworkWorldFusion, March 10 2003  
URL: <http://www.nwfusion.com/news/2003/0310wirelessvpn.html>

- Brooks, Jason. "Wireless LAN Lockdown" eWEEK February 3, 2003  
URL: <http://www.eweek.com/article2/0,3959,865802,00.asp>
- Brewin, Bob. "The Wi-Fi Alliance plans to certify 802.11g WLANs this summer" COMPUTERWORLD, FEBRUARY 25, 2003  
URL: <http://computerworld.com/newsletter/0%2C4902%2C78807%2C0.html?nlid=AM>
- Lawson, Stephen. "WLAN security spec probably due next year" Network World, IDG News Service, 02/21/03  
URL: <http://www.nwfusion.com/news/2003/0221wlansecur.html>
- "802.11's Maturity Propels WLAN Adoption" CommWeb.com, 01/21/03, 11:26 am  
URL: <http://www.networkmagazine.com/article/COM20030121S0002>
- Dornan, Andy. "Roadblocks for War Drivers: Stop Wi-Fi from Making Private Networks Public" Network Magazine, 12/04/02  
URL: <http://www.networkmagazine.com/article/NMG20021203S0006/1>

#### **National Institute of Standards and Technology**

- Karygiannis, Tom, and Owens, Les NIST "SP 800-48 Wireless Network Security: 802.11, Bluetooth, and Handheld Devices" November 2002 URL: [http://csrc.nist.gov/publications/nistpubs/800-48/NIST\\_SP\\_800-48.pdf](http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf)
- Swanson, Marianne. NIST "NIST SP 800-26, "Security Self-Assessment Guide for Information Technology Systems." November 2001 URL: <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>
- NIST. "NIST Security Assessment Tool, Automated Security Self-Evaluation Tool (ASSET)" Version 1.03  
URL: [http://csrc.nist.gov/asset/asset\\_download.html](http://csrc.nist.gov/asset/asset_download.html)
- Ross, Ron and Swanson, Marianne. NIST "NIST SP 800-37, Guidelines for Security Certification and Accreditation of Federal Information Technology Systems" October 2002  
URL: <http://www.csrc.nist.gov/sec-cert/SP-800-37-v1.0.pdf>

- Swanson, Marianne. Bartol, Nayda. Sabato, John. and Hash, Joan.” Draft NIST Special Publication 800-55, Security Metrics Guide for Information Technology Systems”  
URL: <http://www.csrc.nist.gov/publications/drafts/draft800-55.pdf>

#### **National Infrastructure Protection Center**

- “Best Practices for Wireless Fidelity (802.11b) Network Vulnerabilities”  
URL: <http://www.nipcc.gov/publications/nipccpub/bestpract.html>

#### **GCNA Practicals on Wireless Access Points**

- Gryparis, Mark. “Auditing the Cisco Aironet 340 Wireless Access Point” Oct 2002  
URL: [http://www.giac.org/practical/GSNA/Mark\\_Gryparis\\_GSNA.pdf](http://www.giac.org/practical/GSNA/Mark_Gryparis_GSNA.pdf)
- Loomis Angela “Auditing the Wireless Environment: A Mobile Wireless LAN Used for Training in Multiple Sites on a Corporate WAN- An Auditor’s Perspective” Nov 2002  
URL: [http://www.giac.org/practical/Angela\\_Loomis\\_GSNA.doc](http://www.giac.org/practical/Angela_Loomis_GSNA.doc)
- Marcinkowski, Slawomir. “Auditing a Wireless Access Point: The Orinoco Outdoor Router 1000 Configured as a Wireless Access Point” Feb 2002 URL: [http://www.giac.org/practical/Slawomir\\_Marcinkowski\\_GSNA.doc](http://www.giac.org/practical/Slawomir_Marcinkowski_GSNA.doc)
- Coran, Philip J. ”Topics in Auditing- High Level Review of WLAN” July 2002  
URL: [http://www.giac.org/practical/Philip\\_Coran\\_GSNA.doc](http://www.giac.org/practical/Philip_Coran_GSNA.doc)
- Wassom, Darrin “Auditing a Distributed Intrusion Detection System: An Auditors Perspective” July 2002  
URL: [http://www.giac.org/practical/Darrin\\_Wassom\\_GSNA.doc](http://www.giac.org/practical/Darrin_Wassom_GSNA.doc)

#### **Cisco Specific Security Articles:**

- “Cisco Aironet Products Now Include Protected Extensible Authentication Protocol Support” 21/Oct/2002  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_bulletin09186a0080100194.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a0080100194.html)

- “Response to University of Maryland's Security Analysis” 08/Sep/2002  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_bulletin09186a00800a9e74.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00800a9e74.html)
- “Cisco Wireless LAN Security Bulletin on WEP Weaknesses” 25/Sep/2001  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_bulletin09186a008009246f.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a008009246f.html)
- “Cisco Shares Findings From Recent WLAN Security Research” 10/Aug/2001  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_bulletin09186a008009246b.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a008009246b.html)
- “Cisco Secure Access Control Server v2.6” - No. 1264 Sep 2002  
URL: [http://www.cisco.com/warp/public/cc/general/bulletin/sqsw/1264\\_pp.htm](http://www.cisco.com/warp/public/cc/general/bulletin/sqsw/1264_pp.htm)
- “Cisco Aironet Products Now Include Protected Extensible Authentication Protocol Support” Oct 2002  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_bulletin09186a0080100194.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a0080100194.html)
- “Cisco Aironet Wireless LAN Security Overview”  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_brochure09186a0080088829.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a0080088829.html)
- “802.11 Wireless LAN Security” White Paper  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_white\\_paper09186a00800b469f.shtml](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml)
- “Configuring the Cisco Wireless Security Suite” Revision 2.0  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_white\\_paper09186a00800b3d27.shtml](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b3d27.shtml)

### **Cisco Aironet 1200 Series Access Point and Client Firmware and Utilities**

- “Cisco Aironet Client Setup Utility” (ACUv505001.exe )  
URL: <http://www.cisco.com/pcgi-bin/Software/Tablebuild/doftp.pl?ftpfile=pub/wireless/aironet/utilities/windows/ACUv505001.exe>

- “Cisco Aironet 1200 Series Access Point Software Configuration Guide”  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_configuration\\_guide\\_book09186a00800f23b6.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_configuration_guide_book09186a00800f23b6.html)
- “Cisco Aironet 1200 Series Access Point Software Configuration Guide Security Overview Levels of Security”  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_configuration\\_guide\\_chapter09186a008010f63d.html#1024053](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_configuration_guide_chapter09186a008010f63d.html#1024053)

### **Cisco Aironet 1200 Series Wireless Access Point Specific, Security Articles**

- “Cisco SECURITY ADVISORIES” Feb 2003  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_security\\_advisories\\_list.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_security_advisories_list.html)

### **Cisco FIELD NOTICES**

- “Repeater Mode Denies Wireless Client Access” 30/Dec/2002  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps441/products\\_field\\_notice09186a0080125b92.shtml](http://www.cisco.com/en/US/products/hw/wireless/ps441/products_field_notice09186a0080125b92.shtml)
- “LEAP and Broadcast Key Rotation Requires VLAN Config on AP1200” 16/Jan/2003  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_field\\_notice09186a0080126e53.shtml](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_field_notice09186a0080126e53.shtml)
- “Cisco Aironet 1200 Series Access Point Hangs under Bursts of Ethernet Traffic” 03/Jul/2002  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_field\\_notice09186a00800a3de0.shtml](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_field_notice09186a00800a3de0.shtml)

### **Bulletins**

- “Cisco Aironet Regulatory Domain Options” Product Bulletin 1833 08/Jul/2002



URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_bulletin09186a00800a406b.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00800a406b.html)

- “Cisco Aironet Response to Press - Flaws in 802.11 Security” 06/Sep/2001  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_bulletin09186a0080088832.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a0080088832.html)
- “Cisco Aironet Security Solution Provides Dynamic WEP” 06/Sep/2001  
URL: [http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\\_bulletin09186a008009246e.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a008009246e.html)

[Cisco TAC Newsletter](#),

#### **Other Documents and Items**

- Ratliff, Richard L, Internal Auditing: Principles and Techniques. Altamonte Springs: The Institute of Internal Auditors, 1996. 187-193.
- Newton, Stephen. “Security in a box: It's not enough” MARCH 11, 2003 Computerworld  
URL: <http://www.computerworld.com/securitytopics/security/story/0,10801,79083,00.html?nas=SEC-79083>
- Berry Jonathon, “Defense In Depth: Preventing Going Hairless Over Wireless” SANS Reading Room, April 17, 2002 URL: <http://www.sans.org/rr/wireless/hairless.php>
- Goransson, Paul. “802.1X provides user authentication” Network World, 03/25/02,  
URL: <http://www.nwfusion.com/news/tech/2002/0325tech.html>
- Snyder, Joel. “What is 802.1x?” Network World Global Test Alliance Network World Fusion, 05/06/02  
URL: <http://www.nwfusion.com/research/2002/0506whatisit.html>
- Craiger, J. Philip. “802.11, 802.1x, and Wireless Security” SANS Reading Room, June 23, 2002  
URL: <http://www.sans.org/rr/wireless/80211.php>
- “Sans/FBI Top 20 Vulnerabilities Version 3.22” The SANS Institute, March 3, 2003

URL: <http://www.sans.org/top20/>

- “Infosec.19990305.macos.a ” BugTraq May 03, 1999  
URL: <http://lists.insecure.org/lists/bugtraq/1999/May/0056.html>
- Xam, “Default SSID's for several common 802.11 Access Point and PCMCIA card Products” VERSION: 1.0.5, wi2600.org, May 29, 2001 URL: [http://mediawhore.wi2600.org/nf0/wireless/ssid\\_defaults/](http://mediawhore.wi2600.org/nf0/wireless/ssid_defaults/)
- “cisco-aironet-broadcast-ssid (6287)” Internet Security Systems, X-Force Database  
URL: [http://www.iss.net/security\\_center/static/6287.php](http://www.iss.net/security_center/static/6287.php)
- Bogue, Robert L “AiroPeekNX is a wireless security jack-of-all-trades” TechRepublic Mar 19, 2003
- Stubblefield, Adam. Ioannidis, John. Rubin, Aviel D “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP” August 6, 2001  
URL: [http://www.cs.rice.edu/~astubble/wep/wep\\_attack.html](http://www.cs.rice.edu/~astubble/wep/wep_attack.html)
- Huey, Benjamin. “Penetration Testing on 802.11b Networks” SANS Reading Room, February 24, 2002  
URL: [http://www.sans.org/rr/wireless/test\\_80211b.php](http://www.sans.org/rr/wireless/test_80211b.php)
- Song, Dug. “Passwords Found on a Wireless Network” USENIX Technical Conference WIP, June 2000.  
URL: <http://monkey.org/~dugsong/talks/usenix00.ps>
- Montcalm, Erik [How to Avoid Ethical and Legal Issues In Wireless Network Discovery](#) SANS Reading Room November 13, 2002 Sections 5 & 6.  
URL: <http://www.sans.org/rr/wireless/ethical.php>
- “Warchalking, the original (v.0.9) symbols” URL: [http://www.blackbeltjones.com/warchalking/warchalking0\\_9.pdf](http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf)
- “./warchalking” Updated List of Warchalking Symbols URL: <http://wlana.net/warchalking.htm>

- “Securing Desktop Workstations” A practice from the CERT® Security Improvement Modules, April 20, 2001  
URL: <http://www.cert.org/security-improvement/modules/m04.html>
- “Develop a computer deployment plan that includes security issues:” A practice from the CERT® Security Improvement Modules, May 2, 2001  
URL: <http://www.cert.org/security-improvement/practices/p065.html>
- CERT® “Advisory CA-2003-08 Increased Activity Targeting Windows Shares” March 11, 2003.  
URL: <http://www.cert.org/advisories/CA-2003-08.html>
- Nigel Morton, “Remote registry access A practical implementation” IBM e-BIT August 2002  
URL: <http://www-106.ibm.com/developerworks/security/library/s-regacc.html>
- Snitchler, Matt. “Introduction to the Microsoft Windows XP Firewall” SANS Reading Room, August 13, 2001  
URL: [http://www.sans.org/rr/win/XP\\_firewall.php](http://www.sans.org/rr/win/XP_firewall.php)
- “Security Audit Template” WildPackets, Inc.2002 URL: <http://www.wildpackets.com/>
- “Nessus a [free](#), powerful, [up-to-date](#) and easy to use remote security scanner” URL: <http://www.nessus.org/>
- “The Unofficial 802.11 Security Web Page” URL: <http://www.drizzle.com/~aboba/IEEE/>
- Common Vulnerabilities and Exposures (CVE®) A [list](#) of standardized names for vulnerabilities and other information security exposures as referenced in the NESSUS output URL: <http://cve.mitre.org/>

- “WaveLock” a free utility for blocking non administrative access to wireless network adapters in Windows 2000 and Windows XP. URL: [http://securewave.com/products/free\\_utilities/wavelock.html](http://securewave.com/products/free_utilities/wavelock.html)
- IEEE, “RFC 2196, Site Security Handbook” URL: <http://www.ietf.org/rfc/rfc2196.txt>
- IEEE, “RFC3330, “Special-Use IPv4 Addresses” URL: <http://www.rfc-editor.org/rfc/rfc3330.txt>
- CSCdz23591, Cisco “AP stops sending multicast causing config distribution problems” (requires a Cisco account) URL: [http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdz23591&cc\\_product=Cisco+Aironet+1200+Series+Access+Point&fse\\_t=&swver=&keyw=&target=&train=](http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdz23591&cc_product=Cisco+Aironet+1200+Series+Access+Point&fse_t=&swver=&keyw=&target=&train=)
- CSCdz32270, Cisco “ DHCP client id and channel information distributed to all APs.” (requires a Cisco account) URL: [http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdz32270&cc\\_product=Cisco+Aironet+1200+Series+Access+Point&fse\\_t=&swver=&keyw=&target=&train=](http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdz32270&cc_product=Cisco+Aironet+1200+Series+Access+Point&fse_t=&swver=&keyw=&target=&train=)
- [CSCdz15816](#), Cisco “ Enabling MIC will cause PCOMM/SNA not working” (requires a Cisco account) URL: [http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdz15816&cc\\_product=Cisco+Aironet+1200+Series+Access+Point&fse\\_t=&swver=&keyw=&target=&train=](http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdz15816&cc_product=Cisco+Aironet+1200+Series+Access+Point&fse_t=&swver=&keyw=&target=&train=)
- “WirelessAnarchy” URL: <http://wirelessanarchy.com/>
- “80211hotspots.com” The Definitive Source For Wi-Fi Access Points URL: <http://www.80211hotspots.com/>
- “Wigle.net” Nationwide database and mapping of 238,301 wireless networks .URL: <http://www.wigle.net>
- “WiFiMaps.com”. to provide interactive maps of wireless access-points across the globe, URL: <http://mapserver.zhrodaque.net>
- “WorldWideWarDrive” URL: <http://worldwidewardrive.org/>