Global Information Assurance Certification Paper

Auditing a Wireless Access Point: The Orinoco Outdor Router 1000 Configured as a Wireless Access Point

Slawomir Marcinkowski

SANS GSNA Practical (Version 1.2)

February 10, 2002

Table of Contents

GSNA Assignment 1 - Research in Audit, Measurement Practice and Control

GSNA Assignment 2 - Application of Audit Techniques to a Real World System

List of Tables

List of Figures

GSNA Assignment 1 - Research in Audit, Measurement Practice and Control

1. Focus of Audit

The focus of the audit research is an Agere Systems ORINOCO wireless access point (AP), the ORINOCO AP-1000. The AP-1000 runs the ORINOCO Outdoor Router v2.03 software configured to run as an 802.11b access point. The wireless clients run the Client Software Rel 7.4 for MS Windows Win 2000 Release.

2. Current State of Auditing a Wireless Access Point

A search for auditing a wireless local area network (WLAN) was conducted on the Internet. The most relevant information found is briefly described below. Only one list for auditing WLANs was found **(Dillon, 2001)**. The search primarily yielded articles explaining how WLANs ought to be configured for improved security. The material addresses management as well as technical configuration issues that are to be addressed when installing a WLAN. In addition, material and tools were found on how to locate WLAN access points.

As noted in the reference material, WLANs are very easy to install. A major threat to an organization is the rogue wireless access point installed by someone in the organization of which the network administrators nor the security personnel are aware. The organization's entire security perimeter can be compromised by a rogue WLAN AP situated behind the organization's firewall.

2.1 WLAN security articles:

(Dillon, 2001)
http://www.auditnet.org/docs/wireless.doc

Is the only WLAN audit list found on the Internet. The audit list provides an initial take on developing an audit for wireless networking at higher educational institutions. The audit list checks for who controls wireless deployment, whether an assessment was made of the technology, whether there is a business case for the use of WLAN, whether there is technical guidance (a focal point) available to those in the institution wanting to deploy a WLAN, whether the risks are understood, and what precautions are being taken to mitigate the risk of WLAN deployment.

(Schenk, 2001)
http://www.extremetech.com/print_article/0,3428,a%253D13521,00.asp

Provides an excellent overview of what needs to be considered when deploying a WLAN. Presents issues related to WLAN deployment, where to locate the access point, signals travel further than expected, signals can be detected from larger distances than expected

especially when using high gain antennas. WLANs have security mechanisms built in, such as Extended Service Set ID (ESSIS) or Service Set ID (SSID) that need to be changed from their default values to increase security. Enabling the highest WEP protection available, use of access lists where only known MAC addresses are allowed to associate. Using VPNs helps protect sensitive information transmitted over the WLAN. Use of the newer protocol 802.1x would make it difficult to use programs such as AirSnort based on the Fluher, Mantin, and Shamir attack.

(Ellison, 2001)
http://www.extremetech.com/print_article/0,3428,a%253D13880,00.asp

This excellent article presents a 17 point list on keeping a WLAN secure. The article builds on the information provided by the (Schenk, 2001) article. Many of the later found articles on WLAN security were very similar in content to this article.

(Kuehl, 2001)
http://aptools.sourceforge.net/wireless.ppt

Provides a presentation on how to find rogue access points on ones network. While some of the techniques are applicable in general, the emphasis is on Cisco's Aironet Access Point.

(Klaus, 2001)
http://www.iss.net/wireless/WLAN_FAQ.php

Is an excellent FAQ on wireless LAN security. Also, provides default vendor SSID settings. Definitely a must read for anyone deploying a WLAN.

(Orinoco, 2002)
http://www.orinocowireless.com/template.html?section=m131&page=3077&envelope=236

The Orinoco web site on wireless security provides several excellent papers. Security Technical Bulletin No. 002B which presents security issues that need to be addressed by system and security administrators to ensure a secure WLAN deployment. The security bulletin addresses the technical aspects of security (how the WLAN is to be configured), the management issues of policy and procedures (who approves WLAN deployment, what to do if a wireless laptop is stolen), and the architecture needed for a secure deployment. In addition a white paper titled "Wireless Local Area Network Security" provides insight on WLAN security and coming measures to improve WLAN security with the 802.1x protocol, in which the WEP key can be changed on a frequent basis, thus preventing the accumulation of sniffed data to crack the WEP key.

(Orinoco, 2000b)
ftp://ftp.orinocowireless.com/pubs/docs/ORINOCO/MANUALS/ug_OM.pdf

User's Guide that describes how to use the ORiNOCO AP & Client Manager tools for setting up & managing your wireless (indoor) networks, based on the WavePoint-II/AP-1000 access points.

(Orinoco, 2000a)
ftp://ftp.orinocowireless.com/pubs/docs/WaveACCESS/MANUAL/OR/ug_orm.pdf
User's Guide Revision C for the Configuration and Management tool of the ORiNOCO Outdoor Router System.

(wi2600, 2001)
http://www.wi2600.org/mediawhore/nf0/wireless/ssid_deaults/
Provides a listing of default settings (e.g., SSID) by WLAN vendor.

(Bowman, 2001)
http://www.microsoft.com/windowsxp/expertzone/columns/bowman/december03.asp
Provides advice on securing SOHO wireless residential LANs.

(WLANA, 2002)
http://www.wlana.org/learn/security.htm
Provides a series of white papers from the following companies addressing WLAN security: Microsoft, The Wireless Ethernet Compatibility Alliance, Cisco Colubris, and WaveLink.

(Ayyagari & Fout, 2001)
http://www.microsoft.com/windows2000/docs/wirelessec.doc
Provides information on making 802.11 WLANs enterprise ready.

(Klemencic, 2001)
http://www.securityfocus.com/infocus/1199
Provides an overview of WLAN security.

2.2 WLAN Detection Tools

The following WLAN tools are useful in performing an audit were mentioned by the above articles. The emphasis of these tools is to find the rogue wireless AP on the organization's network.

Network Stumbler
http://www.netstumbler.com
Cost: FREE
The software broadcasts a client probe and records all access point responses. For each access point found, it logs the MAC address of the access point, the network name, SSID, manufacturer, channel it was heard on, whether WEP is enabled, signal strength, signal to noise ratio, and various other information. However, the software does not do packet capture -- not a wireless packet sniffer.

Wildpackets AiroPeek
http://www.wildpackets.com/products/airopeek
Cost: $1995; there is a demo version to download
AiroPeek is a comprehensive packet analyzer for IEEE 802.11b wireless LANs, supporting all higher level network protocols such as TCP/IP, AppleTalk, NetBEUI and IPX.

Assessing Wireless Security With AiroPeek can be downloaded from
http://www.wildpackets.com/elements/AiroPeek_Security.pdf

Network Associate's Sniffer Wireless
http://www.sniffer.com/products/sniffer-wireless/default.asp?A=5
Cost: $9995
Is a fully loaded wireless protocol analyzer.

Internet Scanner 6.2
http://www.iss.net/wireless/WLAN_FAQ.php
Cost: $$$$
Provides assessment for 802.11b in X-Press Updates (XPU 4.9 and 4.10)

2.3 WEP Encryption Attack Tool

The following are two utilities that are able to recover WEP encryption keys based on the (Fluhrer, 2001) paper.

AirSnort
http://airsnort.sourceforge.net/
Cost: FREE

WEPCrack
http://wepcrack.sourceforge.net/
Cost: FREE

3. Why are Current Methods and Techniques in Need of Improvement?

The above URLs present an overall discussion on what system administrators need to do in order to have a secure[1] WLAN deployment. The above URLs are a great source of information on what to do from a management and a technical perspective when deploying WLANs. However, the information is written from the perspective on what to do, and not how to verify whether the WLAN is configured properly.

The information from the above URLs can be combined to serve as an auditing checklist for an auditor: (1) to determine whether there are any rogue wireless access points (AP) on the organization's network; (2) to verify whether any WLAN has been configured properly; (3) to determine whether there is policy or procedures governing the use of WLAN; (4) to determine whether there is policy and procedures for WLAN in the event of contingencies.

4. The Wireless Access Point Audit Checklist

The following is an annotated checklist that can be used by an auditor to firm determine whether there exist any rogue wireless access points in the organization. Second, to determine whether any wireless access points in the organization are securely configured.

While the audit checklist is focused specifically on the system being audited, the audit checklist can be applied to wireless LANs of other manufacturers with slight modifications.

Objective Measures

Objective measures are those that can be checked whether a particular option is enabled, and can be verified via an objective observation using a wireless sniffer or some other tool. The auditor need not make judgements based on the organization's security posture. For WLAN all security options should be enabled, for this helps deter the casual drive-by warrior. The objective measures check whether WLAN security options are enabled (e.g., WEP enabled, SSID default changed, Closed System Configuration, Access Control Lists in use). In the audit list, objective measures are denoted by (Objective: ….).

Subjective Measures

Subjective measures are those that the auditor needs to use some judgement in determining whether they are adequate, and these measures deal mostly with procedural and policy issues. The auditor needs to subjectively evaluate whether policy or procedures in place are adequate for the organization's security stance. In the audit list, subjective measures are denoted by (Subjective: ….).

[1] Various attacks have shown that current 802.11 WLANs are not secure.

Conventions Used

In general, each audit step consists of a series of audit questions. The auditor is asked to mark the choices given, or to provide text. Information is provided whether the audit item is objective or subjective. Then for each audit item are the scoring instructions in italics. Following the scoring instructions is space for the score and comments. Next is the Notes section containing screen shots and other information and material that are to be used by the auditor for the audit item.

4.1 Step 1: Seek Permission to Perform the Audit

Auditor is not proceed with the audit unless written authorization has been granted, by the organization whose system is to be audited.

(1) Has the auditor received written authorization by the organization to conduct the audit?

Yes **No**

If NO, the auditor is not to proceed with the audit.

Notes:
Having written authorization is a safeguard for the auditor. The letter of authorization should have at least two signatures authorizing the audit. The person authorizing the audit and their supervisor. As part of the authorization the rules of engagement need to be defined – what will be audited, what types of tools will be used, etc.

4.2 Step 2: Identify Organizational Policy and Procedures

The aim of this step is to identify and review the organization's information security policy(s) and procedures to identify those items related to wireless LANs. This will serve as a reference for the auditor in determining the security stance of the organization, for in some evaluation steps the items to be audited are subjective in nature. The score the auditor assigns for these subjective items will for the most part depend on the security stance of the organization, and the amount of risk the organization is willing to tolerate. What may be a score of PASS for one organization may be a score of FAIL for another organization.

(2) Does the organization have a policy and/or procedures requiring a survey of its perimeter and network using wireless tools or network assessment tools to locate wireless access points?

Yes **No**

(Objective: either policies / procedures exist addressing WLANs or they do not.)

Auditor assign a score of PASS, if the organization has policies specifically addressing wireless LANs. Assign a score of WARNING, if auditing networks is addressed in policy using conventional network scanning tools -- many of the standard network scanning tools do not directly address wireless APs on a network. A score of FAIL, is assigned if no policy exists requiring periodic network scans of any sort.

Score: _____

Comment:

_____
_____
_____

Notes:
Having a policy requiring that a network audit be conducted on a regular basis for wireless access points is highly advisable. A rogue access point set-up by an employee behind the organization's firewall by-passes all perimeter security, thus exposing the organization to all kinds of mischief.

(3) Is there a focal point for the organization's wireless initiatives?

Yes **No**

Who is it? _____

(Objective: Either there is a focal point on wireless initiatives or there is not.)

Auditor assign a score of PASS, if there is an identifiable person in the organization responsible for WLANs. Assign a FAIL, if the organization uses WLANs, but there is no identifiable focal point for such WLAN initiatives.

Score: _____

Comment:

_____
_____
_____

Notes:
Having a focal point within the organization for wireless issues demonstrates that the organization is not approaching wireless in a haphazard way. Hopefully, all wireless LAN activity in the organization has been approved by the focal point. A focal point will be aware of the risks associated with WLANs and risk mitigation techniques.

(4) Does the organization have a hardware / software accreditation process?

Yes **No**

If **YES**, then

(5) Has the wireless AP undergone through the accreditation process?

Yes **No**

(Objective: Either the accreditation process has been followed or not.)

Auditor assign a score of PASS, if the organization has an accreditation process and the WLAN has been approved through this process, otherwise assign a score of FAIL.

Score: _____

Comment:

_____
_____
_____

Notes:
Accreditation is the process by which software and hardware are evaluated on whether they are consistent with the organization's information security posture. With the existence of such a policy and related procedures, any deployed wireless AP should have undergone through this accreditation.

4.3 Step 3: Detecting / Finding a Wireless Access Point

There is no score (Pass, Fail, Warning) for this step. The intent is to identify AP's. If there are rogue sites, the auditor has his or her work cut to determine where exactly is the rogue AP. For approved sites the next step is for the auditor to audit the AP's configuration.

4.3.1 Wireless methods to detect wireless APs on a network

Use a wireless network detector (e.g., NetStumbler) or wireless sniffer (e.g., Wildpackets' AiroPeek, or Network Associate's Sniffer Wireless) to determine whether there are any active wireless access points on the organization's network, as described below. Perform this step by walking through the organization's buildings, on the organization's campus, and immediate surrounding areas. When performing the walk through, consideration should be given in using a high gain antenna to detect weak signals. Radio signals travel in three dimensions and are able to penetrate walls, ceilings, and floors.

(6) Has the wireless network detector software / wireless sniffer software detected any wireless access points?

Yes **No**

(Objective: determines the existence of wireless access point.)

Notes:

Using NetStumbler:

If NetStumbler detects an active wireless access point the following result (Figure 1) is produced. In this instance we note that WEP is enabled for there is a Yes in the WEP field, otherwise the field would be blank. NetStumbler will display the MAC address of the AP's card, the SSID of the network, the name of the network, what channel is being used, the vendor, the type, whether WEP is enabled or not, what flags are set and how often the beacon is transmitted. An important note is that NetStumbler will only detect Orinoco AP's that are not Closed. A Closed AP does not transmit its SSID, and therefore when Netstumbler sends 802.11 Probe Req packets, the AP will not respond with a 802.11 Probe Resp packet because it has not received a probe with the correct SSID. In short, NetStumbler will not detect an Orinoco AP that is configured as Closed (Figure 2). Therefore, a more robust tool, such as a wireless sniffer, needs to be employed for the walk through, otherwise an active but Closed Orinoco AP will not be detected.

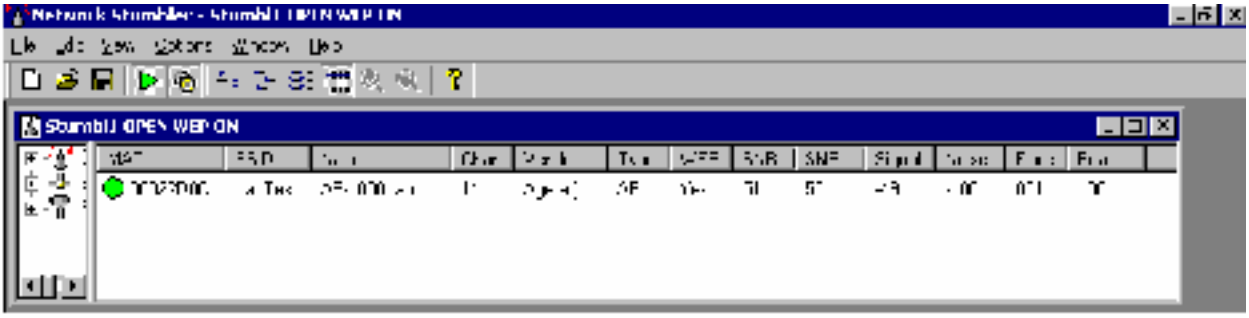


Figure 1 NetStumbler Screen Shot – Not-Closed Orinoco AP

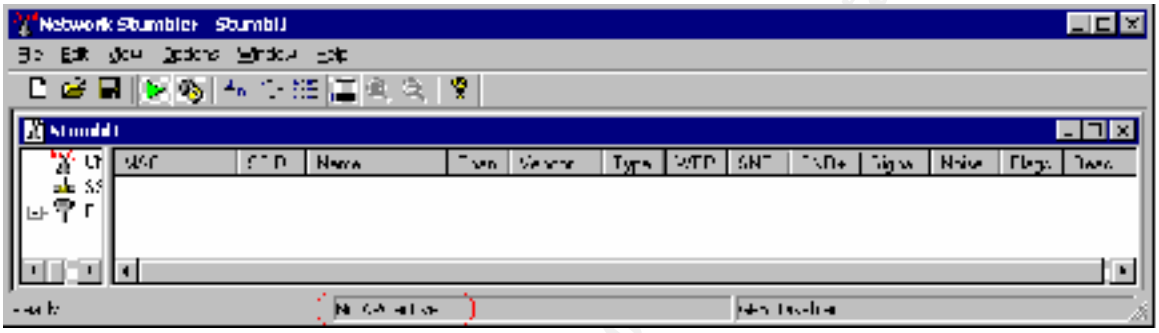


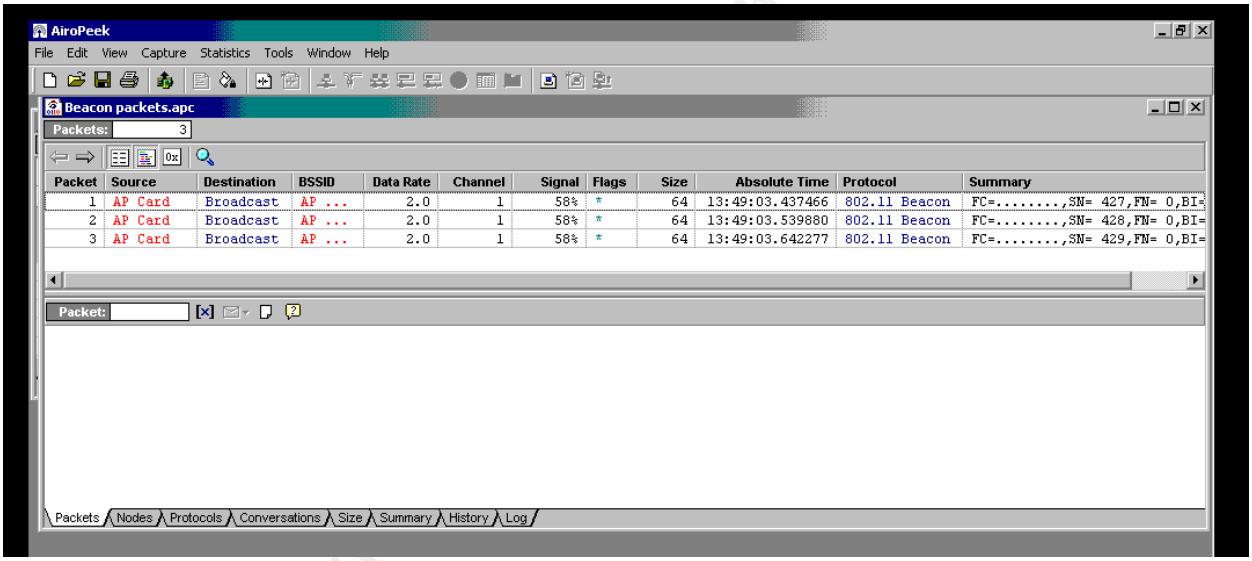
Figure 2 NetStumbler Screen Shot – Closed Orinoco AP

Using wireless packet sniffer:

The auditor needs to use a wireless sniffer (e.g., Wildpackets AiroPeek, Network Associate's Sniffer Wireless) which is a more robust tool than NetStumbler to detect wireless LAN access point in the organization.

In

Figure 3 a wireless sniffer called AiroPeek captures a wireless AP transmitting 802.11b Beacon packets. Figure 4 shows a decoded 802.11b Beacon packet that shows the SSID name, whether WEP is enabled (it is not). Capturing 802.11b Beacon packets indicates the presence of a wireless AP that needs to be investigated and audited. Wireless APs fall into two categories, approved APs which have been approved for use in the organization, and rogue APs set-up within the organization without anyone's knowledge.



Packet	Source	Destination	BSSID	Data Rate	Channel	Signal	Flags	Size	Absolute Time	Protocol	Summary
1	AP Card	Broadcast	AP ...	2.0	1	58%	*	64	13:49:03.437466	802.11 Beacon	FC=.....,SN= 427,FN= 0,BI=
2	AP Card	Broadcast	AP ...	2.0	1	58%	*	64	13:49:03.539880	802.11 Beacon	FC=.....,SN= 428,FN= 0,BI=
3	AP Card	Broadcast	AP ...	2.0	1	58%	*	64	13:49:03.642277	802.11 Beacon	FC=.....,SN= 429,FN= 0,BI=

Figure 3 AiroNet Detects 802.11b Beacon Packet from a Wireless AP

```
Flags:          0x00
  Status:         0x01
  Packet Length:64
  Timestamp:      13:49:03.437466 01/28/2002
  Data Rate:      4   2.0 Mbps
  Channel:        1   2412 MHz
  Signal Level: 58%
802.11 MAC Header
  Version:                0
  Type:                   %00   Management
  Subtype:                %1000   Beacon
  To DS:                  0
  From DS:                0
  More Frag.:             0
  Retry:                  0
  Power Mgmt:             0
  More Data:              0
  WEP:                    0
  Order:                  0
  Duration:               0   Microseconds
  Destination:            FF:FF:FF:FF:FF:FF   Broadcast
  Source:                 00:02:2D:0C:93:28   AP Card
  BSSID:                  00:02:2D:0C:93:28   AP Card
  Seq. Number:            427
  Frag. Number:           0
802.11 Management - Beacon
  Timestamp:              31232382   Microseconds
  Beacon Interval:        100
  ESS:                    1
  IBSS:                   0
  CF Pollable:            0
  CF Poll Req.:           0
  Privacy:                0
  Short Preamble:         0
  PBCC:                   0
  Chan. Agility:          0
  Reserved:               0
  Element ID:             0   SSID
    Length:               7
    SSID:                 LabTest
  Element ID:             1   Supported Rates
    Length:               4
    Supported Rate:       0x82   1.0 Mbps   (BSS Basic Rate)
    Supported Rate:       0x84   2.0 Mbps   (BSS Basic Rate)
    Supported Rate:       0x0B   5.5 Mbps   (Not BSS Basic Rate)
    Supported Rate:       0x16   11.0 Mbps   (Not BSS Basic Rate)
  Element ID:             3   Direct Sequence Parameter Set
    Length:               1
    Channel:              1
  Element ID:             5   Traffic Indication Map
    Length:               4
    DTIM Count:           0
    DTIM Period:          1
    Traffic Ind.:         0
    Bitmap Offset:        0
    Part Virt Bmap:       0x00
FCS - Frame Check Sequence
  FCS (Calculated):       0xEE6A72E0
```


Figure 4 802.11b Beacon Packet – Packet Details

4.3.2 Network scanning software to detect wireless APs on a network

The auditor can use Nmap, Nessus, or ISS Scanner to determine whether wireless access points exist in the organization. The results of using this software is mixed, as described below. Another method of detecting a Orinoco wireless APs on a network is to use the Orinoco Configuration Manager software.

(7) Has the network scanning software detected any wireless access points?
Yes **No**

(Objective: determines the existence of wireless access point.)

Notes:

Using Nmap:
Figure 5 and Figure 6 represent two different types of Nmap scans. In both cases, the scan identifies the Orinoco AP-1000 as an Apple AirPort Wireless Hub Base Station, which is incorrect. But yet, it is useful in that it is able to identify the device in question as a wireless device. The auditor will need to verify whether the device is really a wireless AP or something else. Furthermore, the auditor needs to physically locate the device and determine its make in order to continue with the audit. As Figure 6 depicts, the Orinoco AP-1000 has three UDP ports open.

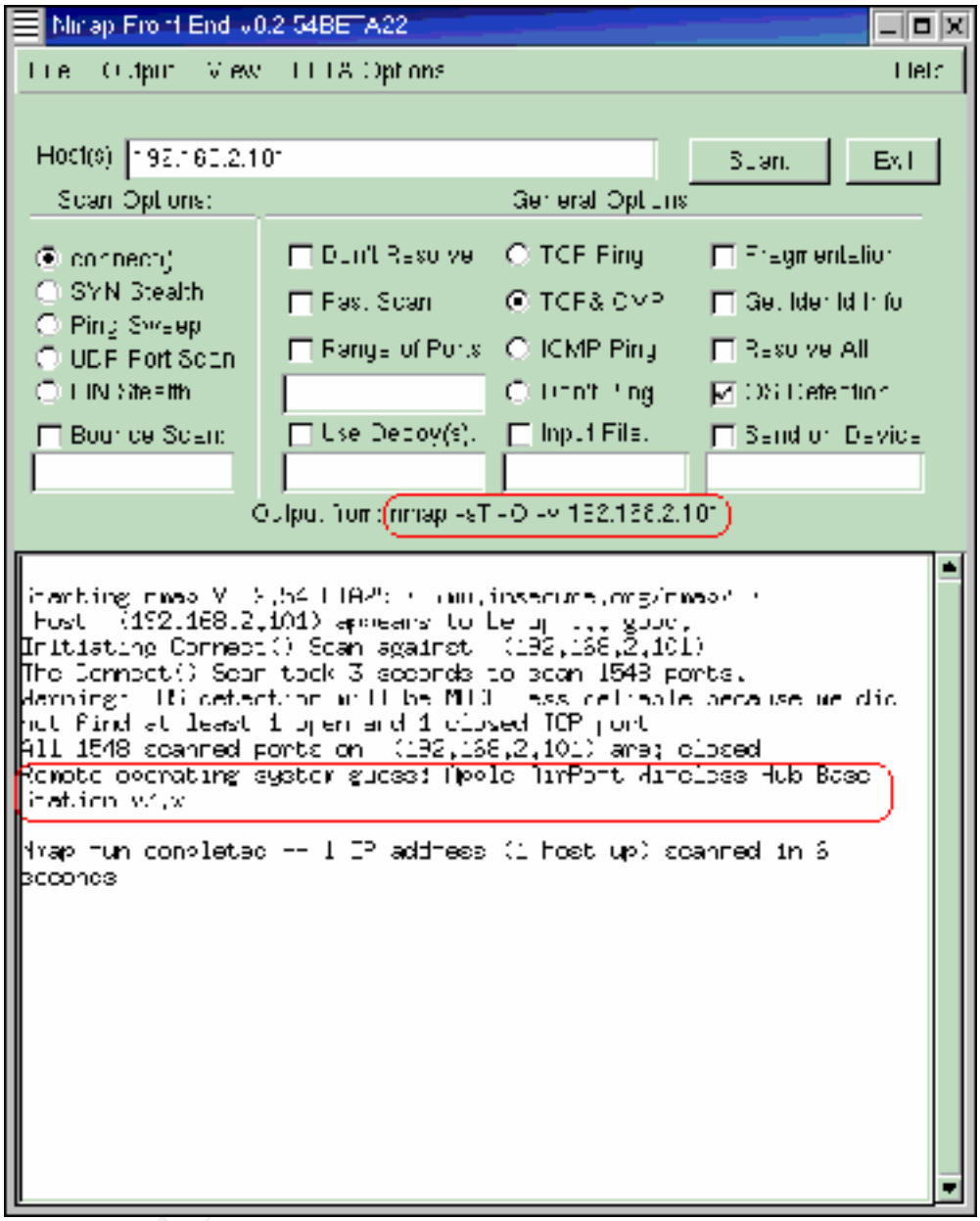


Figure 5 Using Nmap to find wireless AP on network (TCP Scan)

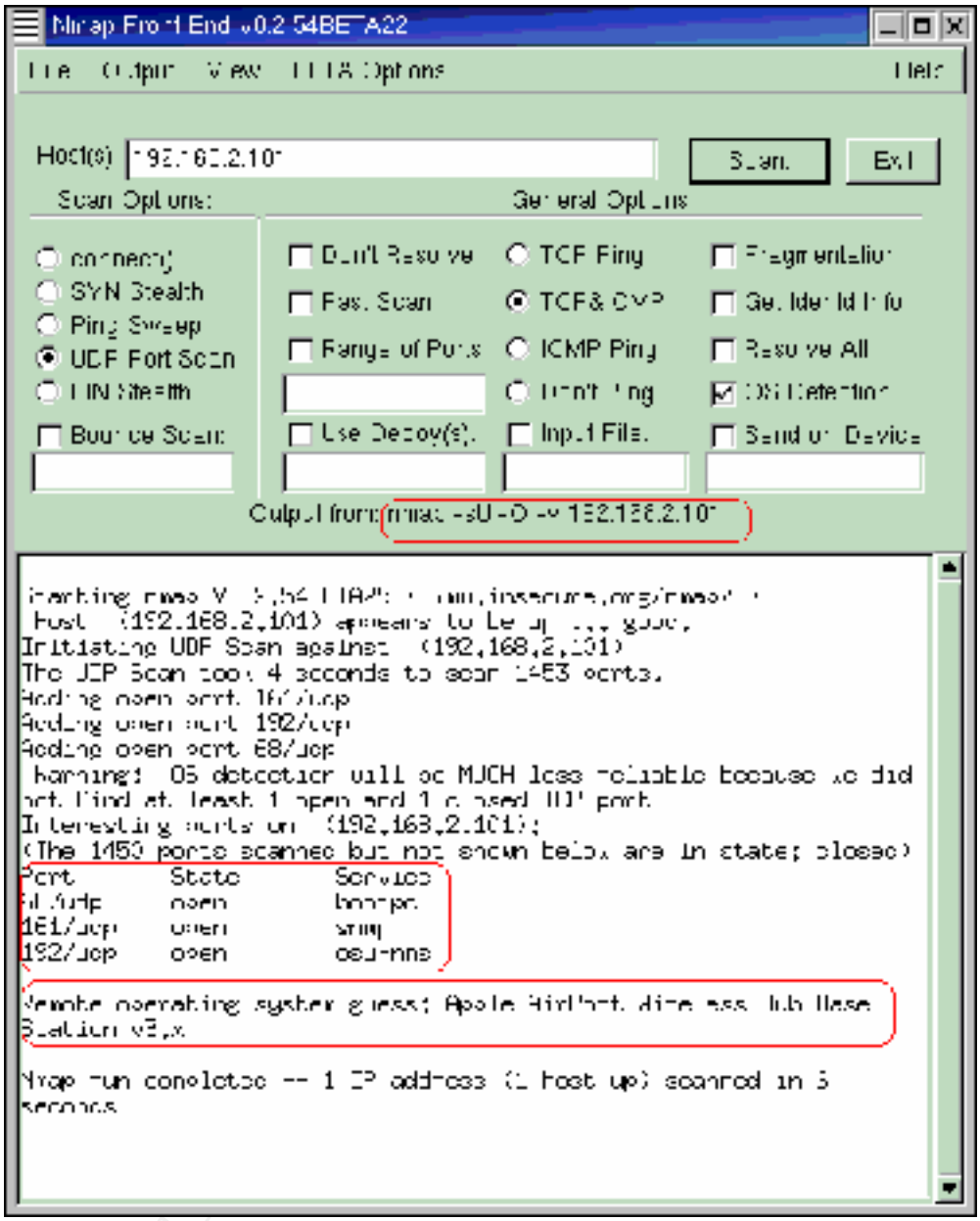


Figure 6 Using Nmap to find wireless AP on network (UDP Scan)

Using Nessus:
Figure 7 and Figure 8 show the Nessus scan-set-up and the resulting report, respectively. As shown in Figure 8, Nessus does not indicate that the device in question is a wireless access point, only indicates what ports are open -- the same as the Nmap results.

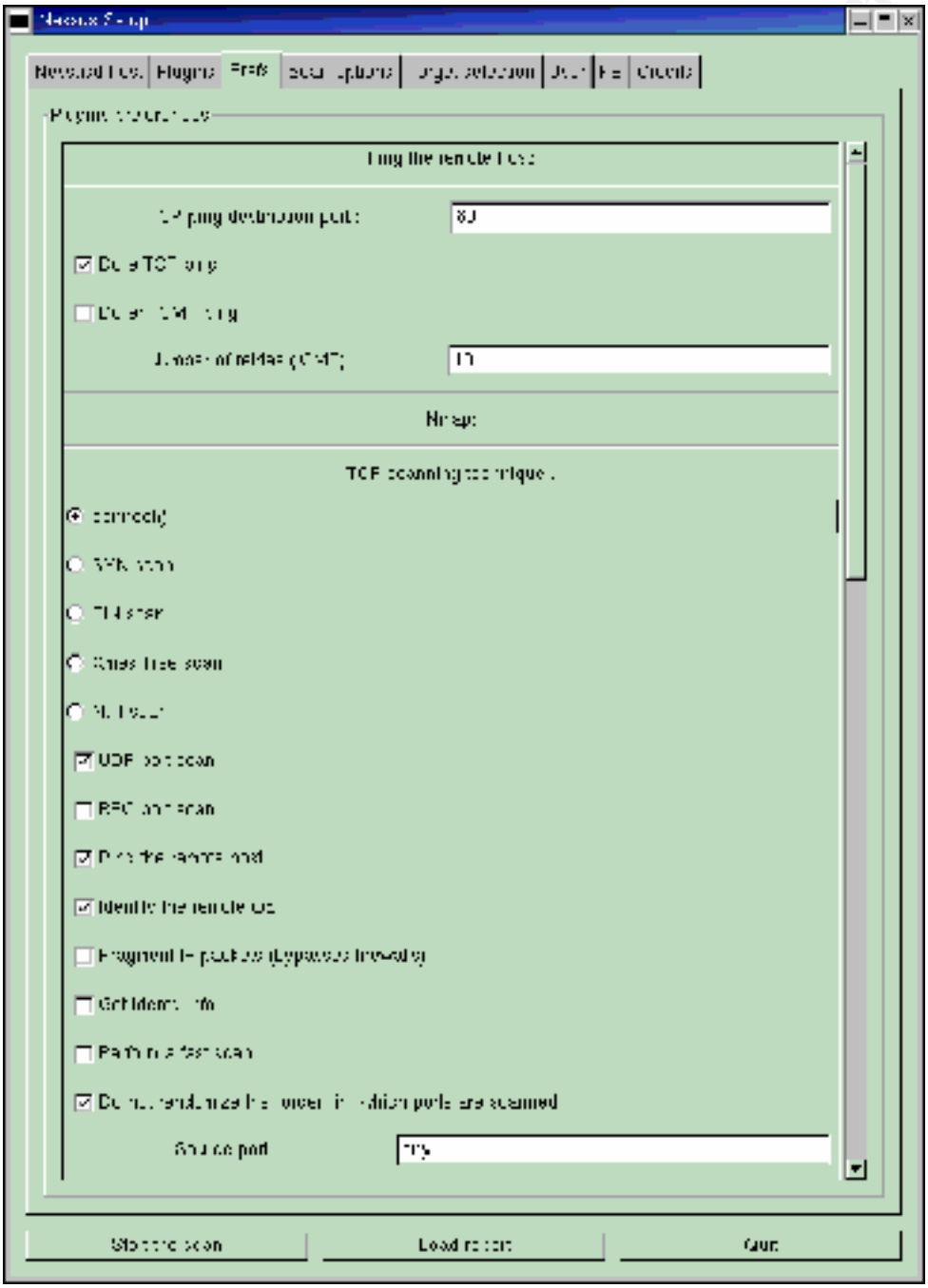


Figure 7 Nessus Scan Setup

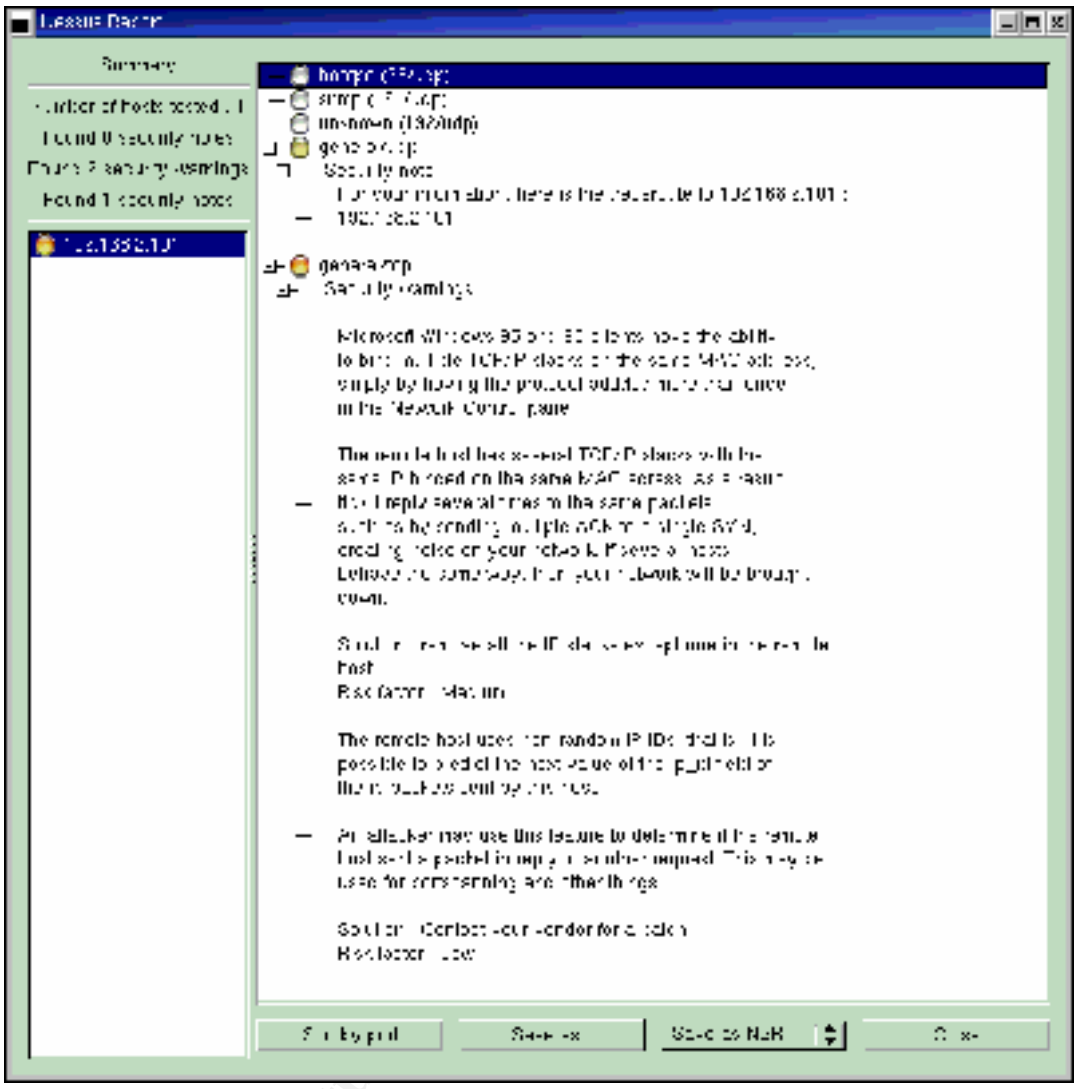


Figure 8 Nessus Scan Report

Using ISS:
According to the ISS website (http://www.iss.net/db_data/xpu/IS.php), ISS is able to detect WLAN vulnerabilities.

> **06-20-2001 X-Press Update 4.10** contains 42 new checks, **29 of which focus on the security of 802.11 Wireless LANs** (emphasis added). These checks will identify WLANS that may expose your network to security risks and will assist you in ensuring they are secure. This XPU also includes 13 checks for other high risk vulnerabilities including the IIS Isapi Idq Buffer Overflow (vulnerability used by the Code Red Worm), IIS Isapi Printer Buffer Overflow, IIS URL Decoding, and FTP Globbing. 37 existing checks are improved in this XPU. This XPU applies to Internet Scanner 6.1.
>
> **04-24-2001 X-Press Update 4.9 contains a check to detect rogue 802.11 access points** (emphasis added). This check will identify wireless LANS on your network, which put your network at risk if left unsecured. The XPU also contains the Solaris snmpXdmidbo check to detect vulnerable versions of the snmpXdmid daemon. This XPU has a total of 14 new checks. This XPU applies to Internet Scanner 6.1

ISS Scanner is an expensive tool that not all auditors may have access to. No results for ISS are presented, for the auditor did not have access to the tool.

Using Orinoco Configuration Manager Software:

This software is only able to detect Orinoco APs and therefore is limited in its practicality. From the File menu, the auditor needs to choose Open Remote Config option. By choosing the Scan button, the software will search out active AP's on the network as shown in Figure 9.

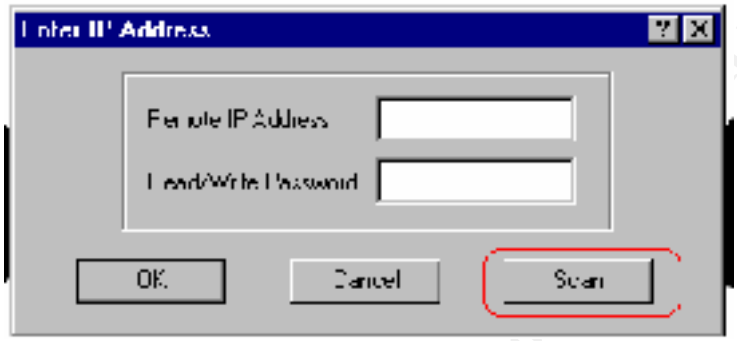


Figure 9 Using Orinoco Configuration Manager Software

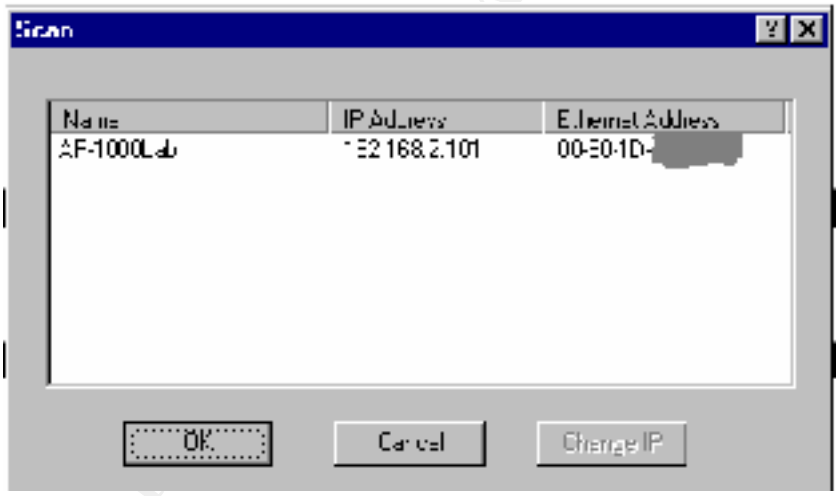


Figure 10 Determining what AP system(s) are available

From the list in Figure 10 the auditor can determine whether there are any Orinoco AP on the network.

4.3.3 Approved or rogue wireless access points

Of the wireless access points detected via wireless network detector software, wireless sniffer software, or via a scan of the organization's network, which are approved and which are rogue sites?

Auditor, list all wireless access points found, and check the appropriate column upon determination whether the wireless access point is an approved organizational wireless access point, or it is a rogue wireless access point.

Wireless Access Point	Approved	Rogue

Table 1 List of Wireless Access Points Located

4.3.4 Check war driving sites

Check war driving sites that post wireless access websites (e.g., http://www.netstumbler.com) that have been found by war drivers.

(8) Are any posted access points on war-driving web sites (e.g., http://www.netstumbler.com) on your organization's network?

Yes **No**

(Objective: determines the existence of wireless access point.)

If **YES**, then

(1) ask the site (e.g., NetStumber) to remove you immediately form the list
(2) locate the wireless access point in your organization
(3) take appropriate measures reflecting your organization's security posture

4.4 Step 4: Auditing the Security Configuration

The aim of this step is to audit whether the built-in security features of the wireless AP have been enabled, and are functioning properly.

To begin auditing the configuration set-up, the auditor must first open the configuration file using the Orinoco Configuration Manager software, from the File menu. Enter in the IP address of the AP from Figure 10 and enter in the READ/WRITE Password (Figure 11), which results in Figure 12. The from the Setup menu, choose Interface Setup to access the configuration screen (Figure 13), and then choose the option for the Orinoco. On Figure 14 the auditor needs to verify that the Outdoor Router Software on the AP-1000 has been configured to act as an IEEE 802.11b Access Point. Choosing the Security option on Figure 14 brings up the Orinoco Security Setup screen (Figure 15).

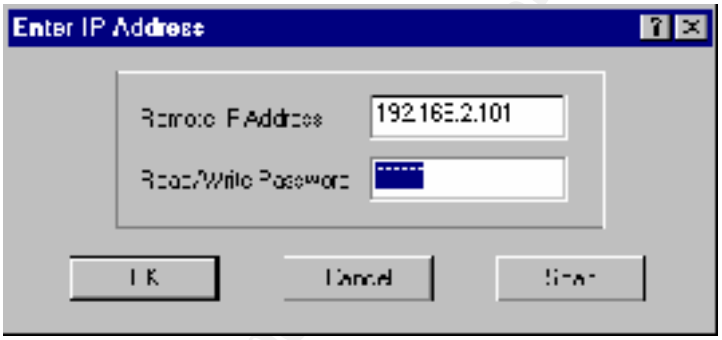


Figure 11 Entering in the READ/WRITE password to open the configuration file

Figure 12 The screen that appears when the correct password is entered

Figure 13 Check the set-up for each Orinoco Interface

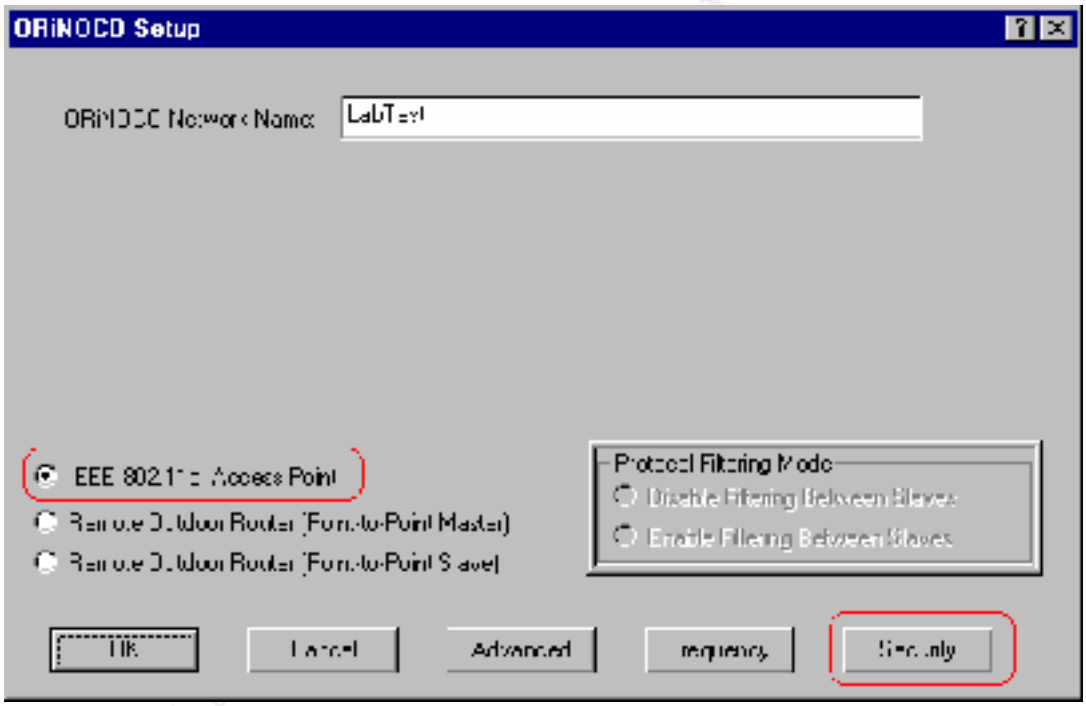


Figure 14 Configured as an IEEE 802.11b Access Point

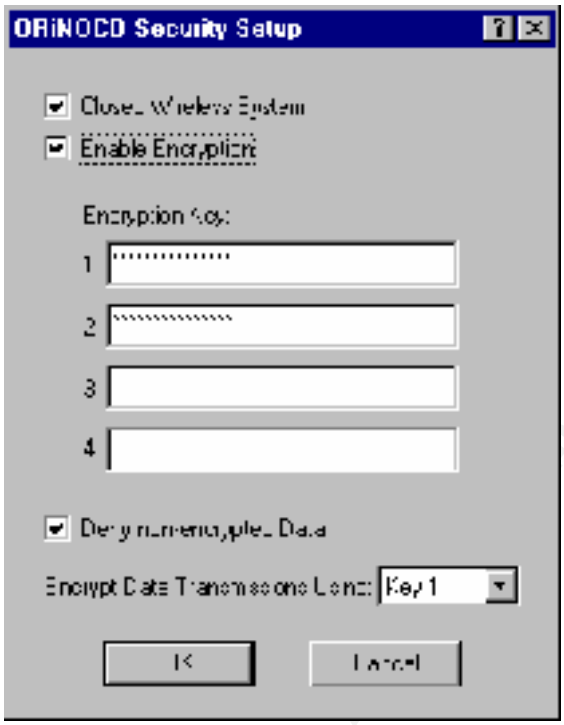


Figure 15 Orinoco Security Setup

(9) What is the security set-up of the AP?

Auditor examine the screen (like the one in Figure 15) on the system being audited, and based on the configuration of the system fill in (Table 2)

				Synopsis of what each wireless tool will detect		
AP's Security Setup (place check)	**Is "Closed Wireless System" checked?**	**IS "Enable Encryption" checked**	**Is "Deny non-encrypted data" checked?**	NetStumbler Detects	AiroPeek Detects	**Score to be Assigned**
	No	**No**		Y	Y	**Fail**
	No	**Yes**	**No**	Y	Y	**Fail**
	No	**Yes**	**Yes**	Y	Y	**Fail**
	Yes	**No**		N		**Fail**
	Yes	**Yes**	**No**	N	Y	**Fail**
	Yes	**Yes**	**Yes**	N	Y	**Pass**

Table 2 The AP's Security Setup

(Objective: verify that security measures are enabled and function properly.)

Auditor is to assign a score of PASS if the Closed Wireless System, Enable Encryption and the Deny non-encrypted Data are enabled, and verified using packets captured by the wireless packet sniffer (refer to notes section for example packet captures). To earn the score of PASS, the 802.11b Beacon packet details need to like that of Figure 17, where the privacy flag is set to one (denotes that WEP encryption is activated), and where the SSID is not transmitted (denotes closed system). Otherwise, the auditor is to assign a score of FAIL.

Score: _____

Comment:

_____

_____

_____

Notes:
The "deny non-encrypted data" is enabled by default. According to (Orinoco, 2000b) the access point has the following behavior when "deny non-encrypted data" is enabled:

- the AP only processes messages encrypted with a valid WEP key
- data is always transmitted using the valid WEP key
- encryption of all multi-cast and broadcast traffic that will transmit on the wireless medium

If the "deny non-encrypted data" is not enabled then the access point behaves as follows:

- AP processes all received wireless messages whether encrypted or not
- AP uses encryption based on the wireless client's capabilities
- uses encryption if the wireless client uses a valid WEP key
- if wireless client does not use encryption for data, data is sent unencrypted
- multicast and broadcast messages are sent in non-encrypted format

There are six basic permutations (Table 2) of the Security Setup (Figure 15) for the AP (Closed Wireless System, Enable Encryption, and Deny non-encrypted data). (Note that Deny non-encrypted data is dependent on whether Enable Encryption is enabled. Using a wireless sniffer (e.g., AiroPeek) one can objectively determine the security setup of AP. Figure 16 shows the packets captured during an association between a wireless client and the AP. The process is the same for all permutations of the security setup. What differs and what is of interest is the 802.11b Beacon packet that is transmitted by the AP for the permutations as presented in the following figures: Figure 17 802.11b Beacon packet details: Closed System ON, Enable Encryption ON; Figure 18 802.11b Beacon packet details: Closed System ON, Enable Encryption OFF; Figure 19 802.11b Beacon packet details: Closed System OFF, Enable Encryption ON; Figure 20 802.11b Beacon packet details: Closed System OFF, Enable Encryption OFF. In a closed system the SSID is not transmitted by the AP. When encryption is enabled the Privacy flag is set to 1.

The OPEN configuration is the standard 802.11 access mode allowing access to all wireless clients with the correct network name, and to all wireless clients with the network name set to "ANY". The CLOSED configuration is proprietary to ORINOCO and disallows access to wireless clients not programmed with the correct network name, and will deny access to a wireless client whose network name is set to "ANY", **and** denies access to wireless clients that are not ONRINOCO clients. The CLOSED configuration is not compliant with the 802.11 WLAN standard.

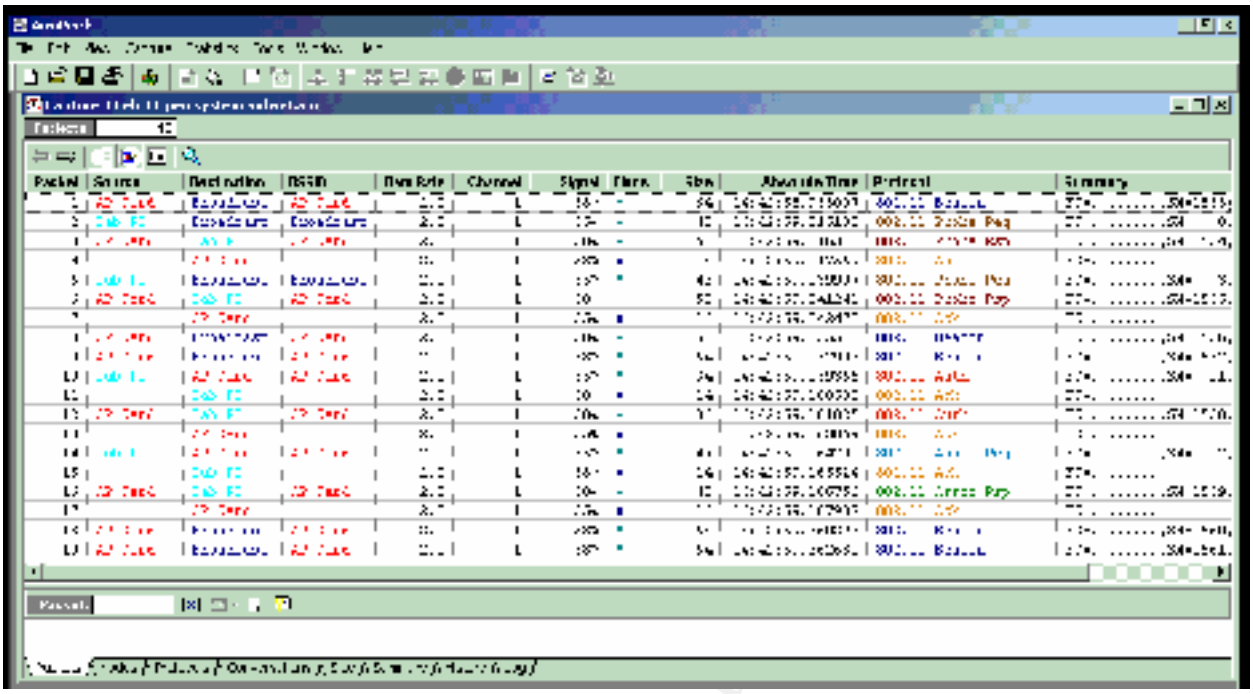
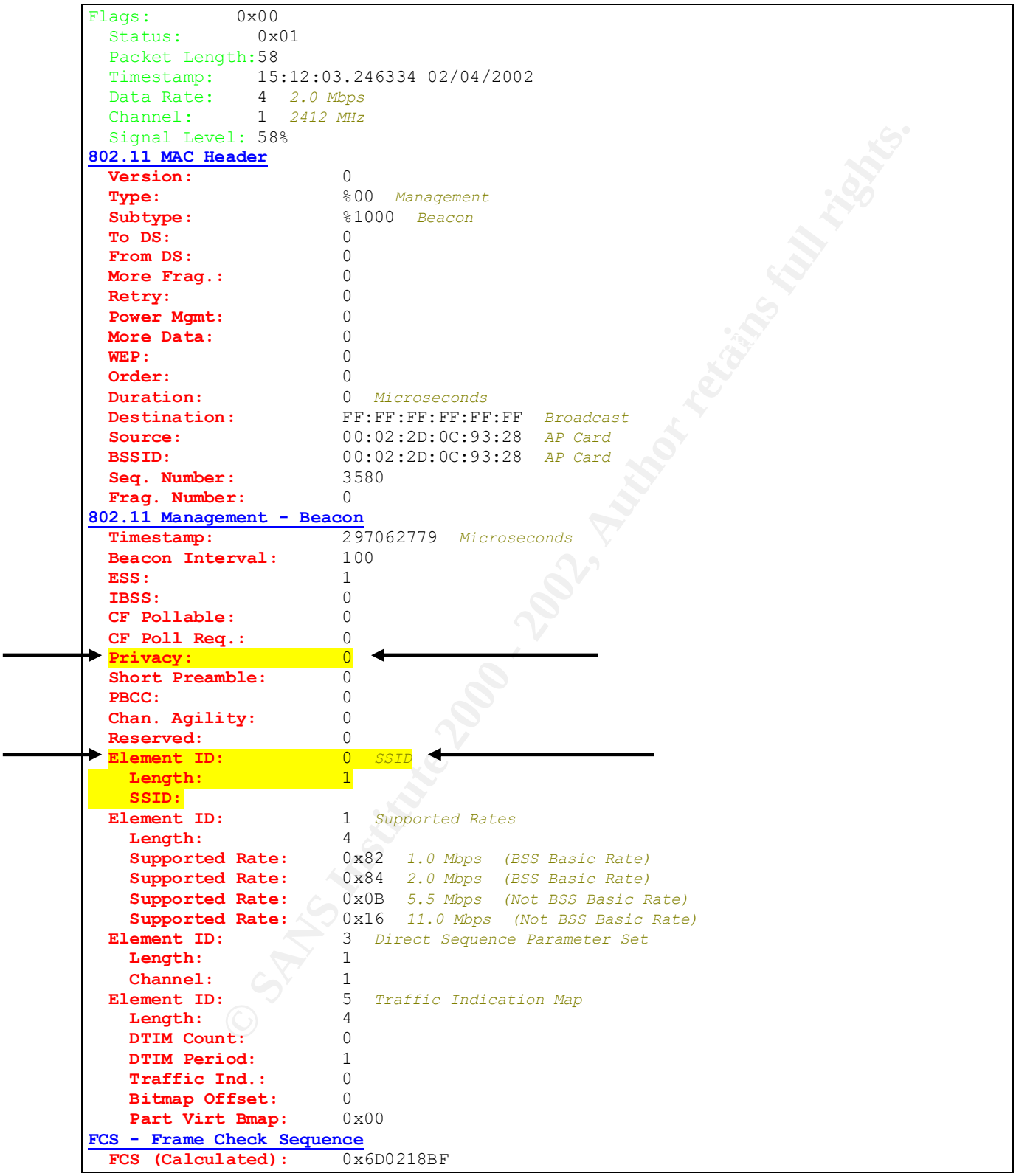


Figure 16 The Association Process

Using AiroPeek

```
Flags:          0x00
  Status:       0x01
  Packet Length:58
  Timestamp:    14:11:55.998625 02/04/2002
  Data Rate:    4   2.0 Mbps
  Channel:      1   2412 MHz
  Signal Level: 58%
802.11 MAC Header
  Version:              0
  Type:                 %00   Management
  Subtype:              %1000   Beacon
  To DS:                0
  From DS:              0
  More Frag.:           0
  Retry:                0
  Power Mgmt:           0
  More Data:            0
  WEP:                  0
  Order:                0
  Duration:             0   Microseconds
  Destination:          FF:FF:FF:FF:FF:FF   Broadcast
  Source:               00:02:2D:0C:93:28   AP Card
  BSSID:                00:02:2D:0C:93:28   AP Card
  Seq. Number:          1398
  Frag. Number:         0
802.11 Management - Beacon
  Timestamp:            1732710781   Microseconds
  Beacon Interval:      100
  ESS:                  1
  IBSS:                 0
  CF Pollable:          0
  CF Poll Req.:         0
  Privacy:              1
  Short Preamble:       0
  PBCC:                 0
  Chan. Agility:        0
  Reserved:             0
  Element ID:           0   SSID
    Length:             1
    SSID:
  Element ID:           1   Supported Rates
    Length:             4
    Supported Rate:     0x82   1.0 Mbps   (BSS Basic Rate)
    Supported Rate:     0x84   2.0 Mbps   (BSS Basic Rate)
    Supported Rate:     0x0B   5.5 Mbps   (Not BSS Basic Rate)
    Supported Rate:     0x16   11.0 Mbps   (Not BSS Basic Rate)
  Element ID:           3   Direct Sequence Parameter Set
    Length:             1
    Channel:            1
  Element ID:           5   Traffic Indication Map
    Length:             4
    DTIM Count:         0
    DTIM Period:        1
    Traffic Ind.:       0
    Bitmap Offset:      0
    Part Virt Bmap:     0x00
FCS - Frame Check Sequence
  FCS (Calculated):     0x2D8AE190
```

Figure 17 802.11b Beacon packet details: Closed System ON, Enable Encryption ON



```
Flags:          0x00
  Status:       0x01
  Packet Length:58
  Timestamp:    15:12:03.246334 02/04/2002
  Data Rate:    4  2.0 Mbps
  Channel:      1  2412 MHz
  Signal Level: 58%
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %1000  Beacon
  To DS:                0
  From DS:              0
  More Frag.:           0
  Retry:                0
  Power Mgmt:           0
  More Data:            0
  WEP:                  0
  Order:                0
  Duration:             0  Microseconds
  Destination:          FF:FF:FF:FF:FF:FF  Broadcast
  Source:               00:02:2D:0C:93:28  AP Card
  BSSID:                00:02:2D:0C:93:28  AP Card
  Seq. Number:          3580
  Frag. Number:         0
802.11 Management - Beacon
  Timestamp:            297062779  Microseconds
  Beacon Interval:      100
  ESS:                  1
  IBSS:                 0
  CF Pollable:          0
  CF Poll Req.:         0
  Privacy:              0
  Short Preamble:       0
  PBCC:                 0
  Chan. Agility:        0
  Reserved:             0
  Element ID:           0  SSID
    Length:             1
    SSID:
  Element ID:           1  Supported Rates
    Length:             4
    Supported Rate:     0x82  1.0 Mbps  (BSS Basic Rate)
    Supported Rate:     0x84  2.0 Mbps  (BSS Basic Rate)
    Supported Rate:     0x0B  5.5 Mbps  (Not BSS Basic Rate)
    Supported Rate:     0x16  11.0 Mbps  (Not BSS Basic Rate)
  Element ID:           3  Direct Sequence Parameter Set
    Length:             1
    Channel:            1
  Element ID:           5  Traffic Indication Map
    Length:             4
    DTIM Count:         0
    DTIM Period:        1
    Traffic Ind.:       0
    Bitmap Offset:      0
    Part Virt Bmap:     0x00
FCS - Frame Check Sequence
  FCS (Calculated):     0x6D0218BF
```


Figure 18 802.11b Beacon packet details: Closed System ON, Enable Encryption OFF

```
Flags:          0x00
  Status:       0x01
  Packet Length:64
  Timestamp:    15:42:24.701161 02/04/2002
  Data Rate:    4  2.0 Mbps
  Channel:      1  2412 MHz
  Signal Level: 61%
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %1000  Beacon
  To DS:                0
  From DS:              0
  More Frag.:           0
  Retry:                0
  Power Mgmt:           0
  More Data:            0
  WEP:                  0
  Order:                0
  Duration:             0  Microseconds
  Destination:          FF:FF:FF:FF:FF:FF  Broadcast
  Source:               00:02:2D:0C:93:28  AP Card
  BSSID:                00:02:2D:0C:93:28  AP Card
  Seq. Number:          2819
  Frag. Number:         0
802.11 Management - Beacon
  Timestamp:            221389182  Microseconds
  Beacon Interval:      100
  ESS:                  1
  IBSS:                 0
  CF Pollable:          0
  CF Poll Req.:         0
  Privacy:              1
  Short Preamble:       0
  PBCC:                 0
  Chan. Agility:        0
  Reserved:             0
  Element ID:           0  SSID
    Length:             7
    SSID:               LabTest
  Element ID:           1  Supported Rates
    Length:             4
    Supported Rate:     0x82  1.0 Mbps  (BSS Basic Rate)
    Supported Rate:     0x84  2.0 Mbps  (BSS Basic Rate)
    Supported Rate:     0x0B  5.5 Mbps  (Not BSS Basic Rate)
    Supported Rate:     0x16  11.0 Mbps  (Not BSS Basic Rate)
  Element ID:           3  Direct Sequence Parameter Set
    Length:             1
    Channel:            1
  Element ID:           5  Traffic Indication Map
    Length:             4
    DTIM Count:         0
    DTIM Period:        1
    Traffic Ind.:       0
    Bitmap Offset:      0
    Part Virt Bmap:     0x00
FCS - Frame Check Sequence
  FCS (Calculated):     0xADBDD4F8
```


Figure 19 802.11b Beacon packet details: Closed System OFF, Enable Encryption ON

```
Flags:          0x00
  Status:       0x01
  Packet Length:64
  Timestamp:    14:42:58.953097 02/04/2002
  Data Rate:    4  2.0 Mbps
  Channel:      1  2412 MHz
  Signal Level: 58%
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %1000  Beacon
  To DS:                0
  From DS:              0
  More Frag.:           0
  Retry:                0
  Power Mgmt:           0
  More Data:            0
  WEP:                  0
  Order:                0
  Duration:             0  Microseconds
  Destination:          FF:FF:FF:FF:FF:FF  Broadcast
  Source:               00:02:2D:0C:93:28  AP Card
  BSSID:                00:02:2D:0C:93:28  AP Card
  Seq. Number:          1553
  Frag. Number:         0
802.11 Management - Beacon
  Timestamp:            144486784  Microseconds
  Beacon Interval:      100
  ESS:                  1
  IBSS:                 0
  CF Pollable:          0
  CF Poll Req.:         0
  Privacy:              0
  Short Preamble:       0
  PBCC:                 0
  Chan. Agility:        0
  Reserved:             0
  Element ID:           0  SSID
    Length:             7
    SSID:               LabTest
  Element ID:           1  Supported Rates
    Length:             4
    Supported Rate:     0x82  1.0 Mbps  (BSS Basic Rate)
    Supported Rate:     0x84  2.0 Mbps  (BSS Basic Rate)
    Supported Rate:     0x0B  5.5 Mbps  (Not BSS Basic Rate)
    Supported Rate:     0x16  11.0 Mbps  (Not BSS Basic Rate)
  Element ID:           3  Direct Sequence Parameter Set
    Length:             1
    Channel:            1
  Element ID:           5  Traffic Indication Map
    Length:             4
    DTIM Count:         0
    DTIM Period:        1
    Traffic Ind.:       0
    Bitmap Offset:      0
    Part Virt Bmap:     0x00
FCS - Frame Check Sequence
  FCS (Calculated):     0xE79664C8
```


Figure 20 802.11b Beacon packet details: Closed System OFF, Enable Encryption OFF

(10) Are data packets actually WEP encrypted?
Yes **No**

(Objective: WEP encryption is either enabled or not.)

Auditor is to assign a score of PASS, when it is verified using a wireless sniffer that the actual data packets between the wireless client and the AP are encrypted. The captured packets need to be like those in Figure 23 and Figure 24.

Score: _____

Comment:
_____
_____
_____

Notes: Figure 21 and Figure 22 show a non-WEP encrypted 802.11 Data packet (802.11b Data) captured by AiroPeek. Figure 22 shows the details of the packet, and the WEP flag is set to 0. Figure 23 and Figure 24 show a 802.11b WEP Data encrypted packet captured by Airopeek. Notice in Figure 24 that in the encrypted packet the WEP flag is set to 1, and there is the field `802.11 WEP Data`, which denotes that the data is encrypted.

Using AiroPeek

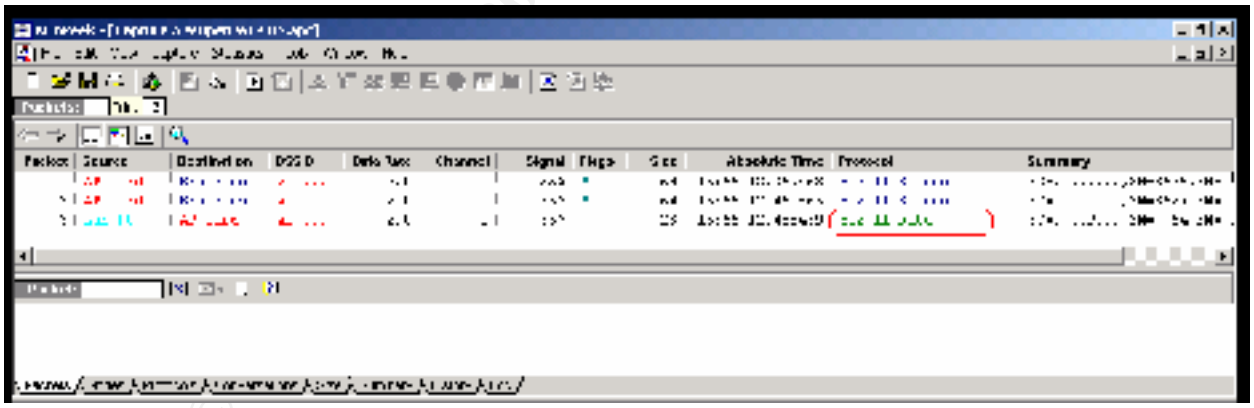


Figure 21 AiroPeek capture of a 802.11 Data packet when WEP is NOT enabled

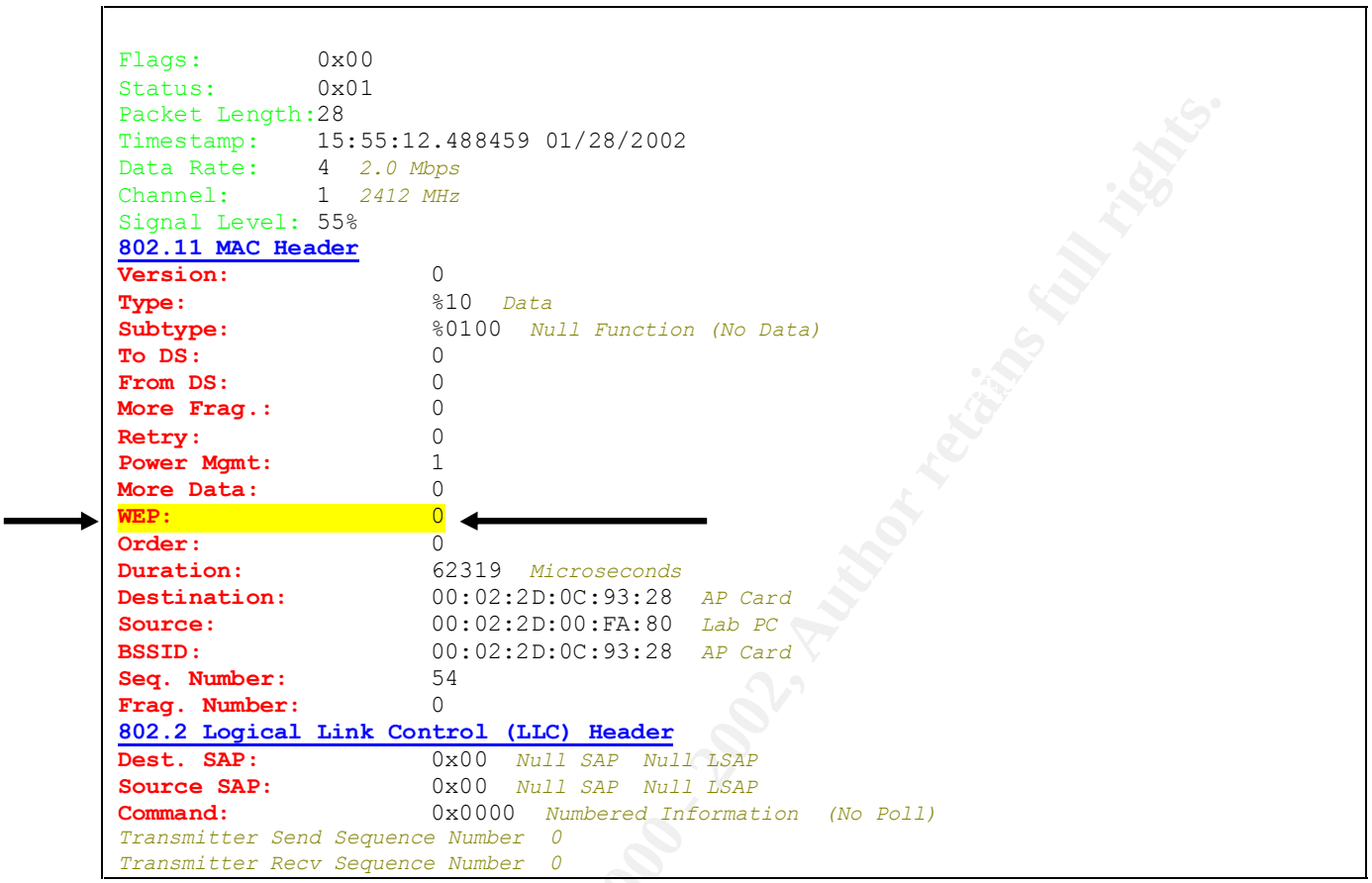


Figure 22 AiroPeek capture of a 802.11 Data packet when WEP is NOT enabled -- packet details

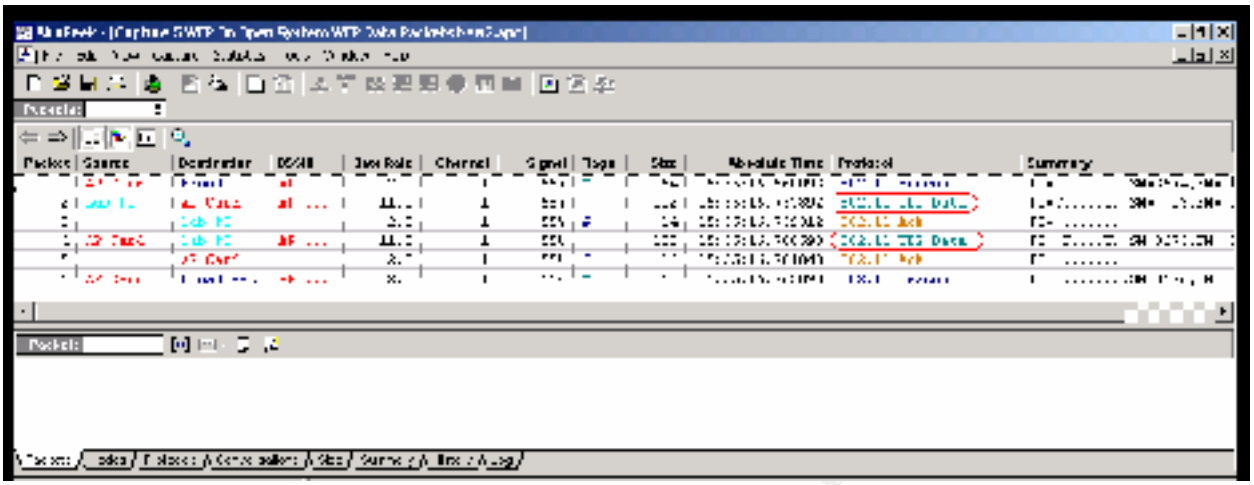


Figure 23 AiroPeek capture of a 802.11 Data packet when WEP IS enabled

```
Flags:          0x00
  Status:       0x01
  Packet Length:102
  Timestamp:    15:55:16.757892 01/28/2002
  Data Rate:    22  11.0 Mbps
  Channel:      1  2412 MHz
  Signal Level: 58%
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:                      1
  Order:                    0
  Duration:                 258  Microseconds
  BSSID:                    00:02:2D:0C:93:28  AP Card
  Source:                   00:02:2D:00:FA:80  Lab PC
  Destination:              00:02:2D:0C:93:28  AP Card
  Seq. Number:              13
  Frag. Number:             0
802.11 WEP Data
  WEP IV:                   0xF6110C
  WEP Key Index:            0  Key ID=1
  WEP Data:
  j<...(#.+......%  6A 3C D0 1F 93 28 23 81 2B 04 9B 87 90 DB 02 25
  /j..\....$....r.  2F 6A D7 FF 5C EB D8 93 9A 24 0B 98 A2 D3 72 A6
  . ..OyP.........  D5 20 CC D3 4F 79 50 B9 08 82 B4 D8 E2 92 DF 88
  .9......O.HE;R..  B1 39 81 A0 8B 00 E2 A8 4F E2 48 45 3B 52 F7 1E
  m.                6D 02
  WEP ICV:              0x230511C3
FCS - Frame Check Sequence
  FCS (Calculated):     0x661D7720
```

Figure 24 AiroPeek capture of a 802.11 Data packet when WEP is enabled -- packet details

(11) What is the level of WEP enabled?

64 bit (40 bit) **128 bit (104 bit)**

(12) What is the highest level of WEP available for the access point being audited?

64 bit (40 bit) **128 bit (104 bit)**

(Objective: the highest WEP available needs to be enabled.)

Notes:
The auditor needs to check the wireless access point's vendor's web site (http://www.orinocowireless.com/) to determine what level of WEP is currently being supported.

(13) Has the wireless access point's firmware/software been upgraded to the latest version?
Yes **No**

(Objective: in general a vendor's latest upgrade has the latest security enhancements.)

Notes: auditor needs to check the wireless access point's vendor's website to determine whether the AP software is the most current version.

(14) Has the wireless access point been upgraded to WEPplus?
Yes **No** **Not available yet**

(Objective: WEPplus is not vulnerable to the stealing of encryption keys using programs such as AirSnort or any other program based on the Fluher et all article.)

Auditor assign a score of PASS if the system being audited is current on its updates and the strongest WEP 128 bit (104 bit) is used, otherwise assign a score of FAIL.

Score: _____

Comment:
_____
_____
_____

Notes:
WEP is vulnerable to programs based on the Fluher et al article (e.g., AirSnort). Orinoco's WEPplus is not vulnerable to such an attack. Thus, if available the wireless access point ought to have WEPplus enabled. WEPplus is only available on Orinoco products.

4.5 Step 5: WEP Key Management

The aim of this audit step is to ascertain the status of WEP key management in the organization. Given enough data transferred wirelessly using the same WEP key, the WEP key can be derived using a program such as AirSnort. AirSnort can be used to derive the WEP key used. It is estimated that between 100 Mbyte and 1 Gigabyte of traffic is required to obtain the WEP key. Therefore, changing the WEP key on a regular basis is highly advisable.

(15) Are the WEP keys changed at regular intervals?

Yes **No**

If **YES**, then answer the following questions.

(16) What is the interval for the WEP key change?

_____

(17) Is the interval for WEP key change adequate?

Yes **No**

(Subjective: depending on the traffic amount over the wireless link and the organization's security posture.)

(18) Does the organization have a WEP key distribution procedure?

Yes **No**

(19) Is the WEP key management adequate?

(Subjective: depends on the number of WLANS and the number of clients per WLAN, and the security posture of the organization.)

Auditor based on your knowledge of the organization, its security stance, and the number of wireless clients indicate whether in your opinion the management of WEP keys is adequate. WEP key management demands a great deal of overhead to distribute keys when they are changed, and to coordinate key usage. Assign a score of PASS, if in your opinion WEP key

management is adequate. Otherwise assign a score of FAIL. Explain your score under comments.

Score: _____

Comment:

_____
_____
_____

Notes:
Distributing WEP keys can be problematic if there are many wireless clients associated with a WLAN and if the update is to occur frequently. For a small number of clients and low traffic, WEP key distribution may not be burdensome and the WEP keys will be changed often enough. While for a WLAN with many wireless clients and high traffic, the WEP key distribution may be burdensome and therefore the WEP keys may not be changed often enough.

In the case of the Orinoco, up to four keys can be defined (Figure 25). After predetermined time intervals, users will need to change to another predefined key. This is not accomplished automatically, but needs to be coordinated by a person so that the AP and the wireless clients are using the same key. It is advisable that keys be changed often, since WEP encryption is susceptible to the AirSnort program. Having a WEP key distribution procedure in place is indicative that WEP keys are probably being changed.

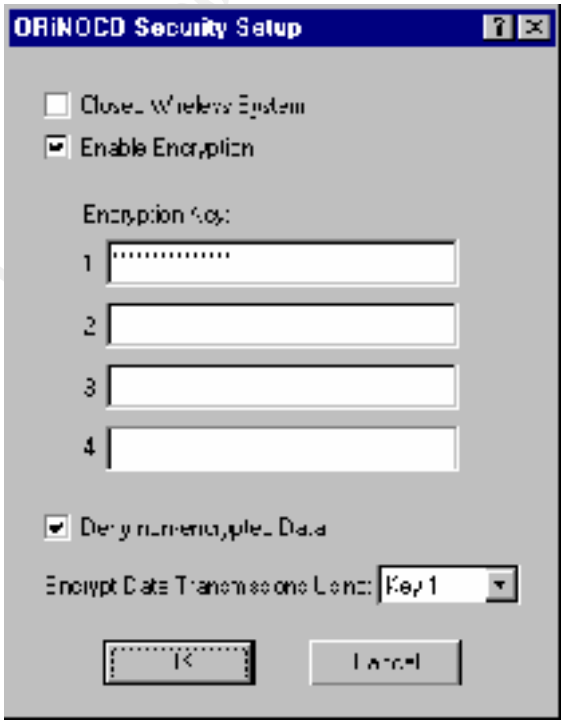


Figure 25 Multiple WEP keys can be used

4.6 Step 6: SSID Configuration

The aim of this step is to audit the AP's SSID.

(20) Has the default SSID been changed?
Yes **No**

(Objective: determines whether the default SSID has been changed or not.)

Auditor is to assign a score of FAIL if the default SSID has not been changed. If the SSID has been changed then assign a score of PASS.

Score: _____

Comment:
_____
_____
_____

Notes:
It is good practice to change the default SSID on the wireless access point. Default SSIDs are known for wireless access points (Klaus, 2001), (Schenk, 2001), and (wi2600, 2001).
The default SSID for the Agere Orinoco system systems is WaveLan network. If the system being audited is not Closed, then the auditor need only to check the AP's SSID in the 802.11b beacon packet as shown in Figure 20

However, if the audited system is Closed, then the auditor needs to configure the wireless client software with the default SSID (WaveLan network) to verify that an association is not made (Figure 26). Figure 27 illustrates the screen when a connection is made. The wireless client will send out 802.11b Probe Req packets (Figure 28), and there will be no 802.11b Probe Resp packets from the AP (
Figure 29).

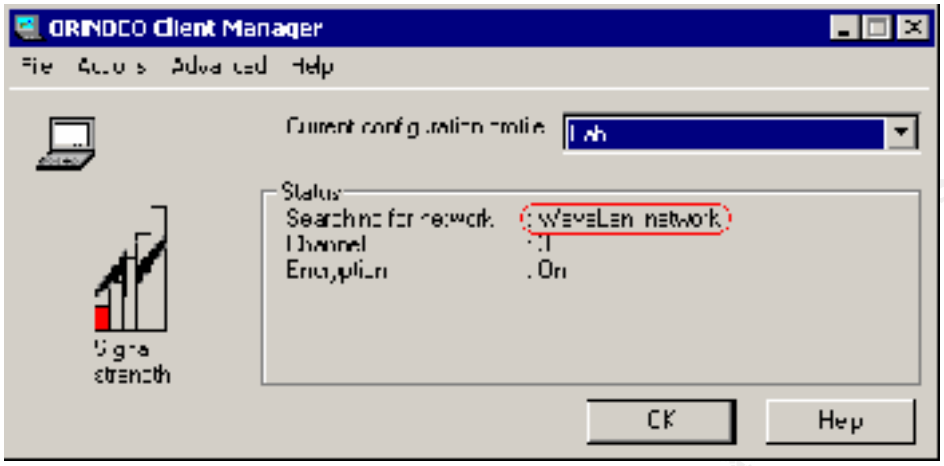


Figure 26 Default SSID is used – no connection made

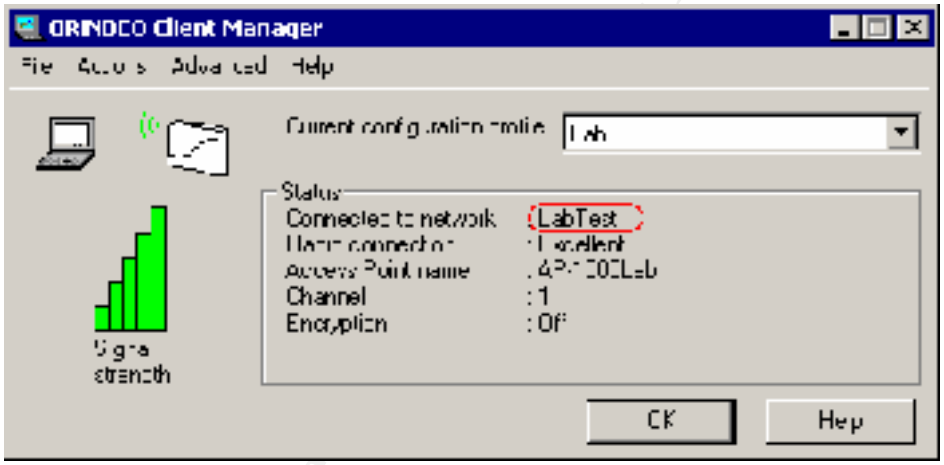


Figure 27 When Correct SSID is used – connection is made

```
Flags:          0x00
  Status:       0x01
  Packet Length:51
  Timestamp:    15:45:39.980200 02/06/2002
  Data Rate:    4  2.0 Mbps
  Channel:      1  2412 MHz
  Signal Level: 55%
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %0100  Probe Request
  To DS:                0
  From DS:              0
  More Frag.:           0
  Retry:                0
  Power Mgmt:           0
  More Data:            0
  WEP:                  0
  Order:                0
  Duration:             0  Microseconds
  Destination:          FF:FF:FF:FF:FF:FF  Broadcast
  Source:               00:02:2D:00:FA:80  Lab PC
  BSSID:                FF:FF:FF:FF:FF:FF  Broadcast
  Seq. Number:          77
  Frag. Number:         0
802.11 Management - Probe Request
  Element ID:           0  SSID
    Length:             15
    SSID:               WaveLan network
  Element ID:           1  Supported Rates
    Length:             4
    Supported Rate:     0x02  1.0 Mbps  (Not BSS Basic Rate)
    Supported Rate:     0x04  2.0 Mbps  (Not BSS Basic Rate)
    Supported Rate:     0x0B  5.5 Mbps  (Not BSS Basic Rate)
    Supported Rate:     0x16  11.0 Mbps  (Not BSS Basic Rate)
FCS - Frame Check Sequence
  FCS (Calculated):     0x2675CC97
```

Figure 28 Wireless Client Probe Request – packet details

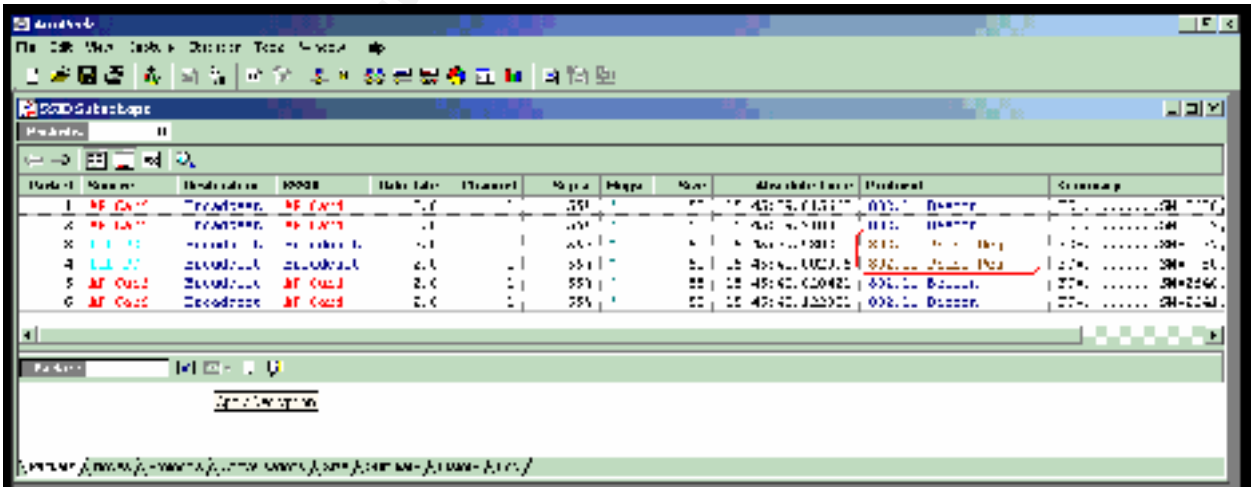


Figure 29 Wireless Client Probe Request – No Probe Response From AP

(21) Is the wireless access point configured to accept a blank or "ANY" SSID? blank SSID?
Yes **No**

(Objective: a SSID needs to be set for the AP.)

Auditor is to assign a score of FAIL if the wireless client is able to associate with the AP using either a blank SSID of the ANY SSID, otherwise assign a PASS.

Score: _____

Comment:
_____
_____
_____

Notes:
With a blank SSID or with the "ANY" parameter set, any wireless client with either a blank SSID set or with SSID set to ANY would be able to associate with the wireless access point. Similar audit steps need to be performed as those when auditing for the default SSID.

(22) Is the SSID a non-obvious SSID?
Yes **No**

(Subjective: it is difficult to determine what is or what is not a non-obvious SSID.)

While it may be subjective to say what is a non-obvious SSID or a strong SSID, the following guidelines can be used. The SSID should bear no reflection on the organization's name, divisions within the organization, products, address, etc. The SSID should use be a mixture of alphanumeric characters. A non-obvious SSID or strong SSID makes it more difficult that it will be guessed. The auditor is to assign a score of PASS, if the auditor believes the SSID is non-obvious or strong. A score of FAIL is to be assigned if the SSID is related to the organization. A score of WARNING is to be assigned, if the SSID could be stronger (e.g., make use of numbers along with letters).

Score: _____

Comment:
_____
_____

_____

(23) Has SSID broadcast been turned off?
Yes No

(Objective: it is either turned on or off.)

Auditor assign a score of PASS, if in Step 2 (look at Table 2*) the system being audited was configured as a Closed Wireless System, otherwise assign a score of FAIL. This item is included for completeness, for this audit can be used with slight modification to audit other vendors' WLAN APs. Closed is Orinoco proprietary, other vendors may denote this differently.*

Score: _____

Comment:
_____
_____
_____

Notes:
For Orinoco systems this is the same as Closed Configuration refer to Step 2 that deals with Closed Wireless System.

Unless SSID broadcast is disabled, the SSID will be broadcast periodically by the access point, thus allowing a wireless client or a sniffer to obtain the SSID. By disabling the broadcast, a wireless client will need to know the SSID of the network in order to associate with the access point. A caveat is that the SSID even if WEP is turned on is not encrypted. Even with the SSID broadcast disabled, a wireless sniffer will still be able to capture the SSID when an authorized wireless client sends the SSID in the clear in the probe message when the wireless client is associated with the AP. In other words, someone with a wireless sniffer need only wait until an authorized wireless client associates with the access point to obtain the SSID.

4.7 Step 7: READ/WRITE and READ Password

The aim of this step is to audit the security of the READ/WRITE and the READ password of the AP. The READ/WRITE password is used to manage the configuration of the AP. Using this password a user can access the configuration, modify, and save the changes. The READ password allows access to the AP so the user can monitor the statistics.

Depending on the security stance of the organization, the organization may want to have different READ/WRITE and READ passwords, thus granting different levels of access and authority over the AP.

(24) Is the READ/WRITE configuration password the default password?

Yes **No**

(Objective: either it is the default password or it is not.)

Auditor assign a score of FAIL, if the default password (public) for the system enables the auditor to access the configuration of the AP, otherwise assign a PASS.

Score: _____

Comment:

_____
_____
_____

Notes:
The default password is in the documentation that comes with the system. For the Orinoco system, the **default password is "public".** If entering the READ/WRITE password of "public" one is denied access, then the READ/WRITE password is not set to the default password.

To audit the READ/WRITE password, the auditor must first open the configuration file using the Orinoco Configuration Manager software, from the File menu. Enter in the IP address of the AP and enter in the READ/WRITE password as shown in (Figure 30), and hit OK. Figure 31 illustrates the screen that appears when the correct READ/WRITE password has been entered. Figure 32 illustrates the screen that appears when the incorrect correct READ/WRITE password has been entered.

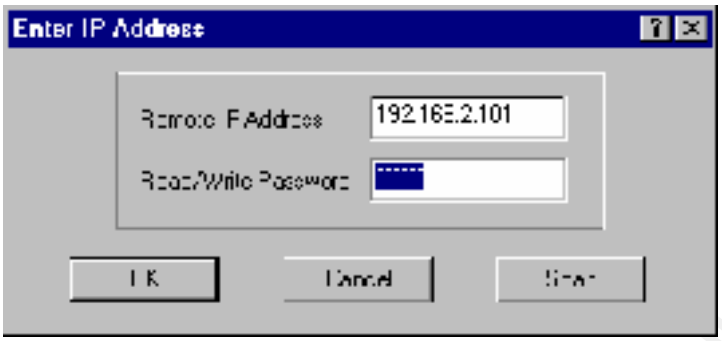


Figure 30 Entering in the READ/WRITE password to open the configuration file

Figure 31 The screen that appears when the correct WRITE password is entered

Figure 32 Read/Write password failure

(25) Is the READ/WRITE configuration password difficult to guess?

Yes **No**

(Subjective: it is difficult to determine whether a password is difficult to guess.)

While it may be subjective to say whether a password is difficult to guess or not, the following guidelines can be used. The READ/WRITE password ought to be at least eight characters in length and be composed of alphanumeric characters. The password should not be a word in a dictionary, or related to the organization (e.g., company name, address, department located in). Auditor assign a PASS if the password is at least eight characters in length and uses a combination of letters and numbers. A score of FAIL is to be assigned, if the password is a dictionary word. A score Warning is to be assigned if the auditor believes the password could be made stronger.

Score: _____

Comment:

_____
_____
_____

(26) Is the READ password the default password?
Yes No

(Objective: either it is the default password or it is not.)

Auditor assign a score of FAIL, if the default password for the system enables the auditor to access the monitoring functions requiring the READ password, otherwise assign a PASS.

Score: _____

Comment:
_____
_____
_____

Notes:
The default password is in the documentation that comes with the system. For the Orinoco system, **the default password is "public"**. If entering the READ password of "public" one is denied access, then the READ password is not set to the default password.

To audit the READ password, the auditor must first make sure that the READ/WRITE password has not been used to open the configuration. From the main menu of the OR Manager choose the Monitor option, and then the Select Another Device (Figure 33). Then enter in the default password of "public" (Figure 34). . Figure 35 illustrates the screen that appears when the correct READ password has been entered. Figure 36 illustrates the screen that appears when the incorrect correct READ password has been entered.

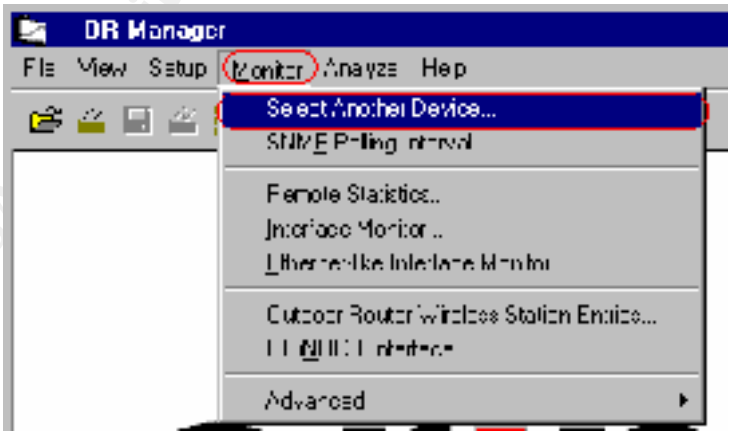


Figure 33 Screen to audit the READ password

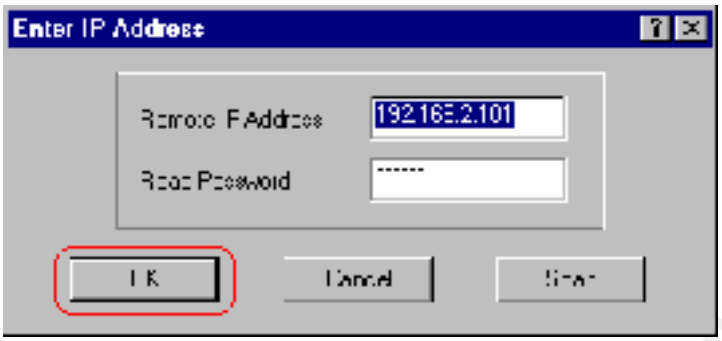


Figure 34 Entering in the READ password in order to access the monitor statistics

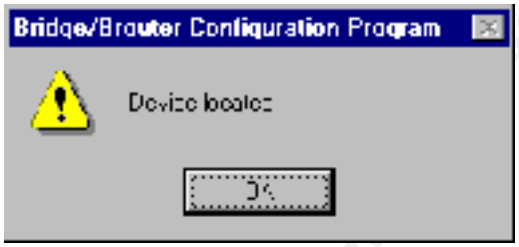


Figure 35 The screen that appears when the correct READ password is entered

Figure 36 READ password failure

(27) Is the READ configuration password difficult to guess?

Yes **No**

(Subjective: it is difficult to determine whether a password is difficult to guess)

While it may be subjective to say whether a password is difficult to guess or not, the following guidelines can be used. The READ password ought to be at least eight characters in length and be composed of alphanumeric characters. The password should not be a word in a dictionary, or related to the organization (e.g., company name, address, department located in). Auditor assign a PASS if the password is at least eight characters in length and uses a combination of letters and numbers. A score of FAIL is to be assigned, if the password is a dictionary word. A score Warning is to be assigned if the auditor believes the password could be made stronger.

Score: _____

Comment:

_____

_____

_____

(28) Is the READ and the READ/WRITE password the same?

Yes **No**

(Subjective: depends on whether the organization wants different levels of authority access to the wireless access point.)

Auditor assign a score of FAIL, if the organization requires that there be a differentiation in access authority to the AP and yet the passwords are the same. Otherwise, assign a score of PASS.

Score: _____

Comment:

_____
_____
_____

Notes:
Having separate passwords enables there to be different levels of authority, certain administrators/users can only READ the information, while those with READ/WRITE have the capability to read and change the parameters. If the intent of the organization is to have different levels of authority, then having the same password set for READ and READ/WRITE can be considered to be insecure.

4.8 Step 8: SNMP Access Control List

The aim of this audit step is to first determine whether the organization, because of policy or its security stance, needs the extra level of security offered by the SNMP IP access control list (Figure 37). This access control list limits which work stations can access the AP's configuration file.

(29) Does the organization make use of the SNMP IP access control list for access to the AP's configuration file?

Yes **No**

(Subjective: depends on the organization's security stance.)

If the answer is NO, then auditor assign a score of FAIL, if the organization is NOT using an SNMP ACL, and yet requires the extra level of security offered by an SNMP ACL, based on what you know of the organization, its security posture, and its policy. Assign a score of PASS, if the organization is using the SNMP ACL.

If the answer is **YES**, then proceed to the next audit item in this step.

Score: _____

Comment:

_____
_____
_____

(30) Is the SNMP IP ACL functioning correctly?

Yes **No**

Score: _____

Comment:

_____
_____
_____

(Objective: either the configuration file is accessible or not from a particular IP.)

Verify whether the SNMP list is functioning correctly, by trying to modify the configuration of the AP from a machine whose address is not in the access control list. If the auditor is able to modify the configuration from a non-authorized IP address then assign a score of FAIL. Auditor

assign a score of PASS if you are unable to modify the configuration of the AP from a non-authorized IP address.

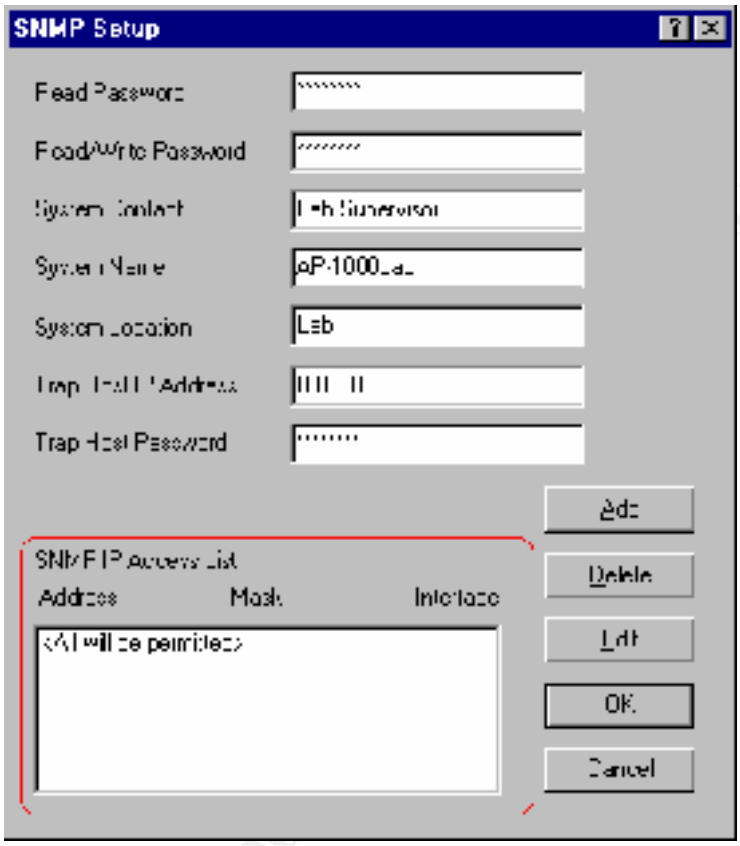


Figure 37 The SNMP ACL Sreen

4.9 Step 9: Trap Host Alerts

The aim of this audit step is to first determine whether the organization, because of policy or its security stance, needs the extra level of security offered by the Trap Host Alert (Figure 38). The Trap Host Alert notifies the designated person if the AP is reset, power is down, AP configuration has been changed, or performs a forced reload, or if there is an authentication failure, or a link up or down is detected.

(31) Does the organization make use of the Trap Host Alert?

Yes **No**

(Subjective: depends on the organization's security stance.)

If the answer is NO, then auditor assign a score of FAIL, if the organization is NOT using the Trap Host Alert, and yet requires the extra level of security offered by it, based on what you know of the organization, its security posture, and its policy, otherwise assign a score of WARNING. Assign a score of PASS, if the organization is using the Trap Host Alert.

If the answer is **YES**, then proceed to the next audit item in this step.

Score: _____

Comment:

_____
_____
_____

(32) Has the Trap Host Alert functioning correctly?

Yes **No**

(Objective: either the Trap Alert is sent or not.)

Verify whether the Trap Host Alert is functioning correctly, by verifying whether the trap alert is sent. Do this by causing one of the events (e.g., rebooting the AP) and observing whether the Trap Alert is sent. Assign a score of Pass if this is successful, otherwise assign a score of Fail.

Score: _____

Comment:

_____
_____
_____

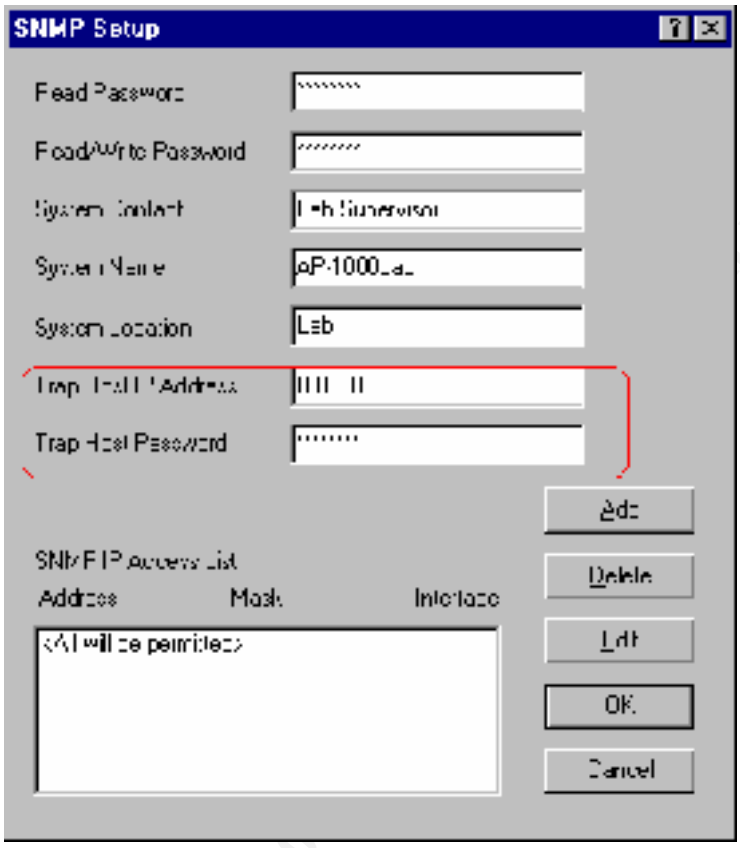


Figure 38 The Trap Alert Screen

4.10 Step 10: Access Control Lists

The aim of this audit step is to determine the use of and proper functioning of access control lists (ACLs). The use of an ACL list for a wireless access point is considered to be more secure than just configuring the access point in CLOSED mode. The access control list contains the MAC addresses of all wireless cards that are allowed access to the access point. By default, there is no restriction on wireless client's MAC addresses that can associated with the access point.

(33) What type of MAC-based access control list is in use by the organization?

_____ No MAC-based access control list is used

_____ wireless access point's internal access control list capability

_____ RADIUS-based authentication

Auditor assign a score of PASS if ACLs are used (e.g., AP's internal ACL list, or a RADIUS ACL), otherwise assign a score of FAIL.

Score: _____

Comment:

_____
_____
_____

Notes:
Only authorized MAC addresses are to be allowed to associate with a wireless access point. The downside is that maintaining the ACL may be a large overhead for the enterprise, if there are frequent additions or deletions to the ACL. Unless the ACL is kept-up-to-date, the benefits of an ACL may quickly dissipate. MAC addresses no longer needing access to the access point need to be removed immediately from the ACL.

MAC addresses are transmitted in the clear, and therefore it is possible for someone to sniff a valid MAC address. Then a valid MAC address can be spoofed in the attempt to gain access. Also, some card wireless cards support changing the MAC address of the card in software, thus a card's MAC address could be changed to a sniffed valid MAC address.

(34) Is the ACL functioning properly?

Yes **No**

Auditor assign a score of PASS if the AP does not allow a wireless client with a MAC address not in the ACL to associate, otherwise assign a score of FAIL.

Score: _____

Comment:

_____
_____
_____

(Objective: either access control lists are used or not.)

Notes:

Figure 39 shows the AP's internal ACL configured with two authorized wireless card MAC addresses. Figure 40 shows the result of using the ipconfig command to determine whether the particular wireless client is associated and connected to the network. Figure 40 shows one of the MAC addresses being removed from the ACL. Figure 41 shows the result of running the ipconfig command to showing that the wireless client is now not connected to the network.

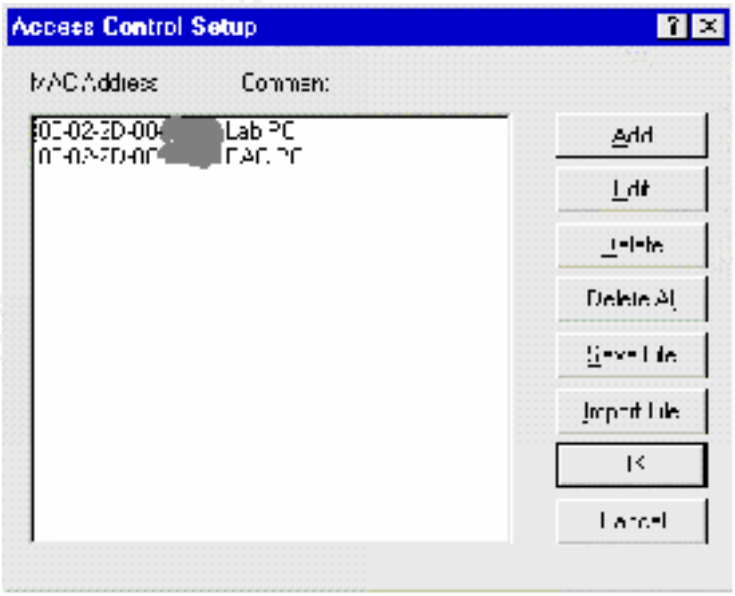


Figure 39 The Access Control List containing two valid MAC addresses

Figure 40 Showing the Lab PC Connected to the network when using the ACL

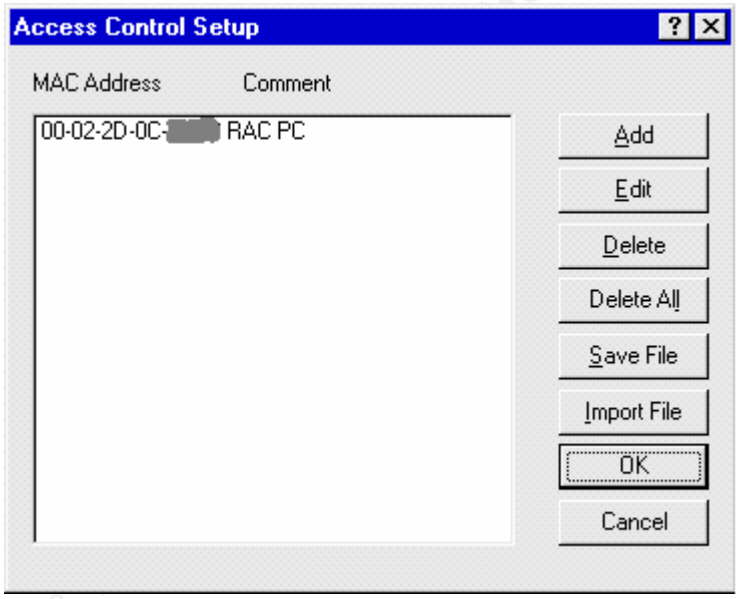


Figure 41 Showing the ACL with a Lab PC MAC address removed

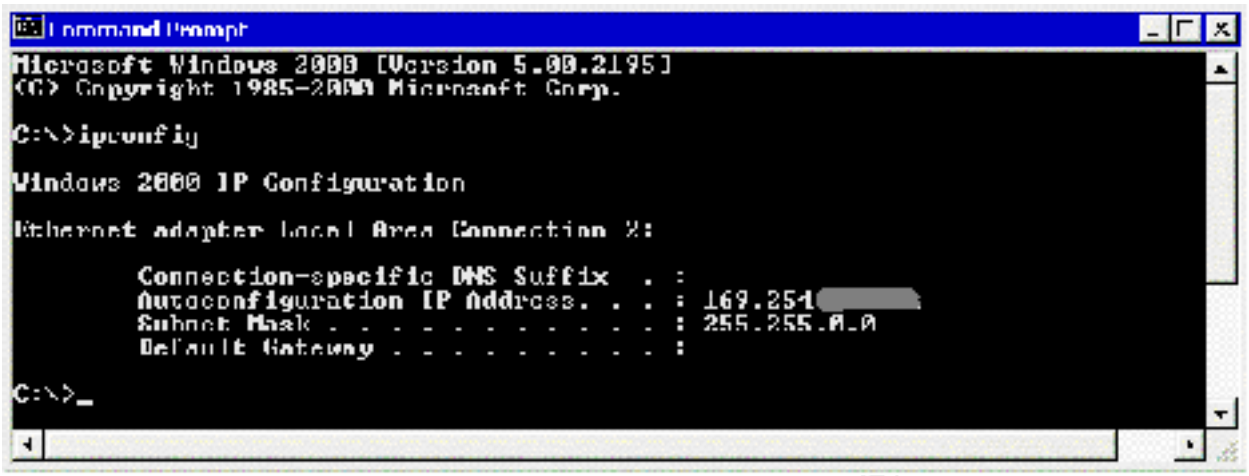


Figure 42 Showing that the Lab PC (not in the ACL) cannot connect to the AP

4.11 Step 11: 802.1x Standard

The aim of this audit step is to determine whether the 802.1x Standard is available for the system being audited.

(35) Does the wireless system being audited have an upgrade to the 802.1x standard?
Yes No

(Subjective: depends on the security posture of the organization.)

Auditor assign a score of FAIL, if an upgrade to the 802.1x Standard is available, but the system has not been upgraded to the 802.1x Standard. Otherwise assign a score of Warning to put the organization on notice that it needs to upgrade to the 802.1x Standard when it becomes available. Assign a score of PASS, if system has been upgraded to the 802.1x Standard.

Score: _____

Comment:

_____
_____
_____

Notes:

If the system being audited has an upgrade to the 802.1x Standard, then the prudent course of action is to upgrade. The 802.1x Standard eliminates the weaknesses inherent in WEP. Different users would have their own encryption key, and the key would be periodically updated automatically.

4.12 Step 12: Physical Location of the Wireless Access Point

The aim of this audit step is to determine the physical location of the AP, thus affecting its physical security, as well as how far its RF transmissions will carry.

(36) Is the wireless access point in a physically secure location?

Yes **No**

(Subjective: depending on the applications used and the security posture of the organization.)

Auditor is to assign a score of PASS, if the wireless AP is not in a location where just anyone can power it on or off, otherwise assign a score of FAIL.

Score: _____

Comment:

_____
_____
_____

Notes:
The wireless access point needs to be protected from an unauthorized reboot, the resetting to manufacturer set settings, or even the malicious or accidental powering on of the AP.

(37) Is the wireless access point near windows or an exterior wall?

Yes **No**

(Subjective: depending on the applications used and the security posture of the organization.)

Auditor assign a score of PASS, if the AP is not near windows, since the radio waves will more readily radiate outside the building through them—preferably the AP should not be near any exterior wall. If the AP is near a window or an exterior wall, then this item needs to be scored with a WARNING or a FAIL based on the auditor's judgement, and reflecting the organization's security stance. The auditor using a wireless sniffer should walk around the exterior perimeter of the building in which the AP is located and determine whether the AP's 802.11b Management packets can be detected. This should needs to be performed with a high gain antenna so as detect and capture weak signals.

Score: _____

Comment:

_____
_____
_____

Notes:
A wireless access point near windows is less secure than one located in the center of the building. Radio waves may travel beyond the building's perimeter. In other words can someone sit in the parking lot and associate with the wireless access point. A great deal depends on the buildings construction.

Place of antennas and use of directional antennas can reduce RF emissions (Marshall, 2001)

4.13 Step 13: Wireless AP and Firewall

The aim of this audit step is to audit whether the wireless AP circumvents the organization's security perimeter. Is the AP behind the firewall, thus by-passing perimeter security?

(38) Is the wireless access point behind the corporate firewall?

Yes **No**

(OBJECTIVE: a wireless access point must never be behind the organization's perimeter security (e.g., the firewall).

Auditor, assign a score of FAIL, if the wireless AP is behind the firewall, and thus within the organization's security perimeter. The AP thus bypasses all the organization's perimeter security, and leaves the organization vulnerable to all kinds of mischief. The auditor needs to bring this to the attention of the organization immediately, and make the case to management that the AP be immediately disconnected.

Score: _____

Comment:

_____
_____
_____

Notes:
Having a wireless point behind the corporate firewall opens the organization to untold mischief. **Any access point located behind the corporation's firewall, should immediately FAIL its audit, and be immediately disconnected.** Such placement bypasses the corporations security perimeter.

4.14 Step 14: Using VPNs and a Wireless AP

The aim of this audit step is to first determine whether the organization, because of policy or its security stance, needs the extra level of security offered by a VPN as depicted in Figure 43.

(39) Does the enterprise use a virtual private network (VPN) to secure the traffic over the wireless link?
Yes **No**

(Subjective: depends on the organization's security posture.)

Auditor assign a score of PASS, if the organization is using VPN to secure its wireless traffic. Auditor is to assign a score of FAIL, if based on what you know of the organization, its security posture, its policy, or the type of information transmitted over the wireless link requires the extra security offered by a VPN, and the organization is not using a VPN. Assign score of WARNING if the organization is not using a VPN, and ought to consider a VPN.

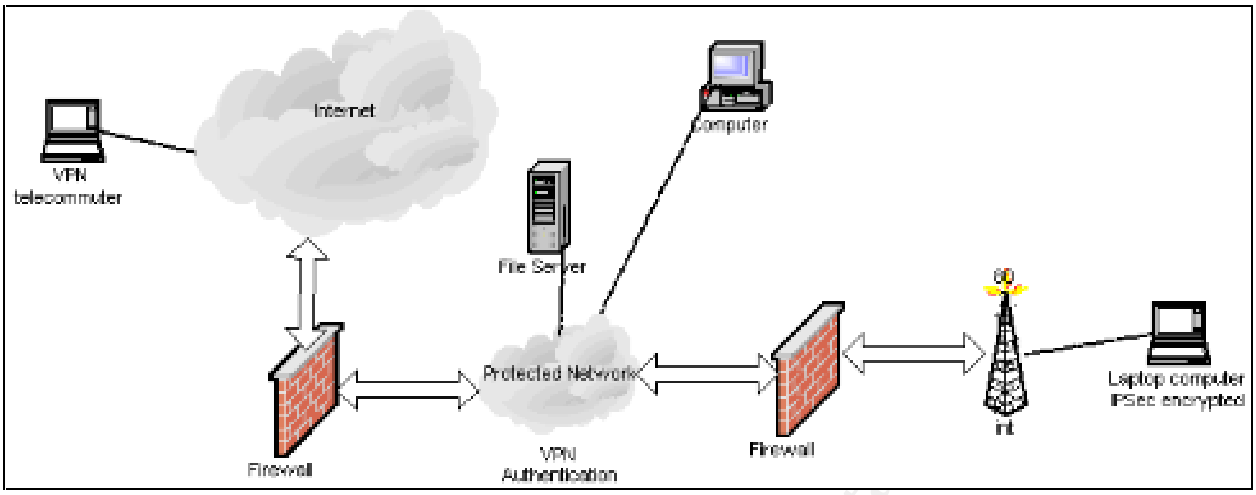
If the answer is **YES**, then proceed to the next audit item in this step.

Score: _____

Comment:
_____
_____
_____

Notes:
Use of a VPN is recommended. The WLAN needs to be protect in the same manner as one would protect the internal LAN from the public Internet. The above diagram illustrates the use of two firewalls to protect the WLAN: one at the gateway into the corporate LAN and the other between the WLAN and the wireless network.

A possible configuration for WLAN and VPN:



(Schenk, 2001) WLAN and VPN

Figure 43 Wireless, Firewall, and VPN Configuration

If the answer is **YES**, then proceed to the next audit item in this step.

(40) Is the wireless firewall configured only to pass VPN traffic?

Yes **No**

(Objective: either the VPN is functioning properly or not.)

The auditor is to give a score of PASS, if the auditor verifies that only VPN traffic passes through the firewall, otherwise a FAIL is assigned. The auditor will need to use a sniffer on the inside of the firewall to determine whether only VPN traffic is being passed.

Score: _____

Comment:

_____

_____

_____

Notes:

This allows the user to associated to the WLAN through a VPN tunnel. By using VPN technology wireless sniffing is thwarted, thus making passive WEP attacks using Air Snort obsolete, for the VPN traffic is encrypted using IPsec.

4.15 Step 15: Contingency Procedures

The aim of this audit step is to determine the adequacy of contingency procedures.

(41) On the client side where is the WEP key and the SSID stored?

WEP KEY _____

SSID _____

Notes:
Knowing where the WEP key and the SSID is stored on the client side is important in determining the risk in the event the wireless card and/or the computer is stolen.
Different manufacturers store the WEP Key in different locations:
From (Klaus, 2001):

- Cisco client software stores the SSID in the Windows registry. Cisco stores the WEP key in the firmware, which is difficult to gain access to.
- Lucent/Cabletron client software stores the SSID in the Windows registry. The WEP is stored in the Windows registry but it is encrypted. The encryption algorithm is not documented.
- 3Com client software stores the SSID in the Windows registry. The WEP key is stored in registry with no encryption.

(42) Does the organization have a policy and/or procedures for reporting the theft or loss of a computer or a wireless card, are they adequate?

Yes **No**

(Objective: either the organization has a policy or procedure(s) or not.)

The auditor is to give a score of PASS, if in your opinion the contingency procedures are adequate to assure security in the event that a wireless card and/or a laptop equipped with a wireless card is lost or stolen, otherwise assign a score of FAIL.

Score: _____

Comment:
_____
_____
_____

5. Identify the Item to Be Audited

The focus of the audit research is an ORINOCO wireless access point (AP), the ORINOCO AP-1000. The AP-1000 runs the ORINOCO Outdoor Router v2.03 software, and the software has been configured so the AP-1000 behaves as a wireless access point and not as an outdoor wireless router. The wireless clients run the Client Software Rel 7.4 for MS Windows Win 2000 Release.

The organization in question does not use the WLAN on an everyday basis. Generally, the WLAN is used to demonstrate to visitors the capabilities of wireless technology when married with standard applications. In addition, the WLAN is used as a wireless link between the organization's LAN and the LAN in a deployable mobile unit, in which case the wireless link is used chiefly to move files from one LAN to the other. Both uses occur infrequently.

6. Evaluate the Risk to the System

As noted above, the wireless AP is used sporadically: to demonstrate the capabilities of wireless technology coupled with standard applications, and to transfer files between the organization's LAN and the LAN in a mobile unit. No organization sensitive information is ever sent using wireless media. However, there is risk to the organization if an intruder is able to gain access to the wireless AP, in which case the intruder may also gain access to the organization's internal LAN. This can occur if the AP is misconfigured, thus allowing anyone with a wireless client to associate with the AP. Another potential risk, is that if the WEP keys are not changed regularly, then someone will be able to capture the WEP keys using AirSnort. This will allow anyone to view any files traversing the wireless link. While the information being transmitted is not sensitive, the knowledge by an intruder of the type of demonstration occurring, may damage the corporation's competitive advantage. Precautions need to be taken, so that the casual drive by warrior is discouraged.

As noted by the auditor, the wireless AP is kept powered-off until needed. However, if someone forgets to turn-off the AP after use, then the corporation may be at risk. In addition, if there is physical access to the AP and it is accidentally or maliciously powered-on and then reset to factory settings, then anyone can associate with the network.

Ideally the wireless AP should not be behind the organization's security perimeter (behind the corporate firewall). Packets from a wireless AP need to be treated the same way as if the packets were coming from the public Internet.

In summary, the wireless access point's configuration needs to assure that only authorized users using wireless clients are able to associate with the AP. The wireless transmissions need to be protected against the casual drive-by warrior, so WEP encryption needs to be enabled. In addition, to prevent a not so casual drive-by warrior from eavesdropping on the wireless

transmissions, it is advisable if the organization changed its WEP key(s) after every use. Otherwise, once the WEP key is captured, all wireless 802.11b transmissions associated with the AP can be monitored. The aim is to as use as many security precautions that make sense from a business and cost incentive.

7. The Audit

7.1 Step 1: Seek Permission to Perform the Audit

Auditor is not proceed with the audit unless written authorization has been granted, by the organization whose system is to be audited.

(1) Has the auditor received written authorization by the organization to conduct the audit?

Yes	No

If NO, the auditor is not to proceed with the audit.

7.2 Step 2: Identify Organizational Policy and Procedures

The aim of this step is to identify and review the organization's information security policy(s) and procedures to identify those items related to wireless LANs. This will serve as a reference for the auditor in determining the security stance of the organization. In some evaluation steps the items to be audited are subjective in nature. The score the auditor assigns for these subjective items will for the most part depend on the security stance of the organization, and the amount of risk the organization is willing to tolerate. What may be a score of PASS for one organization may be a score of FAIL for another organization.

(2) Does the organization have a policy and/or procedures requiring a survey of its perimeter and network using wireless tools or network assessment tools to locate wireless access points?

Yes **No**

(Objective: either policies / procedures exist addressing WLANs or they do not.)

Auditor assign a score of PASS, if the organization has policies specifically addressing wireless LANs. Assign a score of WARNING, if auditing networks is addressed in policy using conventional network scanning tools. This score is assigned for many of the standard network scanning tools do not directly address wireless APs on a network. A score of FAIL, is assigned if no policy exists requiring periodic network scans of any sort.

Score: __WARNING_____

Comment:
The organization performs a vulnerability scan periodically to ascertain if there are any vulnerabilities. There is no specific scan using tools specifically design to check for the existence of wireless APs on the organization's network. The auditor's recommendation for the organization to acquire wireless sniffing tools in order to conduct a vulnerability analysis from wireless APs that may exist in the organization.

(3) Is there a focal point for the organization's wireless initiatives?

Yes	**No**

Who is it? _____The system administrator_____

(Objective: Either there is a focal point on wireless initiatives or there is not.)

Auditor assign a score of PASS, if there is an identifiable person in the organization responsible for WLANs. Assign a FAIL, if the organization uses WLANs, but there is no identifiable focal point for such WLAN initiatives.

Score: __PASS_____

Comment:
System administrator is the focal point. Whenever questions about WLANS arise in the organization the system administrator is asked. The system administrator is knowledgeable about the deficiencies in WEP and the risks associated with WLANs.

(4) Does the organization have a hardware / software accreditation process?

Yes	**No**

If **YES**, then

(5) Has the wireless AP undergone through the accreditation process?

Yes	**No**

(Objective: Either the accreditation process has been followed or not.)

Auditor assign a score of PASS, if the organization has an accreditation process and the WLAN has been approved through this process, otherwise assign a score of FAIL.

Score: __FAIL_____

Comment:
The wireless AP is though of as an experimental device, used only to demonstrate the capabilities of wireless technology, and is not used on a day to day operational basis. Since, it is considered_ experimental, it has never gone through the accreditation process.

7.3 Step 3: Detecting / Finding a Wireless Access Point

There is no score (Pass, Fail, Warning) for this step. The intent is to identify AP's. If there are rogue sites, the auditor has his or her work cut to determine where exactly is the rogue AP. For approved sites the next step is for the auditor to audit the AP's configuration.

7.3.1 Wireless methods to detect wireless APs on a network

Use a wireless network detector (e.g., NetStumbler) or wireless sniffer (e.g., Wildpackets' AiroPeek, or Network Associate's Sniffer Wireless) to determine whether there are any active wireless access points on the organization's network, as described below. Perform this test by walking through the organization's buildings, on the organization's campus, and immediate surrounding areas. When performing the walk through consideration, should be given in using a high gain antenna to detect weak signals. Radio signals travel in three dimensions and are able to penetrate walls, ceilings, and floors.

(6) Has the wireless network detector software / wireless sniffer software detected any wireless access points?

Yes	No

(Objective: determines the existence of wireless access point.)

7.3.2 Network scanning software to detect wireless APs on a network

The auditor can use Nmap, Nessus, or ISS Scanner to determine whether wireless access points exist in the organization. The results of using this software is mixed, as described below. Another method of detecting a Orinoco wireless Aps on a network is to use the Orinoco Configuration Manager software.

(7) Has the network scanning software detected any wireless access points?

Yes	No

(Objective: determines the existence of wireless access point.)

7.3.3 Approved or rogue wireless access points

Of the wireless access points detected via wireless network detector software, wireless sniffer software, or via a scan of the organization's network, which are approved and which are rogue sites?

Auditor, list all wireless access points found, and check the appropriate column upon determination whether the wireless access point is an approved organizational wireless access point, or it is a rogue wireless access point.

Wireless Access Point	Approved	Rogue
SSID: ??????? Note: the SSID name has been replaced by ????? to ensure privacy for the organization audited.	X	

Table 1 List of Wireless Access Points Located

7.3.4 Check war driving sites

Check war driving sites that post wireless access websites (e.g., http://www.netstumbler.com) that have been found by war drivers.

(8) Are any posted access points on war-driving web sites (e.g., http://www.netstumbler.com) on your organization's network?

Yes **No**

(Objective: determines the existence of wireless access point.)

If **YES**, then

(4) ask the site (e.g., NetStumber) to remove you immediately form the list
(5) locate the wireless access point in your organization
(6) take appropriate measures reflecting your organization's security posture

7.4 Step 4: Auditing the Security Configuration

The aim of this step is to audit whether the built-in security features of the wireless AP have been enabled.

To begin auditing the configuration set-up, the auditor must first open the configuration file using the Orinoco Configuration Manager software, from the File menu. Enter in the IP address of the AP from Figure 10 and enter in the READ/WRITE Password (Figure 11), which results in Figure 12. The from the Setup menu, choose Interface Setup to access the configuration screen (Figure 13), and then choose the option for the Orinoco. On Figure 14 the auditor needs to verify that the Outdoor Router Software on the AP-1000 has been configured to act as an IEEE 802.11b Access Point. Choosing the Security option on Figure 14 brings up the Orinoco Security Setup screen (Figure 15).

(9) What is the security set-up of the AP?

Auditor examine the screen (like the one in Figure 15) on the system being audited, and based on the configuration of the system fill in (Table 2)

				Synopsis of what each wireless tool will detect		
AP's Security Setup (place check)	**Is "Closed Wireless System" checked?**	**IS "Enable Encryption" checked**	**Is "Deny non-encrypted data" checked?**	NetStumbler Detects	AiroPeek Detects	**Score to be Assigned**
	No	**No**		Y	Y	**Fail**
	No	**Yes**	**No**	Y	Y	**Fail**
	No	**Yes**	**Yes**	Y	Y	**Fail**
	Yes	**No**		N		**Fail**
	Yes	**Yes**	**No**	N	Y	**Fail**
XXX	**Yes**	**Yes**	**Yes**	N	Y	**Pass**

Table 2 The AP's Security Setup

(Objective: if enabled makes sure that encryption is used, otherwise the wireless access point may communicate in unencrypted mode with a wireless client.)

Auditor is to assign a score of PASS if the Closed Wireless System, Enable Encryption and the Deny non-encrypted Data are enabled, and verified using packets captured by the wireless packet sniffer (refer to notes section for example packet captures). To earn the score of PASS, the

802.11b Beacon packet details need to like that of Figure 17, where the privacy flag is set to one (denotes that WEP encryption is activated), and where the SSID is not transmitted (denotes closed system). Otherwise, the auditor is to assign a score of FAIL.

Score: __PASS_____

Comment: _____

(10) Are data packets actually WEP encrypted?

Yes **No**

(Objective: encryption is either enabled or not)

Auditor is to assign a score of PASS, when it is verified using a wireless sniffer that the actual data packets between the wireless client and the AP are encrypted. The captured packets need to be like those in Figure 23 and Figure 24.

Score: __PASS___

Comment: _____

(11) What is the level of WEP enabled?

64 bit (40 bit) **128 bit (104 bit)**

(12) What is the highest level of WEP available for the access point being audited?

64 bit (40 bit) **128 bit (104 bit)**

(Objective: the highest WEP available needs to be enabled)

(13) Has the wireless access point's firmware/software been upgraded to the latest version?

Yes **No**

(Objective: in general a vendor's latest upgrade has the latest security enhancements)

(14) Has the wireless access point been upgraded to WEPplus?

Yes **No** **Not available yet**

(Objective: WEPplus is not vulnerable to the stealing of encryption keys using programs such as AirSnort or any other program based on the Fluher et all article.)

Auditor assign a score of PASS if the system being audited is current on its updates and the strongest WEP 128 bit (104 bit) is used, otherwise assign a score of FAIL.

Score: _PASS_____

Comment:
Security options are all enabled, and the latest updates have been applied._____

7.5 Step 5: WEP Key Management

The aim of this audit step is to ascertain the status of WEP key management in the organization. Given enough data transferred wirelessly using the same WEP key, the WEP key can be derived using a program such as AirSnort. AirSnort can be used to derive the WEP key used. It is estimated that between 100 Mbyte and 1 Gigabyte of traffic is required to obtain the WEP key. Therefore, changing the WEP key on a regular basis is highly advisable.

(15) Are the WEP keys changed at regular intervals?

Yes **No**

If **YES**, then answer the following questions.

(16) What is the interval for the WEP key change?

_____

(17) Is the interval for WEP key change adequate?

Yes **No**

(Subjective: depending on the traffic amount over the wireless link and the organization's security posture.)

(18) Does the organization have a WEP key distribution procedure?

Yes **No**

(19) Is the WEP key management adequate?

(Subjective: depends on the number of WLANS and the number of clients per WLAN, and the security posture of the organization.)

Auditor based on your knowledge of the organization, its security stance, and the number of wireless clients indicate whether in your opinion the management of WEP keys is adequate. WEP key management demands a great deal of overhead to distribute keys when they are changed, and to coordinate key usage. Assign a score of PASS, if in your opinion WEP key management is adequate. Otherwise assign a score of FAIL. Explain your score under comments.

Score: __FAIL_____

Comment:
The WEP key has never been changed -- system has been in the organization for 1.5 years. Even though the AP is seldom used, there is still the chance that someone may have acquired the WEP key (e.g., using AirSnort, or via other means).

7.6 Step 6: SSID Configuration

The aim of this step is to audit the AP's SSID.

(20) Has the default SSID been changed?

Yes **No**

(Objective: determines whether the default SSID has been changed or not.)

Auditor is to assign a score of FAIL if the default SSID has not been changed. If the SSID has been changed then assign a score of PASS.

Score: __PASS_____

Comment:

_____

(21) Is the wireless access point configured to accept a blank or "ANY" SSID?
blank SSID?

Yes **No**

(Objective: a SSID needs to be set for the AP.)

Auditor is to assign a score of FAIL if the wireless client is able to associate with the AP using either a blank SSID or the ANY SSID, otherwise assign a PASS.

Score: ___PASS_____

Comment:

_____

(22) Is the SSID a non-obvious SSID?

Yes **No**

(Subjective: it is difficult to determine what is or what is not a non-obvious SSID

While it may be subjective to say what is a non-obvious SSID or a strong SSID, the following guidelines can be used. The SSID should bear no reflection on the organization's name, divisions within the organization, products, address, etc. The SSID should use be a mixture of alphanumeric characters. A non-obvious SSID or strong SSID makes it more difficult that it will be guessed. The auditor is to assign a score of PASS, if the auditor believes the SSID is non-obvious or strong. A score of FAIL is to be assigned if the SSID is related to the organization. A score of WARNING is to be assigned, if the SSID could be stronger (e.g., make use of numbers along with letters).

Score: __YES_____

Comment:

_____

(23) Has SSID broadcast been turned off?

Yes **No**

(Objective: it is either turned on or off.)

Auditor assign a score of PASS, if in Step 2 the system being audited was configured as a Closed Wireless System, otherwise assign a score of FAIL. This in included for completeness, for this audit can be used with slight modification to audit other vendors' WLAN APs.

Score: ___PASS_____

Comment:
The system is an Orinoco system configured as a Closed system. A Closed system does not transmit the SSID in its 802.11b Beacon packet.

7.7 Step 7: READ/WRITE and READ Password

The aim of this step is to audit the security of the READ/WRITE and the READ password of the AP. The READ/WRITE password is used to manage the configuration of the AP. Using this password a user can access the configuration, modify, and save the changes. The READ password allows access to the AP so the user can monitor the statistics.

Depending on the security stance of the organization, the organization may want to have different READ/WRITE and READ passwords, thus granting different levels of access and authority over the AP.

(24) Is the READ/WRITE configuration password the default password?

Yes **No**

(Objective: either it is the default password or it is not.)

Auditor assign a score of FAIL, if the default password for the system enables the auditor to access the configuration of the AP, otherwise assign a PASS.

Score: __PASS_____

Comment:

_____

(25) Is the READ/WRITE configuration password difficult to guess?

Yes **No**

(Subjective: it is difficult to determine whether a password is difficult to guess)

While it may be subjective to say whether a password is difficult to guess or not, the following guidelines can be used. The READ/WRITE password ought to be at least eight characters in length and be composed of alphanumeric characters. The password should not be a word in a dictionary, or related to the organization (e.g., company name, address, department located in). Auditor assign a PASS if the password is at least eight characters in length and uses a combination of letters and numbers. A score of FAIL is to be assigned, if the password is a dictionary word. A score Warning is to be assigned if the auditor believes the password could be made stronger.

Score: __PASS_____

Comment:
The system administrator shared the password with the auditor for verification that a hard to guess strong password consisting of mixed case letters and numerals was being used.

(26) Is the READ password the default password?

Yes | **No**

(Objective: either it is the default password or it is not.)

Auditor assign a score of FAIL, if the default password for the system enables the auditor to access the monitoring functions requiring the READ password, otherwise assign a PASS.

Score: __PASS_____

Comment:
The system administrator shared the password with the auditor for verification t-- a hard to guess strong password consisting of mixed case letters and numerals was being used.

(27) Is the READ configuration password difficult to guess?

Yes | **No**

(Subjective: it is difficult to determine whether a password is difficult to guess).

While it may be subjective to say whether a password is difficult to guess or not, the following guidelines can be used. The READ password ought to be at least eight characters in length and be composed of alphanumeric characters. The password should not be a word in a dictionary, or related to the organization (e.g., company name, address, department located in). Auditor assign a PASS if the password is at least eight characters in length and uses a combination of letters and numbers. A score of FAIL is to be assigned, if the password is a dictionary word. A score Warning is to be assigned if the auditor believes the password could be made stronger.

Score: __PASS_____

Comment:
The system administrator shared the password with the auditor for verification that a hard to guess strong password consisting of mixed case letters and numerals was being used.

(28) Is the READ and the READ/WRITE password the same?

Yes	No

(Subjective: depends on whether the organization wants different levels of authority access to the wireless access point.)

Auditor assign a score of FAIL, if the organization requires that there be a differentiation in access authority to the AP and yet the passwords are the same. Otherwise, assign a score of PASS.

Score: __PASS_____

Comment:
There is no operational or policy requirement that there be a differentiation in the access authority to the AP. Since the AP is used only for demonstration purposes with the system administrator in charge.

7.8 Step 8: SNMP Access Control List

The aim of this audit step is to first determine whether the organization, because of policy or its security stance, needs the extra level of security offered by the SNMP IP access control list (Figure 37). This access control list limits which work stations can access the AP's configuration file.

(29) Does the organization make use of the SNMP IP access control list for access to the AP's configuration file?

Yes	**No**

(Subjective: depends on the organization's security stance.)

If the answer is NO, then auditor assign a score of FAIL, if the organization is NOT using an SNMP ACL, and yet requires the extra level of security offered by an SNMP ACL, based on what you know of the organization, its security posture, and its policy. Assign a score of PASS, if the organization is using the SNMP ACL.

If the answer is **YES,** then proceed to the next audit item in this step.

Score: ___PASS_____

Comment:
All client wireless card MAC addresses are entered into the ACL for additional security.

(30) Is the SNMP IP ACL functioning correctly?

Yes	**No**

(Objective: either the configuration file is accessible or not from a particular IP.)

Verify whether the SNMP list is functioning correctly, by trying to modify the configuration of the AP from a machine whose address is not in the access control list. If the auditor is able to modify the configuration from a non-authorized IP address then assign a score of FAIL. Auditor assign a score of PASS if you are unable to modify the configuration of the AP from a non-authorized IP address.

Score: ___PASS_____

Comment:
_____

7.9 Step 9: Trap Host Alerts

The aim of this audit step is to first determine whether the organization, because of policy or its security stance, needs the extra level of security offered by the Trap Host Alert (**Figure 38**). The Trap Host Alert notifies the designated person if the AP is reset (rebooted) (AP is reset, power is down, AP configuration has been changed, or performs a forced reload, or if there is an authentication failure, or a link up or down is detected.

(31) Does the organization make use of the Trap Host Alert?

Yes **No**

(Subjective: depends on the organization's security stance.)

If the answer is NO, then auditor assign a score of FAIL, if the organization is NOT using the Trap Host Alert, and yet requires the extra level of security offered by it, based on what you know of the organization, its security posture, and its policy, otherwise assign a score of WARNING. Assign a score of PASS, if the organization is using the Trap Host Alert.

If the answer is **YES**, then proceed to the next audit item in this step.

Score: _WARNING_____

Comment:
__May want to consider enabling this option._____

(32) Has the Trap Host Alert functioning correctly?

Yes **No**

(Objective: either the Trap Alert is sent or not.)

Verify whether the Trap Host Alert is functioning correctly, by verifying whether the trap alert is sent. Do this by causing one of the events (e.g., rebooting the AP) and observing whether the Trap Alert is sent. Assign a score of Pass if this is successful, otherwise assign a score of Fail.

Score: _____

Comment:
_____

7.10 Step 10: Access Control Lists

The aim of this audit step is to determine the use of and proper functioning of access control lists (ACLs). The use of an ACL list for a wireless access point is considered to be more secure than just configuring the access point in CLOSED mode. The access control list contains the MAC addresses of all wireless cards that are allowed access to the access point. By default, there is no restriction on wireless client's MAC addresses that can associated with the access point.

(33) What type of MAC-based access control list is in use by the organization?

_____ No MAC-based access control list is used

__X__ wireless access point's internal access control list capability

_____ RADIUS-based authentication

Auditor assign a score of PASS if ACLs are used (e.g., AP's internal ACL list, or a RADIUS ACL), otherwise assign a score of FAIL.

Score: __PASS__

Comment:
__Uses the Orinoco's built in ACL functionality to only allow wireless card MAC addresses in the ACL database to associate with the AP.

(34) Is the ACL functioning properly?

Yes **No**

Auditor assign a score of PASS if the AP does not allow a wireless client with a MAC address not in the ACL to associate, otherwise assign a score of FAIL.

Score: __YES___

Comment:
_Verified by trying to associate with a wireless card not in the ACL.

7.11 Step 11: 802.1x Standard

The aim of this audit step is to determine whether the 802.1x Standard is available for the system being audited.

(35) Does the wireless system being audited have an upgrade to the 802.1x standard?

Yes | **No**

(Subjective: depends on the security posture of the organization.)

Auditor assign a score of FAIL, if an upgrade to the 802.1x Standard is available, but the system has not been upgraded to the 802.1x Standard. Otherwise assign a score of Warning to put the organization on notice that it needs to upgrade to the 802.1x Standard when it becomes available. Assign a score of PASS, if system has been upgraded to the 802.1x Standard.

Score: __Warning__

Comment:
There is no upgrade for to the 802.1x standard for the AP. System administrator needs to periodically check if upgrade is available.

7.12 Step 12: Physical Location of the Wireless Access Point

The aim of this audit step is to determine the physical location of the AP, thus affecting its physical security, as well as how far its RF transmissions will carry.

(36) Is the wireless access point in a physically secure location?

Yes | **No**

(Subjective: depending on the applications used and the security posture of the organization.)

Auditor is to assign a score of PASS, if the wireless AP is not in a location where just anyone can power it on or off, otherwise assign a score of FAIL.

Score: FAIL

Comment:
While the AP is in an out of the way place with low traffic volume, it is however, in an unsecured place, where anyone in the organization can power it up. Because it is in an out of the way place, the system administrator may not notice that the AP is on and connected to the internal network.

(37) Is the wireless access point near windows or an exterior wall?

Yes | **No**

(Subjective: depending on the applications used and the security posture of the organization.)

Auditor assign a score of PASS, if the AP is not near windows, since the radio waves will more readily radiate outside the building through them—preferably the AP should not be near any exterior wall. If the AP is near a window or an exterior wall, then this item needs to be scored with a WARNING or a FAIL based on the auditor's judgement and reflecting the organization's security stance. The auditor using a wireless sniffer should walk around the exterior perimeter of the building in which the AP is located and determine whether the AP's 802.11b Management packets can be detected. This should needs to be performed with a high gain antenna so as detect and capture weak signals.

Score: Pass

Comment:
The AP is in an interior room, the walls of the building are one foot thick reinforced concrete and brick. No 802.11b beacon packets using a wireless sniffer and high gain antenna were detected outside the building.

7.13 Step 13: Wireless AP and Firewall

The aim of this audit step is to audit whether the wireless AP circumvents the organization's security perimeter. Is the AP behind the firewall, thus by-passing perimeter security?

(38) Is the wireless access point behind the corporate firewall?

Yes	**No**

(OBJECTIVE: a wireless access point must never be behind the organization's perimeter security (e.g., the firewall).

Auditor, assign a score of FAIL, if the wireless AP is behind the firewall and thus within the organization's security perimeter. The AP thus bypasses all the organization's perimeter security, and leaves the organization vulnerable to all kinds of mischief. The auditor needs to bring this to the attention of the organization immediately, and make the case to management that the AP be immediately disconnected.

Score: ___Fail___

Comment:

The AP was found to be inside the corporate firewall. Whenever the AP is in use for demonstration purposes, there is a direct connection to the corporate LAN from the AP by-passing all perimeter security. The AP needs to be located outside the firewall.

7.14 Step 14: Using VPNs and a Wireless AP

The aim of this audit step is to first determine whether the organization, because of policy or its security stance, needs the extra level of security offered by a VPN as depicted in Figure 43.

(39) Does the enterprise use a virtual private network (VPN) to secure the traffic over the wireless link?

Yes **No**

(Subjective: depends on the organization's security posture.)

Auditor assign a score of PASS, if the organization is using VPN to secure its wireless traffic. Auditor is to assign a score of FAIL, if based on what you know of the organization, its security posture, its policy, or the type of information transmitted over the wireless link requires the extra security offered by a VPN, and the organization is not using a VPN. Assign score of WARNING if the organization is not using a VPN, and ought to consider a VPN.

If the answer is **YES**, then proceed to the next audit item in this step.

Score: __WARNING_____

Comment:
If the organization is to ever make the WLAN an integral part of its operational activities, then use of a VPN needs to be seriously considered.

If the answer is **YES**, then proceed to the next audit item in this step.

(40) Is the wireless firewall configured only to pass VPN traffic?

Yes **No**

(Objective: either the VPN is functioning properly or not.)

The auditor is to give a score of PASS, if the auditor verifies that only VPN traffic passes through the firewall, otherwise a FAIL is assigned. The auditor will need to use a sniffer on the inside of the firewall to determine whether only VPN traffic is being passed.

Score: _____

Comment:

_____

7.15 Step 15: Contingency Procedures

The aim of this audit step is to determine the adequacy of contingency procedures.

(41) On the client side where is the WEP key and the SSID stored?

WEP KEY __Windows Registry in encrypted form_____

SSID __Windows Registry_____

(42) Does the organization have a policy and/or procedures for reporting the theft or loss of a computer or a wireless card, are they adequate?

Yes **No**

(Objective: either the organization has a policy or procedure(s) or not..)

The auditor is to give a score of PASS, if in your opinion the contingency procedures are adequate to assure security in the event that a wireless card and/or a laptop equipped with a wireless card is lost or stolen, otherwise assign a score of FAIL.

Score: __PASS_____

Comment:
The organization does not have a policy addressing, wireless per se, but the system administrator is knowledgeable that in the event a computer with wireless capability is lost or stolen -- the WEP key needs to be changed.

8. Evaluating the System

The organization's policies and procedures were lacking in the wireless arena. However, wireless is not used on a day to day basis, but only for demonstration purposes. Also, it is important to note that the organization is quite small -- less than 50 employees. The chance of there being a rogue wireless AP set-up by any of the employees is quite low. While a network scan using traditional network auditing tools is required by policy, there is no mention of using wireless auditing tools such as a wireless sniffer to detect rogue APs. For a larger more diverse organization, policy and procedures addressing wireless is a must. Since wireless APs are easy to install and their price is dropping, the potential of a rogue AP rises in an organization. The organization's system administrator(s) or security personnel need to have the tools to check whether rogue APs exist on the organization's network or not.

Before any wireless network is deployed it needs to go through an accreditation process. The organization being audited has an accreditation process in place, but the wireless AP was not accredited through this process. The reason being is that it is only used for demo purposes, and it is seldom on. Management's opinion is that it does not pose a threat to the organization, because it is seldom on, and thus they are willing to take the risk. However, management does not realize that the wireless AP bypasses the organization's security perimeter. The auditor has brought this point up to management.

One of the most important things in the audit is to have the correct tools to identify and locate any rogue or authorized wireless APs on the organization's network. A wireless packet sniffer with a high gain antenna is indispensable. With authorized AP's finding the location is easy, the auditor just needs to confirm that the AP detected is the same AP in the same location as the information systems department's records show. If a rogue AP is detected, finding its location is not a trivial matter, and can be time consuming. Walking around with a laptop equipped with a wireless sniffer around is not stealthy. What the auditor really needs is an RF signal locator to help pinpoint the location.

The system audited was well configured, and made use of the most important and necessary security options available. Most importantly, the system was configured as a Closed system, meaning that it was not broadcasting its SSID to everyone. This Closed system option is an Orinoco proprietary system not in the 802.11b Standard. Only other Orinoco wireless clients are able to connect to the Orinoco AP. However, someone using a wireless packet sniffer would be able to acquire the SSID by observing the packet exchange for a successful authentication and association between an authorized wireless client and the AP. The highest WEP encryption was enabled, and the AP was configured to deny any non-encrypted Orinoco systems trying to associate with the AP. Using the wireless sniffer it was confirmed that all these options were set. Also, it was confirmed that WEP packets were indeed being encrypted.

WEP key management at the organization is nonexistent. The same key has been used since the AP was purchased. Fortunately, the WEP key was not the default WEP key or any of the more obvious WEP key sequences. The Orinoco system has the capability of having up to four WEP keys, but only one key can be used at a time. With four keys, it allows the system administrator

to set a timetable for rollover from one key to another. The rollover is not automatic, but needs to be coordinated between the wireless client and the AP by actual people. WEP keys need to be changed often, because if enough traffic is captured the WEP key can be deduced by software (e.g., AirSnort). However, changing keys often can be a nuisance if there are many wireless clients. In using wireless AP's the overhead associated with WEP key management can be quite burdensome. Even if an organization has a WEP key distribution procedure, it is difficult to audit objectively that it is really being done. The auditor needs to interview users of the WLAN in order to determine whether policy on WEP key management is really being adhered to.

Other default settings on the system being audited were also changed, e.g., the SSID, the READ and READ/WRITE password. More importantly, with a SID in place, not just any wireless client can associate with the AP; the wireless client must know the SSID. Changing the SSID to a non-obvious one is important so that it cannot be guessed. Furthermore, the READ/WRITE and READ passwords were the same. For this organization, having the same password for both was acceptable. In other organizations where different levels of authority access to the AP may be required, the two passwords need to be different. The READ/WRITE password is the more important one, for it allows access to the configuration files for the AP. Knowing the READ/WRITE password, the user can change the AP's configuration. To further enhance security the organization implemented an SNMP ACL, thus limiting from which IP address the configuration file can be accessed and modified.

As part of the system administrator's overall effort to enhance the security of the wireless AP, an access control list were used to only allow those wireless card MAC addresses that were in the AP's ACL allow file to associate with the AP.

One of things that the system administrator needs to keep an eye on is for the upgrade to the 802.1x Standard. It is purported that this new standard will address the weaknesses in the 802.11b Standard.

In terms of the physical location of the wireless AP, the scores were mixed. The AP is not in a secure location, which can allow anyone in the organization to turn on the AP. At the least the wireless cards in the AP should not be in the AP, if the AP is not used. The reason they are kept in the AP is so they would not get lost. Management has been advised of this issue, and the AP will be relocated to another location. The organization's building due to its construction keeps the RF signal from leaving the building - unless someone leaves a window open. In many organizations there is the concern that someone sitting in a parking lot can eavesdrop on WLAN communications.

The most serious deficiency in the organization's deployment of the wireless AP is that it is inside the security perimeter. If someone was to gain access to the wireless AP, they would have access to the organization's entire network. This has been brought to management's attention and to the system administrator for corrective action. The auditor also made the recommendation that the organization consider deploying a VPN to secure the traffic over the wireless link. This adds another layer of security, and prevents anyone listening in. The case was made that since the system is being used for demonstration purposes, it would behoove the organization to use a VPN to show how the same application will still work via a VPN.

In summary, the organization has done many things correctly in trying to secure their wireless AP. The auditor gives a score of PASS with the stipulation that the wireless AP be moved so that it sits outside the organization's security perimeter. The wireless AP needs to be treated as n untrusted device.

9. Evaluating the Audit

The audit checklist as it currently stands, is quite comprehensive for it addresses management, policy, and technical issues. The audit checklist while developed for the Orinoco AP can be applied to almost any other wireless AP, exccept for those parts that are specific to the Orinoco AP (e.g., Closed system). To be useful for auditing other AP's, the auditor will need to study closely the vendor's documentation for security features.

Use of a wireless sniffer equipped with a high gain antenna is a must for determining whether rogue wireless APs are present on the organization's network. While NetStumbler is useful in those instances where hardly any steps are taken to protect the network, for example in the Orinoco system, if the system was configured as Closed then NetStumbler was not able to detect the AP. What an organization needs is to use a wireless packet sniffer that can capture packets. In this way the auditor will be able to capture the 802.11b Beacon packets being transmitted by the wireless AP. It is hoped that in the future the traditional free network scanning tools such as Nmap and Nessus will be able to identify AP's. ISS Scanner supposedly is able to do this, but the author did not have access to the software, and therefore cannot comment on ISS Scanner's capability of identifying wireless APs on a network. Physically locating a rogue wireless AP is a time consuming effort, for RF travels in three dimensions, and therefore it may not be easy to identify which network has the rogue AP. Further work on how RF directional finders can be used in the audit process needs to be investigated.

Reviewing and auditing policy is difficult and very subjective. The auditor needs to have a very good understanding of the organization's security posture, to determine whether policy is adequate. The second difficulty is that written policy may be different than applied policy on a day-to-day basis. The auditor really needs to validate policy and the organization's adherence to it through interviews.

Auditing a wireless AP using 802.1x Standard has not been addressed in the audit checklist. The next logical step in continued development of this audit checklist would be to focus on a system using the 802.1x Standard.

10. Bibliography

Ayyagari, A., & Fout, T. (2001, May). Making IEEE 802.11 Networks Enterprise-Ready. http://www.microsoft.com/windows2000/docs/wirelessec.doc

Bowman, B. (2001, December 3). Securing SOHO Wireless Residential LANS. http://www.microsoft.com/windowsxp/expertzone/columns/bowman/december03.asp

Dillon, J. (2001). *Initial Wireless Networking Audit for Higher Educational Institutions* . http://www.auditnet.org/docs/wireless.doc

Ellison, C. (2001, September 4, 2001). Exploiting and Protecting 802.11b Wireless Networks. *ExtremeTech*. http://www.extremetech.com/print_article/0,3428,a%253D13880,00.asp

Fluhrer, S. M., Itsik; Shamir, Adi. (2001). *Weaknesses in the Key Scheduling Algorithm of RC4* .

Klaus, C. (2001). *Wireless LAN 802.11b Security FAQ* : Internet Security Systems. http://www.iss.net/wireless/WLAN_FAQ.php

Klemencic, J. (2001,). Basic Security Mechanisms for Wireless Networks. http://www.securityfocus.com/infocus/1199

Kuehl, K. (2001). *Detecting Rogue 802.11 Access Points within the Enterprise* : Cisco Systems Inc. http:// aptools.sourceforge.net/wireless.ppt

Marshall, T. (2001, October). Antennas Enhance WLAN Security. *BYTE Magazine*. http://www.byte.com/documents/s=1422/byt20010926s0002/

Orinoco. (2000a). *User's Guide for OR Manager Rev. C* . ftp://ftp.orinocowireless.com/pubs/docs/WaveACCESS/MANUAL/OR/ug_orm.pdf

Orinoco. (2000b). *User's Guide for the ORiNOCO Manager's Suite* . ftp://ftp.orinocowireless.com/pubs/docs/ORINOCO/MANUALS/ug_OM.pdf

Orinoco. (2002). Security Section. . http://www.orinocowireless.com/template.html?section=m131&page=3077&envelope=236

Schenk, R. G., Andrew, Iwanchuk, Russ. (2001, August 29, 2001). Wireless LAN Deployment and Security Basics. *ExtremeTech*. http://www.extremetech.com/print_article/0,3428,a%253D13521,00.asp

wi2600. (2001). Default SSIDs. . http://www.wi2600.org/mediawhore/nf0/wireless/ssid_deaults/

WLANA. (2002). Wireless LAN Security.
http://www.wlana.org/learn/security.htm.

Last Updated: August 17th, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**