

# **Global Information Assurance Certification Paper**

# Copyright SANS Institute Author Retains Full Rights

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

# Interested in learning more?

Check out the list of upcoming events offering "Auditing Systems, Applications, and the Cloud (Audit 507)" at http://www.giac.org/registration/gsna Auditing a Cisco Aironet Wireless Network From an Auditors Perspective

**GSNA v2.1 PRACTICAL** 

SANS Conference 2002 Washington D.C.

Ryan Stall 01/09/03

## Abstract/Summary

This paper is submitted as the requirement for a practical in the GSNA certification track. The subject of this audit is a wireless network that will be used in a corporate environment. Various devices such as laptops and PDA's will utilize the wireless network. Securing these devices is out of the scope of this audit. The wireless network is primarily used in conference rooms and training rooms. The eventual goal of wireless usage is to provide network access for workstations and access to wireless devices in the warehouses. Wireless devices in warehouses will be used for warehouse automation. The goal of the practical is to ensure the correct steps have been taken to secure this wireless LAN. The paper can then serve as a framework for future wireless LAN implementations.

#### OUTLINE

Assignment 1	4
Identify the system to be audited	4
Current State of Practice	6
Assignment 2	7
Audit Checklist	7
Assignment 3 – Audit Evidence, Conduct the Audit	16
Measure Residual Risk	33
Is the System auditable?	34
Audit Report	34
Audit Findings	35
Background/risk	36
Audit Recommendations	36
Costs	37
Compensating Controls	37
References	

## Assignment 1

## Identify the system to be audited

This is an audit of a wireless LAN being in a corporate office environment. The wireless LAN consists of a Cisco Aironet 1200 (System Firmware v. 11.56, Radio Firmware v. 5.01.02), a Cisco Aironet 350, (System Firmware v. 11.42, Radio Firmware v. 4.99.38, 802.11a) and two Compaq Ipaq 3850s (Pocket PC 2002). The IPAQs connect to the AP via the Cisco 350 wireless card. This wireless network provides e-mail and internet access for PDA's in the corporate office. The information from this audit will be used in future wireless LAN implementations in the Company.



The figure above shows the placement of the access point on the network. The wireless AP's will connect to one of the core switches, and will be behind the corporate firewall. The wireless LAN will have internet access through the internet connection shown in the diagram. The internet access will provide the wireless users with browser access and access to email.



Figure 2 shows an architectural drawing of the building and the placement of the wireless access points. An access point has been placed at both ends of the building to provide coverage for the entire floor. This allows for use of wireless devices in all of the conference rooms on the east side of the building as well as a training room on the northwest corner of the building.

The scope of this audit is the Cisco Aironet 350 and 1200. The laptop computers and Compaq Ipaq's are out of the scope of the audit.

D' I		
Risk	Probability	Consequences
Unauthorized LAN	High	Loss of company data,
Access from outside the		data integrity, monetary
building		loss
Unauthorized LAN	High	Loss of company data,
Access from inside.		interruption of service
Unauthorized Internet	High	Loss of company data,
Access from the outside		loss of data integrity,
the building.		privacy issues.
Accidental Association	Medium	Loss of company data,
with the Access Point		and data integrity
Disruption of Service to	High	Loss of productivity,
the Wireless Network	-	possible monetary loss.
Disruption of Service to	Medium	Loss of productivity,

the Corporate Network		potential loss of data,
		monetary loss.
Data Loss	High	Loss of productivity, and
		monetary loss.
Misconfigured access	High	Could allow unauthorized
points.		access to the corporate
		network and systems.
		Can also cause
		disruption of service.
Lack of Physical Security	High	Unauthorized individuals
		could gain access to the
		access point causing loss
		of service or
		unauthorized access to
	Ċ.	the corporate network.

# Current State of Practice

It seems everywhere you look, articles in trade magazines, newsgroups, press, wireless networking and security are a discussion. Wireless networks are gaining popularity and becoming much less expensive. Costs for equipment are making wireless LANs an attractive alternative to wired networks. There are still wireless standards being developed (802.IIg, 802.11i), by the IEEE and IETF. Wireless network devices are also becoming increasingly easier to install. Most access points can be utilized out of the box with the default settings. Because of this and the lack of standard procedures and checklists, wireless networks pose a great security concern. There are many articles outlining wireless security vulnerabilities and risks, but not many with specifics on mitigating those risks. Most research was done using the internet and standard search engines such as www.google.com and www.msn.com. A search on wireless networks and wireless security produces a large number of hits. There were a few sites that provided information worth mentioning.

The auditor found two checklists pertaining to the Cisco access point. One is a GSNA practical by Mark Gryparis (<u>http://www.giac.org/practical/GSNA/Mark\_Gryparis\_GSNA.pdf</u>), and GSNA practical by Angela Loomis (<u>http://www.giac.org/practical/Angela\_Loomis\_GSNA.doc</u>).

The National Institute of Standards and Technology published a wireless security recommendations document in July 2002 (<u>http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf</u>)

The National Infrastructure Protection Center has put out a wireless 802.11b best practices document. (<u>http://www.nipc.gov/publications/nipcpub/bestpract.html</u>)

The equipment vendor site was also utilized (<u>www.cisco.com</u>). One article worth noting is the wireless LAN security overview.

(<u>http://www.cisco.com/en/US/products/hw/wireless/ps430/prod\_brochure09186a</u> <u>0080088829.html</u>) Cisco also has a compilation of wireless security articles at their wireless security website.

(http://www.cisco.com/warp/public/779/smbiz/wireless/wlan\_security.shtml)

## Assignment 2

Audit Checklist

1. Obtain Permission to conduct the	
Reference	Class material – 7.1 Auditing Principles
	and Concepts
Control Objective	Signed permission must be obtained to
	use audit tools and gain cooperation of
	the corporate staff.
Risk	Without signed permission the auditor
	may not get the cooperation he needs
	and may be held responsible for any
	problems, issues, or sensitive
	information that is found from
V	performing the audit.
Compliance	Signed permission outlining the tools
	and methods to be used in the audit.
Testing	Obtain signed permission
Objective/Subjective	This is a objective step.

2. Wireless LAN Policy	
Reference	Security Basic Knowledge, Track 7
	course material
Control Objective	Outline policies and standards for the
R	implementation of a wireless network.
Risk	Clearly stated policies regarding
C Y	wireless access leave nothing open to
	interpretation. With a known policy in
	place, management has more leverage
	in the case of an information security
	incident, like in the case of rouge
	access points. A policy is also a
	guideline for auditing.
Compliance	Does the company have a wireless
	LAN policy in place?
Testing	Interview IT management, and obtain a
	copy of the policy and procedure

	manual. Search the manual for wireless policies.
Objective/Subjective	Subjective, the policy should exist and
	leave nothing to interpretation

3. Verify SSID broadcast is disabled	
Reference	Cisco Wireless LAN security overview
	http://www.cisco.com/en/US/products/h
	w/wireless/ps430/prod_brochure09186
	a0080088829.html
Control Objective	Ensure the access point is not
	broadcasting the SSID in the beacon
	packets. The SSID would need to
	obtained by sniffing the probe packets.
Risk	Network access by unauthorized
	persons.
Compliance	SSID broadcast disabled in the access
	point configuration
Testing	Confirm SSID broad cast is disabled using
	the access point configuration web utility.
	The settings are found by clicking set
	properties on the AP Radio configuration
	screen. Allow broadcast of SSID should be
	set to no. Use wireless sniffer to verify
	SSID is not broadcasted in the access point
	beacon packet.
Objective/Subjective	Objective.

4. Verify a strong non-trivial SSID is	
being used.	
Reference	NIST
Control Objective	The SSID should not be an easily
C. Y	guessed phrase such as address,
	company name, or street name.
Risk	Association to the access point by
	unauthorized persons.
Compliance	A strong SSID should be used which
	contains at least 8 alpha and numeric
	characters and contains no dictionary
	words.
Testing	SSID configuration should be confirmed
	using the access point configuration utility.
	The settings are found by clicking set
	properties on the AP Radio configuration
	screen. Check the Service Set ID field.
Objective/Subjective	Objective

5. Verify WEP Configuration	
Reference	Cisco SAFE whitepaper
Control Objective	Client must use WEP to communicate
	with the access point. All
	communications with the access point
	should be encrypted.
Risk	Network and data compromise by an
	unauthorized person.
Compliance	Verify WEP is being used.
Testing	Verify WEP configuration using the
	configuration utility. The settings can be
	found by clicking on security on the setup
	page. Then follow the link for Radio Data
	Encryption. Use of data encryption should
	be set to full encryption. Note: This
	setting is only available if a WEP key is
	set.
Objective/Subjective	Objective

6. Verify the use of MAC address filtering	
Reference	NIST document
Control Objective	Ensure only authorized devices can
	associate with the access point
Risk	Unauthorized association causing
	network interruption and data loss.
Compliance	Verify MAC address filtering is being
	used and the MAC addresses of the
	authorized devices have been entered.
Testing	Check the configuration utility for
i i i i i i i i i i i i i i i i i i i	configuration of MAC address filtering.
	These settings are found by clicking
	Address Filters on the setup page. MAC
GV.	addresses of the authorized devices should
<u> </u>	be listed. Also attempt to associate an
	unauthorized device. This can be done by
	attempting to associate to the access point
	with a wireless card with a MAC address
	not listed.
Objective/Subjective	Objective

7. Verify the access point is configured for the lowest possible power settings.

Reference	NIST Document
	(http://csrc.nist.gov/publications/drafts/draf
	<u>t-sp800-48.pdf)</u> , table 3-3
Control Objective	Ensure the wireless signal is not being
	broadcasted to unauthorized areas
Risk	Unauthorized network access from
	outside of the building or in public
	areas such as the lobby.
Compliance	A wireless device should not be able to
	associate to the access point from
	outside the building or public areas.
Testing	Use Cisco client utilities to check signal
	strength in several areas. Cisco client
	utilities includes a site survey tool which
	measures signal strength and quality.
	Check signal strength especially in areas
	easily accessible to the public. In all of the
	unauthorized or public areas, the survey
	tool should either show very low signal
	strength or not associate.
Objective/Subjective	Subjective, it may not be possible to
	configure the access point for a lower
	setting and still provide an acceptable
V.	level of service.

8. Verify secure placement of the	
access point.	
Reference	NIST Document
	(http://csrc.nist.gov/publications/drafts/draf
	t-sp800-48.pdf), table 3-3
Control Objective	Prevent unauthorized physical access
	to the access point.
Risk	Unauthorized access by an
	unauthorized individual can cause
	disruption of service and loss of data.
Compliance	Verify the access point is mounted in a
	secure location.
Testing	Check each access point and verify it is
	mounted in a secure location. Identify
	who has access to the access points.
Objective/Subjective	Objective

9. Verify default admin password has been changed.	
Reference	Cisco SAFE white paper
Control Objective	Prevent unauthorized admin access to

	the access point due to lack of admin password. The default settings are well published and access can be gained easily with the defaults
Diak	Lineuthorized admin access looves the
RISK	Unautionzed aumin access leaves the
	door open to anyone who can
	determine the access point ip address.
	This can lead to network interruption
	and potential data loss
Compliance	Varify the default admin password has
Compliance	venity the default admin password has
	been changed to a strong nontrivial
	passphrase.
Testing	Interview the network administrators
	and verify the admin password has
	been changed to a strong password
	Verify the necessary anticipal and
	venity the password contains eight
	alphanumeric characters and no
	dictionary words.
Objective/Subjective	Objective

10. Verify that wireless access points have been hardened.	
Reference	NIST wireless security document
V'	(http://csrc.nist.gov/publications/drafts/draf
	<u>t-sp800-48.pdf</u> ), table 3-3
Control Objective	Prevent unauthorized access due to
2	software issues or unneeded services.
Risk	Access to the network or access point
	could be gained through flaws in the
	software, firmware, or unneeded
	services. This is a moderate risk.
Compliance	Verify the software and firmware are at
Charles and the second s	the most current levels. Also verify that
	any unneeded services that can be
	disabled are.
Testing	Verify with the configuration utility.
	Firmware level can be verified on the
	software page. Services are listed on the
	setup page. Each unneeded service should
	be set to disabled.
Objective/Subjective	Objective

11. Verify access point placement does not allow for signal broadcast outside the authorized area.	
Reference	NIST standards

Control Objective	Prevent unauthorized access from the
	ouiside.
Risk	Unauthorized access to the network,
	disruption of service and data loss.
	This is a high risk. Signal broadcast to
	the outside is the first thing an
	individual needs to begin attempting
	access to the network.
Compliance	Verify that there is no signal broadcast
	to unauthorized areas such as outside
	the building due to access point
	placement. The access point should
	not be placed next to windows or areas
	that would allow it's signal to be
	broadcast out of the authorized areas.
Testing	Verify the access point is not placed next to
	windows. Check signal strength at several
	locations Signal strength should be
	verified with the Cisco client utilities site
	survey tool Signal strength should be
	checked in public areas and outside of
	windows
Objective/Subjective	Subjective there may not be many
	Subjective, there may not be many
0.1	options for access point placement to
	provide network access where needed.

12. Check for the existence of rouge access points.	
Reference	Cisco SAFE
Control Objective	Ensure that only access points meeting
	the security requirements are
	connected to the network.
Risk	Rouge, misconfigured access points
	can allow access to the network
	resulting in potential data loss, service
C Y	disruption and data integrity issues.
	This is a high level risk. Rouge access
	points that are not configured properly
	are a high risk to any network.
Compliance	Use netstumbler to check for access point.
	Use switch cam tables to check for mac
	addresses of known access points. On a
	Cisco switch the command would be "sh
	cam dynamic" for dynamic entries or "sh
	cam static" for static entries.
Testing	Use netstumbler to check for access

	point. Use switch cam tables to check for mac addresses of known access points.
Objective/Subjective	Objective

13. Verify access point network configuration has been changed from the defaults.	
Reference	NIST Document
	(http://csrc.nist.gov/publications/drafts/draf
	<u>t-sp800-48.pdf)</u> , table 3-3
Control Objective	Ensure unauthorized access cannot be
	gained because of pre-configured, well-
	known defaults.
Risk	Unauthorized network access
Compliance	Verify all default settings have been
	changed.
Testing	Compare current configurations settings
	with out of the box default settings.
	Record all settings from an access point
	that has been set to factory default.
A	Compare those settings to the current
	configuration.
Objective/Subjective	Objective

14. Verify the use of strong authentication such as RADIUS.	
Reference	ExtremeTech wireless security tips
Control Objective	Verify a higher lever of authentication is
	in use on the wireless network. This
6	gives another layer of protection from
	unauthorized individuals associating
	with the access points.
Risk 🧼	Unauthorized access to the corporate
	network resulting in data loss and loss
<u> </u>	of service.
Compliance	Verify RADIUS authentication is
8	configured properly.
Testing	Verify with the configuration utility that
	RADIUS is configured and in use. These
	settings are found by clicking on
	Authentication on the setup page.
Objective/Subjective	Objective

15. Verify the use of encryption beyond that of WEP

publications/drafts/draf
1
ole 3-3
on scheme is used to
eaknesses in WEP.
ess to the network,
, and privacy issues.
trong encryption
gy with network
se network sniffer to
,

16. Verify access points are turned	S S
off when not in use.	
Reference	NIST Document
	(http://csrc.nist.gov/publications/drafts/draf
	<u>t-sp800-48.pdf</u> ), table 3-3
Control Objective	Reduce the risk of unauthorized access
	by shutting down the WLAN when it is
	not in use.
Risk	The risk on a person successfully
V.	gaining access to the access point
	increases over time.
Compliance	Verify procedures are in place to shut
	down the access point after hours and
	weekends.
Testing	Spot check the access points at times when
	they should be powered down. Verify IT
	policy.
Objective/Subjective	Objective

17. Verify the use of static IP addressing.	
Reference	ExtremeTech tips
Control Objective	Prevent unauthorized access to the
	network by providing IP addresses.
Risk	Unauthorized access to the network.
Compliance	Verify all authorized devices are
	assigned IP addresses and DHCP is
	disabled on the access point.
Testing	Verify the configuration of the access
	point. Also, attempt to use DHCP on
	the client.
Objective/Subjective	Objective.

ST Document
tp://csrc.nist.gov/publications/drafts/draf
<u>p800-48.pdf)</u> , table 3-3
sure that SNMP, if needed, is
nfigured Securely.
authorized access to the network by
Inerabilities in SNMP
rify the use of strong community
ings. Configure SNMP for read only
ossible. Disable SNMP if it is not
eded.
termine the need for SNMP. Check for
use of strong community strings.
ting can be checked by using the
ifiguration tool. The setting can be
ind on the setup page by clicking SNMP.
ind on the setup page by clicking SNMP. om this form SNMP can be enabled or
ind on the setup page by clicking SNMP. om this form SNMP can be enabled or abled. The community string is listed
ind on the setup page by clicking SNMP. om this form SNMP can be enabled or abled. The community string is listed re.
ind on the setup page by clicking SNMP. om this form SNMP can be enabled or abled. The community string is listed re.
ind on the setup page by clicking SNMP. om this form SNMP can be enabled or abled. The community string is listed re. ojective - All necessary settings can verified
ind on the setup page by clicking SNMP. om this form SNMP can be enabled or abled. The community string is listed re. ojective - All necessary settings can verified bjective – SNMP may or may not be
ind on the setup page by clicking SNMP. om this form SNMP can be enabled or abled. The community string is listed re. ojective - All necessary settings can verified bjective – SNMP may or may not be eded. If the administrators use
ind on the setup page by clicking SNMP. om this form SNMP can be enabled or abled. The community string is listed re. ojective - All necessary settings can verified bjective – SNMP may or may not be eded. If the administrators use

19. Verify the use of a firewall between the corporate network and wireless network.	
Reference	NIST Document
	(http://csrc.nist.gov/publications/drafts/draf
	<u>t-sp800-48.pdf)</u> , table 3-3
Control Objective	Use of a firewall ensures only required
	traffic is transmitted to the corporate
	network.
Risk	Unauthorized access to the network.,
	interruption of service
Compliance	Verify the existence of a firewall
	between the wireless network and the
	corporate network.
Testing	Use a port scanner and ping scanner to
	verify the existence of a firewall.
Objective/Subjective	Objective.

2

20. Change the Default channel	
Reference	NIST Document
	(http://csrc.nist.gov/publications/drafts/draf
	<u>t-sp800-48.pdf)</u> , table 3-3
Control Objective	Changing from the default channel
	lowers the risk of interruption of service
	due to radio interference.
Risk	Disruption of service due to Radio
	interference. This is currently a low
	risk in this small wireless network. This
	will be given more consideration as the
	wireless network and the number of
	access points grow.
Compliance	Verify the channel setting has been
	changed from the default setting.
Testing	Verify the channel setting in the access
	point configuration. The setting can be
	found by clicking setup, then clicking on
	the AP Radio. Click set properties on the
	AP Radio page. Here the default radio
A	channel can be set. Also use netstumbler to
	determine the current channel settings.
Objective/Subjective	Objective.

Assignment 3 – Audit Evidence, Conduct the Audit

# Audit Step 1.Checklist Step 1 (A1.C1) – Obtain Permission

The audit objectives were presented to the network team, IT Manager, and VP of Information Technology. We reviewed the need to have a username and password to the wireless access points and audit tools such as netstumber, NAI Sniffer, and Cisco Site Survey were reviewed. The need to interview network administrators was also discussed. Signed permission was given to perform the audit.

Pass: Written permission was obtained

# A2.C2 – Determine company policy and procedures for wireless LANs

The company policy and procedure manual was reviewed and the VP of IT, and HR manager were interviewed. The policy and procedure manual was in electronic format, and was searched for keywords such as wireless and access point. No matches were found. Network administrators were also interviewed for

policy and know procedures. It was determined there is no wireless LAN policy in place.

*Fail:* There is currently no policy in place for wireless LAN's. A policy needs to be written.

## A3.C3 - Verify SSID broadcast is disabled

The configuration of the SSID broadcast parameter was verified with the cisco configuration utility.

As seen in the figure below, allow "Broadcast" SSID to Associate is set to no.

AP350-4. AP Radio Har	dware Cisco Systems
Cisco 350 Series AP 11.06	
Man Hala	Linting & days 03-20-50
Map Men	Opanie, s days, 05:20:50
Service Set ID (SSID):	- 0
Allow Broadcast SSID to Associate /: O y	es Ono
Enable world Mode mult-domain operation	
Data Rates (Mb/sec):	
1.0 basic 💌 2.0 basic 💌 5.5 basic	✓ 11.0 basic ▼
Transmit Power:	100 mW 💙
Frag. Threshold (256-2338):	2338 RTS Threshold (0-2339): 2339
Max. RTS Retries (1-128):	32 Max. Data Retries (1-128): 32
Beacon Period (Kusec):	100 Data Beacon Rate (DTIM): 2
Default Radio Channel:	6 [2437 MHz] V In Use: 6
Search for less-congested Radio Channel?:	no 🜱
Passing Astronom Diversity	Transmit Antonna Diversity
Receive Antenna. Oversity [2]	Transmit Antenna. Oversky ra
Radio Data Encryption (WEP)	R
L	Apply OK Cancel Restore Defaults
-	
[Map]	][Login][Help]
Cisco 350 Series AP 11.06 @ Copyright 3	1000 <u>Cisco Systems. Inc.</u> <u>creditz</u>



The setting was further verified by the use of a wireless sniffer. The results of the sniffer trace is shown in the figure above. The sniffer packet shown is a beacon packet. An analysis of the packet shows the SSID is not being broadcast.

**PASS:** The Allow Broadcast SSID setting in the configuration utility was set to no. The configuration was also verified by using AiroPeek. Beacon packets were captured and the auditor was not able to obtain the SSID.

# A4.C4 – Verify SSID Configuration

The WAP was manually checked using the web interface. SSID configuration was also verified with netstumbler.

W Network Stumbler - 2	200304011635	57		
File Edit View Device Window	v Help			
A 20030401163557				
Channels	MAC	SSID	Name Ch Vend	dor Ty
	004096		6+ Cisc	o AP
004096	0008522100		0	AF
in a SSIDs in a SSIDs				
E 4 apaccesspoint				
Filters				
Encryption On				
BSS (Peer)				
- & CF Pollable - & Short Preamble				
🥏 🚽 🚽 🚽 🚽				
<u> </u>	<	an a		
Ready		No APs active	GPS: Disabled	2/2
				-1- 7
			Cisco Si	STEMS
AP1200-1 - A	P Radio:	Internal Ha	rdware Cisco St	STEMS
AP1200-l · A Cisco 1200 Series AP 11.56	P Radio:	Internal Ha	rdware Cisco Si	IN TEMS
AP1200-l A Cisco 1200 Series AP 11.50 Man Help	P Radio:	Internal Ha	rdware Cisco Si	<b>STEMS</b> 1111111100 vs. 15:03:50
AP1200-l A Cisco 1200 Series AP 11.50 Map Help	P Radio:	Internal Ha	rdware Cisco Si uilliuuu Uptime: 8 da	<b>STEMS</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>11</b> <b>1</b>
AP1200-l A Cisco 1200 Series AP 11.50 <u>Map Help</u> Service Set ID (SSID): Allow "Broadcast" SSID	P Radio:	Internal Ha	rdware Cisco Si utililiuu Uptime: 8 da	<b>STEMS</b> att <b>1111</b>
AP1200-l A Cisco 1200 Series AP 11.50 Map Help Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m	P Radio:	Unternal Ha	rdware Cisco Si uilliuuu Uptime: 8 da	<b>STEMS</b> utilitum® ys, 15:03:50
AP1200-l A Cisco 1200 Series AP 11.50 May Help Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m	P Radio: ε <sub>μ.</sub> to Associate?: ulti-domain oper	Internal Han ○ves ⊙no ratiox?: no ♥	rdware	STEMS (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
AP1200-l A Cisco 1200 Series AP 11.50 <u>Map Help</u> Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m Data Rates (Mb/sec):	P Radio: هبالله to Associate?: ulti-domain oper	Oves Ono ration?: no V	rdware Cisco Si uililiuuu Uptime: 8 da	<b>STEMS</b> utilitie ® ys, 15:03:50
AP1200-l A Cisco 1200 Series AP 11.50 Map Help Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" mu Data Rates (Mb/sec): 1.0 basic 2.0 bas	P Radio: a.p. to Associate?: ulti-domain oper ic   5.5 bas	Internal Ha	rdware Cisco Si uiliiiuuu Uptime: 8 da	<b>STEMS</b> ys, 15:03:50
AP1200-l A Cisco 1200 Series AP 11.50 Map Help Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m Data Rates (Mb/sec): 1.0 basic 2.0 bas	P Radio: ε <sub>μ</sub> . to Associate?: ulti-domain oper ic v 5.5 bas	Internal Han	rdware Cisco Si utililiuu Uptime: 8 da	STEMS 
AP1200-l A Cisco 1200 Series AP 11.50 Map Help Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m Data Rates (Mb/sec): 1.0 basic 2.0 bas Transmit Power:	P Radio: ε <sub>μ</sub> . to Associate?: ulti-domain oper ic • 5.5 bas	Internal Ha	rdware Cisco Si uuiliiuuu Uptime: 8 da	<b>STEMS</b> ys, 15:03:50
AP1200-l A Cisco 1200 Series AP 11.50 May Help Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m Data Rates (Mb/sec): 1.0 basic 2.0 bas Transmit Power: Frag. Threshold (256-23-	P Radio: ε <sub>μ</sub> . to Associate?: ulti-domain oper ic solution for solutions based base	Internal Ha	rdware Cisco Si Uptime: 8 da S Threshold (0-2347):	<b>STEMS</b> (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
AP1200-l A Cisco 1200 Series AP 11.50 Map Help Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m Data Rates (Mb/sec): 1.0 basic 2.0 bas Transmit Power: Frag. Threshold (256-23- Max. RTS Retries (1-25)	P Radio: ε <sub>μ</sub> . to Associate?: ulti-domain oper ic • 5.5 bas 46): 5):	Internal Han ves ono ratioa?: no v sic v 11.0 basic 100 mW v 2346 RT 32 Ma	S Threshold (0-2347): x. Data Retries (1-255):	2347 32
AP1200-l A Cisco 1200 Series AP 11.50 <u>Map</u> <u>Help</u> Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m Data Rates (Mb/sec): 1.0 basic 2.0 bas Transmit Power: Frag. Threshold (256-23) Max. RTS Retries (1-25) Beacon Period (Kusec):	<b>P Radio:</b> <sup>5</sup> <sup>5</sup> <sup>6</sup> <sup>6</sup> <sup>6</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup> <sup>7</sup>	Internal Har ves ono ration?: no v sic v 11.0 basic 100 mW v 2346 RT 32 Ma 100 Dat	S Threshold (0-2347): x. Data Retries (1-255): Ta Beacon Rate (DTIM):	2347 32 1
AP1200-1 A Cisco 1200 Series AP 11.50 Map Help Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m Data Rates (Mb/sec): 1.0 basic 2.0 bas Transmit Power: Frag. Threshold (256-23) Max. RTS Retries (1-25) Beacon Period (Kusec): Default Radio Channel	<b>P Radio:</b> ε <sub>μ.</sub> to Associate?: ulti-domain oper ic    5.5 bas 46): 5):	Internal Har ves ono ration?: no v sic v 11.0 basic 100 mW v 2346 RT 32 Ma 100 Dai 6 [2437 MHz	S Threshold (0-2347): x. Data Retries (1-255): a Beacon Rate (DTIM): I In Use: 6	<b>STEMS</b> ys, 15:03:50 2347 32 1
AP1200-1 A Cisco 1200 Series AP 11.50 Map Help Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m Data Rates (Mb/sec): 1.0 basic 2.0 bas Transmit Power: Frag. Threshold (256-23- Max. RTS Retries (1-25) Beacon Period (Kusec): Default Radio Channel: Search for less-congested	P Radio: <sup>5</sup> to Associate?: ulti-domain oper ic ▼ 5.5 bas 46): 5): 1 Radio Channe	Internal Ha	S Threshold (0-2347): x. Data Retries (1-255): a Beacon Rate (DTIM): I V In Use: 6 strict Searched Channels	2347 1
AP1200-1 A Cisco 1200 Series AP 11.50 <u>Map</u> <u>Help</u> Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m Data Rates (Mb/sec): 1.0 basic 2.0 bas Transmit Power: Frag. Threshold (256-23) Max. RTS Retries (1-25) Beacon Period (Kusec): Default Radio Channel: Search for less-congested Receive Antenna: Divers	P Radio: <sup>5</sup> to Associate?: ulti-domain oper ic ▼ 5.5 ba: 46): 5): 1 Radio Channe ity ▼	Internal Har	S Threshold (0-2347): x. Data Retries (1-255): a Beacon Rate (DTIM): In Use: 6 strict Searched Channels	STEMS ys, 15:03:50 2347 32 1
AP1200-1 A Cisco 1200 Series AP 11.50 <u>Map</u> <u>Help</u> Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m Data Rates (Mb/sec): 1.0 basic 2.0 bas Transmit Power: Frag. Threshold (256-23: Max. RTS Retries (1-25: Beacon Period (Kusec): Default Radio Channel: Search for less-congested Receive Antenna: Divers	P Radio: <sup>2</sup> <sup>2</sup> <sup>2</sup> <sup>2</sup> <sup>2</sup> <sup>2</sup> <sup>2</sup> <sup>2</sup> <sup>2</sup> <sup>2</sup>	Internal Han	S Threshold (0-2347): x. Data Retries (1-255): a Beacon Rate (DTIM): I In Use: 6 strict Searched Channels smit Antenna: Diversity	2347 32 1
AP1200-1 A Cisco 1200 Series AP 11.56 <u>Map</u> <u>Help</u> Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" m Data Rates (Mb/sec): 1.0 basic 2.0 bas Transmit Power: Frag. Threshold (256-23- Max. RTS Retries (1-25: Beacon Period (Kusec): Default Radio Channel Search for less-congested Receive Antenna: Divers Radio Data Encryption (M	P Radio: a <sub>µ</sub> . to Associate?: ulti-domain oper ic ▼ 5.5 bas 46): 5): 1 Radio Channe ity ▼ <u>NEP</u> )	Internal Han	rdware       CISCO SI Lull         Uptime: 8 da         Uptime: 8 da         S Threshold (0-2347):         x. Data Retries (1-255):         ta Beacon Rate (DTIM):         In Use: 6         strict Searched Channels         smit Antenna:         Diversity	2347 32 1
AP1200-1 A Cisco 1200 Series AP 11.50 <u>Map</u> <u>Help</u> Service Set ID (SSID): Allow "Broadcast" SSID Enable "World Mode" nu Data Rates (Mb/sec): 1.0 basic 2.0 bas Transmit Power: Frag. Threshold (256-23) Max. RTS Retries (1-25) Beacon Period (Kusec): Default Radio Channel: Search for less-congested Receive Antenna: Divers Radio Data Encryption (N	P Radio: <sup>a,µ.</sup> <sup>1</sup> to Associate?: ulti-domain oper ic ▼ 5.5 bar 46): 5): 1 Radio Channe ity ▼ <u>NEP</u> )	Internal Han	S Threshold (0-2347): x. Data Retries (1-255): a Beacon Rate (DTIM): I Muse: 6 strict Searched Channels smit Antenna: Diversity	2347 32 1

AP350-4 AP Radio Hard	ware Cisco Systems
Cisco 350 Series AP 11.06	ي بىللىپ بىللىپ
Map Help	Uptime: 8 days, 03:20:50
Service Set ID (SSID): Allow "Broadcast" SSID to Associate?: Oyes Enable "World Mode" multi-domain operation?	ono     ono
Data Rates (Mb/sec): 1.0 basic 2.0 basic 5.5 basic	• 11.0 basic •
Transmit Power:	100 mW 👻
Frag. Threshold (256-2338):	2338 RTS Threshold (0-2339): 2339
Max. RTS Retries (1-128):	32 Max. Data Retries (1-128): 32
Beacon Period (Kusec):	100 Data Beacon Rate (DTIM): 2
Default Radio Channel:	6 [2437 MHz] V In Use: 6
Search for less-congested Radio Channel?:	no 💌
Receive Antenna: Diversity 💙	Transmit Antenna: Diversity 💙
Radio Data Encryption (WEP)	k
A	pply OK Cancel Restore Defaults
[ <u>Map][[</u> Cisco 350 Series AP 11.06 © Copyright 200	.ogin][Help] 0 <u>Cisco Systems, Inc.</u> <u>credits</u>

Pass: The SSID was found to meet the strength requirements.

- SSID is not a dictionary word
- SSID contains more that eight alphanumeric characters

Attempting to associate a device without the correct SSID configured further tested the SSID configuration. The device did not associate.

# A5.C5 – Verify WEP configuration

WEP configuration was verified by using both the configuration utility and netstumbler. Netstumbler was used to detect any access points not using encryption.

△ Network Stumbler - 20030401163557 File Edit View Device Window Help □ 2 日 ● ⑤ 田 ● □ 注 Ⅲ Ⅲ 《 《 ↓ ?					
20030401163557	~				
Channels SSIDs SSIDs Country Channels SSIDs Country C	MAC 004096	SSD	Name Ch Vendor 6+ Cisco 6	AP AP	

The results show that both the access points are not using encryption.

The follows screen shots show the WEP configuration on the access points.

AP1200-1.1	AP Radio:	Internal	Data Encrypt	ion CISCO SYSTEMS
Cisco 1200 Series AP 11	1.56			ally ally
Map Help				Uptime: 8 days, 15:04:52
Use of Data Encryptio	n by Stations is:	Not Available		
Mus	t set an Encrypti	on Key or enabl	e Broadcast Key Rota	ution first
		Open	Shared	Network-EAP
Accept Authentication	Туре:			
Require EAP:				
	Transmit			
	With Key	E	acryption Key	Key Size
WEP Key 1:	1211			not set 💌
WEP Key 2:				not set 💌
WEP Key 3:	121			not set 💌
WEP Key 4:				not set 🛩
	Enter 40-bit WEF Enter 128-bit WE This radio	P keys as 10 hexade P keys as 26 hexade o supports Encrypt	cimal digits (0-9, a-f, or A- cimal digits (0-9, a-f, or A on for all Data Rates.	F). -F). Restore Defaults

AP350-4 AP Radio Data Encryption Cisce 350 Series AP 11.06 Map Help				CISCO SYSTEMS	
Use of Data Encrypt	ion by Stations Mu	is: Not Availabl st set an Encryp	e tion Key first		
Accept Authentication Require EAP:	on Type:	Open V	Shared	Network-EAP	
	Transmit With Key	Fn	cryption Key	Key Size	
WEP Key 1:	-		crypnon xey	not set 🖌	
WEP Key 2:				not set 👻	
WEP Key 3:				not set 👻	
WEP Key 4:	2000 U			not set 🛩	
12	Enter 40-bit WE Enter 128-bit WF This radi	P keys as 10 hexade P keys as 26 hexade o supports Encrypt Apply	cimal digits (0-9, a-f, o ecimal digits (0-9, a-f, o ion for all Data Rates.	r A-F). or A-F).	
Cisco 350 Series AP 11.06		[ <u>Map][Login]</u> © Copyright 2000 <u>Cites</u>	(Help) 2 Svatema, Inc.	creditz	

The configuration utility further verifies encryption is not being used.

*Fail:* The configuration utility shows that WEP is not configured and not being used. Netstumbler was able to find both access points and also shows encryption is not being used.

## A6.C6 – Verify The use of MAC address filtering

The WAP was manually checked using the web interface. The use of filtering was further verified by attempting to associate authorized and unauthorized devices.

MAC address filtering was verified to be in use and the MAC addresses of all authorized devices have been entered. A device with an unlisted MAC address was unable to associate.

AP1200-	ldress Filters	CISCO SYSTEMS
Cisco 1200 Series AP 11.56	La .	برالي برالي
Map Help		Uptime: 8 days, 11:40:26
New MAC Address Filte Dest MAC Address:	er: @Allowed ODisallowed	Add
The default settings for multic interface are specified on the A	ast and unicast destination MAC addresses tran Idvanced Setup page for that network interface.	ismitted from each network
Existing MAC Address	filters:	Deserve
	00:05:46:26 * Allowed 00:05:46:2 * Allowed 00:05:46:2 * Allowed 00:05:46:26 * Allowed 00:05:46:26 * Allowed	Remove
Lookup MAC Address on	Authentication Server if not in Existing Filt	ter List? Oves @no
Is MAC Authentication alc	ne sufficient for a client to be fully authention	cated? Oyes Ono
	Apply OK	Cancel Remove All
	[Map][Login][Help]	
Cisco 1200 Series AP 11.56	Copyright 2002 Cisco Systems, Inc.	<u>credits</u>

The screen shot above shows the entered MAC addresses on the Aironet 1200.

AP Radio: Internal	Advanced		CISCO SYSTEMS
isto 1200 Series AP 11.56			ally ally
Map Help			Uptime: \$ days, 11:36:56
equested Status:	Up 👻		
Jurrent Status:	Up		
acket Forwarding	Enabled 💌		
orwarding State:	Blocking		
Default Multicast Address Filter:	Disallowed 🛩		
faximum Multicast Packets/Second:	0		
	N		
ladio Cell Role:	Access Point/Root	*	
faximum number of Associations	0	Carefold .	
Ise Aironet Extensions:	⊙ves ⊖no		
lassify Workgroup Bridges as Network Infrastructure:	⊙yes Ono		
equire use of Internal Radio Firmware: 5.01.02	⊙yes Ono		
themet Encapsulation Transform:	RFC1042 💌		
nhanced MIC verification for WEP:	None 🛩		
emporal Key Integrity Protocol:	None 🛩		
roadcast WEP Key rotation interval (sec):	0 (0=off)		
	Open	Shared	Network-EAP
ccept Authentication Type:			
lequire EAP:			Contraction of the second
)efault Unicast Address Filter:	Allowed 💌	Allowed 😽	Allowed

This screen shot shows the filter settings on the 1200 access point.

AP350- Jer Ad	dress Filters	CISCO SYSTEMS
Cisco 350 Series P 11.06		and line at line of
Map Help		Uptime: 28 days, 03:06:21
New MAC Address Filte Dest MAC Address:	er: ⊙Allowed ○Disallowed	Add
The default settings for multic nterface are specified on the /	ast and unicast destination MAC addresses tran Advanced Setup page for that network interface	asmitted from each network
Existing MAC Address	Filters:	
	00:07:50: Allowed 00:0b:46: Allowed 00:0b:46:2 Allowed 00:0b:46:2 Allowed	Remove
Lookup MAC Address on	Authentication Server if not in Existing Fil	ter List? Oyes @no
	Apply OK	Cancel Remove All
	[Map][Login][Help]	
Cisco 350 Series AP 11.06	Copyright 2000 Cisco Systems, Inc.	<u>credits</u>

This shot shows the filters in use on the Aironet 350.

AP350-1 2 AP Radio	Advanced		CISCO SYSTEMS
Cisco 350 Series AP 11.06			and be all be
Map Help			Uptime: 28 days, 03:07:07
Requested Status:	Up 💌		
Current Status:	Up		
Packet Forwarding:	Enabled 🐱		
Forwarding State:	Blocking		
Default Multicast Address Filter:	Distance 💙		
Maximum Multicast Packets/Second:	0	R	
Radio Cell Role:	Access Point/Root	~	
Use Aironet Extensions:	@yes Ono		
Require use of Radio Firmware 4.23:	Oyes @no		
Ethernet Encapsulation Transform:	RFC1042 💌		
	Open	Shared	Network-EAP
Accept Authentication Type:	2	O	
Require EAP:		0	
Default Unicast Address Filter:	Allowed	Allowed 💌	Allowed
Specified Access Point 1:	00 00 00 00 00 00		
Specified Access Point 2:	00-00-00-00-00-00		
Specified Access Point 3:	00.00.00.00.00.00		
Specified Access Point 4:	00.00.00.00.00.00		

This shows the MAC filter settings on the Aironet 350.

An attempt was made to associate a device which was not listed in the access list.

Site Survey - 350 Series - F	Passive Mode - [Enterpri 🔀	
Signal Strength	Signal Quality	
Not Associated	Not Associated	
Link Speed		
Overall Link Quality	Not Associated	
Associated Access Point	Not Associated	
Channel (Frequency)	6 (2437 MHz)	.0
Restart Card Setup Start	OK Cancel Help	

As seen from the configuration above, MAC address filtering is in use. It was also verified that unlisted devices could not associate.

**PASS:** MAC address filtering was shown to be in use. The configuration utility listed all of the MAC addresses of authorized devices. An attempt was also made to associate an unauthorized device. The device could not associate

# A7.C7 – Verify access point is configured for the lowest possible setting.

Coverage are was checked with a laptop and a Cisco aironet 340 pcmcia card. Signal strength was tested with the Cisco client utilities. Signal strength was tested at several areas inside and outside the building. Screen shots of the results are shown below.

Outside the front main door on the southeast side

Site Survey - 350 Series - Pas	ssive Mode - [Enterpri 🔀	
Signal Strength	Signal Quality	
53%	90%	
Link Speed 11 Mbps		
Overall Link Quality	Good	
Associated Access Point	AP1200-b121c8	
Access Point IP Address	1	
Channel (Frequency)	6 (2437 MHz)	
Restart Card Setup Start [	OK Cancel Help	

# Southwest door of building

Site Survey - 350 Series - Pas	sive Mode - [Enterpri 🔀			
Signal Strength	Signal Quality			
12%	64%			
Link Speed 11 Mbps				
Overall Link Quality	Poor			
Associated Access Point	AP1200-b121c8			
Channel (Frequency)	6 (2437 MHz)			
onumer (r requency)				
Restart Card Setup Start [	OK Cancel Help			

From the parking lot on the southwest side

Site Survey - 350 Series - P	Passive Mode - [Enterpri 🔀	
Signal Strength	Signal Quality	
Not Associated	Not Associated	
Link Speed		
Overall Link Quality	Not Associated	
Associated Access Point	Not Associated	
Channel (Frequency)	6 (2437 MHz)	
Restart Card Setup Start	OK Cancel Help	

The image below is from the street on the south side of building. This data was obtained while the auditor was sitting in a car on the opposite side of the street.

Signal Strength	Signal Quality
23%	70%
Link Speed 11 Mbps	
Overall Link Quality	Fair
Associated Access Point	AP1200-b121c8
Access Point IP Address	
Channel (Frequency)	6 (2437 MHz)

*Fail:* The Aironet 1200 access point was found to be configured for the highest setting. This configuration is allowing for associating with the access point at unauthorized points. As seen from the screen shots above, the access point Cisco 1200 access point is broadcasting a signal far beyond the areas it is being used. The auditor was able to associate with the access point outside the building at various locations. These locations included the parking lot in front of the building, in the back of the building, and on the street both to the south of the building and east of the building. The signal from the Aironet 350 access point was not broadcast outside of the building.

# A8.C12 - Check for the existence of rouge access points.

To check for the existence of rouge access points the core network switch's MAC address tables, and the router arp tables were checked for know MAC addresses of popular access points. The command on a Cisco router is "sh arp". The command on a Cisco switch is "sh cam dynamic"mA list of access point MAC addresses is shown below.

**3Com** 0001.03|0004.76|0050.da|0800.02 Addtron 0040.33|0090.d1 **Advanced Multimedia** Internet 0050.18 **Apple** 0030.65 Atmel 0004.25 Bay Networks 0020.d8 BreezeNet 0010.e7 Cabletron (Enterasys) 0001.f4|00e0.63 **Camtec** 0000.ff Cisco Aironet 0040.96|000b.5f Compaq 0050.8b **D-Link** 0005.5d|0040.05|0090.4b Delta Networks 0030.ab Intel 0002.b3 Linksys 0003.2f|0004.5a Lucent 0002.2d|0060.1d|0202.2d Nokia 00e0.03 Samsung 0000.f0|0002.78 Senao Intl 0002.6f SMC 00e0.29|0090.d1 **SOHOware** 0080.c6 **Sony** 0800.46 Symbol 00a0.f8|00a0.0f **Z-Com** 0060.b3 **Zoom** 0040.36

The arp table of the core router was captured. This was done by issuing the "show arp" command on the router. This method should also be used all of the company's other locations periodically to search for rouge access points.

He Edit Format. Verw. Help.         P0         Odd. 000F         APA         FastEthermet0/0           Tiererret. 72.1.8         20         000.00C         APA         FastEthermet0/0           Tiererret. 72.1.8         10         0000.00C         APA         FastEthermet0/0           Tiererret. 72.1.8         0         0000.00C         APA         FastEthermet0/0           Tiererret. 72.1.8         0         0000.00C         APA         FastEthermet0/0           Tiererret. 72.1.8         0         0000.00C         APA         FastEthermet0/0           Tiererret. 72.1.8         10         0000.00C         APA         FastEthermet0/0           Tiererret. 72.1.8         10         0000.00C         APA         FastEthermet0/0           Tiererret. 72.1.8         10         0000.00C         APA         FastEthermet0/0           Tiererret. 72.1.8<	🗖 mac -	Notepad							J
Tereme 12.2.16         79         0004.004         APA A         FastEthermet00           Treeme 12.1.16         0         0002.551.         APA A         FastEthermet00           Treeme 12.1.16         19         4200.400.         APA A         FastEthermet00           Treeme 12.1.16         13         0002.551.         APA A         FastEthermet00           Treeme 12.1.16         13         0002.551.         APA A         FastEthermet00           Treeme 12.1.16         13         0002.551.         APA A         FastEthermet00           Treeme 12.1.16         10	File Edit	Format View Help							ľ
	File Edd The file Edd The rest The rest	Note-plot           Type         Jente           172, 115         Jente           172, 115         Jente           172, 116         Jente           172, 116<	727008100000091485712220301602305180102221522221220010112041121889112212224	0004, 00ef, 200 0004, 00ec, 200 0002, 5520, 2554, 200 0002, 5520, 200 0002, 5541, 200 0002, 5547, 200 0004, 4cc6, 200 0004, 4cc6, 200 0004, 4cc6, 200 0004, 4cc6, 200 0004, 4cc6, 200 0007, 0ec8, 200 0000, 4cc4, 200 0001, 0c7, 200 0001, 0	АКРРА ААКРА ААСРА ААКРА	FastEthernet0/0 FastEthernet0/	Cisco Access Point		
	<							2	and the

Netstumbler was also used to find rouge access points. As seen below, only the known access points were found.



*Pass:* The router tables were compared to the list of known access points. Only the MAC addresses of the two Cisco access points were found. Similar results were obtained using NetStumbler. Only the know Cisco access points were found

### A9.C9 – Verify admin access.

Admin access was verified with the configuration utility. The password procedure used by the access point administrators was also verified.

The figures below shows an admin user has been created on the access points.

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 8 da	ys, 11:33:12
	User N	ame	Write	SNMP	Ic	lent	Firmware	Admin
admin		x	x		x	x	x	
							Add	New User
	Ň							

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 28 da	ys, 02:48:08
-	User l	Name	Write	SNMP	I	dent	Firmware	Admin
	adr	nin	x	x		x	x	x
ryasta		sta	x	x		x	x	x
							Add	New User

Cisco 350 Series AP 11.06

Copyright 2000 Cisco Systems, Inc.

<u>credits</u>

AP350-4 User Manager Setu	CISCO SYSTEMS
Cisco 350 Series AP 11.06	باله باله
Map Help	Uptime: 28 days, 06:08:35
User Manager:	
Allow Read-Only Browsing without Login? Oves	e no
Protect Legal Credit Page? Oyes	Dno
(Apply)	OK Cancel Restore Defaults
[Map][Login][H	[elp]
AP120 User Manager Se	CISCO SYSTEMS
	ili ili
Cisco 1200 Series AP 11.56	••••••••••••••••••••••••••••••••••••••
Map Help User Manager: <ul> <li>Enabled</li> <li>Disabled</li> </ul>	Uptime: 8 days, 15:05:35
Allow Read-Only Browsing without Login? Oyes	⊙ no
Apply	OK Cancel Restore Defaults
[ <u>Map][Login</u>	][Help]
Cisco 1200 Series AP 11.56 © Copyright 2002 Cis	co Systems. Inc. credits

The above images show the user manager is enabled and login is required.

The procedure in place for password creation is using randpass.com. The Randpass web site is configured to produce a password of 8 alphanumeric characters containing special symbols. The site can be found at <u>www.randpass.com</u>.

**PASS:** The access points were found to require a login for admin access. The password procedure was also verified and the password criteria was found to follow the strength requirments

## A10.C18 – Verify SNMP configuration

SNMP configuration was verified with the configuration utility and also by performing port scans.

The image below shows SNMP is disabled on the Aironet 1200.

AP1200-b. ' SNMP	Setup CISCO SYSTEMS
Cisco 1200 Series AP 11.56	ي بينا البيب بينا البيب
Map Help	Uptime: 8 days, 11:31:29
Simple Network Management Prot	ocol (SNMP): OEnabled ODisabled
System Description:	Cisco 1200 Series AP 11.56
System Name: 💦	AP1200-L
System Location:	
System Contact:	Aironet Wireless Communications, I
SNMP Trap Destination:	
SNMP Trap Community:	
Browse Management Information Bas	Apply OK Cancel Restore Defaults

This image shows SNMP is disabled on the Aironet 350.

IP Ad	dress	Domain Name	T	ime	T	Ratio:Suc.	
172 16 251 228			1	53ms	63	3:100%	
172.16.251.230				196ms 63		3:100%	
N	2000-000-000-00 20				1.242	CTACK CTHENE (1997)	
4	6						
ort to H	lost 172 16 25	1 228					
Port	Protocol	Service(default)	Time	System T		Ratio:Suc	
23	TCP	Telnet	135ms	20:25:02		3:66%	
80	TCP	Http	180ms	20:25:15		3:100%	

IP Ad	dress	Domain Name	7	Fime	T	Ratio:Suc	
172.16.251.228			1	L53ms	63	3:100%	
172.1	6.251.230		1	196ms	63	3:100%	
Port to F	lost 172 16 2	51 230					_
Port	Protocol	Service(default)	Time	Syste	m T	Ratio:Suc	
23	TCP	Telnet	165ms	20:28	3:44	3:66%	
80	TCP	Http	190ms	20:28	3:58	3:100%	

Both access points were port scanned using the hostscan port scanner. The auditor obtained host scan at <u>http://www.cnetseek.com/eng/hostscan/index.html</u>. The entire local subnet was configured in the tool and scanned. The tool was set up to scan the well know port range. Both access points have only telnet and Http services enabled.

**PASS:** SNMP was found to be disabled in the configuration utility. The access points were port scanned using the Ostrosoft port scanner. The port scanner only found telnet and http open. Both ports are used for administration puposes.

## Measure Residual Risk

Even with all of the checklist steps complete there is still a certain amount of residual risk. Some of the risk is related to the ongoing revision and creation of wireless standards. There are also risks involved in the very security measures being put into place. Encryption is not unbreakable.

The highest residual risk exists in the broadcast of the wireless signal itself. As shown in audit step 7, the signal is currently being broadcast outside the perimeter of the building. Even with controls in place, an individual with a powerful antenna could intercept the signal.

A recommendation to mitigate some of the risk would be to first lower the power settings of the access point. Lowering the signal strength of the access points

may require the purchase of additional access points. Another recommendation would be to locate the Cisco Aironet 1200 in a more interior location in the building.

These changes would be at a minimal cost compared to the cost of data loss or interruption of the wireless network. The wireless networks primary use is in meeting rooms. The meeting rooms are primarily utilized for conferences and web conferences with customers and vendors. At less than \$1000 per access point, the cost to mitigate some of this risk is much lower than the potential interruption or loss of customer data.

## Is the System auditable?

The Cisco wireless access point is mostly auditable. Audit tools such as sniffers can be used as objective test of the WAP security. Most settings can be verified using the access point configuration utility and tools such as netstumbler, and a wireless sniffer. For this audit, the auditor had access to a LAN sniffer, and a wireless sniffer. The auditor used AiroPeek by WildPackets, which supports the Cisco Aironet pcmcia card.

Some of the steps to secure a Cisco WAP are subjective. Some subjective areas include signal strength. While signal strength is measurable with the Cisco client utilities, it may not possible to set at the recommended setting and remain usable.

The objective of this audit was to certify the security of the Cisco wireless access points. The system consists of laptops and PDAs that would also need to be audited.

## Audit Report

## **Executive Summary**

The wireless network at ABC Company was audited in the spring of 2003. The audit examined the risk and vulnerabilities involved when implementing and utilizing a wireless LAN. Below is a summary of findings.

- There is no written company policy regarding wireless networks FAIL
- SSID configuration was found to be of sufficient strength (2.1) **PASS**
- SSID broadcast is disabled PASS
- WEP has not been configured -FAIL
- MAC address filtering is being used and is configured properly PASS

- The current power settings broadcast the signal to unauthorized areas FAIL
- The current access point placement allows for the signal to be broadcast to unauthorized areas *FAIL*
- The default admin password has been changed to a password of sufficient strength – PASS
- The access points have been placed in an area the secures physical access
   *PASS*
- The wireless access points have been updated to the most current release of the software and firmware. All unnecessary services have been disabled. – PASS
- No rouge access points were found on the network PASS
- Access point default configurations have been changed PASS
- DHCP is disabled on the access point and it has been assigned a static IP address – PASS
- Strong authentication such as RADIUS is not being used FAIL
- Encryption beyond WEP is not being used. FAIL
- Access points are being turned off after business hours and weekends -PASS
- SNMP is disabled **PASS**
- A firewall between the LAN and access point is not being used FAIL
- The access points are configured on the default channel FAIL

The WLAN in use at ABC Company was found to have several weaknesses, which in turn expose ABC Company to several risks. These risks include unauthorized access to the corporate LAN, unauthorized use of the internet, data integrity, network disruption, and data loss. The risk could result in monetary loss.

The security weaknesses in the wireless network can mostly be attributed to the lack of written policies for wireless networks.

This audit process can also be used to audit wireless networks that are planned to be added in the coming year.

# Audit Findings

The audit examined the configuration of two wireless access point recently implemented on the corporate network. The IT Manager, Administrators, and IT Staff were interviewed on the current policies, and the configuration of the wireless access points. It was found the no policies or procedures were currently in place for the configuration of wireless networks.

The configuration of the wireless access points was also verified. By viewing the access point configuration, it was found that the default SSID was changed and a strong SSID was in place. The access points were also configured to not broadcast the SSID. It was also verified that encryption was not being utilized.

The auditor also examined signal strength and placement of the wireless access points. The auditor used the Cisco client utilities and a laptop to check signal strength in public areas and areas outside of the building. The auditor found that the Aironet 350 access point was placed in a location surrounded mostly by windows. The Aironet 1200 access point was placed in a location surrounded by cement walls. Both access points were also set at the highest signal strength. The auditor was able to detect a signal outside of the building at both the front and back entrances. The auditor was able to associate with the Aironet 350 access the street in the employee parking lot, and also on the south and west streets. These strength settings coupled with the access point placement create a high risk of an unauthorized individual associating with the access point.

## Background/risk

There were a number of audit findings with a rating of fail. The first item with significant risk is the lack of a written policy on wireless network. The absence of this policy makes the audit steps and recommendations unenforceable. The audit also shows WEP is not in use. Without the utilization of WEP, any individual with a piece of software such as netstumbler or a wireless sniffer can easily gain access to the network. A strong authentication such as RADIUS is also not in use. The lack of both WEP and strong authentication make it fairly easy to gain access to the access points. At this point, only a MAC address and the correct SSID are needed to gain access to the access point. Both of these are obtainable with a sniffer.

Another component that was found to be unsatisfactory is signal strength. Currently the power settings and access point placement are allowing the signal to be broadcast outside of the building. This opens a high risk to an individual outside the building to attempt to gain access.

### Audit Recommendations

First, a clearly written policy that addresses wireless needs to be developed. From the policies, procedures should be written on configuration and operation of the wireless access points. Administrators who will be involved in the setup access points should receive training on the policies and procedures.

ABC Company should consider moving the access point to a more interior location. The access points could then be adjusted to broadcast to the windows and not past. Also, the company should consider installing additional access

points. This would allow for better placement of the access points and the ability to set the signal strength at a lower level. If access point placement next to the glass portion of the building is necessary, the access point should be set at the lowest level.

Encryption should be used on the wireless networks. WEP should be configured at the very least and a VPN solution should be considered.

ABC Company should also consider an implementation of RADIUS authentication. This would ensure only authenticated users could associate to the access point.

## Costs

Additional access points would be the majority of the costs involved. A Cisco Aironet 350 costs less that \$1000. ABC Company would require at least one additional access point, one more would be recommended.

Other recommendation would only require configuration of the access points and time. Configuration of WEP would take about two days. The implementation of additional access points and adjusting the signal strength accordingly on the existing access point would take about 4 days.

Policies and Procedures could be written in less than 2 weeks.

## Compensating Controls

If ABC Company decides not to purchase additional access points, implementing WEP and moving the access points can mitigate some of the risk. SSID configuration is in place as well as MAC address filtering. The addition of WEP would put another control on top of what is already in place making it difficult to associate with the access points without those three pieces of information (WEP key, SSID, and correct MAC address). Moving the access points to a more interior location would also help to mitigate some of the risk with no additional cost.

Informal verbal procedures within the IT department may somewhat compensate for the lack of formal policy. There are no other compensating controls for the lack of written policy and procedures.

## References

Loomis, Angela, "Auditing the Wireless environment: A mobile wireless LAN used for training in multiple sites on a corporate WAN- An Auditor's perspective", September 2002

Convery, Sean and Darrin Miller. "SAFE: Wireless LAN Security in Depth" undated Cisco white paper. 8/2002 URL: <u>http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl\_wp.htm</u>

Ellison, Craig, "Exploiting and Protecting 802.11b Wireless Networks", September 2001 URL: <u>http://www.extremetech.com/article2/0,3973,11400,00.asp</u>

"Cisco Aironet Wireless LAN Security Overview" undated white paper 8/2002. URL: <u>http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w\_ov.htm</u>

"Best Practices for wireless fidelity (802.11b) Network Vulnerabilities", National Infrastructure Protection Center. URL: <u>http://www.nipc.gov/publications/nipcpub/bestpract.html</u>

Special Publication 800-48, National Institute of Standards and Technology, July 2002. (August 2002) URL: <a href="http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf">http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf</a>