



# Airspace Risk Assessment

For: ABC

From: Apr 14, 2008 10:54 AM

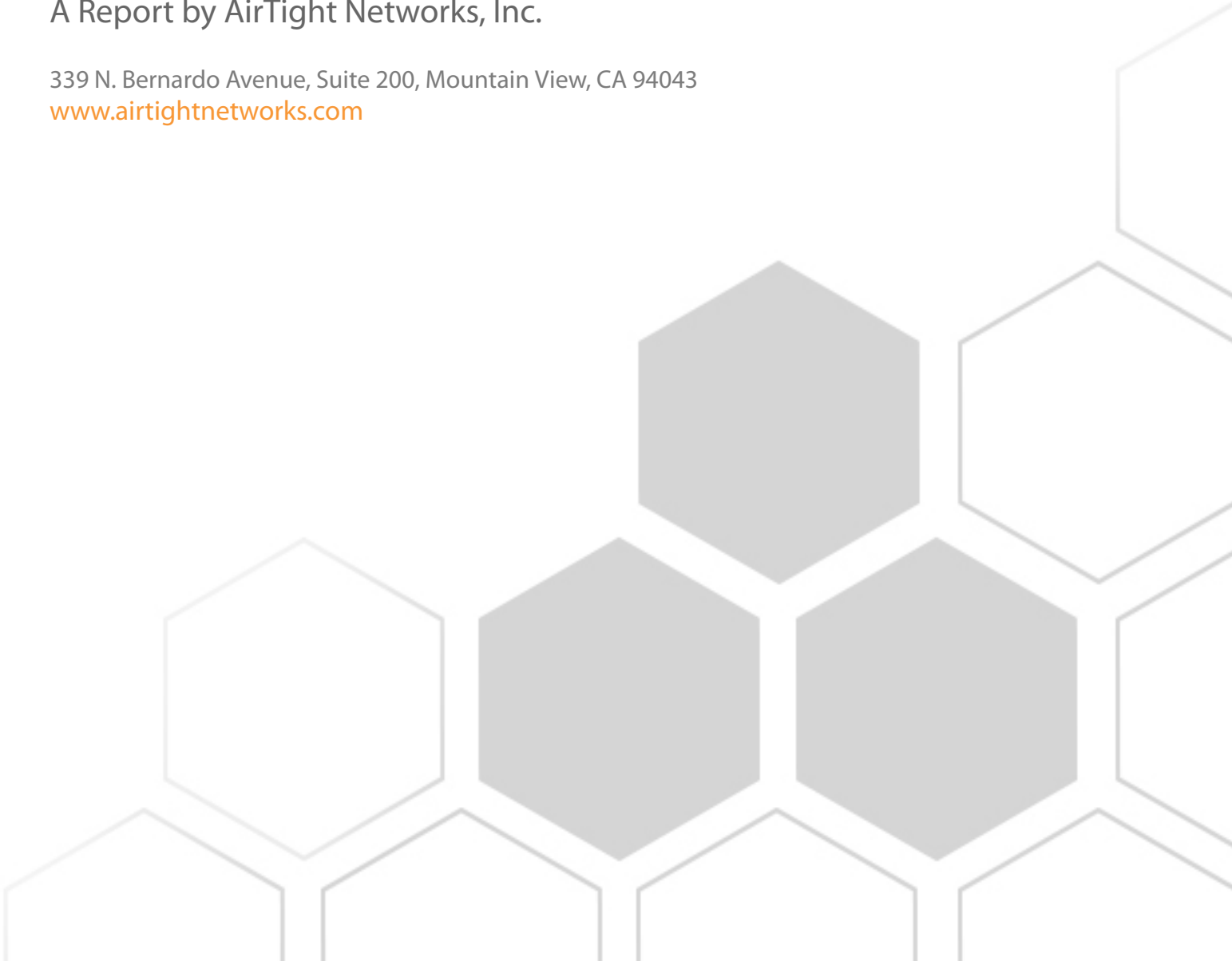
To: Apr 14, 2008 2:54 PM

Location: \\ABC Corp

A Report by AirTight Networks, Inc.

339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043

[www.airtightnetworks.com](http://www.airtightnetworks.com)



# Table of Contents

- About This Report**.....3
- Result Summary**.....4
- Recommended Actions**.....6
- Detailed Results**.....8
  - Critical Vulnerabilities.....8
  - High Severity Vulnerabilities.....9
  - Medium Severity Vulnerabilities.....10
  - Low Severity Vulnerabilities.....11
  - Probable Vulnerabilities.....12
- Appendix A: List of Detected Access Points**..... 14
- Appendix B: List of Detected Clients**..... 15
- Appendix C: List of Wireless Scanners**..... 17
- Appendix D: Severity of Vulnerabilities**..... 18








## About This Report

This report is the first step towards wireless vulnerability assessment of your network and managing its wireless security posture. The report gives you visibility into your airspace in terms of the number and type of wireless devices in your environment, and records the presence of vulnerabilities and potential threats to your network. Vulnerabilities are classified and ranked in terms of their severity and urgency of response.

The crucial next step is to identify your networks and classify your authorized WiFi devices. The context of which networks and devices are yours will allow the system to identify vulnerabilities and threats more accurately in the future, and recommend most suitable remedial actions for improving your network's wireless security posture.

The results in this report are based on your airspace scanned using AirTight Networks' pre-configured wireless scanners. Wireless vulnerability assessment is done by comparing the scanned data with an up-to-date vulnerability database maintained by AirTight Networks. The Common Vulnerability Scoring System (CVSS) standard has been adapted to assess wireless vulnerabilities. The table below classifies vulnerabilities based on their severity and urgency of response. A detailed description of each severity level is given in Appendix D.





Severity	Type	Description
 5	Critical	<b>Security breach or wireless malpractice detected!</b> An intruder may have entered your network; sensitive data is exposed; or your users are bypassing your security policy control (e.g., firewalls, and URL, spam, and malware filters).
 4	High	Known vulnerabilities those ignore basic security measures and naturally expose your network and data assets even to inadvertent unauthorized access.
 3	Medium	Vulnerabilities that violate best practices and can lead to unauthorized usage of your network resources or hackers with medium expertise and knowledge of published exploits can exploit these vulnerabilities in minutes.
 2	Low	Hackers can collect information about your network and may use it to discover other vulnerabilities; high expertise needed to exploit these vulnerabilities.
 1	Probable	Potential vulnerabilities that may pose a threat.

### NOTE:

You should not ignore vulnerabilities with severity levels 3, 4, and 5 in your airspace. We highly recommend that appropriate remedial action be taken to protect your network and data assets against these threats. Compliance to legislative regulations may require you to also address severity level 2 vulnerabilities.

## Result Summary

**Vulnerabilities Total: 16 Overall Security Risk:**  **5 Status: Critical**

Severity Level	Count of Vulnerabilities
 5	4
 4	6
 3	5
 2	1

### Wireless Scanners Summary

Total number of wireless scanners: 2  
 Approximate area scanned for wireless vulnerabilities: 40000 sq. ft  
 Add more scanners for covering additional airspace if necessary.

### Wireless Devices Summary

Total number of access points (APs) detected: 17  
 Total number of clients detected: 45  
 NOTE: A detailed list of all detected wireless devices is shown in the Appendices.

### Categorized Vulnerabilities Summary

**Severity Level:**  **5 Type: Critical Vulnerabilities: 4**

Vulnerabilities	Count
WEP Connections	2
Ad-hoc Network	2

**Severity Level:**  **4 Type: High Vulnerabilities: 6**

Vulnerabilities	Count
Open Access Points	6

**Severity Level:**  **3** **Type:** Medium **Vulnerabilities:** 5

Vulnerabilities	Count
WEP Access Points	5

**Severity Level:**  **2** **Type:** Low **Vulnerabilities:** 1

Vulnerabilities	Count
Access Points using Vulnerable SSID	1

**Severity Level:**  **1** **Type:** Probable **Vulnerabilities:** 0

*Vulnerabilities with Severity Level 1 were not found.*

---

## Recommended Actions

Following this report, it is crucial that you identify your networks, classify your authorized wireless devices, and define your wireless usage and security policies so that:

- Wireless vulnerabilities (e.g., rogue devices, unprotected authorized WLAN, misconfigured authorized devices) can be identified;
- Wireless security attacks or malpractices (e.g., MAC spoofing, honeypots, , misbehaving authorized clients) on your network can be detected; and
- The overall security posture of your network can be determined.

Network identification involves identifying a range of IP addresses that comprise your corporate network and identifying the SSIDs of your authorized WLANs.

Classification of your authorized access points provides the system with a baseline with which it can automatically classify the remaining access points and clients.

Policies for WLAN usage and security allow the system to identify misconfigured devices or malpractices that violate corporate policies. For instance, if you have a “no WiFi” policy, then the system can help enforce the policy on your authorized devices.

If all the expected wireless devices in your airspace were not discovered, you should consider increasing the wireless scanning coverage by adding more wireless scanners. Adding more scanners may help the system to discover and classify wireless devices more accurately as they occur in your airspace.

Once your authorized wireless devices have been classified, you should schedule a wireless vulnerability assessment report to determine your network’s overall wireless security risk, and to learn about remedial actions for improving your network’s wireless security posture.



Detailed Results

## Detailed Results

### Severity 5 Vulnerabilities

Severity Level:  5      Type: Critical      Vulnerabilities: 4

#### WEP Connections

Count: 2

**Threat:** WEP gives a false sense of security. WEP can be easily cracked and your sensitive data can be stolen over-the-air if your authorized clients and APs are using WEP.

Device(s) Involved:

Location	MAC Address	SSID
ABC Corp	00:12:F0:AC:AC:CF	Netgear102
ABC Corp	00:13:CE:86:79:49	Elektra

#### Ad-hoc Networks

Count: 2

**Threat:** If your authorized clients are directly connecting to unauthorized clients, then it is a major security threat; such connections open a backdoor to your network and your authorized devices can be infected with viral SSIDs. Ad-hoc connections even between authorized clients should be discouraged as these connections can bypass your corporate security policies.

Device(s) Involved:

Location	MAC Address	SSID
ABC Corp	00:13:CE:25:B8:48	Free Public Wi-Fi
ABC Corp	00:18:39:01:4C:18	Click

## Severity 4 Vulnerabilities

Severity Level:  4      Type: High      Vulnerabilities: 6

### Open Access Points

Count: 6

**Threat:** Installing APs without any security is a severe violation of WLAN best practices. An open AP is a backdoor through which malicious users can enter the network to which it is connected, eavesdrop on over-the-air data, or conduct illegal activities which may entail liability to the owner of the network. Open APs not only compromise the security of your entire network, but open your network to even inadvertent, unauthorized usage.

Device(s) Involved:

Location	MAC Address	Protocol	SSID
ABC Corp	00:11:95:18:1A:AF	802.11b/g	Malice
ABC Corp	00:11:95:53:4E:65	802.11b/g	default
ABC Corp	00:11:95:53:4E:67	802.11a	dlink11a
ABC Corp	00:15:E9:61:63:CA	802.11b/g	Carib4
ABC Corp	00:19:5B:8C:A8:0C	802.11b/g	Loop-Guest
ABC Corp	00:1E:58:23:BF:27	802.11b/g	blueguest

## Severity 3 Vulnerabilities

Severity Level:  3

Type: Medium

Vulnerabilities: 5

**WEP Access Points**

Count: 5

**Threat:** It is well known that the Wired Equivalent Privacy (WEP) encryption is broken. If you own WEP APs and clients, you are exposed to WEP cracking attacks allowing a hacker to steal sensitive data and possibly to enter your corporate network. Café Latte attack can allow a hacker to take complete control of your WEP laptops and handheld devices even when they are not connected.

Device(s) Involved:

Location	MAC Address	Protocol	SSID
ABC Corp	00:09:5B:FD:73:30	802.11b/g	Alice
ABC Corp	00:0D:0B:2B:0C:1B	802.11b/g	Elektra
ABC Corp	00:11:24:A6:B1:1C	802.11b/g	Virus
ABC Corp	00:11:93:34:BE:90	802.11b/g	Netgear102
ABC Corp	00:40:05:BE:CC:17	802.11b/g	dlink614

## Severity 2 Vulnerabilities

Severity Level:  2

Type: Low

Vulnerabilities: 1

### Access Points using Vulnerable SSID

Count: 1

**Threat:** If your authorized AP is using a commonly used (e.g., factory-default) SSID, it is more likely to attract attention from hackers or inadvertently from outsiders, with their devices usually probing for these SSIDs.

Device(s) Involved:

Location	MAC Address	Protocol	SSID	Security
ABC Corp	00:11:95:53:4E:65	802.11b/g	default	Open

## Severity 1 Vulnerabilities

---

Severity Level:  1

Type: Probable

Vulnerabilities: 0

*Vulnerabilities with severity level 1 were not found.*

## Appendices

## List of Detected Access Points

This is a list of wireless access points (APs) that were detected in your airspace during the reporting interval. Use this AP inventory to quickly gauge the volume and type of wireless deployment in your airspace (e.g., security, SSID, protocol, vendors), identify your authorized APs, and verify if the wireless scanners detected all your authorized APs. If all expected APs are not listed here, then you should consider placing additional wireless scanners for covering more airspace. If you have not officially deployed any APs, then this list essentially represents potential risks from non-authorized APs (e.g., rogue APs) in your airspace.

Location	MAC Address	Protocol	SSID	Security	Vendor
ABC Corp	00:09:5B:FD:73:30	802.11b/g	Alice	WEP	Netgear
ABC Corp	00:0D:0B:2B:0C:1B	802.11b/g	Elektra	WEP	Buffalo
ABC Corp	00:0D:97:04:83:AD	802.11b/g		Unknown	Tropos
ABC Corp	00:0D:97:04:84:5E	802.11b only		Unknown	Tropos
ABC Corp	00:11:24:A6:B1:1C	802.11b/g	Virus	WEP	Apple
ABC Corp	00:11:93:34:BE:90	802.11b/g	Netgear102	WEP	Cisco
ABC Corp	00:11:95:18:1A:AF	802.11b/g	Malice	Open	D-Link
ABC Corp	00:11:95:53:4E:65	802.11b/g	default	Open	D-Link
ABC Corp	00:11:95:53:4E:67	802.11a	dlink11a	Open	D-Link
ABC Corp	00:11:95:E0:F2:D0	802.11a	blueneta	802.11i	D-Link
ABC Corp	00:11:95:E0:F2:D8	802.11b/g	bluenetg	802.11i	D-Link
ABC Corp	00:15:E9:61:63:CA	802.11b/g	Carib4	Open	D-Link
ABC Corp	00:19:5B:8C:A8:0C	802.11b/g	Load-Guest	Open	D-Link
ABC Corp	00:1E:58:23:BF:27	802.11b/g	blueguest	Open	Unknown
ABC Corp	00:20:A6:53:4D:1B	802.11a	rnow	802.11i	Proxim
ABC Corp	00:20:A6:53:4D:1C	802.11b/g	rnow	802.11i	Proxim
ABC Corp	00:40:05:BE:CC:17	802.11b/g	dlink614	WEP	Unknown

## List of Detected Clients

This is a list of active wireless clients that were detected in your airspace during the reporting interval. Use this client inventory to quickly verify if all expected clients were detected. If you have a “no-WiFi” policy, then this list essentially represents potential risks from non-authorized clients as well as authorized clients that may be violating the no-WiFi policy.

Location	MAC Address	Vendor
ABC Corp	00:05:4E:4D:49:2F	Philips
ABC Corp	00:0E:35:52:C6:CC	Intel
ABC Corp	00:0E:35:E1:40:46	Intel
ABC Corp	00:0E:35:FF:54:DF	Intel
ABC Corp	00:12:17:78:FF:D2	Cisco-Linksys
ABC Corp	00:12:F0:7E:7D:73	Intel
ABC Corp	00:12:F0:AC:AC:CF	Intel
ABC Corp	00:13:02:2B:EC:05	Intel
ABC Corp	00:13:CE:25:AD:63	Intel
ABC Corp	00:13:CE:25:B8:48	Intel
ABC Corp	00:13:CE:29:F0:3E	Intel
ABC Corp	00:13:CE:3F:67:1E	Intel
ABC Corp	00:13:CE:79:10:13	Intel
ABC Corp	00:13:CE:82:50:10	Intel
ABC Corp	00:13:CE:86:79:49	Intel
ABC Corp	00:13:E8:1E:E0:19	Intel
ABC Corp	00:16:44:9D:7F:82	Unknown
ABC Corp	00:16:44:9E:AC:17	Unknown
ABC Corp	00:16:6F:09:CF:3C	Intel
ABC Corp	00:16:6F:6D:43:E2	Intel
ABC Corp	00:16:6F:6F:25:B6	Intel
ABC Corp	00:16:6F:79:4C:84	Intel
ABC Corp	00:16:6F:95:B6:65	Intel
ABC Corp	00:16:CF:63:30:A4	Unknown
ABC Corp	00:17:F2:3F:AE:5D	Apple
ABC Corp	00:18:39:01:4C:18	Cisco-Linksys
ABC Corp	00:18:DE:45:9F:48	Intel
ABC Corp	00:19:7D:A7:E7:72	Unknown
ABC Corp	00:19:7E:4D:FC:DE	Unknown
ABC Corp	00:19:D2:6D:3E:AF	Intel
ABC Corp	00:19:D2:92:09:26	Intel
ABC Corp	00:19:D2:92:0B:A6	Intel

Location	MAC Address	Vendor
ABC Corp	00:1A:92:B1:F3:B8	Unknown
ABC Corp	00:1B:77:28:E5:C1	Intel
ABC Corp	00:1B:77:81:29:5A	Intel
ABC Corp	00:1B:77:81:47:9C	Intel
ABC Corp	00:1B:77:A3:A6:6E	Intel
ABC Corp	00:1B:77:A4:A8:7A	Intel
ABC Corp	00:1B:77:D1:28:1C	Intel
ABC Corp	00:1D:4F:EB:0A:83	Unknown
ABC Corp	00:1F:3A:12:D3:41	Unknown
ABC Corp	00:1F:3A:1F:01:3D	Unknown
ABC Corp	00:1F:3A:4C:5F:4F	Unknown
ABC Corp	00:1F:3A:4C:5F:58	Unknown
ABC Corp	00:1F:3A:4C:64:64	Unknown






---

## List of Wireless Scanners

This is a list of wireless scanners that were connected to the server during the reporting interval. Verify if all deployed wireless scanners are listed.

Location	Device Name	MAC Address	IP Address
ABC Corp	AirTight_00:6D:90	00:11:74:00:6D:90	192.168.201.74
ABC Corp	AirTight_10:84:F4	00:11:74:10:84:F4	192.168.201.84

## Severity of Vulnerabilities

Severity	Type	Description
 5	Critical	<b>Wireless malpractice detected!</b>
 4	High	Known vulnerabilities those ignore basic security measures and can naturally expose your network and data assets even to inadvertent unauthorized access.
 3	Medium	Vulnerabilities that violate best practices and can lead to unauthorized usage of network resources or hackers with medium expertise and knowledge of published exploits can exploit these vulnerabilities in minutes.
 2	Low	Hackers may be able to collect information about your network and may use it to discover other vulnerabilities; high expertise needed to exploit these vulnerabilities.
 1	Probable	Potential vulnerabilities that may pose a threat.

**Critical severity:** Occurrence of a critical severity demands your urgent attention. It is raised when malpractices in wireless usage or anomalous activities are detected in your airspace. If these vulnerabilities involve your network, then your entire network's security is potentially at risk. Examples are use of unprotected wireless access and ad-hoc networks. Specific attacks (e.g., MAC spoofing, honeypot attack, misbehaving clients, unauthorized connections) in this category can be accurately detected only after your network and devices are identified.

**High severity:** Ignoring basics of wireless security (e.g., installing open APs) leads to these vulnerabilities that can give outsiders easy access to the network in question and a security breach is imminent; deliberate effort to hack into the network is not necessary. Vulnerabilities relevant to your network (e.g., rogue APs, your devices operating in ad hoc mode) can be accurately detected only after your network and devices are classified.

**Medium severity:** Violating WLAN best practices usually results in these vulnerabilities (e.g., using the broken Wired Equivalent Privacy (WEP) encryption standard, and lack of policies to control how and to which WLANs your WiFi clients can connect). If these vulnerabilities occur in your network, then hackers can break through these weak security settings, or lure users to connect to them (e.g., honeypots) gaining access to sensitive data or backdoor entry into your network.

**Low severity:** If these vulnerabilities occur in your network then they can leak information about your WLAN configuration and attract unwarranted attention from outsiders to your network. Hackers can use such information to discover and exploit other vulnerabilities in your network. If these vulnerabilities occur in your airspace they can attract your users to connect to external WLANs, e.g., APs using vulnerable or hotspot SSIDs.

**Probable:** These are potential vulnerabilities that may pose limited threat to security or performance of a WLAN. You should manually verify the existence and credibility of these probable threats. For instance: an extraordinary number of wireless frame errors indicate a potential jamming attack or inadvertent interference from another RF source; a large number of broadcast messages indicate a potential attack or misconfiguration.