802.11 Wireless Security Vulnerability Assessment Report

from 2009-08-31 14:06:32 to 2009-09-01 14:06:32

System Name: AirDefense
Domain: System
Generated: 2009-09-01 14:07:44
Version: 7.3.3-12
Time Zone: EDT - Eastern Daylight Time

Rogue Activity Threat

Rogue Access Points:	2
Unauthorized APs:	169
Rogue Stations:	13
Unauthorized Stations:	127

Misconfiguration Threat

APs Broadcasting SSID:	3
APs using Weak Authentication:	8
APs using Weak Encryption:	7
APs using Incorrect Data Rates:	0
APs Changing ESSIDs:	0
APs Using Unauthorized Channels:	0
AP Using Default Settings:	0

Wireless Station Threat

Ad-Hoc Stations:	2
Accidental Associations:	0
Roaming Violations:	0
Probing Stations	251

Intrusion Threat

Identity Theft Attacks:	0
Reconnaissance Activity	2
Authentication Failures	0
Active Stations on Watch List	0
Denial of Service Attacks	0
Soft APs:	1
After Hours Activity:	0

Wired Leakage

Multicast Network Protocols	0
Unknown Wired Stations	0

Rogue Activity

These are devices that the AirDefense system has definitively determined to be connected to your wired network. These are the most dangerous of all rogue devices because they are exposing your network to the outside world and potentially are not following your security standards to guard against intrusions.

Rogue Access Points (Latest 50 Seen)

Rogue Devices Connected to the Network	2

Device	AP MAC	SSID	Signal Strength	Start Time	Location	Group
Symbol:d0:1f:98[a]	00:15:70:d0:1f:98	AM-Wireless	-76	8/31/09 3:32 AM	Atlanta, GA Office	1st Floor
Symbol:d0:25:a8[b,g]	00:15:70:d0:25:a8	AM-Wireless	-71	8/5/09 7:13 PM	Atlanta, GA Office	1st Floor

Rogue Stations (Latest 50 Seen)

Rogue Stations: 13

Device	SSID	AP	Signal Strength	Start Time	Sensor
Intel:07:00:58[a,b,g]	M-Wireless	Symbol:50:1f:40[a,g]	-63	8/31/09 6:58 PM	AP300-SensorLab[a,b,g]
Nathan Station[a,b,g]	M-Wireless		-65	8/31/09 12:04 PM	AP300-SensorLab[a,b,g]
Asustek:de:d2:45[a,b,g]	AM-Wireless	Symbol:d0:25:a8[b,g]	-60	8/31/09 10:51 AM	AP300-SensorLab[a,b,g]
Hon:c1:cc:c8[a,b,g]	M-Wireless	Symbol:4f:e4:80[a,b,g]	-59	8/31/09 10:36 AM	AP300-SensorLab[a,b,g]
Intel:0f:63:c0[a,b,g]	M-Wireless	Symbol:50:1f:40[a,g]	-61	8/31/09 10:19 AM	AP300-SensorLab[a,b,g]
Intel:07:88:2c[a,b,g]	M-Wireless	Symbol:4f:de:64[a,g]	-64	8/31/09 10:08 AM	AP300-SensorLab[a,b,g]
Intel:07:00:6c[a,b,g]	M-Wireless	Symbol:50:1f:40[a,g]	-69	8/31/09 10:01 AM	AP300-SensorLab[a,b,g]
Intel:07:c0:40[a,b,g]	M-Wireless	Symbol:4f:de:64[a,g]	-53	8/31/09 9:29 AM	AP300-SensorLab[a,b,g]
Gemtek:d8:0f:ff[a,b,g]	M-Wireless	Symbol:50:1f:40[a,g]	-82	8/31/09 9:08 AM	AP300-SensorLab[a,b,g]
Hon:4c:4e:1b[a,b,g]	M-Wireless	Symbol:4f:e4:80[a,b,g]	-58	8/31/09 8:08 AM	AP300-SensorLab[a,b,g]
Hon:b3:98:09[a,b,g]	M-Wireless	Symbol:50:1e:54[a,b,g]	-67	8/26/09 9:27 AM	AP300-SensorLab[a,b,g]
Intel:07:ae:1e[a,b,g]	M-Wireless	Symbol:50:1f:40[a,g]	-50	8/24/09 10:19 AM	AP300-SensorLab[a,b,g]
Nintendo:f1:f2:64[b,g]	ralphsnart	Belkin:c2:ff:c3[b,g]	-47	8/11/09 7:21 PM	Raggo_M520[a,b,g]

Wireless Station Threat

This section details the specific threats associated with Stations that have been detected in your wireless LAN. Wireless stations are a key component of the WLAN and can create numerous vulnerabilities by associating to the incorrect Access Points either via Accidental, Malicious, unauthorized Roaming or Ad-Hoc connections. Stations need to be viewed as potential entry points into your network and thus need to be analyzed appropriately to ensure there are not vulnerabilities.

Ad-Hoc Stations (Latest 50 Seen)

These are stations that the AirDefense system has determined to be either looking to form an Ad-Hoc network or are actively participating in an Ad-Hoc network. Ad-Hoc networks pose a significant threat to the security of your network. These inherently insecure connections allow malicious users to be able to sniff or worse join the network and potentially breach the security of your network.

Ad-Hoc Stations: 0

Device	Device MAC	SSID	Channel	Signal Strength	Location	Group

Accidental Association (Latest 50 Seen)

These are authorized stations that the AirDefense system has determined to have connected to Access Points which are not authorized in your system. An Accidental association can either be non-malicious - where a user connects to a neighboring Access Point unintentionally, or it can be malicious - where a hacker lures your authorized user to connect to their Access Point in order to compromise the security of your network. Knowing about these unauthorized connections in your WLAN and taking protective action such as Terminating the connection over the air can help prevent security breach in your network.

Accidental Associations: 0

Device	Device MAC	SSID	Channel	Signal Strength	Location	Group

Stations with Roaming Violations (Latest 50 Seen)

These are authorized stations that the AirDefense system has determined to have connected to authorized Access Points but are not allowed by policy to roam to those Access Points. This can happen if the Wireless Infrastructure uses the same credential information across the WLAN but the users are supposed to use wireless in their own departments, buildings etc. This is not a major threat, but points to potential internal activity that is out of the room.

Stations with Roaming Violations: 0

Device	SSID	Channel	Signal Strength	Location	Group

Probing Stations (Latest 50 Seen)

These are stations that the AirDefense system has determined to be active and Probing to connect non standard wireless Networks. As part of the 802.11 protocol wireless stations which are active and unconnected always send out Probe requests for their preferred networks hoping to establish connectivity to the WLAN. These probing stations can be phished by hackers by masquerading as the legitimate AP with the appropriate SSID. This situation can be huge vulnerability if the station is connected on the wired side and can be potentially bridging the wireless network to the internal wired network.

Stations Probing 251

Station	Station MAC	ESSID	Last Seen	Average Signal Strength	Location	Group
Intel:8e:9b:90[a,b,g]	00:16:ea:8e:9b:90	WXYZ	9/1/09 2:05 PM	-73	Atlanta, GA Office	1st Floor
Symbol:6a:00:dd[b]	00:a0:f8:6a:00:dd	KO	9/1/09 2:05 PM	-85	Atlanta, GA Office	1st Floor
Juniper:a0:3c:ea[a,b,g]	00:12:1e:a0:3c:ea		9/1/09 2:05 PM	0	Atlanta, GA Office	1st Floor
Intel:07:c0:40[a,b,g]	00:21:6a:07:c0:40	Symbol5100	9/1/09 2:05 PM	-53	Atlanta, GA Office	1st Floor
Intel:07:ae:34[a,b,g]	00:21:6a:07:ae:34	MZ7131_3R_CB1	9/1/09 2:05 PM	-41	Atlanta, GA Office	1st Floor
Apple:2a:49:3a[a,b,g]	00:25:4b:2a:49:3a	Conference 1125	9/1/09 2:05 PM	-77	Atlanta, GA Office	1st Floor
Intel:07:65:f4[a,b,g]	00:21:6a:07:65:f4	SUNNY	9/1/09 2:05 PM	-65	Atlanta, GA Office	1st Floor
Gemtek:ee:4f:8b[b]	00:21:00:ee:4f:8b		9/1/09 2:05 PM	-91	Auburn, GA	Auburn
Smc:3e:14:a0[a,b]	00:13:f7:3e:14:a0		9/1/09 2:05 PM	-78	Atlanta, GA Office	1st Floor
Intel:66:1e:37[a,b,g]	00:1d:e0:66:1e:37	A-MSFTWLAN	9/1/09 2:05 PM	-54	Atlanta, GA Office	1st Floor
Intel:03:fb:2d[a,b,g]	00:1f:3b:03:fb:2d	A-MSFTWLAN	9/1/09 2:05 PM	-57	Atlanta, GA Office	1st Floor
Intel:07:00:6c[a,b,g]	00:21:6a:07:00:6c	M-Wireless	9/1/09 2:05 PM	-69	Atlanta, GA Office	1st Floor
Intel:07:ae:1e[a,b,g]	00:21:6a:07:ae:1e	M-Wireless	9/1/09 2:05 PM	-50	Atlanta, GA Office	1st Floor
Intel:05:bd:30[a,b,g]	00:21:6a:05:bd:30	SukiPrasad	9/1/09 2:04 PM	-70	Atlanta, GA Office	1st Floor
Senao:43:f8:52[a,b,g]	00:02:6f:43:f8:52		9/1/09 2:04 PM	-58	Atlanta, GA Office	1st Floor
Cisco-linksys:ff:c8:e8[a,b,g]	00:1e:e5:ff:c8:e8	FK_1200_b	9/1/09 2:04 PM	-53	Atlanta, GA Office	1st Floor
Intel:11:26:a4[a,b,g]	00:1b:77:11:26:a4	A-MSFTWLAN	9/1/09 2:04 PM	-57	Atlanta, GA Office	1st Floor

Station	Station MAC	ESSID	Last Seen	Average Signal Strength	Location	Group
Intel:b8:45:00[a,b]	00:13:02:b8:45:00	A-MSFTWLAN	9/1/09 2:04 PM	-73	Atlanta, GA Office	1st Floor
Intel:8e:fe:86[a,b,g]	00:16:ea:8e:fe:86	M-Wireless	9/1/09 2:04 PM	-68	Atlanta, GA Office	1st Floor
Intel:3a:a0:78[a,b,g]	00:21:6a:3a:a0:78	M-Wireless	9/1/09 2:04 PM	-82	Atlanta, GA Office	1st Floor
Nathan Station[a,b,g]	00:19:d2:49:46:c8	M-Wireless	9/1/09 2:04 PM	-66	Atlanta, GA Office	1st Floor
Intel:af:fa:6d[a,b]	00:1f:3b:af:fa:6d		9/1/09 2:04 PM	0	Atlanta, GA Office	1st Floor
Intel:48:a7:58[a,b]	00:21:6a:48:a7:58	A-MSFTWLAN	9/1/09 2:04 PM	-79	Atlanta, GA Office	1st Floor
Intel:5a:ac:39[a,b]	00:1f:3b:5a:ac:39		9/1/09 2:04 PM	0	Atlanta, GA Office	1st Floor
Intel:c4:51:13[a,b,g]	00:d0:b7:c4:51:13	M-Wireless	9/1/09 2:04 PM	-57	Atlanta, GA Office	1st Floor
Intel:8e:66:86[a,b,g]	00:16:ea:8e:66:86	M-Wireless	9/1/09 2:03 PM	-73	Atlanta, GA Office	1st Floor
Symbol:c8:16:d0[b]	00:15:70:c8:16:d0	FK_MESH	9/1/09 2:03 PM	-78	Atlanta, GA Office	1st Floor
Intel:bb:78:3b[a,b,g]	00:19:d2:bb:78:3b	M-Wireless	9/1/09 2:03 PM	-72	Atlanta, GA Office	1st Floor
Intel:85:4d:16[a,b,g]	00:19:d2:85:4d:16	ARCHPRIV	9/1/09 2:03 PM	-81	Atlanta, GA Office	1st Floor
Intel:8d:76:ec[a,b,g]	00:16:ea:8d:76:ec		9/1/09 2:03 PM	0	Atlanta, GA Office	1st Floor
Intel:55:86:2f[a,b]	00:1d:e0:55:86:2f		9/1/09 2:02 PM	-77	Atlanta, GA Office	1st Floor
Intel:af:e4:fb[a,b,g]	00:1f:3b:af:e4:fb	A-MSFTWLAN	9/1/09 2:02 PM	-52	Atlanta, GA Office	1st Floor
Symbol:e0:db:c2[a,b]	00:15:70:e0:db:c2	RADNet	9/1/09 2:01 PM	-53	Atlanta, GA Office	1st Floor
Wistron:d9:30:24[a,b]	00:0b:6b:d9:30:24		9/1/09 2:00 PM	-83	Atlanta, GA Office	1st Floor
Intel:17:97:be[a,b]	00:21:6a:17:97:be		9/1/09 2:00 PM	-70	Atlanta, GA Office	1st Floor
Intel:59:e6:f5[a,b]	00:1d:e0:59:e6:f5	A-MSFTWLAN	9/1/09 2:00 PM	-82	Atlanta, GA Office	1st Floor
Gemtek:13:b1:1e[a]	00:21:00:13:b1:1e		9/1/09 2:00 PM	-42	Atlanta, GA Office	1st Floor
Intel:1c:e5:34[a,b]	00:1b:77:1c:e5:34		9/1/09 2:00 PM	0	Atlanta, GA Office	1st Floor
Intel:af:fe:bf[a,b]	00:1f:3b:af:fe:bf		9/1/09 2:00 PM	0	Atlanta, GA Office	1st Floor
Intel:24:f5:2e[a,b]	00:13:02:24:f5:2e	ARCHPRIV	9/1/09 2:00 PM	-80	Atlanta, GA Office	1st Floor
Askey:16:48:af[a,b,g]	00:11:f5:16:48:af	QAFREE	9/1/09 1:59 PM	-84	Atlanta, GA Office	1st Floor
Intel:53:c5:0d[a,b,g]	00:21:5c:53:c5:0d	A-MSFTWLAN	9/1/09 1:59 PM	-78	Atlanta, GA Office	1st Floor
Intel:29:43:de[a,b]	00:21:6a:29:43:de	A-MSFTWLAN	9/1/09 1:59 PM	-79	Atlanta, GA Office	1st Floor
Intel:07:00:58[a,b,g]	00:21:6a:07:00:58	M-Wireless	9/1/09 1:58 PM	-63	Atlanta, GA Office	1st Floor
Intel:50:e7:e7[a,b,g]	00:21:5c:50:e7:e7	A-MSFTWLAN	9/1/09 1:58 PM	-54	Atlanta, GA Office	1st Floor
Gemtek:d8:0f:ff[a,b,g]	00:14:a5:d8:0f:ff	M-Wireless	9/1/09 1:58 PM	-81	Atlanta, GA Office	1st Floor
Cisco:67:20:e1[a,b,g]	00:07:0e:67:20:e1	MSFTGUEST	9/1/09 1:56 PM	-80	Atlanta, GA Office	1st Floor

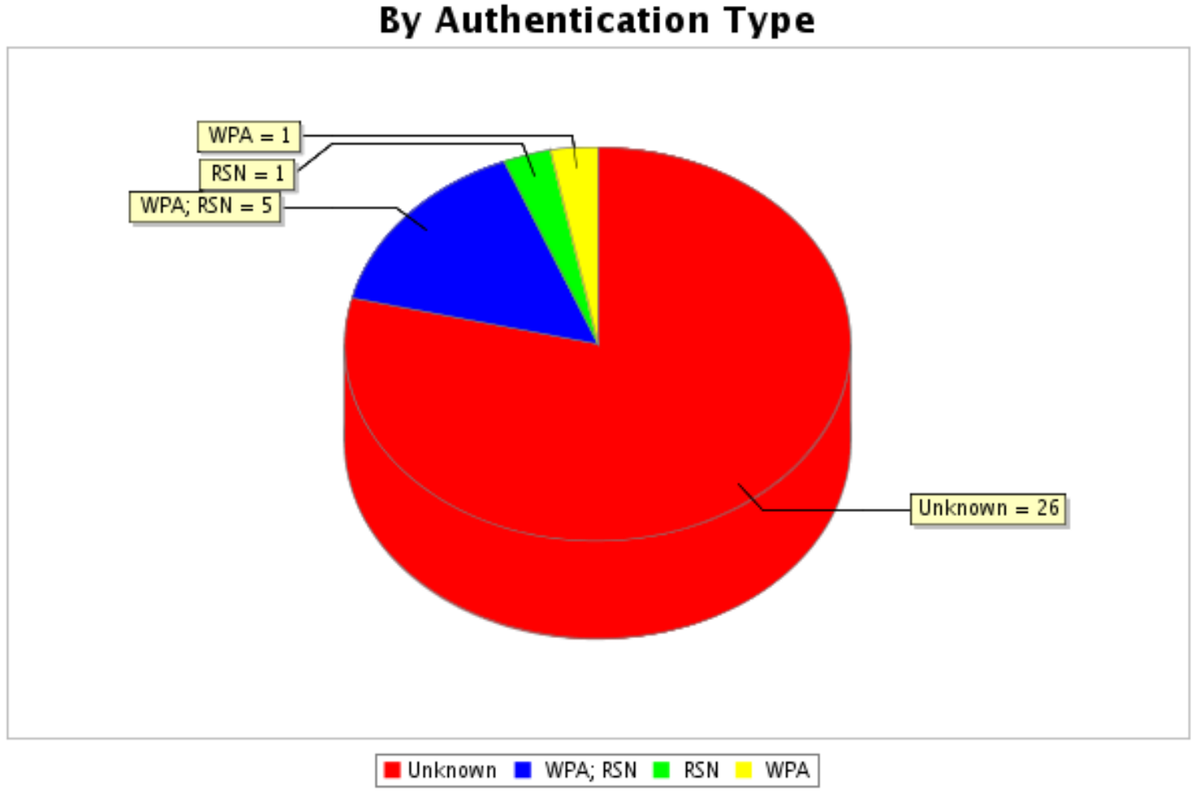
Station	Station MAC	ESSID	Last Seen	Average Signal Strength	Location	Group
Intel:07:d4:24[a,b,g]	00:21:6a:07:d4:24	M-Wireless	9/1/09 1:56 PM	-70	Atlanta, GA Office	1st Floor
Intel:11:5a:be[a,b]	00:21:6a:11:5a:be		9/1/09 1:56 PM	-87	Atlanta, GA Office	1st Floor
Intel:22:88:d3[a,b]	00:21:5c:22:88:d3		9/1/09 1:56 PM	0	Atlanta, GA Office	1st Floor

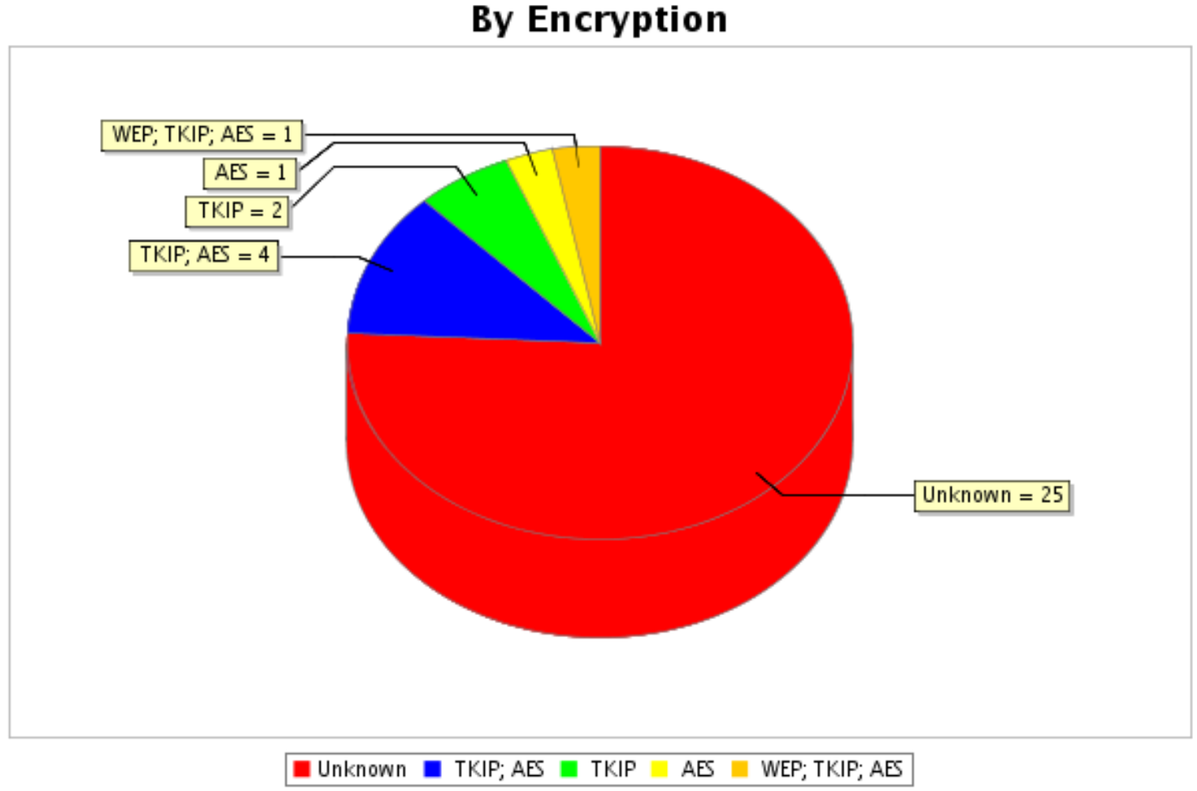
Misconfiguration Threat

This section details the specific threats associated with the misconfiguration of devices in your wireless LAN. Policies and procedures must be in place to ensure that the Access Points are configured properly including mechanisms for the authentication and encryption. Configuration management is a key part in managing your infrastructure. Misconfigurations are common due to user error, forgotten temporary or debugging changes, flaws in firmware updates which may reset configurations or for some non-commercial grade Access points the reset button on the device can reset the configuration to factory defaults. Any such changes can create vulnerabilities in your WLAN.

APs Broadcasting SSID:	3	AP Changing ESSID	0
APs with Weak Authentication:	8	APs Using Unauthorized Channels	0
APs with Weak Encryption:	7	AP Utilizing Default Settings	0
APs Using Unauthorized Data Rates	0		

Access Points by Authentication & Encryption Types





Misconfiguration Violations (Latest 50 Seen)

Device	SubCategory	Type	Start Time	Signal Strength	Location	Group
Symbol:50:1e:54[a,b,g]	802.11 Encryption	80211 Encryption Modes Violated	9/1/09 1:13 PM	-76	Atlanta, GA Office	1st Floor

Device	SubCategory	Type	Start Time	Signal Strength	Location	Group
Symbol:4f:e4:1c[a,b,g]	802.11 Encryption	80211 Encryption Modes Violated	9/1/09 12:48 PM	-85	Atlanta, GA Office	1st Floor
Apple:1a:30:d4[a,b,g]	Environment	Ad-Hoc Network Violation Unauthorized Device	8/31/09 3:08 PM	-63	Atlanta, GA Office	1st Floor
Askey:05:6f:39[a,b,g]	Environment	Ad-Hoc Network Violation Unauthorized Device	8/31/09 3:05 PM	-57	Atlanta, GA Office	1st Floor
Micro-star:91:f8:36[b]	Environment	Ad-Hoc Network Violation Unauthorized Device	8/31/09 10:05 AM	-80	Atlanta, GA Office	1st Floor
Htc:1c:72:b0[b]	Environment	Ad-Hoc Network Violation Unauthorized Device	8/31/09 10:03 AM	-83	Atlanta, GA Office	1st Floor
Symbol:4f:de:64[a,g]	802.11 Encryption	80211 Encryption Modes Violated	8/31/09 9:29 AM	-46	Atlanta, GA Office	1st Floor
Symbol:50:1f:40[a,g]	802.11 Encryption	80211 Encryption Modes Violated	8/31/09 9:08 AM	-72	Atlanta, GA Office	1st Floor
Symbol:4f:e4:80[a,b,g]	802.11 Encryption	80211 Encryption Modes Violated	8/31/09 8:08 AM	-50	Atlanta, GA Office	1st Floor
Belkin:c2:ff:c3[b,g]	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	8/11/09 6:50 PM	-77	Auburn, GA	Auburn
Belkin:c2:ff:c3[b,g]	Advanced Key Generation	Advanced Key Generation Modes Violated	8/11/09 6:49 PM	-79	Auburn, GA	Auburn
Belkin:c2:ff:c3[b,g]	Authentication	Extended Authentication Modes Violated	8/11/09 6:49 PM	-79	Auburn, GA	Auburn
Symbol:4f:e4:1c[a,b,g]	Authentication	Extended Authentication Modes Violated	8/5/09 5:05 PM	-85	Atlanta, GA Office	1st Floor
Cisco:b9:00:20[a,b,g]	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	8/5/09 5:03 PM	-27	Atlanta, GA Office	1st Floor
Symbol:50:1f:40[a,g]	Authentication	Extended Authentication Modes Violated	8/5/09 5:02 PM	-72	Atlanta, GA Office	1st Floor
Cisco:b9:00:20[a,b,g]	802.11 Encryption	80211 Encryption Modes Violated	8/5/09 5:02 PM	-34	Atlanta, GA Office	1st Floor
Nortel:76:7d:40[a,b,g]	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	8/5/09 5:02 PM	-37	Atlanta, GA Office	1st Floor
Symbol:4f:de:64[a,g]	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	-47	Atlanta, GA Office	1st Floor
Symbol:50:1e:54[a,b,g]	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	-76	Atlanta, GA Office	1st Floor
Symbol:4f:e4:80[a,b,g]	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	-49	Atlanta, GA Office	1st Floor
Nortel:76:7d:40[a,b,g]	802.11 Encryption	80211 Encryption Modes Violated	8/5/09 5:01 PM	-37	Atlanta, GA Office	1st Floor
Nortel:76:7d:40[a,b,g]	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	-37	Atlanta, GA Office	1st Floor
Askey:05:6f:39[a,b,g]	Environment	Ad-Hoc Network Violation Unauthorized Device	undefined time	-58	Atlanta, GA Office	1st Floor
Apple:1a:30:d4[a,b,g]	Environment	Ad-Hoc Network Violation Unauthorized Device	undefined time	-57	Atlanta, GA Office	1st Floor

Intrusion Threat

This section details the specific threats associated with intrusions in your Wireless LAN. These include reconnaissance activities to collect information about your Wireless network, active penetration attempts such as failed authentications, associations or EAP handshakes, various types of protocol frame floods such as Probe requests, Probe responses, authentication requests etc which can potentially utilize the channel bandwidth as well as overload the Access points causing them to reset or lock up, Denial of Service attacks via Deauthentication and Disassociation attacks, Identify theft of authorized devices to bypass MAC filtering mechanisms, Activity of Stations which have been marked on Watch List, After hours activities on channels which are supposed to be under lock-down and presence of Fake AP and Soft APs.

Active Stations on Watched List:	0	Identity Theft Attacks:	0
Denial of Service Attacks:	0	Reconnaissance Activity:	2
Soft APs:	1	Authentication Failures:	0
After Hours Activity:	0		

Intrusion Violations (Latest 50 Seen)

Device	Device MAC	Type	Signal Strength	Start Time	Location	Group
Nortel:76:7d:41[a]	00:18:b0:76:7d:41	Unauthorized AP Using Authorized SSID	-34	8/5/09 5:05 PM	Atlanta, GA Office	1st Floor
WKH764@motorola.com[a,b,g,n]	00:21:6a:07:6f:98	Null Probe Response	-55	undefined time	Atlanta, GA Office	1st Floor
Intel:99:10:61[a,b]	00:13:02:99:10:61	Null Probe Response	-73	undefined time	Atlanta, GA Office	1st Floor

Wired Leakage Threat Details

This section details the specific threats associated with leakage of wired side traffic into the airwaves. Leaked wired traffic can pose a significant risk to the security of your network. Since glue protocols (VRRP,HSRP,CDP,OSRF,IGRP)were not setup with security in mind, malicious users can indulge in Network DoS or routing/Spanning tree based attacks to mis-configure or melt-down your wired side network. AirDefense system can help identify the type of traffic leaking into the airwaves to give you a handle of your potential exposure to this vulnerability. If AirDefense is unable to investigate the specific leaked protocols, it can still warn you regarding leaked wired traffic from your Access Points. If an Access Point is not configured as a bridge, any potential wired-to-wired traffic is a concern that should be investigated.

Multicast HSRP	0	Unknown Wired Stations	0
Multicast IGMP	0	Netbios Traffic	0
Multicast IGRP Routers	0	Multicast all systems on Network	0
Multicast OSFP All Routers	0	Multicast DHCP Server/Relay Agent	0
Multicast OSFP Designated Routers	0	Multicast VRRP	0
Multicast RIP2 Routers	0		

Wired Traffic Leakage Violations (Latest 50 Seen)

Device	Device MAC	Type	Signal Strength	Start Time	Location	Group