Applied Methodologies, Inc.

Wireless Security RF Coverage Audit and Traffic Analysis Report

November 2006

Prepared for
New York Insurance Company

Prepared by
Applied Methodologies, Inc.

Table Of Contents

1.0 Introduction

New York Insurance Company(NYI) needed to conduct a brief wireless area footprint survey to determine RF cell size and access point exposure for a new deployment of access points on the 11th floor. The 11th floor of NYI hosts the New York Insurance Company Investment Management(NYIIM) organization. NYI needs to determine whether a new wireless deployment on one the 11th floor is "leaking" RF or wireless signals onto other floors for coverage and security reasons. NYI needs to determine where the wireless leaking points are and what type of traffic can be seen from such points.

The goal of the survey was to determine what wireless Access Points(AP)s on the 11th floor were showing up on the 10th and 12th, and if any non NYI APs are present on the 10th and 11th floors.

After reviewing preliminary information NYI presented via a phone meeting conducted on August 1st 2006, Applied Methodologies, inc.(AMI) has outlined the following project elements which were detailed in the Statement or Work submitted to NYI also on August 1st 2006.

1. Conduct a brief review of the current 11th floor deployment by reviewing any documentation or site survey information provided by NYI
2. Conduct wireless cell Access Point enumeration on the to identify coverage areas and cell footprint
3. Conduct wireless leak point analysis if applicable
4. Protocol analysis of traffic found at leak points or on general coverage areas observed
5. Identify any immediate and critical issues
6. Document all findings and provide recommendations

It is expected that the reader of this report is familiar with general data networking terms, concepts and protocols as well as Wireless LAN concepts, constructs and protocols.

As of this writing only one NYIIM AP MAC(medium access control) address was supplied to AMI so it is difficult and time consuming to ascertain the remaining NYIIM 11th floor AP cells with all of the other co-located and adjacent cells without knowing specifically which MAC addresses the 11th floor NYIIM APs are using. A comparison of the scans from the 10th and the 11th floors may provide some consistent information in terms of what APs appear and when. However, without the specific NYIIM APs to focus the survey on it is difficult to determine their range and leaky points with all the other cells present. So, NYI and AMI agreed to conduct a general analysis of all the floors involved and outside the building to acquire enough data to compare to the actual 11th fl configuration information when it becomes available at a later date. When NYI personnel obtains the remaining NYIIM AP MAC addresses they can compare that information to the data in this report to determine if any additional issues are present.

As of this writing one 11th floor AP MAC address was supplied to be applied against the data in this report. The AP is **NYICAP,** resides on channel 1 and its MAC address is: **0018.1894.a6c0.** This AP was found in most Netstumbler reports and will always be highlighted in RED for easier reference.

The next section will outline a summary of findings followed by the detailed sections and recommendations.

2.0 Summary of Findings

The 10th and 11th floors belong to New York Insurance Company and the 12th floor is a NYI tenant floor. Several passes/scans on the 10th. and 11th. floor were conducted using different radio cards and various antennas to determine signal levels of the APs discovered

The following floors/areas were walked through and scanned:

- 10th floor NYI Internet Development
- 11th floor NYI Investment Management(NYIIM)
- 12th floor Engineering Company (tenant)
- The outside of the building on all four sides from across the street on each side and aiming the antenna at the building to see what was emanating from it.

The following is an outline of general findings:

Most of the non NYI traffic from outside the building does show up on the NYI floors but mostly on the perimeter of the floors. Slow packet activity in middle of floors suggest only NYI beacons and NYI related traffic is propagating there and not the ambient traffic from the neighboring buildings. Most of the heavy packet activity observed was on the perimeter of the floors comes from the radiated traffic through the windows. Native NYI traffic can best be observed in the towards the center of the floor.

- The NYIIM AP NYICAPAP has been identified on the 10, and 12th floors
- The NYIIM AP NYICAPAP beacons can also be seen on channels 2 and 3
- The NYIIM AP NYICAPAP was NOT observed on the outside street reports
- NYI tenant APs were observed outside the building
- No NYIIM NYICAPAP cell layer 3 data related traffic was observed
- Established and unsecured Ad-hoc wireless networks are present on the 10th and 11th floors
- A majority of the cells observed are 802.11g based
- The most prevalent channels observed are 1 6 and 11
- NYI and tenant cells are leaking onto floors below each other
- NYI and tenant cells sizes leaking onto floors above each other
- Many different cells above and below the 11th floor and outside are leaking into the NYI building for NYIIM users to possibly connect to by accident

- Cell channels are overlapping due to other business, residential and consumer APs
- Spanning-Tree traffic was observed on some cells
- Other possible NYI APs that are unsecured were observed on the floors surveyed
- Unsecured consumer grade APs with high signal levels were observed on the floors surveyed
- NYI router login banner provides too much information

The following sections shall delve into the details of the findings outlined above.

3.0 What was discovered using Netstumbler

This section will review what was discovered using a general wardriving/enumeration tool called Netstumbler. Two different radio cards were used with Netstumbler to verify and ensure that the Access Points(AP)s identified could be picked up by different radio power levels and RSSI settings. Netstumbler was used to simulate what most casual or first pass hackers would use to identify open APs. More detailed information may be available in the CommView section of this document.

Also, the use of the two radios used are the most common and help to illustrate that what was discovered on the floors could be discovered by anyone on the floors or possibly outside using the same easy to acquire and use equipment.

The two cards used are as follows:

Proxim(Orinoco) 11b/g Gold 8470-WD card for it's 100mW power capability
Cisco Aironet 802.11a/b/g Air-CB21AG-A-Kp for its RSSI and 802.11a capability

The Ubiquiti SRC 300mW 802.11a/b/g card was provided but not used for the point that if APs can still be detected using the lower wattage and RSSI cards the chances of all the same APs will be found on the Ubiquiti as well.

The 10th and 11th floors belong to New York Insurance Company and the 12th floor is a tenant floor. Several passes/scans on the 10th and 11th floor were conducted using different radio cards and various Dipole and Yagi antennas to determine signal and SNR levels of APs discovered . A 5dBi gain Dipole and a 14.5 gain Yagi from Hyperlink Technologies were used. All PC cards and any external antennas used were positioned for Vertical Polarization. No cross polarization discrimination or scanning of the Horizontal plan was conducted due to time constraints.

What was discovered on the 10th floor using Netstumbler

What was observed on the 10th floor from the first scan around 8:50am on November 14th is outlined in the Netstumbler output on the subsequent pages. This scan used the Proxim radio with no external antenna and all conference rooms and middle sections of the floor were walked through. All Netstumbler reports are sorted by the SNR+ column. NYI can read the supplied Netstumbler files at anytime to sort based on other criteria such as channel, vendor, MAC address or AP name.

There were 87 devices detected yet on follow-up passes in the morning the number changed from 82-87. The APs shaded in Grey were the APs with the best SNR+, meaning they have the strongest signal for a workstation to possibly associate to.

Note the SNR+ ratio column the lower the number the larger the gap between a clean signal and the RF noise floor. SNRs that approach the teens are usually not signals that can be used to associate unless a more sensitive and more powerful radio and an external antenna are used. So, all the other APs listed with SNRs in the 20s on down are either from other floors and from outside the NYI building. The ones with high SNRs in grey that are not NYI are obviously strong enough for someone to associate to in NYI.

Another note is that the stronger APs identified on the 10th floor range in channel frequency. This may be an issue, for channels adjacent to NYI channels may pick up NYI beacons and vise versa. Other observations from this scan and similar passes with the same setup and results:

The top AP noticed on several passes is an open Linksys.

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
02166F046188	11	linksys	-49	51	-100	54 Mbps			100

The NYICAPAP 11th fl. AP was identified on the 10th floor and due to its decent SNR+ ratio, stations on the 10th floor could possibly associate to it if the authentication mechanisms are circumvented. Different Netstumbler reports will show NYICAPAP with a weaker SNR+ ratio. This is because of the time and location it was picked up during the scan. Had the address been known in advanced AMI would have determined the best SNR+ ration found with different radios and antennas and the locations on the 10th floor where they were observed.

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor
00181894A6C0	1		-69	31	-100	54 Mbps	(Fake)

Below is a list of possible other NYI Cisco APs from the 11th or 9th floor due to good SNR+ levels. Since these APs have the same OUI prefix as the NYICAPAP they may be the other APs on the 11th floor.

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor
00181894A930	8		-69	31	-100	54 Mbps	(Fake)
00181894A550	4		-80	20	-100	54 Mbps	(Fake)

The following NYI APs that were found on the same channel and possibly located on the 16th floor due to the SSID name and the low SNR+ observed on 10 are as follows:

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
0014BF184D1A	6	NYI-br	-84	16	-100	54 Mbps	(Fake)		100
0014BF184D17	6	NYI-1619	-85	15	-100	54 Mbps	(Fake)		100

Note that there is no security listed in the beacons for these APs.

A few of the following APs showed up on 10 as well. Here is an example of one. The MAC OUI for TT_Guest 00-0F-BB is registered to Siemens and this AP belongs to NYI tenant Engineering Company.

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
000FBB06B4D8	1	TT_Guest	-84	16	-100	54 Mbps		WEP	100

However, a scan on the 12th floor shows the same AP but with a better SNR suggesting that it belongs to that floor. It does appear to be a strong enough signal to traverse two floors to get to the 10th but on the 10th the signal is too weak to associate to. The TT_Guest APs are presumed to belong to the 12th floor Tenant Engineering Company and are also present on the outside street Netstumbler reports as well.

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
000FBB06B4D8	1	TT_Guest	-59	-41	-100	54 Mbps		WEP	100

The following AP showed up not only on the 10th floor but also on the 6th floor as well leading to believe that based on its SNR it is probably an AP from the outside.

Mac	Ch	Name
1839403150	6	raj

There are many other APs that are not NYI owned among the NLY APs listed NYI should review the Netstumbler output from the 8:50am scan on the following page for specific details.

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
02166F046188	11	linksys	-49	51	-100	54 Mbps	(User-defined)		100
00181894A930	8		-69	31	-100	54 Mbps	(Fake)	WEP	100
00181894A6C0	1		-69	31	-100	54 Mbps	(Fake)	WEP	100
001310B3E586	1	Chatham_Showroom	-69	31	-100	54 Mbps	(Fake)	WEP	100
00120E168C7B	6		-75	25	-100	54 Mbps	(Fake)	WEP	200
00904C600400	6	Bormioli	-75	25	-100	54 Mbps	Epigram	WEP	100
00115CE55060	5	TPG-Wifi	-77	23	-100	54 Mbps	(Fake)	WEP	100
9A334CD26D39	11	Wireless Network	-78	22	-100	11 Mbps	(User-defined)		100
001217609F90	6	camsil	-79	21	-100	54 Mbps	(Fake)		100
02166F046166	11	linksys	-79	21	-100	54 Mbps	(User-defined)		100
000FBB06BAE9	6		-80	20	-100	54 Mbps		WEP	100
00181894A550	4		-80	20	-100	54 Mbps	(Fake)	WEP	100
000FBB065049	1		-80	20	-100	54 Mbps		WEP	100
1839403150	6	raj	-80	20	-100	54 Mbps	(Fake)	WEP	100
00115CE54010	9	TPG-Wifi	-80	20	-100	54 Mbps	(Fake)	WEP	100
0014F1605A80	8	royaldoulton	-81	19	-100	54 Mbps	(Fake)	WEP	100
00115CE55020	6	TPG-Wifi	-81	19	-100	54 Mbps	(Fake)	WEP	100
000FBB065048	1	TT_Guest	-81	19	-100	54 Mbps		WEP	100
00120E45222F	6	06B408711356	-82	18	-100	54 Mbps	(Fake)	WEP	200
00175A10C270	6	PSNET	-82	18	-100	54 Mbps	(Fake)	WEP	100
000FBB066988	6	TT_Guest	-82	18	-100	54 Mbps		WEP	100
000FBB06BAE8	6	TT_Guest	-82	18	-100	54 Mbps		WEP	100
000FBB06B4D9	1		-83	17	-100	54 Mbps		WEP	100
000FBB06B518	11	TT_Guest	-83	17	-100	54 Mbps		WEP	100
000FBB06BAA9	1		-84	16	-100	54 Mbps		WEP	100
000FBB06B519	11		-84	16	-100	54 Mbps		WEP	100
0014BF184D1A	6	nyl-br	-84	16	-100	54 Mbps	(Fake)		100
001759EFC170	1	PSNET	-84	16	-100	54 Mbps	(Fake)	WEP	100
00115CE54020	4	TPG-Wifi	-84	16	-100	54 Mbps	(Fake)	WEP	100
000FBB06AFC8	6	TT_Guest	-84	16	-100	54 Mbps		WEP	100
000FBB06B4D8	1	TT_Guest	-84	16	-100	54 Mbps		WEP	100
000FBB066649	1		-85	15	-100	54 Mbps		WEP	100
000FBB06AFC9	6		-85	15	-100	54 Mbps		WEP	100
0040C82D27CB	4		-85	15	-100	54 Mbps	Milan		100
001310856B95	11	HCI-CCA	-85	15	-100	54 Mbps	(Fake)	WEP	100
001346A7C9DA	6	M2M	-85	15	-100	54 Mbps	(Fake)		100
0014BF184D17	6	nyl-1619	-85	15	-100	54 Mbps	(Fake)		100
000FBB06B8A8	11	TT_Guest	-85	15	-100	54 Mbps		WEP	100
000B851B047F	1		-86	14	-100	54 Mbps	Airespace		100
00028A9E9A57	3		-86	14	-100	11 Mbps	Ambit	WEP	100
1195556573	6	ED	-86	14	-100	54 Mbps	(Fake)	WEP	100
000625F1482F	6	eric	-86	14	-100	11 Mbps	Linksys	WEP	100
0016B6D76335	6	linksys	-86	14	-100	54 Mbps	(Fake)		100
00186E188706	3	mndubhq	-86	14	-100	54 Mbps	(Fake)	WEP	100
000FBB0650C9	1		-87	13	-100	54 Mbps		WEP	100
00120E40FD36	6	06B408756748	-87	13	-100	54 Mbps	(Fake)	WEP	200
0016B6DD4C31	6	alexander	-87	13	-100	54 Mbps	(Fake)	WEP	100
00186E188704	3	cvcwahq-bg	-87	13	-100	54 Mbps	(Fake)	WEP	100
0014BF7305A2	9	IntuitionUS-Wifi	-87	13	-100	54 Mbps	(Fake)	WEP	100
0015E96BA91C	6	Kennex New York Sh...	-87	13	-100	54 Mbps	(Fake)		100
1310416394	6	linksys	-87	13	-100	54 Mbps	(Fake)		100
0013100376AA	1	nikkoshrm	-87	13	-100	54 Mbps	(Fake)	WEP	100
00115CE54070	5	TPG-Wifi	-87	13	-100	54 Mbps	(Fake)	WEP	100
000FBB0650C8	1	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB066648	1	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB06BAA8	1	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB06B8E8	11	TT_Guest	-87	13	-100	54 Mbps		WEP	100
00186E188702	3	WiFiMusic	-87	13	-100	54 Mbps	(Fake)	WEP	100
000BACE53B86	3	WMF2003	-87	13	-100	11 Mbps	3Com Europe	WEP	100
000FBB06B8A9	11		-88	12	-100	54 Mbps		WEP	100
00119570817E	6		-88	12	-100	54 Mbps	(Fake)	WEP	100
000C41D7F454	6	386SAS500	-88	12	-100	54 Mbps	Linksys	WEP	100
0213CE0000A8	11	eng107	-88	12	-100	54 Mbps	(User-defined)		100
00186E188700	3	Manhattan	-88	12	-100	54 Mbps	(Fake)	WEP	100
00120E4EB46D	11	Noritake	-88	12	-100	54 Mbps	(Fake)	WEP	200
001759EFC440	1	PSNET	-88	12	-100	54 Mbps	(Fake)	WEP	100
000FB561E17E	11	TANNETGEAR	-88	12	-100	54 Mbps		WEP	100
001121D49290	1	TPG-Wifi	-88	12	-100	54 Mbps	(Fake)	WEP	100
001124A11D9E	11	TWM	-88	12	-100	54 Mbps	(Fake)	WEP	100
000FBB06BA89	11		-89	11	-100	54 Mbps		WEP	100
000B851BE93F	1		-89	11	-100	54 Mbps	Airespace		100
000FBB06BA59	11		-89	11	-100	54 Mbps		WEP	100
0012170B9AB9	6	carey	-89	11	-100	54 Mbps	(Fake)	WEP	100
000F6623E91B	6	klein	-89	11	-100	11 Mbps	Linksys		100
00146C7F112C	11	NETGEAR	-89	11	-100	54 Mbps	(Fake)		100
0017C5057571	1	SNG-WiFi	-89	11	-100	54 Mbps	(Fake)	WEP	100
000FBB06B818	6	TT_Guest	-89	11	-100	54 Mbps		WEP	100
000FBB066538	6	TT_Guest	-89	11	-100	54 Mbps		WEP	100
000D02543A59	7	WARPSTAR-1A458C	-89	11	-100	54 Mbps		WEP	100
00A0C5DDE000	8		-90	10	-100	11 Mbps	Zyxel		100
00181894A860	3		-90	10	-100	54 Mbps	(Fake)	WEP	100
001217AAEB28	11	G-11	-90	10	-100	54 Mbps	(Fake)	WEP	100
000D72521611	6	Peperhd	-90	10	-100	22 Mbps	2Wire	WEP	100
000FBB06BA58	11	TT_Guest	-90	10	-100	54 Mbps		WEP	100
7AE44F4A741A	10	WLAN	-90	10	-100	11 Mbps	(User-defined)		100
000E9BC199B7	6	679d	-91	9	-100	54 Mbps	(Fake)	WEP	100
0015F9297980	3	CDAS	-92	8	-100	54 Mbps	(Fake)	WEP	100

Conducting a Netstumbler scan using the 14.5 dBi Yagi antenna

Walking the 10th floor and aiming the Yagi towards the ceiling at the 11th floor yielded some differences. Since the Yagi increase the output gain and receive sensitivity from the use of a narrower beam width, additional APs were discovered. In this scan 128 were discovered. There were some changes to the top APs by SNR+ as expected but the ones that were close to the previous non antenna scan may have been picked up by the Yagi's front and back beam width lobes.

Note that now AP **NYI-1619** from the previous non antenna scan had the following statistics:

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
0014BF184D17	6	NYI-1619		-85	15	-100	54 Mbps	(Fake)	100

Is now further up the scan list of sorted best SNR+s observed APs than the previous one:

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
0014BF184D17	6	NYI-1619		-75	25	-100	54 Mbps	(Fake)	100

Note: that the signal is now 10dBm lower and the SNR+ is 10dBm higher when aiming the Yagi towards the 11th floor.

Also, note that the NYICAPAP was picked up using the Yagi, but remember that when using a Yagi the beam width is very narrow so the SNR+ will change as you walk to and from the AP you are scanning. Had AMI had known the NYICAPAP MAC address during this scan, AMI would have been able to determine what section on the 10th floor its signal had the best SNR+ and thus the leaky point would have been defined.

The following page is a full Netstumbler report from a scan using the Yagi

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
02166F046188	11	linksys	-50	50	-100	54 Mbps	(User-defined)		100
00181894A550	4		-63	37	-100	54 Mbps	(Fake)	WEP	100
00120E168C7B	6		-63	37	-100	54 Mbps	(Fake)	WEP	200
00181894A860	3		-67	33	-100	54 Mbps	(Fake)	WEP	100
000FBB06B519	11		-70	30	-100	54 Mbps		WEP	100
000B851B047F	1		-71	29	-100	54 Mbps	Airespace		100
00181894A930	8		-71	29	-100	54 Mbps	(Fake)	WEP	100
000FBB06B518	11	TT_Guest	-73	27	-100	54 Mbps		WEP	100
1839403150	6	raj	-74	26	-100	54 Mbps	(Fake)	WEP	100
0014BF184D17	6	nyl-1619	-75	25	-100	54 Mbps	(Fake)		100
0213CE0000A8	11	eng107	-75	25	-100	54 Mbps	(User-defined)		100
001346A7C9DA	6	M2M	-75	25	-100	54 Mbps	(Fake)		100
001759EFC170	1	PSNET	-77	23	-100	54 Mbps	(Fake)	WEP	100
001217609F90	6	camsil	-78	22	-100	54 Mbps	(Fake)		100
9A334CD26D39	11	Wireless Network	-78	22	-100	11 Mbps	(User-defined)		100
00904C600400	6	Bormioli	-78	22	-100	54 Mbps	Epigram	WEP	100
001310B3E586	1	Chatham_Showroom	-78	22	-100	54 Mbps	(Fake)	WEP	100
00181894A6C0	1		-78	22	-100	54 Mbps	(Fake)	WEP	100
000B851BE93F	1		-80	20	-100	54 Mbps	Airespace		100
000FBB065048	1	TT_Guest	-80	20	-100	54 Mbps		WEP	100
00115CE55060	5	TPG-Wifi	-81	19	-100	54 Mbps	(Fake)	WEP	100
0013100376AA	1	nikkoshrm	-81	19	-100	54 Mbps	(Fake)	WEP	100
00120E45222F	6	06B408711356	-81	19	-100	54 Mbps	(Fake)	WEP	200
000F6623E91B	6	klein	-82	18	-100	11 Mbps	Linksys		100
00175A10C270	6	PSNET	-82	18	-100	54 Mbps	(Fake)	WEP	100
0014BF184D1A	6	nyl-br	-82	18	-100	54 Mbps	(Fake)		100
000FBB06B4D8	1	TT_Guest	-82	18	-100	54 Mbps		WEP	100
3A69D271CBB5	11	linksys	-83	17	-100	11 Mbps	(User-defined)		100
0015E96BA91C	6	Kennex New York Sh...	-83	17	-100	54 Mbps	(Fake)		100
0012179E5275	6	ZSZGuest	-83	17	-100	54 Mbps	(Fake)	WEP	100
00115CE54010	9	TPG-Wifi	-83	17	-100	54 Mbps	(Fake)	WEP	100
00115CE54020	4	TPG-Wifi	-83	17	-100	54 Mbps	(Fake)	WEP	100
000FBB06B859	1		-83	17	-100	54 Mbps		WEP	100
0040C82D27CB	4		-83	17	-100	54 Mbps	Milan		100
000FBB06B4D9	1		-83	17	-100	54 Mbps		WEP	100
0016B6D76335	6	linksys	-83	17	-100	54 Mbps	(Fake)		100
000FBB06B8A8	11	TT_Guest	-84	16	-100	54 Mbps		WEP	100
000FBB06B8E8	11	TT_Guest	-84	16	-100	54 Mbps		WEP	100
000FBB066989	6		-84	16	-100	54 Mbps		WEP	100
001124A11D9E	11	TWM	-84	16	-100	54 Mbps	(Fake)	WEP	100
00115CE54070	5	TPG-Wifi	-84	16	-100	54 Mbps	(Fake)	WEP	100
0014F1605A80	8	royaldoulton	-84	16	-100	54 Mbps	(Fake)	WEP	100
0015F9297980	3	CDAS	-84	16	-100	54 Mbps	(Fake)	WEP	100
001759EFC440	1	PSNET	-84	16	-100	54 Mbps	(Fake)	WEP	100
000E9B2A2DA9	6	59ab	-84	16	-100	54 Mbps	(Fake)	WEP	100
7AE44F4A741A	10	WLAN	-84	16	-100	11 Mbps	(User-defined)		100
000F668147D6	6	Mij	-85	15	-100	54 Mbps	Linksys	WEP	100
000FBB0650C8	1	TT_Guest	-85	15	-100	54 Mbps		WEP	100
00186E188702	3	WiFiMusic	-85	15	-100	54 Mbps	(Fake)	WEP	100
00186E188700	3	Manhattan	-85	15	-100	54 Mbps	(Fake)	WEP	100
000FBB06BA58	11	TT_Guest	-85	15	-100	54 Mbps		WEP	100
0016B6DD4C31	6	alexander	-85	15	-100	54 Mbps	(Fake)	WEP	100
000FBB065049	1		-85	15	-100	54 Mbps		WEP	100
000FBB06AFC8	6	TT_Guest	-85	15	-100	54 Mbps		WEP	100
00146C9F166A	11	DAUM	-86	14	-100	54 Mbps	(Fake)	WEP	100
000FBB066649	1		-86	14	-100	54 Mbps		WEP	100
000FBB06BAE8	6	TT_Guest	-86	14	-100	54 Mbps		WEP	100
000FBB06B818	6	TT_Guest	-86	14	-100	54 Mbps		WEP	100
000FBB06B819	6		-86	14	-100	54 Mbps		WEP	100
000FBB06BAF9	11		-86	14	-100	54 Mbps		WEP	100
000FBB06BAF8	11	TT_Guest	-86	14	-100	54 Mbps		WEP	100
000B851B020F	1		-86	14	-100	54 Mbps	Airespace		100
00175EFA6E0	6	PSNET	-86	14	-100	54 Mbps	(Fake)	WEP	100
000FBB06B949	11		-86	14	-100	54 Mbps		WEP	100
00115CE55020	6	TPG-Wifi	-86	14	-100	54 Mbps	(Fake)	WEP	100
000FBB06B948	11	TT_Guest	-86	14	-100	54 Mbps		WEP	100
00120E17456C	6	SDNY/TARHONG	-86	14	-100	54 Mbps	(Fake)	WEP	200
00028A9E9A57	3		-86	14	-100	11 Mbps	Ambit	WEP	100
000FBB06AFC9	6		-86	14	-100	54 Mbps		WEP	100
000FBB06BD58	11	TT_Guest	-86	14	-100	54 Mbps		WEP	100
000FBB066988	6	TT_Guest	-86	14	-100	54 Mbps		WEP	100
000FBB0650C9	1		-87	13	-100	54 Mbps		WEP	100
000FBB06BA59	11		-87	13	-100	54 Mbps		WEP	100
00A0C5DDE000	8		-87	13	-100	11 Mbps	Zyxel		100
000FBB066648	1	TT_Guest	-87	13	-100	54 Mbps		WEP	100
0014BF4A4E42	6	linksys	-87	13	-100	54 Mbps	(Fake)		100
000FBB06BA38	11	TT_Guest	-87	13	-100	54 Mbps		WEP	100
001310856B95	11	HCI-CCA	-87	13	-100	54 Mbps	(Fake)	WEP	100
1380042850	11		-87	13	-100	54 Mbps	(Fake)	WEP	100
0202F82AB97E	10	airportthru	-87	13	-100	11 Mbps	(User-defined)		100
000FBB06B8E9	11		-87	13	-100	54 Mbps		WEP	100
000FBB06BAA8	1	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB06BD59	11		-87	13	-100	54 Mbps		WEP	100
000F668C070F	11	scafati	-88	12	-100	11 Mbps	Linksys	WEP	100
00904B0B4B14	6	nlm	-88	12	-100	11 Mbps	Gemtek	WEP	100
000FBB06B8A9	11		-88	12	-100	54 Mbps		WEP	100
000C41FA3089	6	DTG	-88	12	-100	54 Mbps	Linksys	WEP	100
0012171BB24F	6	Goldman-WiFi	-88	12	-100	54 Mbps	(Fake)	WEP	100
000C41D7F454	6	386SAS500	-88	12	-100	54 Mbps	Linksys	WEP	100
0012170B9AB9	6	carey	-88	12	-100	54 Mbps	(Fake)	WEP	100
000FBB06BAE9	6		-88	12	-100	54 Mbps		WEP	100
000E9BA06E54	6	13d3	-88	12	-100	54 Mbps	(Fake)	WEP	100
001121D49290	1	TPG-Wifi	-88	12	-100	54 Mbps	(Fake)	WEP	100
000FBB06B938	1	TT_Guest	-88	12	-100	54 Mbps		WEP	100
0014BFF93D99	4	RD	-88	12	-100	54 Mbps	(Fake)	WEP	100
0015C7ABB980	6		-89	11	-100	54 Mbps	(Fake)	WEP	100
000FBB066539	6		-89	11	-100	54 Mbps		WEP	100
0017C5057571	1	SNG-WiFi	-89	11	-100	54 Mbps	(Fake)	WEP	100
000FB561E17E	11	TANNETGEAR	-89	11	-100	54 Mbps		WEP	100
00119570817E	6		-89	11	-100	54 Mbps	(Fake)	WEP	100
1195556573	6	ED	-89	11	-100	54 Mbps	(Fake)	WEP	100
00120E40FD36	6	06B408756748	-89	11	-100	54 Mbps	(Fake)	WEP	200
000B851BA3DF	1		-89	11	-100	54 Mbps	Airespace		100
000B851B029F	1		-89	11	-100	54 Mbps	Airespace		100
00115023B4D2	1	siliwap4	-89	11	-100	54 Mbps	(Fake)	WEP	100
000FBB06BA88	11	TT_Guest	-89	11	-100	54 Mbps		WEP	100
000FBB06B858	1	TT_Guest	-89	11	-100	54 Mbps		WEP	100
0012171DCD8F	6	Rachel	-90	10	-100	54 Mbps	(Fake)	WEP	100
000FBB066538	6	TT_Guest	-90	10	-100	54 Mbps		WEP	100
00186E188704	3	cvcwahq-bg	-90	10	-100	54 Mbps	(Fake)	WEP	100
001150982ED7	10	Alternet_WIFI	-90	10	-100	54 Mbps	(Fake)	WEP	100
000FBB06BAA9	1		-90	10	-100	54 Mbps		WEP	100
000B851BECBF	1		-90	10	-100	54 Mbps	Airespace		100
000BACE53B86	3	WMF2003	-90	10	-100	11 Mbps	3Com Europe	WEP	100
0017C5057652	1	SNG-WiFi	-91	9	-100	54 Mbps	(Fake)	WEP	100
F6434F50AB1F	10	pcswifi	-91	9	-100	11 Mbps	(User-defined)		100
0014BF7305A2	9	IntuitionUS-Wifi	-91	9	-100	54 Mbps	(Fake)	WEP	100
000FBB06B939	1		-91	9	-100	54 Mbps		WEP	100
00186E188706	3	mndubhq	-91	9	-100	54 Mbps	(Fake)	WEP	100
000A95F18499	10	Venini Showroom	-92	8	-100	54 Mbps	Apple	WEP	100
000FBB06BCF9	1		-92	8	-100	54 Mbps		WEP	100
00095BF808E1	3	nrbnrb	-92	8	-100	54 Mbps	Netgear	WEP	100
000FBB06B989	1		-92	8	-100	54 Mbps		WEP	100
000FBB06B988	1	TT_Guest	-92	8	-100	54 Mbps		WEP	100
0015C7ABCFA1	1	qeex0000	-92	8	-100	54 Mbps	(Fake)	WEP	100
001310B6C896	1	loft	-93	7	-100	54 Mbps	(Fake)	WEP	100
0015C7ABCFA0	1		-93	7	-100	54 Mbps	(Fake)	WEP	100
00135FFA83A2	1	blue	-94	6	-100	54 Mbps	(Fake)	WEP	100

What was discovered using the Cisco radio card with Netstumbler

The same AP noted during the Proxim scans are also present during the Cisco scans with the exception of the three 802.11a Unlicensed National Information Infrastructure(UNII) channels highlighted in yellow on the following Netstumbler report. Eighty one APs were listed which is consistent with all of the other scans in terms of a margin of +/- a couple of APs based on position of the surveyor at the time. The following page is the Netstumbler report for this scan.

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
02166F046188	11	linksys	-48	52	-100	54 Mbps	(User-defined)		100
000FBB06BAE9	6		-55	45	-100	54 Mbps		WEP	100
000FBB06AFC8	6	TT_Guest	-55	45	-100	54 Mbps		WEP	100
000FBB06AFC9	6		-55	45	-100	54 Mbps		WEP	100
000FBB06B4D9	1		-55	45	-100	54 Mbps		WEP	100
000FBB06B4D8	1	TT_Guest	-55	45	-100	54 Mbps		WEP	100
1839403150	6	raj	-58	42	-100	54 Mbps	(Fake)	WEP	100
0015C7ABB980	6		-60	40	-100	54 Mbps	(Fake)	WEP	100
0016B6D76335	6	linksys	-64	36	-100	54 Mbps	(Fake)		100
000FBB066648	1	TT_Guest	-68	32	-100	54 Mbps		WEP	100
000FBB066988	6	TT_Guest	-68	32	-100	54 Mbps		WEP	100
000FBB066989	6		-68	32	-100	54 Mbps		WEP	100
000FBB066539	6		-68	32	-100	54 Mbps		WEP	100
001346A7C9DA	6	M2M	-68	32	-100	54 Mbps	(Fake)		100
000FBB06B518	11	TT_Guest	-75	25	-100	54 Mbps		WEP	100
00120E168C7B	6		-81	19	-100	54 Mbps	(Fake)	WEP	200
0014F1605A80	8	royaldoulton	-81	19	-100	54 Mbps	(Fake)	WEP	100
00115CE55060	5	TPG-Wifi	-81	19	-100	54 Mbps	(Fake)	WEP	100
00115CE54070	5	TPG-Wifi	-81	19	-100	54 Mbps	(Fake)	WEP	100
00115CE54020	4	TPG-Wifi	-81	19	-100	54 Mbps	(Fake)	WEP	100
000FBB06B8A9	11		-81	19	-100	54 Mbps		WEP	100
000FBB06B8A8	11	TT_Guest	-81	19	-100	54 Mbps		WEP	100
000FBB065049	1		-81	19	-100	54 Mbps		WEP	100
000FBB065048	1	TT_Guest	-81	19	-100	54 Mbps		WEP	100
000B851B047F	1		-81	19	-100	54 Mbps	Airespace		100
0013100376AA	1	nikkoshrm	-81	19	-100	54 Mbps	(Fake)	WEP	100
00181894A930	8		-81	19	-100	54 Mbps	(Fake)	WEP	100
00904C600400	6	Bormioli	-81	19	-100	54 Mbps	Epigram	WEP	100
001310B3E586	1	Chatham_Showroom	-81	19	-100	54 Mbps	(Fake)	WEP	100
00181894A6C0	1		-81	19	-100	54 Mbps	(Fake)	WEP	100
000FB561E17E	11	TANNETGEAR	-83	17	-100	54 Mbps		WEP	100
00181894A550	4		-83	17	-100	54 Mbps	(Fake)	WEP	100
000FBB06B519	11		-83	17	-100	54 Mbps		WEP	100
9A334CD26D39	11	Wireless Network	-83	17	-100	11 Mbps	(User-defined)		100
00028A9E9A57	3		-84	16	-100	11 Mbps	Ambit	WEP	100
000B851BE93F	1		-85	15	-100	54 Mbps	Airespace		100
00115CE54010	9	TPG-Wifi	-85	15	-100	54 Mbps	(Fake)	WEP	100
000F6623E91B	6	klein	-86	14	-100	11 Mbps	Linksys		100
0014BF184D17	6	nyl-1619	-86	14	-100	54 Mbps	(Fake)		100
000FBB06B4D0	36		-86	14	-100	54 Mbps		WEP	100
00181894A860	3		-87	13	-100	54 Mbps	(Fake)	WEP	100
001217609F90	6	camsil	-87	13	-100	54 Mbps	(Fake)		100
000FBB06B8E9	11		-87	13	-100	54 Mbps		WEP	100
000FBB06B8E8	11	TT_Guest	-87	13	-100	54 Mbps		WEP	100
0213CE0000A8	11	eng107	-88	12	-100	54 Mbps	(User-defined)		100
001759EFC440	1	PSNET	-88	12	-100	54 Mbps	(Fake)	WEP	100
001759EFC170	1	PSNET	-88	12	-100	54 Mbps	(Fake)	WEP	100
001124A11D9E	11	TWM	-89	11	-100	54 Mbps	(Fake)	WEP	100
000B850E26BF	6		-89	11	-100	54 Mbps	Airespace		100
000FBB06BA58	11	TT_Guest	-89	11	-100	54 Mbps		WEP	100
000FBB06BA50	36		-89	11	-100	54 Mbps		WEP	100
000FBB06B819	6		-89	11	-100	54 Mbps		WEP	100
00175A10C270	6	PSNET	-89	11	-100	54 Mbps	(Fake)	WEP	100
001310856B95	11	HCI-CCA	-89	11	-100	54 Mbps	(Fake)	WEP	100
00120E45222F	6	06B408711356	-89	11	-100	54 Mbps	(Fake)	WEP	200
000FBB06BA59	11		-90	10	-100	54 Mbps		WEP	100
000FBB06B858	1	TT_Guest	-90	10	-100	54 Mbps		WEP	100
000FBB06B859	1		-90	10	-100	54 Mbps		WEP	100
001121D49290	1	TPG-Wifi	-90	10	-100	54 Mbps	(Fake)	WEP	100
000FBB06BA88	11	TT_Guest	-90	10	-100	54 Mbps		WEP	100
000FBB06BAF9	11		-90	10	-100	54 Mbps		WEP	100
000FBB06BAF0	36		-90	10	-100	54 Mbps		WEP	100
0015E96BA91C	6	Kennex New York Sh...	-90	10	-100	54 Mbps	(Fake)		100
0012179E5275	6	ZSZGuest	-90	10	-100	54 Mbps	(Fake)	WEP	100
000BACE53B86	3	WMF2003	-90	10	-100	11 Mbps	3Com Europe	WEP	100
0040C82D27CB	4		-90	10	-100	54 Mbps	Milan		100
000FBB066538	6	TT_Guest	-91	9	-100	54 Mbps		WEP	100
0014BF184D1A	6	nyl-br	-92	8	-100	54 Mbps	(Fake)		100
000B851B029F	1		-93	7	-100	54 Mbps	Airespace		100
00175A10BD30	11	PSNET	-93	7	-100	54 Mbps	(Fake)	WEP	100
0014BFF93D99	4	RD	-94	6	-100	54 Mbps	(Fake)	WEP	100
00186E188700	3	Manhattan	-94	6	-100	54 Mbps	(Fake)	WEP	100
00186E188704	3	cvcwahq-bg	-94	6	-100	54 Mbps	(Fake)	WEP	100
000B851BECBF	1		-94	6	-100	54 Mbps	Airespace		100
00115CE55020	6	TPG-Wifi	-94	6	-100	54 Mbps	(Fake)	WEP	100
00186E188702	3	WiFiMusic	-95	5	-100	54 Mbps	(Fake)	WEP	100
000FBB06BA89	11		-95	5	-100	54 Mbps		WEP	100
000B851B020F	1		-95	5	-100	54 Mbps	Airespace		100
7AE44F4A741A	10	WLAN	-95	5	-100	11 Mbps	(User-defined)		100
000D02543A59	7	WARPSTAR-1A458C	-95	5	-100	54 Mbps		WEP	100
000FBB06BAA8	1	TT_Guest	-96	4	-100	54 Mbps		WEP	100

What was discovered on the 11th floor with Netstumbler

NYICAPAP was identified on the 11th floor and its good SNR + indicates it is on this floor.

A Netstumbler scan was conducted on the 11th floor using the same approach and tools as the 10th with several passes executed for control purposes. On the following page is the full Netstumbler report for the 11th floor and notice that the following highlighted entries are now close to the top of the SNR+ scale, compared to the 10th floor reports, as well as a series of Cisco AP MAC addresses which may be the local APs for this floor. NYICAPAP was identified on the 11th floor and its good SNR + indicates it is on this floor.

Remember, the NYI-BR and NYI-1619 OUIs are Cisco-Linksys while the others listed are just Cisco. About 52 devices were noted on this floor and about the same were noted using the Cisco radio plus the addition of a few 802.11a UNII networks listed below:

MAC	Chan	SSID	Signal+	SNR+	Noise-	Sp	eed	Vendor	Encryption	Bea...
000FBB066980	36		-66	34	-100	54	Mbps		WEP	100
000FBB06B4D0	36		-73	27	-100	54	Mbps		WEP	100
000FBB06B8E0	149		-86	14	-100	54	Mbps		WEP	100
000FBB06B510	149		-87	13	-100	54	Mbps		WEP	100

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
00120E168C7B	6		-43	57	-100	54 Mbps	(Fake)	WEP	200
0014BF184D17	6	nyl-1619	-46	54	-100	54 Mbps	(Fake)		100
00181894A860	3		-46	54	-100	54 Mbps	(Fake)	WEP	100
00181894A6C0	1		-47	53	-100	54 Mbps	(Fake)	WEP	100
00181894A550	4		-49	51	-100	54 Mbps	(Fake)	WEP	100
00181894A930	8		-51	49	-100	54 Mbps	(Fake)	WEP	100
0014BF184D1A	6	nyl-br	-52	48	-100	54 Mbps	(Fake)		100
0213CE0000A8	11	eng107	-65	35	-100	54 Mbps	(User-defined)		100
BAE34E4CA6BD	10	sanswire	-66	34	-100	11 Mbps	(User-defined)		100
0014F1605A80	8	royaldoulton	-75	25	-100	54 Mbps	(Fake)	WEP	100
000FBB06B4D9	1		-78	22	-100	54 Mbps		WEP	100
02166F046188	11	linksys	-80	20	-100	54 Mbps	(User-defined)		100
001217609F90	6	camsil	-80	20	-100	54 Mbps	(Fake)		100
1839403150	6	raj	-80	20	-100	54 Mbps	(Fake)	WEP	
00904C600400	6	Bormioli	-81	19	-100	54 Mbps	Epigram	WEP	100
000FBB06B519	11		-82	18	-100	54 Mbps		WEP	100
000FBB06B518	11	TT_Guest	-82	18	-100	54 Mbps		WEP	100
0016B62EF798	6	linksys	-82	18	-100	54 Mbps	(Fake)		100
000FBB06AFC8	6	TT_Guest	-82	18	-100	54 Mbps		WEP	100
000FBB06B4D8	1	TT_Guest	-82	18	-100	54 Mbps		WEP	100
00115CE54070	5	TPG-Wifi	-83	17	-100	54 Mbps	(Fake)	WEP	100
000FBB06AFC9	6		-83	17	-100	54 Mbps		WEP	100
00115CE54010	9	TPG-Wifi	-84	16	-100	54 Mbps	(Fake)	WEP	100
001310B3E586	1	Chatham_Showroom	-84	16	-100	54 Mbps	(Fake)	WEP	100
000FBB06B8E8	11	TT_Guest	-85	15	-100	54 Mbps		WEP	100
000F660B9FE1	6	mitchell	-85	15	-100	54 Mbps	Linksys		100
0015E96BA91C	6	Kennex New York Sh...	-85	15	-100	54 Mbps	(Fake)		100
00115CE55020	6	TPG-Wifi	-86	14	-100	54 Mbps	(Fake)	WEP	100
000FBB06BAA8	1	TT_Guest	-86	14	-100	54 Mbps		WEP	100
001346A7C9DA	6	M2M	-86	14	-100	54 Mbps	(Fake)		100
0016B6D76335	6	linksys	-86	14	-100	54 Mbps	(Fake)		100
00175A10C270	6	PSNET	-87	13	-100	54 Mbps	(Fake)	WEP	100
000B851B047F	1		-87	13	-100	54 Mbps	Airespace		100
000FBB06B8E9	11		-87	13	-100	54 Mbps		WEP	100
00115CE55060	5	TPG-Wifi	-87	13	-100	54 Mbps	(Fake)	WEP	100
001346BDD420	6	LORR-NYC	-88	12	-100	54 Mbps	(Fake)	WEP	100
000D02543A59	7	WARPSTAR-1A458C	-88	12	-100	54 Mbps		WEP	100
001121D49290	1	TPG-Wifi	-89	11	-100	54 Mbps	(Fake)	WEP	100
000FBB06B819	6		-89	11	-100	54 Mbps		WEP	100
0011249AA0DA	1	StrawberryFrog	-89	11	-100	54 Mbps	(Fake)	WEP	100
00146CD57C24	6	AGA	-90	10	-100	54 Mbps	(Fake)		100
00186E188700	3	Manhattan	-90	10	-100	54 Mbps	(Fake)	WEP	100
000B850E26BF	6		-90	10	-100	54 Mbps	Airespace		100
001759EFC170	1	PSNET	-90	10	-100	54 Mbps	(Fake)	WEP	100
000FBB06BAA9	1		-90	10	-100	54 Mbps		WEP	100
00115CE54020	4	TPG-Wifi	-90	10	-100	54 Mbps	(Fake)	WEP	100
0013100376AA	1	nikkoshrm	-90	10	-100	54 Mbps	(Fake)	WEP	100
000B851B029F	1		-91	9	-100	54 Mbps	Airespace		100
00120E45222F	6	06B408711356	-91	9	-100	54 Mbps	(Fake)	WEP	200
000FBB06B939	1		-91	9	-100	54 Mbps		WEP	100
000FBB06B938	1	TT_Guest	-91	9	-100	54 Mbps		WEP	100

Conducting a Netstumbler scan using 5dBi Dipole Antenna

Using a small Dipole antenna and walking with the tablet pc additional APs were observed. The same top SNR+ were present plus some new APs from either other floors and around the building. Notice that using the Dipole antenna we get a better reading of NYICAPAP. The Netstumbler report outlining this scan for comparison is on the following page.

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
00120E168C7B	6		-40	60	-100	54 Mbps	(Fake)	WEP	200
0014BF184D1A	6	nyl-br	-43	57	-100	54 Mbps	(Fake)		100
00181894A6C0	1		-45	55	-100	54 Mbps	(Fake)	WEP	100
00181894A550	4		-46	54	-100	54 Mbps	(Fake)	WEP	100
BAE34E4CA6BD	10	sanswire	-59	41	-100	11 Mbps	(User-defined)		100
0213CE0000A8	11	eng107	-68	32	-100	54 Mbps	(User-defined)		100
0014BF184D17	6	nyl-1619	-69	31	-100	54 Mbps	(Fake)		100
00181894A860	3		-71	29	-100	54 Mbps	(Fake)	WEP	100
001217609F90	6	camsil	-72	28	-100	54 Mbps	(Fake)		100
000FBB06B4D8	1	TT_Guest	-76	24	-100	54 Mbps		WEP	100
00904C600400	6	Bormioli	-77	23	-100	54 Mbps	Epigram	WEP	100
000FBB06AFC9	6		-78	22	-100	54 Mbps		WEP	100
000FBB06B4D9	1		-78	22	-100	54 Mbps		WEP	100
0014F1605A80	8	royaldoulton	-79	21	-100	54 Mbps	(Fake)	WEP	100
001310B3E586	1	Chatham_Showroom	-79	21	-100	54 Mbps	(Fake)	WEP	100
000FBB06B519	11		-80	20	-100	54 Mbps		WEP	100
000FBB06AFC8	6	TT_Guest	-80	20	-100	54 Mbps		WEP	100
000FBB06B8D9	11		-81	19	-100	54 Mbps		WEP	100
000FBB06B938	1	TT_Guest	-81	19	-100	54 Mbps		WEP	100
000F668147D6	6	Mij	-82	18	-100	54 Mbps	Linksys	WEP	100
000FBB06BA88	11	TT_Guest	-82	18	-100	54 Mbps		WEP	100
00181894A930	8		-82	18	-100	54 Mbps	(Fake)	WEP	100
000FBB06B518	11	TT_Guest	-83	17	-100	54 Mbps		WEP	100
000FBB06B939	1		-83	17	-100	54 Mbps		WEP	100
00115CE55020	6	TPG-Wifi	-84	16	-100	54 Mbps	(Fake)	WEP	100
001346A7C9DA	6	M2M	-84	16	-100	54 Mbps	(Fake)		100
000FBB06B8A9	11		-84	16	-100	54 Mbps		WEP	100
000FBB06B8A8	11	TT_Guest	-84	16	-100	54 Mbps		WEP	100
0040C82D27CB	4		-84	16	-100	54 Mbps	Milan		100
0015F9297980	3	CDAS	-85	15	-100	54 Mbps	(Fake)	WEP	100
00115CE54010	9	TPG-Wifi	-85	15	-100	54 Mbps	(Fake)	WEP	100
000B851B047F	1		-85	15	-100	54 Mbps	Airespace		100
00115CE54020	4	TPG-Wifi	-85	15	-100	54 Mbps	(Fake)	WEP	100
000FBB06BAF9	11		-85	15	-100	54 Mbps		WEP	100
00146C9F166A	11	DAUM	-85	15	-100	54 Mbps	(Fake)	WEP	100
00120E45222F	6	06B408711356	-85	15	-100	54 Mbps	(Fake)	WEP	200
0011249AA0DA	1	StrawberryFrog	-85	15	-100	54 Mbps	(Fake)	WEP	100
000FBB06BCF8	1	TT_Guest	-85	15	-100	54 Mbps		WEP	100
000FB561E17E	11	TANNETGEAR	-86	14	-100	54 Mbps		WEP	100
1839403150	6	raj	-86	14	-100	54 Mbps	(Fake)	WEP	100
000FBB066988	6	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB06BD58	11	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB06B8E9	11		-87	13	-100	54 Mbps		WEP	100
000FBB06B8E8	11	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB06BA38	11	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB06BA58	11	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB06BAF8	11	TT_Guest	-87	13	-100	54 Mbps		WEP	100
0015E96BA91C	6	Kennex New York Sh...	-87	13	-100	54 Mbps	(Fake)		100
000FBB06BA39	11		-87	13	-100	54 Mbps		WEP	100
1195556573	6	ED	-87	13	-100	54 Mbps	(Fake)	WEP	100
000FBB06B819	6		-87	13	-100	54 Mbps		WEP	100
000FBB06B8D8	11	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB06BA89	11		-87	13	-100	54 Mbps		WEP	100
0014BF7305A2	9	IntuitionUS-Wifi	-87	13	-100	54 Mbps	(Fake)	WEP	100
000FBB06B948	11	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB06B949	11		-87	13	-100	54 Mbps		WEP	100
00183956B6B3	6	linksys	-87	13	-100	54 Mbps	(Fake)		100
000C41FA3089	6	DTG	-87	13	-100	54 Mbps	Linksys	WEP	100
000FBB06BD59	11		-88	12	-100	54 Mbps		WEP	100
00131082AB98	6	Scorpion	-88	12	-100	54 Mbps	(Fake)	WEP	100
00146CD57C24	6	AGA	-88	12	-100	54 Mbps	(Fake)		100
00186E188704	3	cvcwahq-bg	-88	12	-100	54 Mbps	(Fake)	WEP	100
00A0C5DDE000	8		-88	12	-100	11 Mbps	Zyxel		100
000FBB06BAE8	6	TT_Guest	-88	12	-100	54 Mbps		WEP	100
000FBB06B818	6	TT_Guest	-88	12	-100	54 Mbps		WEP	100
000FBB06BA59	11		-88	12	-100	54 Mbps		WEP	100
00028A9E9A57	3		-88	12	-100	11 Mbps	Ambit	WEP	100
0011249A9FB2	11	StrawberryFrog	-88	12	-100	54 Mbps	(Fake)	WEP	100
00120064A750	11		-89	11	-100	54 Mbps	(Fake)	WEP	100
000FBB06BAE9	6		-89	11	-100	54 Mbps		WEP	100
000FBB06BAA8	1	TT_Guest	-89	11	-100	54 Mbps		WEP	100
000B850E26BF	6		-89	11	-100	54 Mbps	Airespace		100
00115CE54070	5	TPG-Wifi	-89	11	-100	54 Mbps	(Fake)	WEP	100
000FBB066538	6	TT_Guest	-89	11	-100	54 Mbps		WEP	100
0016B648750D	6	2305th	-89	11	-100	54 Mbps	(Fake)	WEP	100
0013100376AA	1	nikkoshrm	-89	11	-100	54 Mbps	(Fake)	WEP	100
000FBB06BCF9	1		-89	11	-100	54 Mbps		WEP	100
0016CBF76650	1	StrawberryFrog	-89	11	-100	54 Mbps	(Fake)	WEP	100
000FBB065048	1	TT_Guest	-90	10	-100	54 Mbps		WEP	100
000B851B029F	1		-90	10	-100	54 Mbps	Airespace		100
00175A10C270	6	PSNET	-90	10	-100	54 Mbps	(Fake)	WEP	100
000FBB06BAA9	1		-90	10	-100	54 Mbps		WEP	100
000B851BE93F	1		-90	10	-100	54 Mbps	Airespace		100
001121D49290	1	TPG-Wifi	-90	10	-100	54 Mbps	(Fake)	WEP	100
000FBB06B858	1	TT_Guest	-90	10	-100	54 Mbps		WEP	100
0006B114F491	1	dsjs	-90	10	-100	54 Mbps	Sonicwall		100
000FBB065049	1		-91	9	-100	54 Mbps		WEP	100
000FBB0650C8	1	TT_Guest	-91	9	-100	54 Mbps		WEP	100
001759EFC170	1	PSNET	-91	9	-100	54 Mbps	(Fake)	WEP	100
00115CE55060	5	TPG-Wifi	-91	9	-100	54 Mbps	(Fake)	WEP	100
0017C5057652	1	SNG-WiFi	-91	9	-100	54 Mbps	(Fake)	WEP	100
000FBB06B859	1		-91	9	-100	54 Mbps		WEP	100
000FBB0650C9	1		-92	8	-100	54 Mbps		WEP	100
00135FFA83A2	1	blue	-93	7	-100	54 Mbps	(Fake)	WEP	100
001759EFC440	1	PSNET	-93	7	-100	54 Mbps	(Fake)	WEP	100

What was discovered on the 12th floor with Netstumbler

A walk through the entire 12th floor, except conference rooms, was accomplished on Tuesday 11/14 in the afternoon. The following Netstumbler report shows what was observed. There were not as many APs detected compared to the other floors and this may be due to the short time allowed on the 12th floor. This may explain why NYICAPAP was not observed. However, the CommView report in the next section will also list a scan using the CommView wireless protocol analyzer for comparison. It appears that any of the Cisco or Linksys APs that were present on the 10th or 11th floor are not present on the 12th. However, this may be from the short time to scan the floor.

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
000FBB06B4D9	1		-58	42	-100	54 Mbps		WEP	100
000FBB06B4D8	1	TT_Guest	-59	41	-100	54 Mbps		WEP	100
000FBB06BAA9	1		-71	29	-100	54 Mbps		WEP	100
000FBB06B938	1	TT_Guest	-73	27	-100	54 Mbps		WEP	100
000FBB06AFC8	6	TT_Guest	-74	26	-100	54 Mbps		WEP	100
000FBB06AFC9	6		-75	25	-100	54 Mbps		WEP	100
000FBB06B939	1		-76	24	-100	54 Mbps		WEP	100
000FBB06BAA8	1	TT_Guest	-77	23	-100	54 Mbps		WEP	100
000FBB06BD58	11	TT_Guest	-78	22	-100	54 Mbps		WEP	100
000FBB06BD59	11		-79	21	-100	54 Mbps		WEP	100
000FBB06B518	11	TT_Guest	-81	19	-100	54 Mbps		WEP	100
0015C7ABCFA0	1		-83	17	-100	54 Mbps	(Fake)	WEP	100
000FBB06B519	11		-83	17	-100	54 Mbps		WEP	100
000FBB06B8E9	11		-83	17	-100	54 Mbps		WEP	100
000FBB06BA39	11		-84	16	-100	54 Mbps		WEP	100
02166F05C294	11	linksys	-84	16	-100	54 Mbps	(User-defined)		100
0015C7ABB981	6	qeex0000	-85	15	-100	54 Mbps	(Fake)	WEP	100
00120E168C7B	6		-85	15	-100	54 Mbps	(Fake)	WEP	200
000FBB06BA38	11	TT_Guest	-85	15	-100	54 Mbps		WEP	100
DABB4F4DFE03	10	Jet Blue hot spot	-85	15	-100	11 Mbps	(User-defined)		100
000FBB06BA59	11		-87	13	-100	54 Mbps		WEP	100
000FBB06B8E8	11	TT_Guest	-87	13	-100	54 Mbps		WEP	100
001647A0A870	6		-88	12	-100	54 Mbps	(Fake)	WEP	100

What was discovered in the afternoon using Netstumbler

Additional scans from the 10th. floor were conducted in the afternoon of AMI's first day visit for control purposes. There appeared to be less APs accounted for in the afternoon and subsequent scans showed the similar results. Below is the afternoon Netstumbler of the 10th floor only using the Cisco radio. Note that the NYICAPAP was not picked up during this scan.

MAC	Ch...	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryp	Bea...
02166F05D570	11	linksys	-59	41	-100	54 Mbps	(User-defined)		100
000FBB06B4D9	1		-60	40	-100	54 Mbps		WEP	100
1839403150	6	raj	-60	40	-100	54 Mbps	(Fake)	WEP	100
001346A7C9DA	6	M2M	-63	37	-100	54 Mbps	(Fake)		100
000FBB06B4D8	1	TT_Guest	-66	34	-100	54 Mbps		WEP	100
00120E168C7B	6		-75	25	-100	54 Mbps	(Fake)	WEP	200
000FBB06B518	11	TT_Guest	-75	25	-100	54 Mbps		WEP	100
02166F046188	11	linksys	-76	24	-100	11 Mbps	(User-defined)		100
7AE44F4A741A	10	WLAN	-78	22	-100	11 Mbps	(User-defined)		100
0213CE29D244	11	eng107	-79	21	-100	54 Mbps	(User-defined)		100
00181894A930	8		-80	20	-100	54 Mbps	(Fake)	WEP	100
000FBB065048	1	TT_Guest	-81	19	-100	54 Mbps		WEP	100
00904C600400	6	Bormioli	-81	19	-100	54 Mbps	Epigram	WEP	100
000B851B047F	1		-81	19	-100	54 Mbps	Airespace		100
001310B3E586	1	Chatham_Showroom	-81	19	-100	54 Mbps	(Fake)	WEP	100
00181894A550	4		-81	19	-100	54 Mbps	(Fake)	WEP	100
000FBB06BA59	11		-82	18	-100	54 Mbps		WEP	100
000FBB06BA58	11	TT_Guest	-82	18	-100	54 Mbps		WEP	100
000FBB06B519	11		-82	18	-100	54 Mbps		WEP	100
0011249A9FB2	11	StrawberryFrog	-82	18	-100	54 Mbps	(Fake)	WEP	100
000FBB06B8D8	11	TT_Guest	-82	18	-100	54 Mbps		WEP	100
000FBB06B8E9	11		-82	18	-100	54 Mbps		WEP	100
000FBB06B8D9	11		-82	18	-100	54 Mbps		WEP	100
000FBB06B8E8	11	TT_Guest	-82	18	-100	54 Mbps		WEP	100
000FBB066989	6		-83	17	-100	54 Mbps		WEP	100
000FBB066988	6	TT_Guest	-83	17	-100	54 Mbps		WEP	100
00115CE54020	4	TPG-Wifi	-84	16	-100	54 Mbps	(Fake)	WEP	100
9A334CD26D39	11	Wireless Network	-84	16	-100	11 Mbps	(User-defined)		100
000FBB06B819	6		-84	16	-100	54 Mbps		WEP	100
001759EFC170	1	PSNET	-84	16	-100	54 Mbps	(Fake)	WEP	100
000B851BE93F	1		-84	16	-100	54 Mbps	Airespace		100
000FBB06BAA9	1		-84	16	-100	54 Mbps		WEP	100
000FBB06B8A0	52		-86	14	-100	54 Mbps		WEP	100
0012179E5275	6	ZSZGuest	-86	14	-100	54 Mbps	(Fake)	WEP	100
000B851B029F	1		-86	14	-100	54 Mbps	Airespace		100
001121D49290	1	TPG-Wifi	-86	14	-100	54 Mbps	(Fake)	WEP	100
0014BF184D17	6	nyl-1619	-86	14	-100	54 Mbps	(Fake)		100
00181894A860	3		-86	14	-100	54 Mbps	(Fake)	WEP	100
00115CE55060	5	TPG-Wifi	-87	13	-100	54 Mbps	(Fake)	WEP	100
16AB37775D73	11	concourse	-87	13	-100	11 Mbps	(User-defined)		100
000FBB0650C8	1	TT_Guest	-87	13	-100	54 Mbps		WEP	100
0013100376AA	1	nikkoshrm	-87	13	-100	54 Mbps	(Fake)	WEP	100
00115CE54010	9	TPG-Wifi	-87	13	-100	54 Mbps	(Fake)	WEP	100
00175A10C270	6	PSNET	-87	13	-100	54 Mbps	(Fake)	WEP	100
000FBB065049	1		-88	12	-100	54 Mbps		WEP	100
001124A11D9E	11	TWM	-88	12	-100	54 Mbps	(Fake)	WEP	100
000FBB06B8A8	11	TT_Guest	-89	11	-100	54 Mbps		WEP	100
001217609F90	6	camsil	-89	11	-100	54 Mbps	(Fake)		100
000FBB06B858	1	TT_Guest	-91	9	-100	54 Mbps		WEP	100
00120E45222F	6	06B408711356	-92	8	-100	54 Mbps	(Fake)	WEP	200
0040C82D27CB	4		-92	8	-100	54 Mbps	Milan		100
00186E188700	3	Manhattan	-93	7	-100	54 Mbps	(Fake)	WEP	100
001759EFC440	1	PSNET	-94	6	-100	54 Mbps	(Fake)	WEP	100

What was discovered by Netstumbler outside the building

The flowing Netstumbler reports outline the devices discovered outside the New York Insurance Company building around 9:30am on Thursday 11/16.

The building was scanned from across the street from each building side using a 14.5dBi Yagi antenna. Each scan lasted several minutes on each face side of the building and covered the lower to higher floors. The Netstumbler report is sorted per channel to give NYI personnel an easier view of devices per channel to compare to their internal database of devices. It should be noted that the NYICAPAP AP was not detected in these scans but there were other APs with the similar MAC address prefix so these lists should be reviewed when the other NYIIM AP MAC addresses are disclosed.

NYI 1st Avenue Netstumbler Report

MAC	Chan	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
000FBB066649	1		-84	16	-100	54 Mbps		WEP	100
000FBB066648	1	TT_Guest	-84	16	-100	54 Mbps		WEP	100
001121D49290	1	TPG-Wifi	-84	16	-100	54 Mbps	(Fake)	WEP	100
001310B6C896	1	loft	-83	17	-100	54 Mbps	(Fake)	WEP	100
000FBB06BCF9	1		-89	11	-100	54 Mbps		WEP	100
000FBB06BCF8	1	TT_Guest	-87	13	-100	54 Mbps		WEP	100
000FBB06B4D8	1	TT_Guest	-86	14	-100	54 Mbps		WEP	100
000B8523674D	1	guest	-80	20	-100	54 Mbps	Airespace		100
000B8523674E	1		-82	18	-100	54 Mbps	Airespace	WEP	100
0020A64EEA13	1	My Wireless Network..	-78	22	-100	54 Mbps			100
00146C677824	1	DenTekOC	-84	16	-100	54 Mbps	(Fake)	WEP	100
000F6634FE7E	1	scott	-79	21	-100	11 Mbps	Linksys	WEP	100
000B851BECBF	1		-87	13	-100	54 Mbps	Airespace		100
000B8523649E	1		-87	13	-100	54 Mbps	Airespace	WEP	100
000B850E3A3F	1		-85	15	-100	54 Mbps	Airespace		100
000B851BD19F	1		-85	15	-100	54 Mbps	Airespace		100
0014A9D4F430	1		-81	19	-100	54 Mbps	(Fake)	WEP	100
0017C5057571	1	SNG-WiFi	-83	17	-100	54 Mbps	(Fake)	WEP	100
00141BB71AD0	1	Gr1mmD3l19h7	-78	22	-100	54 Mbps	(Fake)	WEP	100
000B852367ED	1	guest	-90	10	-100	54 Mbps	Airespace		100
000B852367EE	1		-86	14	-100	54 Mbps	Airespace	WEP	100
001759EFC170	1	PSNET	-76	24	-100	54 Mbps	(Fake)	WEP	100
0016B6F8FB05	1		-74	26	-100	54 Mbps	(Fake)	WEP	100
0016CBF76596	1	Apple Network f76596	-76	24	-100	54 Mbps	(Fake)		100
000B8523649D	1	guest	-77	23	-100	54 Mbps	Airespace		100
0006B12807D5	3	MOGIL	-85	15	-100	54 Mbps	Sonicwall		100
001244B156E0	3		-89	11	-100	54 Mbps	(Fake)	WEP	100
0015F9297980	3	CDAS	-69	31	-100	54 Mbps	(Fake)	WEP	100
0014BFF93D99	4	RD	-89	11	-100	54 Mbps	(Fake)	WEP	100
00115CE54020	4	TPG-Wifi	-89	11	-100	54 Mbps	(Fake)	WEP	100
00181894A550	4		-84	16	-100	54 Mbps	(Fake)	WEP	100
001360E271A0	4		-76	24	-100	54 Mbps	(Fake)	WEP	100
001150512FF	5	Valley	-85	15	-100	54 Mbps	(Fake)	WEP	100
00E098FA24F5	6	05B403544460	-85	15	-100	54 Mbps	AboCom		200
1839403150	6	raj	-85	15	-100	54 Mbps	(Fake)	WEP	100
0011920CACB0	6	ICS1	-87	13	-100	54 Mbps	(Fake)	WEP	100
00120E124654	6	05B408941251	-86	14	-100	54 Mbps	(Fake)		200
00E098DA0FB4	6	386DMPLLC	-86	14	-100	54 Mbps	AboCom	WEP	200
000E9B2A2771	6	6edc	-89	11	-100	54 Mbps	(Fake)	WEP	100
1195556573	6	ED	-86	14	-100	54 Mbps	(Fake)	WEP	100
00E098D8D337	6	04B412679037	-88	12	-100	54 Mbps	AboCom		200
000D88BB0719	6	2125459016	-77	23	-100	54 Mbps	D-Link	WEP	100
0013106CF6EF	6	linksys	-86	14	-100	54 Mbps	(Fake)		100
00115093C376	6	MPress Records	-88	12	-100	54 Mbps	(Fake)	WEP	100
000FB5DF0D65	6	TP Unwired	-87	13	-100	54 Mbps		WEP	100
00E098CFA023	6	Bakery	-89	11	-100	54 Mbps	AboCom	WEP	200
00A0C59BA789	6	Park Avenue Country .	-68	32	-100	11 Mbps	Zyxel		100
00E098D9CA20	6		-78	22	-100	54 Mbps	AboCom	WEP	200
000D88BC0FAB	6	rinarina	-80	20	-100	54 Mbps	D-Link	WEP	100
00173F213A8F	6	EMG	-76	24	-100	54 Mbps	(Fake)	WEP	100
0014BFD472E8	6	asrlaw	-79	21	-100	54 Mbps	(Fake)	WEP	100
0016B6DEBC4C	6	CwtProductions	-90	10	-100	54 Mbps	(Fake)	WEP	100
00045A0F2E3E	6	linksys	-89	11	-100	11 Mbps	Linksys		100
000ED794C420	6	KWD-Guest	-86	14	-100	54 Mbps	Cisco	WEP	100
00120E454E06	6	06B408588383	-88	12	-100	54 Mbps	(Fake)	WEP	200
00120E452705	6	06B409819941	-86	14	-100	54 Mbps	(Fake)	WEP	200
0016B69E2981	6	eastbia	-85	15	-100	54 Mbps	(Fake)	WEP	100
000625E66BB3	6		-87	13	-100	11 Mbps	Linksys	WEP	100
001310191A65	6	SendTec	-78	22	-100	54 Mbps	(Fake)	WEP	100
000625F1482F	6	eric	-64	36	-100	11 Mbps	Linksys	WEP	100
00146CD57C24	6	AGA	-80	20	-100	54 Mbps	(Fake)		100
000C41D7F454	6	386SAS500	-64	36	-100	54 Mbps	Linksys	WEP	100
00175A10C270	6	PSNET	-70	30	-100	54 Mbps	(Fake)	WEP	100
00121774A142	6	wireless2	-78	22	-100	54 Mbps	(Fake)	WEP	100
0012179E5275	6	ZSZGuest	-80	20	-100	54 Mbps	(Fake)	WEP	100
0016B65036B2	6	ZSZNYWireless	-92	8	-100	54 Mbps	(Fake)	WEP	100
00120E41EBF9	6	06B408612547	-75	25	-100	54 Mbps	(Fake)	WEP	200
0016B663D693	6		-77	23	-100	54 Mbps	(Fake)		100
0014BF0EABC0	6	internal	-71	29	-100	54 Mbps	(Fake)	WEP	100
0015E932F591	6	default	-58	42	-100	54 Mbps	(Fake)		100
001839CAFF6B	6	linksys	-67	33	-100	54 Mbps	(Fake)		100
000FB53F0DBE	7	OPLUSB	-86	14	-100	54 Mbps			100
000FF7EA0220	7	biwap	-84	16	-100	54 Mbps	Cisco		100
0015C7FE5500	7	Advanced Focus	-91	9	-100	54 Mbps	(Fake)		100
000AB8553950	8	KPL	-88	12	-100	54 Mbps	Cisco	WEP	100
00095B5BBD7F	8		-79	21	-100	54 Mbps	Netgear	WEP	100
000F8F474000	9		-85	15	-100	54 Mbps	Cisco	WEP	100
00115CE54010	9	TPG-Wifi	-82	18	-100	54 Mbps	(Fake)	WEP	100
00146A074500	9		-63	37	-100	54 Mbps	(Fake)	WEP	100
00022D2D1B3E	9	zstation	-73	27	-100	11 Mbps	Proxim (Ager...	WEP	100
3E7F4F4DF035	10	hhonors	-71	29	-100	11 Mbps	(User-defined)		100
000D93820354	10	NYCNet2	-90	10	-100	54 Mbps	Apple	WEP	100
EE404F4E2542	10	linksys	-86	14	-100	11 Mbps	(User-defined)		100
CAC52053BCCF	10	wshotel1	-87	13	-100	54 Mbps	(User-defined)		100
0202F82AB97E	10	airportthru	-84	16	-100	11 Mbps	(User-defined)		100
0212F0052E33	10,	...Free Public WiFi	-81	19	-100	11 Mbps	(User-defined)		100
0012177088D9	11	PunchStock-NY	-88	12	-100	54 Mbps	(Fake)	WEP	100
524C3E5F609F	11	Guest	-85	15	-100	11 Mbps	(User-defined)		100
00146C00D800	11	ANNNETGEAR	-88	12	-100	54 Mbps	(Fake)		100
00146C5029F6	11	apmny	-83	17	-100	54 Mbps	(Fake)	WEP	100
00115C81C540	11		-84	16	-100	54 Mbps	(Fake)	WEP	100
001310C798C5	11		-82	18	-100	54 Mbps	(Fake)	WEP	100
00095B5BBABD	11		-81	19	-100	54 Mbps	Netgear	WEP	100
02A1BFDAB4F2	11	MH30882	-83	17	-100	11 Mbps	(User-defined)	WEP	100
065B98A8547B	11	Wireless Network	-83	17	-100	11 Mbps	(User-defined)		100
EAB84ED7223B	11	linksys	-87	13	-100	11 Mbps	(User-defined)		100
0016B6681A29	11	IMS NY 2	-87	13	-100	54 Mbps	(Fake)	WEP	100
0012A9D2A9B9	11	DIS Wireless	-75	25	-100	54 Mbps	(Fake)	WEP	100
21500003277	11								
East Lot Exit	-80	20 -100	54 Mbps	(User-def	ined)	100			
00175A10BE70	11	PSNET	-83	17	-100	54 Mbps	(Fake)	WEP	100
0212F000038F	11	Free Public WiFi	-89	11	-100	54 Mbps	(User-defined)		100
0012176D4560	11	cbs	-72	28	-100	54 Mbps	(Fake)	WEP	100
0014F1AEAAF0	11		-88	12	-100	54 Mbps	(Fake)	WEP	99
76D233C02597	11	MH31977	-65	35	-100	11 Mbps	(User-defined)	WEP	100
00C049F1C19A	11	Porcao	-84	16	-100	54 Mbps	US Robotics		100
00112491A59C	11	Olive Guests	-83	17	-100	54 Mbps	(Fake)	WEP	100
02C604DAB456	11	MH30925	-88	12	-100	11 Mbps	(User-defined)	WEP	100
000ED79FCFF0	11	KWD-Guest	-76	24	-100	54 Mbps	Cisco	WEP	100
56F7CC1AAE47	11	hpsetup	-80	20	-100	11 Mbps	(User-defined)		100
1346443648	11	2p	-87	13	-100	54 Mbps	(Fake)		100
5E9E835CD935	11	Linksys	-81	19	-100	54 Mbps	(User-defined)		100
001217AAEB28	11	G-11	-71	29	-100	54 Mbps	(Fake)	WEP	100
0215000365F3	11	gems*4WWaccess	-78	22	-100	54 Mbps	(User-defined)		100
000FB561CA24	11	Lewis	-77	23	-100	54 Mbps			100

NYI Corner of 2nd Avenue and 16th Street Netstumbler Report

MAC	Chan	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
000D6179FECB	1	Wireless	-90	10	-100	54 Mbps		WEP	100
000B851B047F	1		-89	11	-100	54 Mbps	Airespace		100
000B8523674D	1	guest	-82	18	-100	54 Mbps	Airespace		100
000FB5DA0AD1	1		-79	21	-100	54 Mbps		WEP	100
000FBB066648	1	TT_Guest	-88	12	-100	54 Mbps		WEP	100
000FBB06BCF9	1		-84	16	-100	54 Mbps		WEP	100
000FBB06BCF8	1	TT_Guest	-85	15	-100	54 Mbps		WEP	100
000FBB065048	1	TT_Guest	-82	18	-100	54 Mbps		WEP	100
000FBB066649	1		-88	12	-100	54 Mbps		WEP	100
000FBB065049	1		-80	20	-100	54 Mbps		WEP	100
000FBB0650C9	1		-83	17	-100	54 Mbps		WEP	100
000FBB0650C8	1	TT_Guest	-81	19	-100	54 Mbps		WEP	100
0017C5057652	1	SNG-WiFi	-86	14	-100	54 Mbps	(Fake)	WEP	100
001310B3E586	1	Chatham_Showroom	-80	20	-100	54 Mbps	(Fake)	WEP	100
001150728D54	1	ciscotemp	-91	9	-100	54 Mbps	(Fake)	WEP	100
00115023B4D2	1	siliwap4	-86	14	-100	54 Mbps	(Fake)	WEP	100
001759EFC170	1	PSNET	-70	30	-100	54 Mbps	(Fake)	WEP	100
0013100376AA	1	nikkoshrm	-70	30	-100	54 Mbps	(Fake)	WEP	100
0013C4CEA840	2		-90	10	-100	54 Mbps	(Fake)	WEP	100
0015F9297980	3	CDAS	-82	18	-100	54 Mbps	(Fake)	WEP	100
000BACE53B86	3	WMF2003	-84	16	-100	11 Mbps	3Com Europe	WEP	100
0012D9FB6360	3		-79	21	-100	54 Mbps	(Fake)	WEP	100
00115CE55060	5	TPG-Wifi	-89	11	-100	54 Mbps	(Fake)	WEP	100
00175A10C270	6	PSNET	-80	20	-100	54 Mbps	(Fake)	WEP	100
00146C1F23A9	6	nywifi	-80	20	-100	54 Mbps	(Fake)	WEP	100
4E0298039402	6	MH31960	-89	11	-100	11 Mbps	(User-defined)	WEP	100
1310416394	6	linksys	-81	19	-100	54 Mbps	(Fake)		100
0014BFED2E08	6		-85	15	-100	54 Mbps	(Fake)		100
0016B6D76335	6	linksys	-89	11	-100	54 Mbps	(Fake)		100
0016B65036B2	6	ZSZNYWireless	-79	21	-100	54 Mbps	(Fake)	WEP	100
00121774A142	6	wireless2	-79	21	-100	54 Mbps	(Fake)	WEP	100
000F661863FE	6	certified	-74	26	-100	54 Mbps	Linksys		100
0050F2C8C5EE	6	MSHOME	-86	14	-100	11 Mbps	Microsoft		100
000C41B1D2A0	6	secret	-80	20	-100	11 Mbps	Linksys	WEP	100
000D88946BD1	6	DJMHome	-85	15	-100	11 Mbps	D-Link	WEP	100
0014BF184D17	6	nyl-1619	-88	12	-100	54 Mbps	(Fake)		100
001310D0D43A	6	golden	-80	20	-100	54 Mbps	(Fake)	WEP	100
00146C14861E	6	souter	-80	20	-100	54 Mbps	(Fake)	WEP	100
1839403150	6	raj	-86	14	-100	54 Mbps	(Fake)	WEP	100
001217C5A706	6	R&B,NY	-70	30	-100	54 Mbps	(Fake)	WEP	100
00183980F156	6	Fum2	-73	27	-100	54 Mbps	(Fake)	WEP	100
0015E96B91B6	6	GRANITEfilms	-87	13	-100	54 Mbps	(Fake)	WEP	100
00904C600400	6	Bormioli	-77	23	-100	54 Mbps	Epigram	WEP	100
0016B69E2981	6	eastbia	-67	33	-100	54 Mbps	(Fake)	WEP	100
001217609F90	6	camsil	-78	22	-100	54 Mbps	(Fake)		100
000F6637517A	6	linksys	-71	29	-100	54 Mbps	Linksys	WEP	100
0015E96BA91C	6	Kennex New York Sh...	-81	19	-100	54 Mbps	(Fake)		100
0016B6D7632F	6	linksys	-73	27	-100	54 Mbps	(Fake)		100
00120E45222F	6	06B408711356	-79	21	-100	54 Mbps	(Fake)	WEP	200
00183956B6B3	6	linksys	-62	38	-100	54 Mbps	(Fake)		100
02021F6EBBBD	7	MJ$-Prn	-82	18	-100	11 Mbps	(User-defined)		100
000FB53F0DBE	7	OPLUSB	-87	13	-100	54 Mbps			100
0014F1605A80	8	royaldoulton	-79	21	-100	54 Mbps	(Fake)	WEP	100
1562973670	8		-71	29	-100	54 Mbps	(Fake)	WEP	100
00115CE54010	9	TPG-Wifi	-86	14	-100	54 Mbps	(Fake)	WEP	100
00026F36AA0C	10	Junxion_Box	-80	20	-100	11 Mbps	Senao Intl		100
000D93EB5D5D	10	Hunter Wireless	-77	23	-100	54 Mbps	Apple	WEP	100
02008D2BFD47	10	hpsetup	-74	26	-100	11 Mbps	(User-defined)		100
0202F82AB97E	10	airportthru	-78	22	-100	11 Mbps	(User-defined)		100
000D93EBBF85	10	Hunter Wireless	-74	26	-100	54 Mbps	Apple	WEP	100
000A95F18499	10	Venini Showroom	-73	27	-100	54 Mbps	Apple	WEP	100
000FBB06B8A8	11	TT_Guest	-83	17	-100	54 Mbps		WEP	100
000FB5590498	11	jpprod	-81	19	-100	54 Mbps		WEP	100
000F668C070F	11	scafati	-67	33	-100	11 Mbps	Linksys	WEP	100
001310856B95	11	HCI-CCA	-85	15	-100	54 Mbps	(Fake)	WEP	100
1380042850	11		-81	19	-100	54 Mbps	(Fake)	WEP	100
0200BBC88869	11	LiteShow	-72	28	-100		(User-defined)		100
00141B61D2E0	11		-77	23	-100	54 Mbps	(Fake)	WEP	100
F2FC914A4175	11	Free Internet Access	-77	23	-100	11 Mbps	(User-defined)		100
00146C9F166A	11	DAUM	-68	32	-100	54 Mbps	(Fake)	WEP	100
02166F0000E5	11	hpsetup	-71	29	-100	54 Mbps	(User-defined)	WEP	100

NYI 2nd Avenue Netstumbler Report

MAC	SSID	Chan	Signal+	Noise-	SNR+	Speed	Vendor	Type	Enc...	Beac...
000FBB06B939		1	-84	-100	16	54 Mbps		AP	WEP	100
0014A481F1B6	1c1f	1	-85	-100	15	54 Mbps	(Fake)	AP	WEP	100
000FBB06BAA9		1	-80	-100	20	54 Mbps		AP	WEP	100
000FBB06BAA8	TT_Guest	1	-81	-100	19	54 Mbps		AP	WEP	100
0015C7ABBA80		1	-82	-100	18	54 Mbps	(Fake)	AP	WEP	100
1193248340	tsunami	1	-85	-100	15	54 Mbps	(Fake)	AP		100
0014A9D4F430		1	-82	-100	18	54 Mbps	(Fake)	AP	WEP	100
000FBB066649		1	-71	-100	29	54 Mbps		AP	WEP	100
000FBB066648	TT_Guest	1	-76	-100	24	54 Mbps		AP	WEP	100
00141BB71AD0	Gr1mmD3l19h7	1	-87	-100	13	54 Mbps	(Fake)	AP	WEP	100
000B85236B7D	guest	1	-85	-100	15	54 Mbps	Airespace	AP		100
000B85236B7E		1	-84	-100	16	54 Mbps	Airespace	AP	WEP	100
000B8523674E		1	-91	-100	9	54 Mbps	Airespace	AP	WEP	100
00135FFBCE90		1	-83	-100	17	11 Mbps	(Fake)	AP		100
0016CBF76596	Apple Network f76596	1	-82	-100	18	54 Mbps	(Fake)	AP		100
000B8523674D	guest	1	-84	-100	16	54 Mbps	Airespace	AP		100
001686F8F805		1	-68	-100	32	54 Mbps	(Fake)	AP	WEP	100
000F6634FE7E	scott	1	-72	-100	28	11 Mbps	Linksys	AP	WEP	100
0017C5057571	SNG-WiFi	1	-69	-100	31	54 Mbps	(Fake)	AP	WEP	100
000FBB0650C8	TT_Guest	1	-88	-100	12	54 Mbps		AP	WEP	100
000FBB06B858	TT_Guest	1	-87	-100	13	54 Mbps		AP	WEP	100
0014517579DB	Hunter Wireless	1	-88	-100	12	54 Mbps	(Fake)	AP	WEP	100
000FBB0650C9		1	-86	-100	14	54 Mbps		AP	WEP	100
000FBB06BCF9		1	-88	-100	12	54 Mbps		AP	WEP	100
000D6179FECB	Wireless	1	-90	-100	10	54 Mbps		AP	WEP	100
0013100376AA	nikkoshrm	1	-86	-100	14	54 Mbps	(Fake)	AP	WEP	100
001310B3E586	Chatham_Showroom	1	-83	-100	17	54 Mbps	(Fake)	AP	WEP	100
000FBB06B4D9		1	-77	-100	23	54 Mbps		AP	WEP	100
00115023B4D2	siliwap4	1	-75	-100	25	54 Mbps	(Fake)	AP	WEP	100
0016B66A08BC	ChumbaWumba2	1	-87	-100	13	54 Mbps	(Fake)	AP	WEP	100
000FBB06B4D8	TT_Guest	1	-77	-100	23	54 Mbps		AP	WEP	100
0013C4CEA840		2	-82	-100	18	54 Mbps	(Fake)	AP	WEP	100
00028A9E9A57		3	-77	-100	23	11 Mbps	Ambit	AP	WEP	100
0012D9FB6360		3	-78	-100	22	54 Mbps	(Fake)	AP	WEP	100
0015F9297980	CDAS	3	-83	-100	17	54 Mbps	(Fake)	AP	WEP	100
001360E271A0		4	-86	-100	14	54 Mbps	(Fake)	AP	WEP	100
00181894A550		4	-71	-100	29	54 Mbps	(Fake)	AP	WEP	100
000F34891153	Carlton	4	-87	-100	13	11 Mbps	Cisco	AP		100
0014BFF93D99	RD	4	-78	-100	22	54 Mbps	(Fake)	AP	WEP	100
0014BF184D1A	nyl-br	6	-88	-100	12	54 Mbps	(Fake)	AP		100
4E0298039402	MH31960	6	-86	-100	14	11 Mbps	(User-d...	Peer	WEP	100
00146C1477D4		6	-88	-100	12	54 Mbps	(Fake)	AP	WEP	100
000F66E4D487		6	-88	-100	12	54 Mbps	Linksys	AP		100
0014A44D58DB	f7e4	6	-84	-100	16	54 Mbps	(Fake)	AP	WEP	100
000E9B2A2DA9	59ab	6	-85	-100	15	54 Mbps	(Fake)	AP	WEP	100
000FBB06BAE8	TT_Guest	6	-86	-100	14	54 Mbps		AP	WEP	100
000FBB066989		6	-80	-100	20	54 Mbps		AP	WEP	100
000FBB066538	TT_Guest	6	-89	-100	11	54 Mbps		AP	WEP	100
00120E168C7B		6	-88	-100	12	54 Mbps	(Fake)	AP	WEP	200
000FBB066988	TT_Guest	6	-75	-100	25	54 Mbps		AP	WEP	100
000F66089FE1	mitchell	6	-91	-100	9	54 Mbps	Linksys	AP		100
0013109E731A	19507489	6	-85	-100	15	54 Mbps	(Fake)	AP	WEP	100
0016B6D76335	linksys	6	-86	-100	14	54 Mbps	(Fake)	AP		100
00134686B4F6	Zoe	6	-75	-100	25	54 Mbps	(Fake)	AP	WEP	100
001346A7C9DA	M2M	6	-81	-100	19	54 Mbps	(Fake)	AP		100
000FBB066539		6	-83	-100	17	54 Mbps		AP	WEP	100
00E098CFA023	Bakery	6	-85	-100	15	54 Mbps	AboCom	AP	WEP	200
001647A0A870		6	-58	-100	42	54 Mbps	(Fake)	AP	WEP	100
0014A416D501	602d	6	-82	-100	18	54 Mbps	(Fake)	AP	WEP	100
001310191A65	SendTec	6	-87	-100	13	54 Mbps	(Fake)	AP	WEP	100
00A0C59BA789	Park Avenue Country ...	6	-84	-100	16	11 Mbps	Zyxel	AP		100
00E098DA0FB4	386DMPLLC	6	-81	-100	19	54 Mbps	AboCom	AP	WEP	200
001310EE96BF		6	-89	-100	11	54 Mbps	(Fake)	AP		100
0012179E5275	ZSZGuest	6	-87	-100	13	54 Mbps	(Fake)	AP	WEP	100
000625F1482F	eric	6	-71	-100	29	11 Mbps	Linksys	AP	WEP	100
000FCC678010	3170 7734	6	-86	-100	14	54 Mbps		AP	WEP	100
00173F213A8F	EMG	6	-87	-100	13	54 Mbps	(Fake)	AP	WEP	100
000D88BB0719	2125459016	6	-85	-100	15	54 Mbps	D-Link	AP	WEP	100
00E098D9CA20		6	-77	-100	23	54 Mbps	AboCom	AP	WEP	200
0014BFD472E8	asrlaw	6	-81	-100	19	54 Mbps	(Fake)	AP	WEP	100
0014BF0EABC0	internal	6	-73	-100	27	54 Mbps	(Fake)	AP	WEP	100
00175A10C270	PSNET	6	-85	-100	15	54 Mbps	(Fake)	AP	WEP	100
000C41D7F454	386SAS500	6	-71	-100	29	54 Mbps	Linksys	AP	WEP	100
0050F2CF5B20	ElIMel	6	-89	-100	11	11 Mbps	Microsoft	AP		100
000D88BC0FAB	rinarina	6	-84	-100	16	54 Mbps	D-Link	AP	WEP	100
00146CD57C24	AIGA	6	-77	-100	23	54 Mbps	(Fake)	AP		100
0016B69E2981	eastbia	6	-91	-100	9	54 Mbps	(Fake)	AP	WEP	100
00045A0F2E3E	linksys	6	-86	-100	14	11 Mbps	Linksys	AP		100
001217AA4177	WENN-NY	6	-85	-100	15	54 Mbps	(Fake)	AP	WEP	100
00E098FA24F5	05B405544460	6	-80	-100	20	54 Mbps	AboCom	AP		200
00183980F156	Fum2	6	-80	-100	20	54 Mbps	(Fake)	AP	WEP	100
000F3D00D089	grantass	6	-76	-100	24	54 Mbps		AP	WEP	100
00121774A142	wireless2	6	-76	-100	24	54 Mbps	(Fake)	AP	WEP	100
00131034977	michigan	6	-86	-100	14	54 Mbps	(Fake)	AP	WEP	100
0016B6503A7F	ZSZMADISON	6	-85	-100	15	54 Mbps	(Fake)	AP	WEP	100
1839403150	raj	6	-72	-100	28	54 Mbps	(Fake)	AP	WEP	100
00120E45222F	06B408711356	6	-83	-100	17	54 Mbps	(Fake)	AP	WEP	200
00904C600400	Bormioli	6	-85	-100	15	54 Mbps	Epigram	AP	WEP	100
1310416394	linksys	6	-74	-100	26	54 Mbps	(Fake)	AP		100
0016B6D7632F	linksys	6	-80	-100	20	54 Mbps	(Fake)	AP		100
0015E96B91B6	GRANITEfilms	6	-88	-100	12	54 Mbps	(Fake)	AP	WEP	100
0015E96BA91C	Kennex New York Sh...	6	-80	-100	20	54 Mbps	(Fake)	AP		100
000F661863FE		6	-81	-100	19	54 Mbps	Linksys	AP		100
0016B65036B2	ZSZNYWireless	6	-69	-100	31	54 Mbps	(Fake)	AP	WEP	100
001310C8AE44	linksys-srx	6	-84	-100	16	54 Mbps	(Fake)	AP	WEP	100
00183956B6B3	linksys	6	-80	-100	20	54 Mbps	(Fake)	AP		100
001217609F90	camsil	6	-77	-100	23	54 Mbps	(Fake)	AP		100
000F6637517A	linksys	6	-71	-100	29	54 Mbps	Linksys	AP	WEP	100
0013461D698C	PERLMAN	7	-84	-100	16	54 Mbps	(Fake)	AP	WEP	100
000FF7EA0220	biwap	7	-70	-100	30	54 Mbps	Cisco	AP		100
000FB53F0DBE	OPLUSB	7	-77	-100	23	54 Mbps		AP		100
00095B5BBD7F		8	-88	-100	12	54 Mbps	Netgear	AP	WEP	100
0014F1605A80	royaldoulton	8	-80	-100	20	54 Mbps	(Fake)	AP	WEP	100
1562973670		8	-64	-100	36	54 Mbps	(Fake)	AP	WEP	100
001360E263F0		9	-74	-100	26	54 Mbps	(Fake)	AP	WEP	100
000F8F474000		9	-83	-100	17	54 Mbps	Cisco	AP	WEP	100
00022D2D1B3E	zstation	9	-82	-100	18	11 Mbps	Proxim (...	AP	WEP	100
00146A074500		9	-55	-100	45	54 Mbps	(Fake)	AP	WEP	100
00095BC98D94	NETGEAR	9	-85	-100	15	54 Mbps	Netgear	AP	WEP	100
0013C4CE8C30		9	-87	-100	13	54 Mbps	(Fake)	AP	WEP	100
968FB188CE2F	Guest	10	-85	-100	15	11 Mbps	(User-d...	Peer		100
8AA74F4D3655	Jet Blue hot spot	10	-75	-100	25	11 Mbps	(User-d...	Peer		100
3E7F4F4DF035	hotspot	10	-71	-100	29	11 Mbps	(User-d...	Peer		100
000D93EBBF85	Hunter Wireless	10	-80	-100	20	54 Mbps	Apple	AP	WEP	100
BA384F4AE713	1	10	-82	-100	18	11 Mbps	(User-d...	Peer		100
00026F36AA0C	Junxion_Box	10	-73	-100	27	11 Mbps	Senao Intl	AP		100
0202F82AB97E	airportthru	10	-83	-100	17	11 Mbps	(User-d...	Peer		100
365BA64BD57B	STRIVE-E	10	-72	-100	28	11 Mbps	(User-d...	Peer		100
001124053D6B	Apple Network 053d6b	11	-86	-100	14	54 Mbps	(Fake)	AP	WEP	100
0011500055CD	belkin54g	11	-87	-100	13	54 Mbps	(Fake)	AP	WEP	100
EAB84ED7223B	linksys	11	-87	-100	13	11 Mbps	(User-d...	Peer		100
001124A11D9E	TWM	11	-88	-100	12	54 Mbps	(Fake)	AP	WEP	100
00120064A750		11	-89	-100	11	54 Mbps	(Fake)	AP	WEP	100
000FBB06B519		11	-83	-100	17	54 Mbps		AP	WEP	100
000FBB06B518	TT_Guest	11	-83	-100	17	54 Mbps		AP	WEP	100
000FBB06BA59		11	-80	-100	20	54 Mbps		AP	WEP	100
00095BFA9980	QUEENSRYCHE	11	-87	-100	13	54 Mbps	Netgear	AP	WEP	100
3A3E4F4E2E73	Free Public WiFi	11	-83	-100	17	54 Mbps	(User-d...	Peer		100
0011249AA0DA	StrawberryFrog	11	-87	-100	13	54 Mbps	(Fake)	AP	WEP	100
000FBB06B8E8	TT_Guest	11	-69	-100	31	54 Mbps		AP	WEP	100
000FBB06BD59		11	-76	-100	24	54 Mbps		AP	WEP	100
0012A95546D6	zdm*2828	11	-78	-100	22	54 Mbps	(Fake)	AP	WEP	100
86E25448BB26	linksys	11	-78	-100	22	54 Mbps	(User-d...	Peer		100
02166F0000A4	PWC80211	11	-69	-100	31	54 Mbps	(User-d...	Peer		100
000FBB06BA58	TT_Guest	11	-84	-100	16	54 Mbps		AP	WEP	100
000FBB06BD58	TT_Guest	11	-76	-100	24	54 Mbps		AP	WEP	100
00112491A59C	Olive Guests	11	-83	-100	17	54 Mbps	(Fake)	AP	WEP	100
065B98A8547B	Wireless Network	11	-81	-100	19	11 Mbps	(User-d...	Peer		100
001310C798C5		11	-85	-100	15	54 Mbps	(Fake)	AP	WEP	100
56F7CC1AAE47	hpsetup	11	-85	-100	15	11 Mbps	(User-d...	Peer		100
0012A9D2A9B9	DIS Wireless	11	-83	-100	17	54 Mbps	(Fake)	AP	WEP	100
00095B5BBABD		11	-83	-100	17	54 Mbps	Netgear	AP	WEP	100
00121770B8D9	PunchStock-NY	11	-85	-100	15	54 Mbps	(Fake)	AP	WEP	100
0012176D4560	cbs	11	-77	-100	23	54 Mbps	(Fake)	AP	WEP	100
00115C81C540		11	-87	-100	13	54 Mbps	(Fake)	AP	WEP	100
00146C5029F6	apmny	11	-83	-100	17	54 Mbps	(Fake)	AP	WEP	100
001217AAEB28	G-11	11	-66	-100	34	54 Mbps	(Fake)	AP	WEP	100
000F668C070F	scafati	11	-82	-100	18	11 Mbps	Linksys	AP	WEP	100
000FBB06B8E9		11	-68	-100	32	54 Mbps		AP	WEP	100
0213CE0000E1	freeaccess.les.net	11	-88	-100	12	54 Mbps	(User-d...	Peer		100
001310B56B95	HCI-CCA	11	-83	-100	17	54 Mbps	(Fake)	AP	WEP	100
00120E4EB46D	Noritake	11	-75	-100	25	54 Mbps	(Fake)	AP	WEP	200
02166F0000AB	tmobile	11	-82	-100	18	54 Mbps	(User-d...	Peer		100
0200BBC88869	LiteShow	11	-82	-100	18		(User-d...	Peer		100
F2FC914A4175	Free Internet Access	11	-70	-100	30	11 Mbps	(User-d...	Peer		100

NYI 16th Street Netstumbler Report

MAC	Chan	SSID	Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
000B8523674D	1	guest	-86	14	-100	54 Mbps	Airespace		100
000FBB0650C9	1		-83	17	-100	54 Mbps		WEP	100
000FBB0650C8	1	TT_Guest	-81	19	-100	54 Mbps		WEP	100
000B85236B7E	1		-84	16	-100	54 Mbps	Airespace	WEP	100
000ED794C440	1	KWD-Guest	-66	34	-100	54 Mbps	Cisco	WEP	100
000FBB06B858	1	TT_Guest	-88	12	-100	54 Mbps		WEP	100
000750D65F3F	1		-85	15	-100	11 Mbps	Cisco	WEP	100
000B8523674E	1		-84	16	-100	54 Mbps	Airespace	WEP	100
000FBB06BCF9	1		-85	15	-100	54 Mbps		WEP	100
000FBB06BCF8	1	TT_Guest	-88	12	-100	54 Mbps		WEP	100
00141BB71AD0	1	Gr1mmD3l19h7	-77	23	-100	54 Mbps	(Fake)	WEP	100
001759EFC170	1	PSNET	-69	31	-100	54 Mbps	(Fake)	WEP	100
001150728D54	1	ciscotemp	-78	22	-100	54 Mbps	(Fake)	WEP	100
0013100376AA	1	nikkoshrm	-70	30	-100	54 Mbps	(Fake)	WEP	100
000FB5DA0AD1	1		-77	23	-100	54 Mbps		WEP	100
001310B3E586	1	Chatham_Showroom	-71	29	-100	54 Mbps	(Fake)	WEP	100
0018396B5246	1	Devinsky	-83	17	-100	54 Mbps	(Fake)	WEP	100
000BACE53B86	3	WMF2003	-87	13	-100	11 Mbps	3Com Europe	WEP	100
0015F9297980	3	CDAS	-79	21	-100	54 Mbps	(Fake)	WEP	100
0012D9FB6360	3		-83	17	-100	54 Mbps	(Fake)		100
00115CE55060	5	TPG-Wifi	-85	15	-100	54 Mbps	(Fake)	WEP	100
0013469863BD	6	GSBINC	-80	20	-100	54 Mbps	(Fake)	WEP	100
00183957B74B	6	DO NOT USE	-87	13	-100	54 Mbps	(Fake)	WEP	100
00120E45222F	6	06B408711356	-86	14	-100	54 Mbps	(Fake)	WEP	200
00120E41EBF9	6	06B408612547	-84	16	-100	54 Mbps	(Fake)	WEP	200
0012179E5275	6	ZSZGuest	-72	28	-100	54 Mbps	(Fake)	WEP	100
0016B663D693	6		-83	17	-100	54 Mbps	(Fake)		100
001195E6793D	6	default	-69	31	-100	54 Mbps	(Fake)		100
000ED794C420	6	KWD-Guest	-73	27	-100	54 Mbps	Cisco	WEP	100
00146C14861E	6	souter	-86	14	-100	54 Mbps	(Fake)	WEP	100
0015E96BA91C	6	Kennex New York Sh...	-74	26	-100	54 Mbps	(Fake)		100
000C41B1D2A0	6	secret	-90	10	-100	11 Mbps	Linksys	WEP	100
00175A10C270	6	PSNET	-83	17	-100	54 Mbps	(Fake)	WEP	100
0016B65036B2	6	ZSZNYWireless	-81	19	-100	54 Mbps	(Fake)	WEP	100
001217609F90	6	camsil	-73	27	-100	54 Mbps	(Fake)		100
0012171DCD8F	6	Rachel	-89	11	-100	54 Mbps	(Fake)	WEP	100
00121774A142	6	wireless2	-86	14	-100	54 Mbps	(Fake)	WEP	100
00904C600400	6	Bormioli	-72	28	-100	54 Mbps	Epigram	WEP	100
000FBB06AFC8	6	TT_Guest	-85	15	-100	54 Mbps		WEP	100
001217C5A706	6	R&B,NY	-66	34	-100	54 Mbps	(Fake)	WEP	100
000D88946BD1	6	DJMHome	-77	23	-100	11 Mbps	D-Link	WEP	100
000F6637517A	6	linksys	-84	16	-100	54 Mbps	Linksys	WEP	100
0016B62EF798	6	linksys	-92	8	-100	54 Mbps	(Fake)		100
0016B69E2981	6	eastbia	-64	36	-100	54 Mbps	(Fake)	WEP	100
001310D0D43A	6	golden	-79	21	-100	54 Mbps	(Fake)	WEP	100
00183956B6B3	6	linksys	-75	25	-100	54 Mbps	(Fake)		100
0016B6AD94BC	8	spearsimes	-82	18	-100	54 Mbps	(Fake)	WEP	100
1562973670	8		-79	21	-100	54 Mbps	(Fake)	WEP	100
0014F1605A80	8	royaldoulton	-75	25	-100	54 Mbps	(Fake)	WEP	100
00022D2D1B3E	9	zstation	-83	17	-100	11 Mbps	Proxim (Ager...	WEP	100
8233EB40D562	10	hpsetup	-74	26	-100	11 Mbps	(User-defined)		100
0202F82AB97E	10	airportthru	-84	16	-100	11 Mbps	(User-defined)		100
02008D2BFD47	10	hpsetup	-68	32	-100	11 Mbps	(User-defined)		100
000D93EB5D5D	10	Hunter Wireless	-67	33	-100	54 Mbps	Apple	WEP	100
FEC4A45969A7	10	SMARTSIGHT	-77	23	-100	11 Mbps	(User-defined)		100
000A95F18499	10	Venini Showroom	-79	21	-100	54 Mbps	Apple	WEP	100
56F7CC1AAE47	11	hpsetup	-85	15	-100	11 Mbps	(User-defined)		100
1380043700	11		-83	17	-100	54 Mbps	(Fake)	WEP	100
02150000009A	11	Wireless Network	-80	20	-100	54 Mbps	(User-defined)		100
21500003277	11								
East Lot Exit	-79	21 -100	54 Mbps	(User-def	ined)	100			
02166F0002D3	11	ATIS_WiFi	-84	16	-100	54 Mbps	(User-defined)		100
02150000013B	11	Harvard University	-87	13	-100	54 Mbps	(User-defined)		100
0215000365F3	11	gems*4WWaccess	-82	18	-100	54 Mbps	(User-defined)		100
000ED79FCFF0	11	KWD-Guest	-81	19	-100	54 Mbps	Cisco	WEP	100
00C049F1C19A	11	Porcao	-61	39	-100	54 Mbps	US Robotics		100
2.15E+15	11	MOBILE	-75	25	-100	54 Mbps	(User-defined)		100
000FBB06BA88	11	TT_Guest	-77	23	-100	54 Mbps		WEP	100
000FBB06B8A8	11	TT_Guest	-76	24	-100	54 Mbps		WEP	100
1380042850	11		-81	19	-100	54 Mbps	(Fake)	WEP	100
000FBB06B8A9	11		-75	25	-100	54 Mbps		WEP	100
001310856B95	11	HCI-CCA	-91	9	-100	54 Mbps	(Fake)	WEP	100
00141B61D2E0	11		-67	33	-100	54 Mbps	(Fake)	WEP	100
00120E4EB46D	11	Noritake	-88	12	-100	54 Mbps	(Fake)	WEP	200
000F668C070F	11	scafati	-76	24	-100	11 Mbps	Linksys	WEP	100
02166F0000E5	11	hpsetup	-88	12	-100	54 Mbps	(User-defined)	WEP	100
00146C9F166A	11	DAUM	-69	31	-100	54 Mbps	(Fake)	WEP	100

NYI 17th Street Netstumbler Report

MAC	Chan	SSID		Signal+	SNR+	Noise-	Speed	Vendor	Encryption	Bea...
001310B3E586	1	Chatham_	Showroom	-85	15	-100	54 Mbps	(Fake)	WEP	100
0015C7ABCFA1	1	qeex0000		-88	12	-100	54 Mbps	(Fake)	WEP	100
0015C7ABCFA0	1			-88	12	-100	54 Mbps	(Fake)	WEP	100
000FBB06B939	1			-87	13	-100	54 Mbps		WEP	100
0016B66A08DC	1	ChumbaWu	mba2	-87	13	-100	54 Mbps	(Fake)	WEP	100
0017C5057652	1	SNG-WiFi		-85	15	-100	54 Mbps	(Fake)	WEP	100
000FBB06BCF9	1			-90	10	-100	54 Mbps		WEP	100
0012A9558A3D	1	zdm*2828		-84	16	-100	54 Mbps	(Fake)	WEP	100
000FBB06B938	1	TT_Guest		-87	13	-100	54 Mbps		WEP	100
0015C7ABBA81	1	qeex0000		-83	17	-100	54 Mbps	(Fake)	WEP	100
00112498D4F9	1	Strawber	ryFrog	-88	12	-100	54 Mbps	(Fake)	WEP	100
000FBB06B4D8	1	TT_Guest		-83	17	-100	54 Mbps		WEP	100
000FBB06B4D9	1			-84	16	-100	54 Mbps		WEP	100
06395F7C14D0	1	Wireless	Network	-87	13	-100	54 Mbps	(User-defined)		100
0014A9D4F430	1			-82	18	-100	54 Mbps	(Fake)	WEP	100
0014A481F1B6	1	1c1f		-88	12	-100	54 Mbps	(Fake)	WEP	100
0017C5057571	1	SNG-WiFi		-70	30	-100	54 Mbps	(Fake)	WEP	100
0016B6F8FB05	1			-72	28	-100	54 Mbps	(Fake)	WEP	100
000F6634FE7E	1	scott		-73	27	-100	11 Mbps	Linksys	WEP	100
000FBB066649	1			-80	20	-100	54 Mbps		WEP	100
000FBB066648	1	TT_Guest		-79	21	-100	54 Mbps		WEP	100
0013C4CEA840	2			-88	12	-100	54 Mbps	(Fake)	WEP	100
0012D9FB6360	3			-76	24	-100	54 Mbps	(Fake)		100
0015F9297980	3	CDAS		-82	18	-100	54 Mbps	(Fake)	WEP	100
0014BFF93D99	4	RD		-70	30	-100	54 Mbps	(Fake)	WEP	100
00181894A550	4			-77	23	-100	54 Mbps	(Fake)	WEP	100
001217AA4177	6	WENN-NY		-84	16	-100	54 Mbps	(Fake)	WEP	100
0016B6D7632F	6	linksys		-89	11	-100	54 Mbps	(Fake)		100
000F6637517A	6	linksys		-83	17	-100	54 Mbps	Linksys	WEP	100
000FBB066538	6	TT_Guest		-87	13	-100	54 Mbps		WEP	100
0014BF184D1A	6	nyl-br		-84	16	-100	54 Mbps	(Fake)		100
000F66186A8F	6	gold		-86	14	-100	54 Mbps	Linksys	WEP	100
000F66E4D487	6			-76	24	-100	54 Mbps	Linksys		100
001839ACD15E	6	offermat	ica	-85	15	-100	54 Mbps	(Fake)	WEP	100
000F3D00D089	6	grantass		-81	19	-100	54 Mbps		WEP	100
00120E1036D7	6	05B40864	8279	-81	19	-100	54 Mbps	(Fake)		200
0014A44D58DB	6	f7e4		-82	18	-100	54 Mbps	(Fake)	WEP	100
00183956B6B3	6	linksys		-78	22	-100	54 Mbps	(Fake)		100
0013109E731A	6	19507489		-87	13	-100	54 Mbps	(Fake)	WEP	100
0016B65036B2	6	ZSZNYWir	eless	-80	20	-100	54 Mbps	(Fake)	WEP	100
00121774A142	6	wireless	2	-83	17	-100	54 Mbps	(Fake)	WEP	100
000E9B2A2DA9	6	59ab		-81	19	-100	54 Mbps	(Fake)	WEP	100
0016B6E4BE80	6	Motivic		-87	13	-100	54 Mbps	(Fake)	WEP	100
0012171BB24F	6	Goldman-	WiFi	-79	21	-100	54 Mbps	(Fake)	WEP	100
000F660B9FE1	6	mitchell		-86	14	-100	54 Mbps	Linksys		100
00E098DA0FB4	6	386DMPLL	C	-82	18	-100	54 Mbps	AboCom	WEP	200
0016B6D76335	6	linksys		-78	22	-100	54 Mbps	(Fake)		100
0014A416D501	6	602d		-68	32	-100	54 Mbps	(Fake)	WEP	100
00A0C59BA789	6	Park Ave	nue Country .	-88	12	-100	11 Mbps	Zyxel		100
000FBB066539	6			-90	10	-100	54 Mbps		WEP	100
001310C8AE44	6	linksys-	srx	-84	16	-100	54 Mbps	(Fake)	WEP	100
000FCC678010	6	3170 773	4	-76	24	-100	54 Mbps		WEP	100
00146C1477D4	6			-85	15	-100	54 Mbps	(Fake)	WEP	100
000625F1482F	6	eric		-76	24	-100	11 Mbps	Linksys	WEP	100
000D88BB0719	6	21254590	16	-78	22	-100	54 Mbps	D-Link	WEP	100
0014BFD472E8	6	asrlaw		-79	21	-100	54 Mbps	(Fake)	WEP	100
00120E124654	6	05B40894	1251	-88	12	-100	54 Mbps	(Fake)		200
000C41D7F454	6	386SAS50	0	-70	30	-100	54 Mbps	Linksys	WEP	100
00175A10C270	6	PSNET		-86	14	-100	54 Mbps	(Fake)	WEP	100
1839403150	6	raj		-75	25	-100	54 Mbps	(Fake)	WEP	100
00E098FA24F5	6	05B40354	4460	-76	24	-100	54 Mbps	AboCom		200
0013468684F6	6	Zoe		-74	26	-100	54 Mbps	(Fake)	WEP	100
001647A0A870	6			-70	30	-100	54 Mbps	(Fake)	WEP	100
001346A7C9DA	6	M2M		-83	17	-100	54 Mbps	(Fake)		100
00146CD57C24	6	AGA		-74	26	-100	54 Mbps	(Fake)		100
000E387A3E6F	7	Authoriz	ed Access O..	-88	12	-100	11 Mbps	Cisco	WEP	100
000FF7EA0220	7	biwap		-81	19	-100	54 Mbps	Cisco		100
000FB53F0DBE	7	OPLUSB		-78	22	-100	54 Mbps			100
0014F1605A80	8	royaldou	lton	-84	16	-100	54 Mbps	(Fake)	WEP	100
1562973670	8			-73	27	-100	54 Mbps	(Fake)	WEP	100
000FB3B9603B	9	IHI-NY-L	LC	-90	10	-100	54 Mbps		WEP	200
000F8F474000	9			-81	19	-100	54 Mbps	Cisco	WEP	100
00022D2D1B3E	9	zstation		-85	15	-100	11 Mbps	Proxim (Ager...	WEP	100
00146A074500	9			-67	33	-100	54 Mbps	(Fake)	WEP	100
001360E263F0	9			-77	23	-100	54 Mbps	(Fake)	WEP	100
365BA64BD57B	10	STRIVE-E		-86	14	-100	11 Mbps	(User-defined)		100
00026F36AA0C	10	Junxion_	Box	-74	26	-100	11 Mbps	Senao Intl		100
0202F82AB97E	10	airportt	hru	-85	15	-100	11 Mbps	(User-defined)		100
BA384F4AE713	10	1		-78	22	-100	11 Mbps	(User-defined)		100
8AA74F4D3655	10	Jet Blue	hot spot	-86	14	-100	11 Mbps	(User-defined)		100
D24A4648BB26	10	linksys		-72	28	-100	54 Mbps	(User-defined)		100
BE344948BB26	10	linksys		-86	14	-100	54 Mbps	(User-defined)		100
00120E4EB46D	11	Noritake		-86	14	-100	54 Mbps	(Fake)	WEP	200
065B98A8547B	11	Wireless	Network	-85	15	-100	11 Mbps	(User-defined)		100
000FBB06BA58	11	TT_Guest		-90	10	-100	54 Mbps		WEP	100
000FBB06BD59	11			-86	14	-100	54 Mbps		WEP	100
000FBB06B8D9	11			-89	11	-100	54 Mbps		WEP	100
000FBB06B8D8	11	TT_Guest		-83	17	-100	54 Mbps		WEP	100
00120064A750	11			-82	18	-100	54 Mbps	(Fake)	WEP	100
001124A11D9E	11	TWM		-76	24	-100	54 Mbps	(Fake)	WEP	100
0213CE000138	11	CNET_pub	lic	-85	15	-100	54 Mbps	(User-defined)		100
000F668C070F	11	scafati		-88	12	-100	11 Mbps	Linksys	WEP	100
0012A95546D6	11	zdm*2828		-82	18	-100	54 Mbps	(Fake)	WEP	100
0011249AA0DA	11	Strawber	ryFrog	-88	12	-100	54 Mbps	(Fake)	WEP	100
000FBB06B8E9	11			-83	17	-100	54 Mbps		WEP	100
000FBB06B519	11			-88	12	-100	54 Mbps		WEP	100
001217AAEB28	11	G-11		-85	15	-100	54 Mbps	(Fake)	WEP	100
0011500055CD	11	belkin54	g	-90	10	-100	54 Mbps	(Fake)	WEP	100
00095BFA9980	11	QUEENSRY	CHE	-88	12	-100	54 Mbps	Netgear	WEP	100
000FBB06B8E8	11	TT_Guest		-82	18	-100	54 Mbps		WEP	100
00115C81C540	11			-89	11	-100	54 Mbps	(Fake)	WEP	100
02C638C70CC9	11	MH06073		-72	28	-100	11 Mbps	(User-defined)	WEP	100
02166F0000A4	11	PwC80211		-76	24	-100	54 Mbps	(User-defined)		100
56F7CC1AAE47	11	hpsetup		-88	12	-100	11 Mbps	(User-defined)		100
000FBB06BD58	11	TT_Guest		-84	16	-100	54 Mbps		WEP	100
F2FC914A4175	11	Free Int	ernet Access	-85	15	-100	11 Mbps	(User-defined)		100
00146C5029F6	11	apmny		-86	14	-100	54 Mbps	(Fake)	WEP	100
0012176D4560	11	cbs		-76	24	-100	54 Mbps	(Fake)	WEP	100

Cisco MAC Address List Summary

The following tables are the Netstumbler observed Cisco MAC address list for cross reference with previous Netstumbler reports. NYI can uses these lists to search for the NYI 11th Floor AP MAC addresses for cross reference purposes once the remaining addresses are disclosed.

10th floor Netstumbler MACs Observed that are Cisco, Cisco-Linksys or Airspace assigned.

MAC	Type	
000B850E26BF	Airspace	
000B851B020F	Airspace	
000B851B029F	Airspace	
000B851B047F	Airspace	
000B851BA3DF	Airspace	
000B851BE93F	Airspace	
000B851BECBF	Airspace	
001121D49290	Cisco	
001124A11D9E	Cisco	
00115CE54010	Cisco	
00115CE54020	Cisco	
00115CE54070	Cisco	
00115CE55020	Cisco	
00115CE55060	Cisco	
00135FFA83A2	Cisco	
0014F1605A80	Cisco	
0015C7ABB980	Cisco	
0015C7ABCFA0	Cisco	
0015C7ABCFA1	Cisco	
0015F9297980	Cisco	
001759EFA6E0	Cisco	
001759EFC170	Cisco	
001759EFC440	Cisco	
00175A10BD30	Cisco	
00175A10C270	Cisco	
00181894A550	Cisco	
00181894A6C0	Cisco	NYLCAPAP
00181894A860	Cisco	
00181894A930	Cisco	
000F6623E91B	Cisco-Linksys	
000F6623E91B	Cisco-Linksys	
000F668147D6	Cisco-Linksys	
000F668C070F	Cisco-Linksys	
0012170B9AB9	Cisco-Linksys	
0012171BB24F	Cisco-Linksys	
0012171DCD8F	Cisco-Linksys	
001217609F90	Cisco-Linksys	
0012179E5275	Cisco-Linksys	
001217AAEB28	Cisco-Linksys	
0013100376AA	Cisco-Linksys	
001310856B95	Cisco-Linksys	
001310B3E586	Cisco-Linksys	
001310B6C896	Cisco-Linksys	
0014BF184D17	Cisco-Linksys	
0014BF184D1A	Cisco-Linksys	
0014BF4A4E42	Cisco-Linksys	
0014BF7305A2	Cisco-Linksys	
0014BFF93D99	Cisco-Linksys	
0016B6D76335	Cisco-Linksys	
0016B6D76335	Cisco-Linksys	
0016B6DD4C31	Cisco-Linksys	
000625F1482F	Linksys	
000C41D7F454	Linksys	
000C41FA3089	Linksys	

11th floor Netstumbler MACs Observed that are Cisco, Cisco-Linksys or Airspace assigned.

MAC	Type
000B850E26BF	Airspace
000B851B029F	Airspace
000B851B047F	Airspace
000B851BE93F	Airspace
001121D49290	Cisco
00115CE54010	Cisco
00115CE54020	Cisco
00115CE54020	Cisco
00115CE54070	Cisco
00115CE55020	Cisco
00115CE55060	Cisco
00120064A750	Cisco
00135FFA83A2	Cisco
0015F9297980	Cisco
001759EFC170	Cisco
001759EFC440	Cisco
00175A10C270	Cisco
00181894A550	Cisco
00181894A6C0	Cisco
00181894A860	Cisco
00181894A930	Cisco
0014F1605A80	Cisco
000F660B9FE1	Cisco-Linksys
000F668147D6	Cisco-Linksys
0012171BB24F	Cisco-Linksys
001217609F90	Cisco-Linksys
0013100376AA	Cisco-Linksys
00131082AB98	Cisco-Linksys
001310856B95	Cisco-Linksys
001310B3E586	Cisco-Linksys
0014BF184D17	Cisco-Linksys
0014BF184D1A	Cisco-Linksys
0014BF7305A2	Cisco-Linksys
0016B62EF798	Cisco-Linksys
0016B648750D	Cisco-Linksys
0016B6D76335	Cisco-Linksys
00183956B6B3	Cisco-Linksys

12th floor Netstumbler MACs Observed that are Cisco, Cisco-Linksys or Airspace assigned.

MAC	Type
0015C7ABCFA0	Cisco
001647A0A870	Cisco

12th floor MAC addresses discovered using CommView

The following table lists the 12Th floor MAC address observed using CommView. During the 12th floor scan AMI conducted a Netstumbler and CommView scan simultaneously to ensure as much relevant data is captured as possible within the limited floor access time. NYI should review this list to see if other NYIIM APs MAC addresses are noted when disclosed.

MAC/Alias
SolomonExt:27:C6:2B
SolomonExt:07:2C:43
SolomonExt:1C:55:34
SiemensIcn:06:BA:F9
SiemensIcn:06:BA:F8
SiemensIcn:06:50:C9
SiemensIcn:06:BA:88
SiemensIcn:06:BA:E9
SiemensIcn:06:65:39
SiemensIcn:06:66:49
SiemensIcn:06:B8:18
SiemensIcn:06:BA:E8
SiemensIcn:06:B8:19
SiemensIcn:06:50:C8
SiemensIcn:06:BC:F8
SiemensIcn:06:BC:F9
SiemensIcn:06:50:48
SiemensIcn:06:B9:88
SiemensIcn:06:50:49
SiemensIcn:06:BA:89
SiemensIcn:06:B8:58
SiemensIcn:06:B8:59
SiemensIcn:06:B9:89
SiemensIcn:06:B8:A9
SiemensIcn:06:B8:A8
SiemensIcn:06:69:88
SiemensIcn:06:AF:C9
SiemensIcn:06:B4:D9
SiemensIcn:06:B4:D8
SiemensIcn:06:B5:19
SiemensIcn:06:B5:18
SiemensIcn:06:AF:C8
SiemensIcn:06:BD:59
SiemensIcn:06:B9:38
SiemensIcn:06:BA:A8
SiemensIcn:06:BA:A9
SiemensIcn:06:BD:58
SiemensIcn:06:B9:39
SiemensIcn:06:BA:58
SiemensIcn:06:B8:E9

SiemensIcn:06:66:48
SiemensIcn:06:69:89
SiemensIcn:06:B8:E8
SiemensIcn:06:B8:D9
SiemensIcn:06:65:38
SiemensIcn:06:BA:39
SiemensIcn:06:BA:38
SiemensIcn:06:BA:59
SiemensIcn:06:B9:48
SiemensIcn:06:B9:49
Proxim:DB:09:ED
Private:29:75:4D
PhilipsCom:50:77:AA
PhilipsCom:4D:E5:F7
PhilipsCom:4E:55:B5
PhilipsCom:42:2C:96
PhilipsCom:4F:0E:90
PhilipsCom:4F:05:B4
PhilipsCom:4D:E6:70
PhilipsCom:4E:FE:5D
PhilipsCom:4E:73:DB
PhilipsCom:51:41:D3
Netgear:4F:93:98
MilanTechn:2D:27:CB
LinksysGro:FC:8F:87
LinksysGro:74:30:7F
IntelCorpo:A8:B4:93
IntelCorpo:11:3C:08
IntelCorpo:98:EC:34
IntelCorpo:1A:F5:18
IntelCorpo:B8:07:05
IntelCorpo:B4:D6:F2
IntelCorpo:DB:67:9B
IntelCorpo:18:A4:C4
IntelCorpo:56:94:29
IntelCorpo:C8:0D:5B
IntelCorpo:D0:71:AF
IntelCorpo:22:6E:D2
IntelCorpo:5E:FE:C5
IntelCorpo:B4:E2:C0
IntelCorpo:7F:E4:D1
IntelCorpo:2F:D1:21
IntelCorpo:B3:2F:05
IntelCorpo:A6:AF:79
IntelCorpo:12:59:21
Intel:92:50:B6
Intel:9E:9B:BF
Intel:60:C1:A8
Intel:4B:A6:BB
Intel:6F:1A:E0
Intel:DD:22:6B

Intel:5F:31:CB
Intel:74:E2:6B
Intel:C6:7E:10
Intel:75:4E:76
Intel:CC:1E:7E
HonHaiPrec:3A:02:00
HonHaiPrec:04:32:DA
HighTechCo:B2:29:34
GroupedMulticast
GemtekTech:7B:0B:98
GemtekTech:7B:47:44
GemtekTech:76:87:7C
GemtekTech:4B:89:D6
GemtekTech:83:E7:B4
GemtekTech:6B:8A:69
GemtekTech:40:6B:E1
GemtekTech:41:AC:A9
GemtekTech:7B:4E:12
GemtekTech:0A:12:22
Epigram:60:04:00
DeltaNetwo:22:93:6F
D-Link:A7:C9:DA
D-Link:5C:A1:0E
Cisco-Link:18:4D:1A
Cisco-Link:8C:07:0F
Cisco-Link:03:76:AA
Cisco-Link:85:6B:95
Cisco-Link:B3:E5:86
Cisco-Link:60:9F:90
Cisco-Link:1D:CD:8F
Cisco-Link:9A:A8:33
Cisco-Link:9E:52:75
Cisco-Link:82:AB:98
Cisco:04:28:50
Cisco:64:A7:50
Cisco:E5:40:10
Cisco:04:37:00
Cisco:E5:50:20
Cisco:E5:50:60
Cisco:E5:40:20
Cisco:60:5A:80
Cisco:D4:92:90
Cisco:E5:40:70
Broadcast
AskeyCompu:B1:35:AB
AskeyCompu:34:27:77
AskeyCompu:CE:FF:80
AppleCompu:9A:9F:B2
AironetWir:54:A2:AC
Airespace:23:67:40
Airespace:0E:26:BF

Airespace:1B:E9:3F
Airespace:1B:04:7F
Airespace:0E:26:B0
Airespace:1B:04:70
Airespace:1B:A3:D0
Abocom:16:8C:7B
Abocom:17:45:6C
Abocom:45:22:2F
3comEurope:E5:3B:86
02:16:6F:05:C2:94
00:18:DE:92:A1:5D
00:18:DE:69:8D:98
00:18:DE:14:48:C6
00:18:39:56:B6:B3
00:18:39:40:31:50
00:18:18:94:A9:30
00:18:18:94:A8:60
00:18:18:94:A6:C0 NYICAPAP
00:18:18:94:A5:50
00:17:F2:3F:F9:72
00:17:C5:05:76:52
00:17:C5:05:75:71
00:17:5A:BD:A7:3F
00:17:5A:10:C2:70
00:17:59:EF:C4:40
00:17:59:EF:C1:70
00:16:CE:63:59:7E
00:16:CE:24:1A:5B
00:16:B6:DD:4C:31
00:16:B6:D7:63:35
00:16:B6:9E:29:81
00:16:6F:77:A1:24
00:16:6F:1B:BF:52
00:16:6F:0D:08:4D
00:16:6F:01:BB:3E
00:16:46:2B:53:87
00:15:F9:29:79:80
00:15:E9:6B:A9:1C
00:15:C7:AB:B9:81
00:15:C7:AB:B9:80
00:15:00:23:A0:B1
00:15:00:23:97:AE
00:00:00:00:FA:BE

4.0 What was discovered using CommView for protocol analysis

A wireless protocol analyzer was used to not only scan the same areas as with Netstumbler for control purposes but to also gather a sampling of packets and layer two/layer three connectivity statistics of any channels specifically analyzed. The use of CommView for Wifi from TamoSoft was used since it can use the same radio adaptors used in the Netstumber and its ability for 802.11 MAC layer packet creation and generation for stimuli testing if needed. Some of the CommView scans and traces were also conducted on the same floors using various antennas. CommView can generate different reports that can be compared to other reports from different floors for coverage and AP determination. The reports can be compared to the previous section's NetStumbler reports. This section shall outline any issues or findings related to the 11th floor NYIIM wireless deployment from a protocol/packet analysis perspective. Complete packet capture trace files will also be provided to NYI for their own review, report generation and documentation. The CommView trace files were converted to WildPackets EtherPeek and OmniPeek file formats so NYI can read them with the freely available popular Ethereal and OmniPeek personal protocol analyzers. The packet details included in this document are from OmniPeek and CommView.

CommView has a scanning function similar to Netstumbler for AP enumeration but it also generates a trace file saving all the packets scanned from each channel so packet details from different channels can also be reviewed.

NYICAPAP was observed on the 10th, 11th and 12th floor scans.

Note: no NYICAPAP layer 3 data related traffic was observed in the traces indicating that the NYIIM cells are not heavily used yet.

What was observed on the 10th floor using CommView

Since this address falls under the Cisco-Linksys category NYI should verify if the node's MAC address is not one of its client's this node is sending out unencrypted SNMPv1 traffic.

Source	Destination	BSSID	Address 1	Address 2
142.128.1.239	12.130.22.02	00:14:BF:18:4D:17	00:14:BF:18:4D:17	Ambit Micro:D8:63:50 00:14:B

SNMP - Simple Network Management Protocol
Version Number: 0 Version 1
Community: public
PDU Type: 0xA0 Get Request
Request ID: 134
Error Status: 0 No Error
Error Index: 0
Object
Identifier: {1.3.6.2.2.1.25.3.2.1.3.1}
Description: iso.org.dod.internet.mgmt.mib-2
Value: NULL
Object

Identifier: {1.3.6.2.2.1.25.3.5.1.3.1}
Description: iso.org.dod.internet.mgmt.mib-2
Value: NULL
Object
Identifier: {1.3.6.2.2.1.25.3.5.1.3.1}
Description: iso.org.dod.internet.mgmt.mib-2
Value: NULL

4.1 Ad-hoc networks

Ad-hoc networks are independent peer to peer networks where stations communicate directly with each other, without the use of an access point (AP). Ad-hoc mode is also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required. Ad-hoc mode networks offer a potential security issue due to two main concerns.

1. No encryption is usually used
2. Peer stations are still plugged into the enterprises' wired infrastructure.

Users usually establish these peer to peer networks to share and copy files between machines without using the local wired infrastructure for many different reasons.

This is a concern for NYI because if any of NYI's employees are using this mode to be somewhat productive they may be providing an attacker a potential path into NYI's network. A peer attack can be formulated from an attacker either from outside or from another floor(possibly a NYI tenant floor). This attacker can target the Ad-hoc node and conduct the following types of attacks:

- Compromise the NYI user's machine and install a Rootkit, Keylogger or Zombie to launch a Smurf type of attack to a different target outside of NYI
- Compromise the NYI user's machine to install a Rootkit, Keylogger or Zombie to launch an attack against NYI computing resources
- Compromise the NYI user's machine to install a Rootkit, Keylogger or Zombie to be able to access NYI critical financial data repositories and send them or store them unknowingly on the user's machine for access at a later time
- Compromise the NYI user's machine to install a Rootkit, Keylogger or Zombie to be able to access all NYI data resources via the user's laptop while the user is connected to NYI's network at home via the NYI VPN.
- Deposit a virus or worm to attack NYI or another target

- Use the NYI user's machine as a router to get into the NYI network anytime the NYI user is connected to the NYI wired infrastructure or VPN while in Ad-hoc mode.

- Regardless if the NYI user is connected to the NYI network via the wired or VPN paths the Ad-hoc users not using encryption expose the peers to remote protocol analyzer(sniffer) based attacks in which important NYI information could possibly be gleaned over the air since the traffic is not encrypted.

Several Ad-hoc networks were identified on the 10th and 11th floor during AMI's visit. On Thursday 11/6 AMI conducted three in-depth packet capture sessions on the 10th floor using the 5dBi Dipole antenna and analyzing channels 1, 6 and 11 respectively.

What was immediately found were three active Ad-hoc networks on the 10th floor. One of the local programmers admitted he had one running when asking about AMI's activity during the analysis. The possible cubical locations where the Ad-hoc networks resided are 28, 62 and 89. The following NYI personnel Ad-hoc networks immediately identified are below:

Channel 11 Ad hoc Linksys no encryption 00:16:6f:89:c4:46
Channel 11 ad hoc Wireless Network no encryption 00:14:a5:84:9f:9f
Channel 11 ad hoc eng107 no encryption 00:13:ce:d2:4a:fc

Below is a snapshot of the Channel 11 Ad-hoc networks observed on the 10th floor during the afternoon of 11/16.

No	Protocol	Src MAC	Dest MAC	Time	Signal	Rate	More details
17399	MNGT/BEACON	SiemensIcn:06:BA:58	Broadcast	15:21:37.262612	25	1	TT_Guest(Infra.), Ch.#11
17400	MNGT/BEACON	SiemensIcn:06:BA:59	Broadcast	15:21:37.264319	20	1	(Infra.), Ch.#11
17401	MNGT/BEACON	IntelCorpo:D2:4A:FC	Broadcast	15:21:37.291522	26	1	eng107(Ad Hoc), Ch.#11
17402	MNGT/BEACON	SolomonExt:07:2C:43	Broadcast	15:21:37.339226	20	1	linksys(Ad Hoc), Ch.#11
17403	MNGT/BEACON	SiemensIcn:06:BA:58	Broadcast	15:21:37.364977	28	1	TT_Guest(Infra.), Ch.#11
17404	MNGT/BEACON	SiemensIcn:06:BA:59	Broadcast	15:21:37.366716	8	1	(Infra.), Ch.#11
17405	MNGT/BEACON	IntelCorpo:D2:4A:FC	Broadcast	15:21:37.393651	20	1	eng107(Ad Hoc), Ch.#11
17406	MNGT/BEACON	GemtekTech:84:9F:9F	Broadcast	15:21:37.415525	10	1	Wireless Network(Ad Hoc), Ch.#11
17407	MNGT/BEACON	SolomonExt:07:2C:43	Broadcast	15:21:37.441557	8	1	linksys(Ad Hoc), Ch.#11
17408	MNGT/BEACON	SiemensIcn:06:BA:58	Broadcast	15:21:37.467528	11	1	TT_Guest(Infra.), Ch.#11
17409	MNGT/BEACON	SiemensIcn:06:BA:59	Broadcast	15:21:37.469251	11	1	(Infra.), Ch.#11
17410	MNGT/PROBE REQ.	AmbitMicro:D8:63:50	Broadcast	15:21:37.470403	60	1	
17411	MNGT/PROBE RESP.	GemtekTech:84:9F:9F	AmbitMicro:D8:63:50	15:21:37.471302	25	1	Wireless Network(Ad Hoc), Ch.#11
17412	MNGT/PROBE RESP.	GemtekTech:84:9F:9F	AmbitMicro:D8:63:50	15:21:37.472895	21	1	
17413	MNGT/PROBE RESP.	GemtekTech:84:9F:9F	AmbitMicro:D8:63:50	15:21:37.474573	20	1	Wireless Network(Ad Hoc), Ch.#11
17414	CTRL/ACK	N/A	GemtekTech:84:9F:9F	15:21:37.474884	56	1	
17415	MNGT/BEACON	IntelCorpo:D2:4A:FC	Broadcast	15:21:37.496223	16	1	eng107(Ad Hoc), Ch.#11
17416	MNGT/BEACON	GemtekTech:84:9F:9F	Broadcast	15:21:37.517944	21	1	Wireless Network(Ad Hoc), Ch.#11
17417	MNGT/BEACON	SolomonExt:07:2C:43	Broadcast	15:21:37.544375	15	1	linksys(Ad Hoc), Ch.#11
17418	MNGT/BEACON	IntelCorpo:D2:4A:FC	Broadcast	15:21:37.598335	15	1	eng107(Ad Hoc), Ch.#11
17419	MNGT/BEACON	GemtekTech:84:9F:9F	Broadcast	15:21:37.620471	11	1	Wireless Network(Ad Hoc), Ch.#11
17420	MNGT/PROBE RESP.	IntelCorpo:D2:4A:FC	Proxim:91:CA:EF	15:21:37.628372	18	1	eng107(Ad Hoc), Ch.#11
17421	MNGT/PROBE RESP.	IntelCorpo:D2:4A:FC	Proxim:91:CA:EF	15:21:37.630101	20	1	eng107(Ad Hoc), Ch.#11
17422	MNGT/PROBE RESP.	GemtekTech:84:9F:9F	Proxim:91:CA:EF	15:21:37.633453	8	1	Wireless Network(Ad Hoc), Ch.#11
17423	MNGT/PROBE RESP.	SolomonExt:07:2C:43	Proxim:91:CA:EF	15:21:37.678452	18	1	linksys(Ad Hoc), Ch.#11
17424	MNGT/PROBE RESP.	GemtekTech:84:9F:9F	Proxim:91:CA:EF	15:21:37.682197	15	1	Wireless Network(Ad Hoc), Ch.#11
17425	MNGT/BEACON	IntelCorpo:D2:4A:FC	Broadcast	15:21:37.700813	20	1	eng107(Ad Hoc), Ch.#11
17426	MNGT/BEACON	GemtekTech:84:9F:9F	Broadcast	15:21:37.723096	13	1	Wireless Network(Ad Hoc), Ch.#11
17427	MNGT/BEACON	SolomonExt:07:2C:43	Broadcast	15:21:37.749222	11	1	linksys(Ad Hoc), Ch.#11
17428	MNGT/BEACON	IntelCorpo:D2:4A:FC	Broadcast	15:21:37.803292	11	1	eng107(Ad Hoc), Ch.#11
17429	MNGT/BEACON	SolomonExt:07:2C:43	Broadcast	15:21:37.851548	13	1	linksys(Ad Hoc), Ch.#11
17430	MNGT/PROBE REQ.	AmbitMicro:D8:63:50	Broadcast	15:21:37.913722	35	1	
17431	MNGT/PROBE REQ.	AmbitMicro:D8:63:50	Broadcast	15:21:37.921993	46	1	
17432	MNGT/BEACON	GemtekTech:84:9F:9F	Broadcast	15:21:37.927526	10	1	Wireless Network(Ad Hoc), Ch.#11
17433	MNGT/PROBE REQ.	AmbitMicro:D8:63:50	Broadcast	15:21:37.930145	48	1	
17434	MNGT/BEACON	SolomonExt:07:2C:43	Broadcast	15:21:37.953835	11	1	linksys(Ad Hoc), Ch.#11
17435	MNGT/BEACON	SiemensIcn:06:BA:58	Broadcast	15:21:37.979668	15	1	TT_Guest(Infra.), Ch.#11
17436	MNGT/BEACON	GemtekTech:84:9F:9F	Broadcast	15:21:38.030078	10	1	Wireless Network(Ad Hoc), Ch.#11
17437	MNGT/BEACON	SolomonExt:07:2C:43	Broadcast	15:21:38.056287	10	1	linksys(Ad Hoc), Ch.#11
17438	MNGT/BEACON	SiemensIcn:06:BA:58	Broadcast	15:21:38.081771	13	1	TT_Guest(Infra.), Ch.#11

A beacon packet from the Ad-hoc network Wireless Network is depicted below:

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000000
  Packet Length:        82
  Timestamp:            06:15:53.351000000 11/17/2006
  Data Rate:            2   1.0 Mbps
  Channel:              11  2462MHz  802.11bg
  Signal Level:         13%
  Signal dBm:           0
  Noise Level:          0%
  Noise dBm:            0
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %1000  Beacon
Frame Control Flags:    %00000000
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System

  Duration:             0  Microseconds
  Destination:          FF:FF:FF:FF:FF:FF  Ethernet Broadcast
  Source:               00:14:A5:84:9F:9F
  BSSID:                06:5B:98:A8:54:7B
  Seq Number:           2788
  Frag Number:          0
802.11 Management - Beacon
  Timestamp:            23931188082  Microseconds
  Beacon Interval:      100
  Capability Info:      %0000000000000010
                        0....... ........ Immediate Block Ack Not Allowed
                        .0...... ........ Delayed Block Ack Not Allowed
                        ..0..... ........ DSSS-OFDM is Not Allowed
                        ...0.... ........ Reserved
                        ....0... ........ APSD is not supported
                        .....0.. ........ G Mode Short Slot Time [20 microseconds]
                        ......0. ........ QoS is Not Supported
                        .......0 ........ Spectrum Mgmt Disabled
                        ........ 0....... Channel Agility Not Used
                        ........ .0...... PBCC Not Allowed
                        ........ ..0..... Short Preamble Not Allowed
                        ........ ...0.... Privacy Disabled
                        ........ ....0... CF Poll Not Requested
                        ........ .....0.. CF Not Pollable
                        ........ ......1. IBSS Type Network
                        ........ .......0 Not an ESS Type Network

SSID
  Element ID:           0  SSID
  Length:               16
  SSID:                 Wireless Network
```

```
Supported Rates
  Element ID:           1  Supported Rates
  Length:               4
  Supported Rate:       1.0  Mbps  (BSS Basic Rate)
  Supported Rate:       2.0  Mbps  (BSS Basic Rate)
  Supported Rate:       5.5  Mbps  (BSS Basic Rate)
  Supported Rate:       11.0  Mbps  (BSS Basic Rate)

Direct Sequence Parameter Set
  Element ID:           3  Direct Sequence Parameter Set
  Length:               1
  Channel:              11

IBSS Parameter Set
  Element ID:           6  IBSS Parameter Set
  Length:               2
  ATIM Window:          0

Vendor Specific
  Element ID:           221  Vendor Specific - Broadcom
  Length:               9
  Value:
  .........         00 10 18 02 00 10 00 00 00

FCS - Frame Check Sequence
  FCS:                  0xB0B2809B  Calculated
```

Ad-hoc networks observed by CommView listed per floor

The following reports are from the CommView traces and outline all the Ad-hoc networks observed during AMI's visit. It should be noted that Ad-hoc networks from the other buildings and floors were also observed. NYI should review these lists against its MAC address wireless adaptor inventory for laptops supplied to NYI employees to see if any are present. Also, it should be noted that in these reports there were duplicate Ad-hoc peer nodes observed but on different channels and sometimes WEP was used and other times not. What this means is that the potential NYI or rogue Ad-hoc users are changing channels and may not always use the same settings from day to day. The duplicate Ad-hoc nodes are outlined in yellow. The following reports are also sorted by the channel number.

10th floor Ad-hoc networks observed

10th Floor observed ADHOC Nodes				
Node	**ESSID**	**Type 5**	**Chan**	**Encryption**
00:0F:BB:06:50:C9		ADHOC	1	
00:0F:BB:06:B8:18		ADHOC	1	
00:88:04:00:00:E0		ADHOC	1	
36:86:59:EF:C1:70		ADHOC	1	
44:14:12:02:76:AA		ADHOC	1	
66:A2:80:1B:E9:3F		ADHOC	1	WEP
Airespace:93:FD:36		ADHOC	1	
00:0F:BB:26:9B:D5		ADHOC	2	
00:17:79:FF:C7:44		ADHOC	2	
00:18:90:B2:A9:60		ADHOC	2	
00:2E:B2:DE:83:E1		ADHOC	2	

00:4B:A1:1B:B7:7E	ADHOC	2
20:21:1B:90:A8:60	ADHOC	2
98:1F:37:CE:B7:42	ADHOC	2
9C:E2:A7:0B:EE:F5	ADHOC	2
00:15:F9:29:19:CD	ADHOC	3
66:12:1C:0C:37:72	ADHOC	3
90:F0:98:62:4B:A1	ADHOC	3
00:16:6F:CD:C6:46	ADHOC	4
00:11:5C:E5:10:44	ADHOC	5
00:11:5C:E5:40:80	ADHOC	5
00:17:5A:F0:69:BE	ADHOC	5
00:28:7E:31:9A:34	ADHOC	5
00:2E:04:BF:82:69	ADHOC	5
00:2E:B4:20:84:E1	ADHOC	5
00:37:48:10:C2:B0	ADHOC	5
00:75:D0:D7:52:39	ADHOC	5
0C:39:5B:EF:A6:C2	ADHOC	5
80:DA:29:48:B3:E8	ADHOC	5
92:5E:6C:47:42:19	ADHOC	5
00:0F:F8:55:9C:34	ADHOC	6
00:0F:F8:55:AD:EA	ADHOC	6
00:11:5C:C5:81:E0	ADHOC	6
00:12:A6:53:22:2F	ADHOC	6
00:17:5A:F1:FF:FF	ADHOC	6
02:51:FD:1F:12:CC	ADHOC	6
22:C5:5E:30:30:ED	ADHOC	6
68:59:2D:B1:ED:37	ADHOC	6
Stratex:18:4D:17	ADHOC	6
00:17:96:E6:E5:E2	ADHOC	7
00:37:C0:36:E3:17	ADHOC	7
06:18:39:40:31:50	ADHOC	7
48:18:18:BF:A5:30	ADHOC	7
5E:A3:0A:6B:49:C9	ADHOC	7
A8:02:BF:18:4D:17	ADHOC	7
Comm Dev:63:04:00	ADHOC	7
Visionglobal Net:16:8C:7B	ADHOC	7
80:46:A4:42:22:1C	ADHOC	8
00:16:2B:8B:C4:46	ADHOC	9
04:2A:9F:46:CB:27	ADHOC	9
20:54:E8:8C:44:8F	ADHOC	9
60:22:F1:60:5A:80	ADHOC	9
96:14:FC:66:63:EC	ADHOC	9
00:13:CE:D2:4A:FC	ADHOC	10
00:14:A5:84:9F:9F	ADHOC	10
00:36:7D:89:C4:46	ADHOC	10
00:3F:BA:06:35:EF	ADHOC	10
00:87:7F:80:44:0E	ADHOC	10
24:07:E3:EF:7A:BD	ADHOC	10
3E:9B:CA:D2:4A:FC	ADHOC	10
A0:71:D7:C9:57:46	ADHOC	10
C8:99:AF:EF:9B:50	ADHOC	10

Philipsonents:4A:A4:C3	ADHOC	10	
00:0F:BB:06:BA:09	ADHOC	11	
00:0F:BB:26:2A:0E	ADHOC	11	
00:0F:F8:55:9A:79	ADHOC	11	
00:13:CE:D2:4A:7C	ADHOC	11	
00:13:CE:D2:4A:FC	ADHOC	11	
00:14:A5:84:9F:9F	ADHOC	11	
00:14:E9:CA:AF:84	ADHOC	11	
00:16:6F:89:C4:46	ADHOC	11	WEP
00:16:6F:89:C4:46	ADHOC	11	
00:16:E7:8D:C4:46	ADHOC	11	WEP
00:16:F7:84:C4:46	ADHOC	11	
00:94:CF:85:DF:AB	ADHOC	11	
60:B3:D6:04:DA:8C	ADHOC	11	
80:47:AB:0F:32:3B	ADHOC	11	
98:B9:BE:84:C4:46	ADHOC	11	
DC:D3:15:62:8A:69	ADHOC	11	
Gemtek Tech:6B:8A:69	ADHOC	11	
Gemtek Tech:7F:81:80	ADHOC	11	
Intel Corp:B4:04:6C	ADHOC	11	
Solomon Extreme:06:1F:35	ADHOC	11	
Solomon Extreme:07:2C:43	ADHOC	11	
Solomon Extreme:AE:09:35	ADHOC	11	
00:52:6D:89:C4:46	ADHOC	12	
00:9E:6B:89:C4:66	ADHOC	12	
98:DE:AC:06:35:07	ADHOC	12	
00:16:6F:89:C4:46	ADHOC	13	
00:26:7C:75:25:5F	ADHOC	13	

11th floor Ad-hoc networks observed

11th Floor observed ADHOC Nodes				
Node	**ESSID**	**Type 5**	**Cha**	**Enycryption**
00:B5:8E:DC:DA:B8		ADHOC	1	
Philipsonents:4C:56:FC		ADHOC	1	
Philipsonents:50:7B:36		ADHOC	1	
Solomon Extreme:06:1F:35		ADHOC	1	
00:13:32:B2:E5:86		ADHOC	2	
00:16:0A:37:04:3E		ADHOC	2	
00:18:18:94:A8:20		ADHOC	2	
00:18:18:94:A8:E5		ADHOC	2	
00:18:33:98:A8:B0		ADHOC	2	
00:18:3A:95:A6:C0		ADHOC	2	
00:1E:76:0D:A0:3C		ADHOC	2	
00:2E:B2:DE:83:E1		ADHOC	2	
00:98:FA:91:37:17		ADHOC	2	
08:18:18:94:B6:BB		ADHOC	2	
08:95:39:28:51:F1		ADHOC	2	
48:01:0B:07:50:48		ADHOC	2	
80:40:11:94:E6:A4		ADHOC	2	
80:B4:E3:FC:BE:38		ADHOC	2	

8A:2C:1D:80:6D:8C	ADHOC	2	
Harmonix:28:51:C1	ADHOC	2	
00:14:A5:84:9F:9F	ADHOC	3	
00:31:4E:E5:90:04	ADHOC	3	
00:18:18:94:B5:D1	ADHOC	4	
10:11:18:D0:AA:F1	ADHOC	4	
20:0A:98:DC:88:E3	ADHOC	4	
32:1A:31:16:EB:F6	ADHOC	4	
5C:A8:DE:84:B5:3A	ADHOC	4	
92:9A:35:28:51:C1	ADHOC	4	
96:3C:B9:8E:C4:AC	ADHOC	4	
A0:9F:46:59:BD:B6	ADHOC	4	WEP
C0:95:FD:DD:7E:B7	ADHOC	4	
00:14:2F:9C:46:9F	ADHOC	5	
00:14:BF:18:4D:BF	ADHOC	5	
00:14:BF:F8:89:16	ADHOC	5	
00:14:F3:83:9A:34	ADHOC	5	
00:17:4A:19:C2:F0	ADHOC	5	
00:64:BF:35:9A:F0	ADHOC	5	
00:82:4F:16:8C:7B	ADHOC	5	
00:C5:1B:34:D1:FD	ADHOC	5	
00:D4:1F:E9:82:7A	ADHOC	5	
10:AF:A2:AB:84:E1	ADHOC	5	
20:A5:1E:91:49:0A	ADHOC	5	
22:19:39:40:31:81	ADHOC	5	
4A:CE:D8:0D:8E:F9	ADHOC	5	
64:94:FA:1C:EB:9A	ADHOC	5	
C0:F8:98:D6:21:1A	ADHOC	5	
CA:23:5C:30:9A:6E	ADHOC	5	
Epigram:50:6F:C9	ADHOC	5	
00:11:5C:E5:70:62	ADHOC	6	
00:12:79:B0:4C:1B	ADHOC	6	
00:14:BF:18:4D:A6	ADHOC	6	
00:18:D7:94:86:80	ADHOC	6	
00:31:4E:E5:00:04	ADHOC	6	
00:9F:5E:10:C2:70	ADHOC	6	
30:FC:FF:FF:FF:FF	ADHOC	6	
7E:99:93:39:55:E1	ADHOC	6	
80:9D:E2:3D:F9:EC	ADHOC	6	
E4:D8:5C:E5:10:BC	ADHOC	6	
F6:17:BF:18:4D:1A	ADHOC	6	
00:11:5C:E5:D0:2C	ADHOC	7	
00:14:17:1E:44:1A	ADHOC	7	
00:14:BF:18:C5:4F	ADHOC	7	
00:14:EB:EB:E4:06	ADHOC	7	
00:18:3D:CA:54:18	ADHOC	7	
00:7E:93:98:41:E1	ADHOC	7	
00:91:CC:6F:6A:28	ADHOC	7	
00:B4:E5:60:3E:77	ADHOC	7	

02:A4:BC:34:DF:23	ADHOC	7	
04:14:BF:35:12:19	ADHOC	7	
08:34:E4:A9:5B:53	ADHOC	7	
10:1D:BF:18:4D:1A	ADHOC	7	
20:54:7F:64:71:56	ADHOC	7	
24:10:BF:38:06:BF	ADHOC	7	
24:38:0A:94:E9:14	ADHOC	7	
44:56:3B:78:83:98	ADHOC	7	
94:6B:5D:29:C2:F0	ADHOC	7	
AC:B2:7E:25:93:FF	ADHOC	7	
BE:5C:67:B1:DC:31	ADHOC	7	
C0:BD:54:59:03:00	ADHOC	7	WEP
CC:1E:7F:71:36:12	ADHOC	7	
CC:6D:5F:1A:B4:93	ADHOC	7	
Cisco-linksys:0B:BD:F1	ADHOC	7	
E2:11:37:84:CA:94	ADHOC	7	
E4:BF:5B:29:53:61	ADHOC	7	
00:6A:34:94:A9:54	ADHOC	8	
00:67:2F:0A:54:DC	ADHOC	9	
04:97:06:C8:A8:9F	ADHOC	9	
80:02:05:05:A2:7A	ADHOC	9	
96:8F:38:2A:53:49	ADHOC	9	
C0:79:23:58:20:F8	ADHOC	9	
Packetlight Net:4D:56:DE	ADHOC	9	WEP
Philipsonents:6C:CC:F8	ADHOC	9	
00:13:2E:24:0A:7F	ADHOC	10	
00:13:7F:C0:4A:FC	ADHOC	10	
00:13:CE:D2:4A:BC	ADHOC	10	
00:2C:5E:96:C4:46	ADHOC	10	
00:4F:86:D7:2B:D8	ADHOC	10	
00:9B:9E:D9:4A:FC	ADHOC	10	
20:01:CE:D2:4A:7C	ADHOC	10	
28:FE:D4:76:02:FC	ADHOC	10	
48:13:5F:43:5A:E5	ADHOC	10	
Philipsonents:4A:A4:C3	ADHOC	10	
Philipsonents:4A:A4:E3	ADHOC	10	
Philipsonents:4C:56:FC	ADHOC	10	
00:12:F0:D3:BE:70	ADHOC	11	
00:13:CE:D2:4A:FC	ADHOC	11	
00:13:CE:D2:4A:FC	ADHOC	11	WEP
00:14:A5:84:9F:9F	ADHOC	11	
00:16:6F:3D:1C:A6	ADHOC	11	
00:16:6F:89:C4:46	ADHOC	11	
00:27:4F:0C:2A:7E	ADHOC	11	
00:45:E2:0C:10:FE	ADHOC	11	
36:BD:53:AF:F4:DD	ADHOC	11	
58:0C:4E:6C:85:7A	ADHOC	11	
E4:3C:BB:22:ED:FF	ADHOC	11	
F4:99:91:98:60:FE	ADHOC	11	

Gemtek Tech:6B:8A:69		ADHOC	11
Gemtek Tech:B3:16:BC		ADHOC	11
Philipsonents:4C:DE:F8		ADHOC	11
Solomon Extreme:07:2C:43		ADHOC	11

12th floor Ad-hoc networks observed

12th Floor observed ADHOC Nodes				
Node	**ESSID**	**Type 5**	**Cha**	**Encryption**
F8:00:BB:06:50:49		ADHOC	1	
Fuji Machines:89:FF:FF		ADHOC	1	
00:17:59:EF:C4:40	PSNET	ADHOC	1	
80:47:BB:06:A9:20		ADHOC	2	
56:2D:ED:B6:30:78		ADHOC	2	
00:26:20:66:3B:FE		ADHOC	2	
00:11:7C:C7:6B:6B		ADHOC	4	WEP
80:3C:76:0D:5E:91		ADHOC	5	
76:B7:1F:EE:D1:6D		ADHOC	6	WEP
00:92:46:16:8C:6B		ADHOC	7	
08:0F:BB:06:AF:C9		ADHOC	7	
E6:BB:2D:17:5E:91		ADHOC	7	
08:43:BB:06:AF:C9		ADHOC	7	
00:11:5C:65:F5:FF		ADHOC	9	
96:3C:B9:42:63:58		ADHOC	9	
00:11:5C:E5:40:90		ADHOC	9	
00:22:B8:CA:81:20		ADHOC	10	
02:02:BB:06:B6:93		ADHOC	10	
00:0F:BB:26:A7:18		ADHOC	10	
Intel:9E:9B:BF		ADHOC	11	
Gemtek Tech:6B:8A:69		ADHOC	11	

4.2 NYIIM NYICAPAP Beacon management frames

Due to the tight spectrum allocation of radio channels in the 2.4gHz range below is an example of where Beacons can be seen on adjacent channels for the casual observer or potential attacker to discover information about the NYIIM wireless network. This behavior could also be a result to the radio power levels set on the NYICAPAP for channel 1.

NYI Beacon frames observed on the 10th floor

The following Beacon frame a frame generated by the NYIIM NYICAPAP access point on its allocated channel, channel 1.

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000000
  Packet Length:        115
  Timestamp:            04:47:29.904000000 11/17/2006
  Data Rate:            2   1.0 Mbps
  Channel:              1  2412MHz  802.11bg
  Signal Level:         20%
  Signal dBm:           0
  Noise Level:          0%
  Noise dBm:            0
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %1000  Beacon
Frame Control Flags:    %00000000
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System

  Duration:             0  Microseconds
  Destination:          FF:FF:FF:FF:FF:FF  Ethernet Broadcast
  Source:               00:18:18:94:A6:C0
  BSSID:                00:18:18:94:A6:C0
  Seq Number:           1416
  Frag Number:          0
802.11 Management - Beacon
  Timestamp:            2750914765198  Microseconds
  Beacon Interval:      100
  Capability Info:      %0000010000010001
                        0....... ........ Immediate Block Ack Not Allowed
                        .0...... ........ Delayed Block Ack Not Allowed
                        ..0..... ........ DSSS-OFDM is Not Allowed
                        ...0.... ........ Reserved
                        ....0... ........ APSD is not supported
                        .....1.. ........ G Mode Short Slot Time [9 microseconds]
                        ......0. ........ QoS is Not Supported
                        .......0 ........ Spectrum Mgmt Disabled
                        ........ 0....... Channel Agility Not Used
                        ........ .0...... PBCC Not Allowed
                        ........ ..0..... Short Preamble Not Allowed
                        ........ ...1.... Privacy Enabled
                        ........ ....0... CF Poll Not Requested
                        ........ .....0.. CF Not Pollable
                        ........ ......0. Not an IBSS Type Network
                        ........ .......1 ESS Type Network

SSID
  Element ID:           0  SSID
  Length:               6
  SSID:                 ......
```

```
Supported Rates
  Element ID:           1  Supported Rates
  Length:               8
  Supported Rate:       1.0  Mbps  (BSS Basic Rate)
  Supported Rate:       2.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       5.5  Mbps  (Not BSS Basic Rate)
  Supported Rate:       6.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       9.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       11.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       12.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       18.0  Mbps  (Not BSS Basic Rate)

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

Traffic Indication Map
  Element ID:           5  Traffic Indication Map
  Length:               4
  DTIM Count:           0
  DTIM Period:          2
  Bitmap Offset:        0  xxxx xxx.
  Traffic Ind.:         0  .... ...0
  Part Virt Bmap:       0x00

ERP Information
  Element ID:           42  ERP Information
  Length:               1
  ERP Flags:            %00000010
                        x... .... Reserved
                        .x.. .... Reserved
                        ..x. .... Reserved
                        ...x .... Reserved
                        .... x... Reserved
                        .... .0.. Not Barker Preamble Mode
                        .... ..1. Use Protection
                        .... ...0 Non-ERP Not Present


Extended Supported Rates
  Element ID:           50  Extended Supported Rates
  Length:               4
  Supported Rate:       24.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       36.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       48.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       54.0  Mbps  (Not BSS Basic Rate)

Vendor Specific
  Element ID:           221  Vendor Specific - Cisco
  Length:               6
  OUI:                  0x00-0x40-0x96
  Data:
  ...                01 01 00

Vendor Specific
  Element ID:           221  Vendor Specific - Cisco
  Length:               5
  OUI:                  0x00-0x40-0x96
  Version:              3
  CCX Version:          2

Vendor Specific
  Element ID:           221  Vendor Specific - Cisco
```

```
  Length:               22
  OUI:                  0x00-0x40-0x96
  Data:
  ......."...AC..a  04 00 0A 06 A4 00 00 22 A4 00 00 41 43 00 00 61
  2..               32 00 00

FCS - Frame Check Sequence
  FCS:                  0xFAF2E915  Calculated
```

This Beacon frame is also the NYICAPAP frame but observed on channel 2.

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000000
  Packet Length:        115
  Timestamp:            04:53:46.636000000 11/17/2006
  Data Rate:            2   1.0 Mbps
  Channel:              2  2417MHz  802.11bg
  Signal Level:         13%
  Signal dBm:           0
  Noise Level:          0%
  Noise dBm:            0
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %1000  Beacon
Frame Control Flags:    %00000000
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System

  Duration:             0  Microseconds
  Destination:          FF:FF:FF:FF:FF:FF  Ethernet Broadcast
  Source:               00:18:18:94:A6:C0
  BSSID:                00:18:18:94:A6:C0
  Seq Number:           1720
  Frag Number:          0
802.11 Management - Beacon
  Timestamp:            2751291494798  Microseconds
  Beacon Interval:      100
  Capability Info:      %0000010000010001
                        0....... ........ Immediate Block Ack Not Allowed
                        .0...... ........ Delayed Block Ack Not Allowed
                        ..0..... ........ DSSS-OFDM is Not Allowed
                        ...0.... ........ Reserved
                        ....0... ........ APSD is not supported
                        .....1.. ........ G Mode Short Slot Time [9 microseconds]
                        ......0. ........ QoS is Not Supported
                        .......0 ........ Spectrum Mgmt Disabled
                        ........ 0....... Channel Agility Not Used
                        ........ .0...... PBCC Not Allowed
                        ........ ..0..... Short Preamble Not Allowed
                        ........ ...1.... Privacy Enabled
                        ........ ....0... CF Poll Not Requested
                        ........ .....0.. CF Not Pollable
                        ........ ......0. Not an IBSS Type Network
                        ........ .......1 ESS Type Network
```

```
SSID
  Element ID:           0  SSID
  Length:               6
  SSID:                 ......

Supported Rates
  Element ID:           1  Supported Rates
  Length:               8
  Supported Rate:       1.0  Mbps  (BSS Basic Rate)
  Supported Rate:       2.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       5.5  Mbps  (Not BSS Basic Rate)
  Supported Rate:       6.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       9.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       11.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       12.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       18.0  Mbps  (Not BSS Basic Rate)

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

Traffic Indication Map
  Element ID:           5  Traffic Indication Map
  Length:               4
  DTIM Count:           1
  DTIM Period:          2
  Bitmap Offset:        0  xxxx xxx.
  Traffic Ind.:         0  .... ...0
  Part Virt Bmap:       0x00

ERP Information
  Element ID:           42  ERP Information
  Length:               1
  ERP Flags:            %00000010
                        x... .... Reserved
                        .x.. .... Reserved
                        ..x. .... Reserved
                        ...x .... Reserved
                        .... x... Reserved
                        .... .0.. Not Barker Preamble Mode
                        .... ..1. Use Protection
                        .... ...0 Non-ERP Not Present


Extended Supported Rates
  Element ID:           50  Extended Supported Rates
  Length:               4
  Supported Rate:       24.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       36.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       48.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:       54.0  Mbps  (Not BSS Basic Rate)

Vendor Specific
  Element ID:           221  Vendor Specific - Cisco
  Length:               6
  OUI:                  0x00-0x40-0x96
  Data:
  ...                01 01 00
```

```
Vendor Specific
  Element ID:           221  Vendor Specific - Cisco
  Length:               5
  OUI:                  0x00-0x40-0x96
  Version:              3
  CCX Version:          2

Vendor Specific
  Element ID:           221  Vendor Specific - Cisco
  Length:               22
  OUI:                  0x00-0x40-0x96
  Data:
  .......".AC..a  04 00 0A 06 A4 00 00 22 A4 00 00 41 43 00 00 61
  2..             32 00 00

FCS - Frame Check Sequence
  FCS:                  0x90378D00  Calculated
```

This is the NYICAPAP Beacon frame observed on channel 3 on the 12th floor.

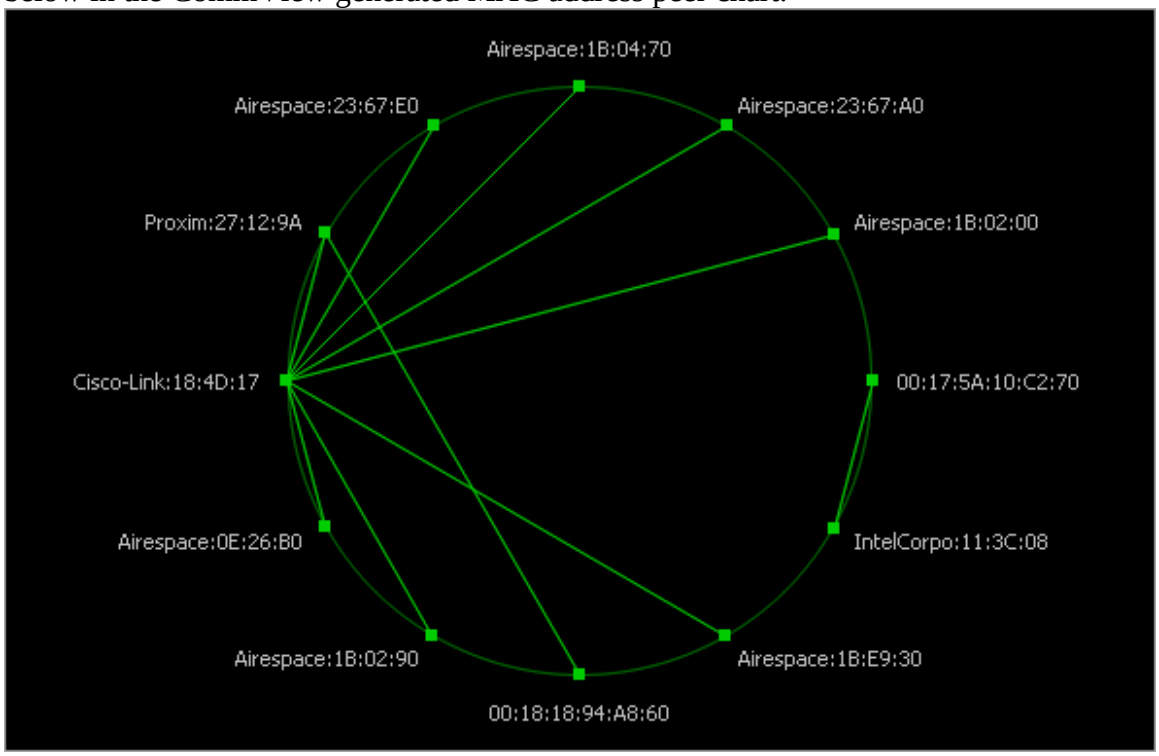
```
Packet Info
  Flags:                0x00000000
  Status:               0x00000000
  Packet Length:        115
  Timestamp:            06:16:45.467000000 11/17/2006
  Data Rate:            2   1.0 Mbps
  Channel:              3  2422MHz  802.11bg
  Signal Level:         25%
  Signal dBm:           0
  Noise Level:          0%
  Noise dBm:            0
802.11 MAC Header
  Version:              0
  Type:                 %00  Management
  Subtype:              %1000  Beacon
Frame Control Flags:    %00000000
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 0... This is not a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..0. Not an Exit from the Distribution System
                        .... ...0 Not to the Distribution System

  Duration:             0  Microseconds
  Destination:          FF:FF:FF:FF:FF:FF  Ethernet Broadcast
  Source:               00:18:18:94:A6:C0
  BSSID:                00:18:18:94:A6:C0
  Seq Number:           201
  Frag Number:          0
802.11 Management - Beacon
  Timestamp:            2767071232400  Microseconds
  Beacon Interval:      100
  Capability Info:      %0000010000010001
                        0....... ........ Immediate Block Ack Not Allowed
                        .0...... ........ Delayed Block Ack Not Allowed
                        ..0..... ........ DSSS-OFDM is Not Allowed
                        ...0.... ........ Reserved
                        ....0... ........ APSD is not supported
                        .....1.. ........ G Mode Short Slot Time [9 microseconds]
```

```
                          ......0. ........ QoS is Not Supported
                          .......0 ........ Spectrum Mgmt Disabled
                          ........ 0....... Channel Agility Not Used
                          ........ .0...... PBCC Not Allowed
                          ........ ..0..... Short Preamble Not Allowed
                          ........ ...1.... Privacy Enabled
                          ........ ....0... CF Poll Not Requested
                          ........ .....0.. CF Not Pollable
                          ........ ......0. Not an IBSS Type Network
                          ........ .......1 ESS Type Network

SSID
  Element ID:             0  SSID
  Length:                 6
  SSID:                   ......

Supported Rates
  Element ID:             1  Supported Rates
  Length:                 8
  Supported Rate:         1.0  Mbps  (BSS Basic Rate)
  Supported Rate:         2.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:         5.5  Mbps  (Not BSS Basic Rate)
  Supported Rate:         6.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:         9.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:         11.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:         12.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:         18.0  Mbps  (Not BSS Basic Rate)

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

Traffic Indication Map
  Element ID:             5  Traffic Indication Map
  Length:                 4
  DTIM Count:             0
  DTIM Period:            2
  Bitmap Offset:          0  xxxx xxx.
  Traffic Ind.:           0  .... ...0
  Part Virt Bmap:         0x00

ERP Information
  Element ID:             42  ERP Information
  Length:                 1
  ERP Flags:              %00000010
                          x... .... Reserved
                          .x.. .... Reserved
                          ..x. .... Reserved
                          ...x .... Reserved
                          .... x... Reserved
                          .... .0.. Not Barker Preamble Mode
                          .... ..1. Use Protection
                          .... ...0 Non-ERP Not Present


Extended Supported Rates
  Element ID:             50  Extended Supported Rates
  Length:                 4
  Supported Rate:         24.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:         36.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:         48.0  Mbps  (Not BSS Basic Rate)
  Supported Rate:         54.0  Mbps  (Not BSS Basic Rate)

Vendor Specific
  Element ID:             221  Vendor Specific - Cisco
```

```
  Length:                6
  OUI:                   0x00-0x40-0x96
  Data:
  ...                01 01 00

Vendor Specific
  Element ID:            221  Vendor Specific - Cisco
  Length:                5
  OUI:                   0x00-0x40-0x96
  Version:               3
  CCX Version:           2

Vendor Specific
  Element ID:            221  Vendor Specific - Cisco
  Length:                22
  OUI:                   0x00-0x40-0x96
  Data:
  .......".AC..a  04 00 0A 06 A4 00 00 22 A4 00 00 41 43 00 00 61
  2..             32 00 00

FCS - Frame Check Sequence
  FCS:                   0x422B44E1  Calculated
```

4.3 What was discovered on the 11th floor using Commview

Packet traces on the 11th floor show that the device **Cisco-Dlink:18:4D:17**, which is the **NYI-1619** AP on channel 6, communicate with each of the Airspace devices as outlined below in the CommView generated MAC address peer chart.



A review of the packets captured during a scan of the floor shows that the **Cisco-Link:18:D4:17 NYI-1619** AP on channel 6 communicates to all the Airspace devices. Below is a sample of the type of packets and data observed. If this is a NYI resource then broadcast traffic should be encrypted using a broadcast encryption method that employs some form of Group Master Key and Group Temporal Key for unicast and multicast traffic.

Source	Destination	Address 1	Address 2
122.219.5.19	122.219.5.255	Airespace:1B:02:90	00:14:BF:18:4D:17

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000000
  Packet Length:        120
  Timestamp:            05:26:08.024000000 11/17/2006
  Data Rate:            2   1.0 Mbps
  Channel:              6  2437MHz  802.11bg
  Signal Level:         10%
  Signal dBm:           0
  Noise Level:          0%
  Noise dBm:            0
802.11 MAC Header
  Version:              0
  Type:                 %10  Data
  Subtype:              %0000  Data Only
Frame Control Flags:    %00001011
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 1... This is a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..1. Exit from the Distribution System
                        .... ...1 To the Distribution System

  Duration:             314  Microseconds
  Receiver:             00:0B:85:1B:02:90  Airespace:1B:02:90
  Transmitter:          00:14:BF:18:4D:17
  Destination:          FF:FF:FF:FF:FF:FF  Ethernet Broadcast
  Seq Number:           221
  Frag Number:          0
  Source:               00:02:8A:D8:63:50  Ambit Micro:D8:63:50
802.2 Logical Link Control (LLC) Header
  Dest. SAP:            0xAA  SNAP
  Source SAP:           0xAA  SNAP
  Command:              0x03  Unnumbered Information
  Vendor ID:            0x000000
  Protocol Type:        0x0800  IP
IP Header - Internet Protocol Datagram
  Version:              4
  Header Length:        5  (20 bytes)
  Differentiated Services:%00000000
                        0000 00.. Default
                        .... ..00 Not-ECT

  Total Length:         78
  Identifier:           12062
  Fragmentation Flags:  %000
                        0.. Reserved
                        .0. May Fragment
                        ..0 Last Fragment
```

```
  Fragment Offset:      0  (0 bytes)
  Time To Live:         128
  Protocol:             17  UDP
  Header Checksum:      0x86C4
  Source IP Address:    192.168.1.109
  Dest. IP Address:     192.168.1.255
UDP - User Datagram Protocol
  Source Port:          137  netbios-ns
  Destination Port:     137  netbios-ns
  Length:               58
  UDP Checksum:         0x626A
NetBIOS Name Service - Network Basic Input/Output System
  Identification:       0x9FC8
  DNS Flags:            0x0110
                        0... .... .... .... Query
                        .000 0... .... .... Standard Query
                        .... .0.. .... .... (Non-Authoritative Answer)
                        .... ..0. .... .... (Message Not Truncated)
                        .... ...1 .... .... Recursion Desired
                        .... .... 0... .... (Recursion Not Available)
                        .... .... .0.. .... (Reserved)
                        .... .... ..0. .... (Authenticated Not Data)
                        .... .... ...1 .... Checking Disabled

  Questions:            1
  Answers:              0
  Authority:            0
  Additional:           0
Question
  Domain Name:          VIGNETTE <1C>
  Type:                 32  NetBIOS General Name Service
  Class:                1  Internet

FCS - Frame Check Sequence
  FCS:                  0xCBC682B7  Calculated
```

Here is another related unencrypted multicast packet that was observed on the 11th and 10th floors.

Source	Destination	Address 1	Address 2
192.168.1.244	239.255.255.250	Airespace:1B:E9:30	00:14:BF:18:4D:17

```
Packet Info
  Flags:                0x00000000
  Status:               0x00000000
  Packet Length:        396
  Timestamp:            05:25:40.611000000 11/17/2006
  Data Rate:            2   1.0 Mbps
  Channel:              6  2437MHz  802.11bg
  Signal Level:         53%
  Signal dBm:           0
  Noise Level:          0%
  Noise dBm:            0
802.11 MAC Header
  Version:              0
  Type:                 %10  Data
  Subtype:              %0000  Data Only
```

```
Frame Control Flags:    %00001011
                        0... .... Non-strict order
                        .0.. .... Non-Protected Frame
                        ..0. .... No More Data
                        ...0 .... Power Management - active mode
                        .... 1... This is a Re-Transmission
                        .... .0.. Last or Unfragmented Frame
                        .... ..1. Exit from the Distribution System
                        .... ...1 To the Distribution System

  Duration:             314  Microseconds
  Receiver:             00:0B:85:1B:E9:30  Airespace:1B:E9:30
  Transmitter:          00:14:BF:18:4D:17
  Destination:          01:00:5E:7F:FF:FA
  Seq Number:           3622
  Frag Number:          0
  Source:               00:14:BF:18:4D:15
802.2 Logical Link Control (LLC) Header
  Dest. SAP:            0xAA  SNAP
  Source SAP:           0xAA  SNAP
  Command:              0x03  Unnumbered Information
  Vendor ID:            0x000000
  Protocol Type:        0x0800  IP
IP Header - Internet Protocol Datagram
  Version:              4
  Header Length:        5  (20 bytes)
  Differentiated Services:%00000000
                        0000 00.. Default
                        .... ..00 Not-ECT

  Total Length:         354
  Identifier:           0
  Fragmentation Flags:  %010
                        0.. Reserved
                        .1. Do Not Fragment
                        ..0 Last Fragment

  Fragment Offset:      0  (0 bytes)
  Time To Live:         4
  Protocol:             17  UDP
  Header Checksum:      0xC2F4
  Source IP Address:    192.168.1.244
  Dest. IP Address:     239.255.255.250
UDP - User Datagram Protocol
  Source Port:          1900  ssdp
  Destination Port:     1900  ssdp
  Length:               334
  UDP Checksum:         0xE8C0
SSDP - Simple Service Discovery Protocol
  Method:               NOTIFY
  Uniform Resource Id:  *
  Version:              HTTP/1.1
  Host:                 239.255.255.250:1900
  Cache Control:        max-age=180  seconds until advertisement expires
  Location:             http://192.168.1.244:5431/dyndev/uuid:0014-bf18-
4d15000099dc  URL for UPnP
  Service Type:         NT: urn:schemas-upnp-org:device:WANDevice:1
  Service Type:         NTS: ssdp:alive
  Server:               INUX/2.4 UPnP/1.0 BRCM400/1.0
  Unique Service Name:  uuid:0014-bf18-4d15010099dc::urn:schemas-upnp-
org:device:WANDevice:1  UUID advertisement
FCS - Frame Check Sequence
  FCS:                  0x1E2AFC6B  Calculated
```

If the above trace excerpts are related to NYI devices, these devices may provide another path for an attacker to gain access or provide some useful technical information for a social engineering attack. NYI should investigate the devices related to Airspace and Vignette ECM systems.

4.4 Other discoveries

Spanning-Tree packets observe onto the wireless cell

There were several instance of where Spanning Tree traffic was observed while reviewing packet traces for NYICAPAP related frames. NYI should verify that its access points do not allow Spanning-Tree BPDUs to propagate onto the wireless cell. This wastes clear channel access cycles and is unneeded traffic on the cell.

Router login banner

While visiting NYI AMI was provided network access. AMI experienced trouble connecting to the local infrastructure and while troubleshooting tried to telnet to the local default gateway router to see if connectivity to that point existed. Upon connecting a login banner exposing details about the NYI network was depicted. This information provides a would be attacker plenty of information to launch a technical based social engineering attack on unsuspecting help-desk or network-desk support personnel.
The following screen capture of the router login banner is shown below:

The banner above provides the would be attacker the following information for a social engineering attack.

- Routing protocol used
- Routing protocol detailed features used – removed here
- Construe configuration of this part of the network via the user and server Vlan statements
- Redistributed routes identified as part of the configuration
- Indication of PIX and VoIP server functions on this router
- Router name and location
- Name of the network engineer supporting this router for name dropping techniques

From this one banner a tremendous amount of information is available for a social engineering attack to be conducted, especially if this information was obtained using a wireless Ad-hoc path into the network.

5.0 Recommendations and next steps required

NYI should first compare the Netstumbler and CommView reports outlined in this report against any APs currently deployed on the 11th floor and all other NYI and tenant floors to determine if and where each floor AP shows up on other floors and outside the building. After such cross referencing is completed NYI should then consider testing their AP features to reduce power levels thus reducing its cell size exposure onto other floors and possibly outside. Also, antenna placement should be considered in terms of polarization and direction for optimal and secure cell range on each floor. Oversized cells, even secured ones, still expose NYI to remote DOS attacks. Refer to the following research paper from AMI for further details about this type of rogue activity:

http://www.amilabs.com/HTM/HTM80211.pdf

The NYICAPAP AP can be seen from several floors and this could again be a result of the radio power, multipath, refraction and reflection behavior in the environment so reducing the cell size or adjusting the antennas to control ambient cell radiation should be considered. Further details on how to do this is outlined at the end of this section.

NYI should look into the NYI-1619 and NYI-BR unsecured APs outlined in previous sections to determine if the VIGNETTE Enterprise Content Management related traffic belongs to NYI 10th floor development teams or another group on the 11th floor. These APs are open and unsecured, yet have a NYI prefix in their SSID. NYI must investigate further whether these APs are actually connected to the NYI wired infrastructure and/or are rogue APs placed by NYI users for connectivity convenience.

Ad-hoc networks must be investigated for the reasons outlined in the Ad-hoc section of this report. NYI must identify all devices listed as Ad-hoc to determine if it is a NYI asset or not. Then NYI must track down the devices on each floor to ensure that they are no longer used and educate the users to the security issues outlined in the Ad-hoc section of this report. Unsecured Ad-hoc networks connected to the NYI infrastructure are a major security breach.

NYI should consider conducting a wireless AP enumeration survey and packet analysis for the entire building once a quarter or twice a year depending on resources available. This practice is necessary so NYI can build an inventory of AP which lists which are approved NYI AP deployed, non NYI AP and rogues deployed by NYI employees or outsiders. This practice should continue until a Wireless Intrusion Detection/Prevention(WIDS/WIPS) systems is in place.

NYI must ensure that its client radio adaptors are set to active scanning for a specific SSID for NYI APs only. Further research into NYI wireless adaptors used(Cisco or other) should be conducted to see if client side connectivity utility profiles can be configured to only use NYI APs. Home users of same laptops may require a different profile. This is important for there were several stronger consumer grade APs noted on NYI floors either coming from other floors or across the street that NYI personnel may inadvertently associate too for basic web browsing and could be compromised, especially if the stronger signal AP is a rogue conducting a man in the middle attack or Fake AP attack. A WIPS/WIDS helps in mitigating such activity.

NYI must review its router and switch login banners to determine how much useful information is actually needed on such banners. As outlined in the previous section a router login banner was discovered providing too much information for a social engineering attack. NYI must review all such banners on all networking equipment and apply a standard banner as per its security policy for this topic if one is defined.

NYI should consider using a multi factor and mutual authentication based security architecture for wireless clients and APs. Mutual authentication ensures that the client and AP credentials are valid. Mutual authentication ensures that the user cannot access the wireless cell unless the client/supplicant and AP are authenticated by each other and a an authentication server. This two-way login validates the authentication server to the client as well. This authentication architecture prevents man in the middle or Fake AP attacks to ensure users do not associate to a rogue AP temporarily to have their laptop compromised.

NYI should check their AP configurations to ensure that Spanning-Tree BPDU are not sent onto the wireless cell. There are IOS commands available on the AP and switch connected to the AP to prevent BPDUs from exiting out the switch or radio interface.

NYI should review its tenant floor clients and determine if they should be notified that their signals are emanating outside the building and inside through several floors. The same recommendations outlined in this report for NYI wireless assets can be applied to the tenant floors as well.

NYI should look into reducing the APs cell transmitted power output to reduce the cell sizes to ensure that NYIIM APs cell coverage is not radiated easily on the 10th and 12th floors. A sample of one IOS command to do this is the ***power*** command displayed below. AMILABS uses a Cisco 1230ag AP. Such commands may vary depending on IOS version and APs used by NYI.

```
AMILABSAP(config)#int dot110
AMILABSAP(config-if)#power
AMILABSAP(config-if)#power ?
  client  Client radio transmitter power level
  local   Local radio transmitter power level

AMILABSAP(config-if)#power loc
AMILABSAP(config-if)#power local ?
  cck   Set local power for CCK rates
  ofdm  Set local power for OFDM rates

AMILABSAP(config-if)#power local OFDM ?
  <1 - 30>  One of: 1 5 10 20 30
  maximum   Set local power to allowed maximum

AMILABSAP(config-if)#power local OFDM
```

NYI should test different power values, rescan the floors above and below NYIIM to determine the acceptable cell size.

Other Cisco AP IOS options are available such as the ***antenna gain*** command.

```
AMILABSAP(config-if)#antenna ?
  gain      Configure Resultant Antenna Gain
  receive   receive antenna setting
  transmit  transmit antenna setting

AMILABSAP(config-if)#antenna gain ?
  <-128 - 128>  Resultant Antenna Gain in dB
```

There are a host of AP IOS commands that can be used such as the ***dot11 adjacent-ap.*** NYI should consider reviewing all the features of the IOS that applies to the recommendations in this report. Another such option is the ***Wireless Management Frame protection feature,*** if applicable.

Another aspect of cell size tuning for range and security purposes is the placement of antennas. If the APs are placed in the ceiling the polarization of the antennas can make a difference in terms of the beam width generated from the AP and the area covered. NYI should look into adjusting the AP antennas(depending on the type), if applicable, for the AP to see if the desired cell range observed for security purposes is achieved.

NYI should consider using patch or panel type APs, or using patch or panel antennas to redirect the RF cell shape from the perimeter walls inward, instead from the ceiling and down and outward like a donut shape.

One such Panel type AP is the Cisco Aironet 1130AG Series packages high capacity, high security, and enterprise-class features delivering wireless LAN access for a low total cost of ownership. Designed for wireless LAN coverage in offices and similar RF environments, this unobtrusive access point features integrated antennas and dual IEEE 802.11a/g radios for robust and predictable coverage, delivering a combined capacity of 108 Mbps. The Cisco Aironet 1130AG Series is ready to install and easy to manage, reducing the cost of deployment and ongoing maintenance. The device is available in either a lightweight version, or as an autonomous version that may be field-upgraded to lightweight operation.

If NYI is deploying a wireless infrastructure across all its building floors it should consider the use of a WIPS/WIDS to monitor and manage its wireless infrastructure. A WIPS/WIDS offers the following features to name a few:

- Asset allocation of all devise
- Identification of rogue devices and alerts administrators
- Identification of rogue devices and takes actions such as dissociation from the cell or tar pitting the device by flooding or keeping it busy until NYI personnel can investigate
- Detailed reports and logs for security audits, tuning and scaling purposes
- Network and security management of all APs and client devices
- Centralized control of all APs for RF cell size adjustment and security functions.
- No need to conduct manual scans of device identification

Cisco offers several solutions and with the acquisition of Airspace their portfolio of products in this area is broad. NYI should investigate the use of a WIPS/WIDS for enhanced security and management of their wireless infrastructure. Below is some additional information and part numbers on the components that NYI can utilize to achieve its wireless security goals.

Cisco WCS includes tools for wireless LAN planning and design, RF management, location tracking, Intrusion Prevention System (IPS), and wireless LAN systems configuration, monitoring, and management. Patch antennas include:
AIR-ANT2485P-R
AIR-ANT2460P-R
AIR-ANT2465P-R
AIR-ANT5170P-R
AIR-ANT5195P-R
AIR-ANT3213 Pillar mount
Diversity / Omni directional ceiling mounts
AIR-ANT5145V-R
AIR-ANT5959

6.0 Packet trace and Netstumbler logs files for NYI's reference

The packet trace files supplied by AMI to NYI were duplicated into three file formats for NYI to use depending on which protocol analyzer they utilize.

The trace files are formatted as follows:

Program	**File Format**
ComView for Wifi	.NCF
Ehterpeek, Ethereal and Packetyzer	.PKT
OmniPeek Personal or Airo Peek	.APC

A trial version of CommView for Wifi can be downloaded from www.tamosoft.com and the files can be loaded into the program and reports generated for NYI to review.

Ethereal can be downloaded for free at www.ethereal.com for NYI to review specific packet detail.

Packetyzer can be downloaded for free at www.packetyzer.com for NYI to review specific packet detail.

OmniPeek Person which is free and can be used to read the trace files to generate reports can be downloaded at www.wildpackets.com

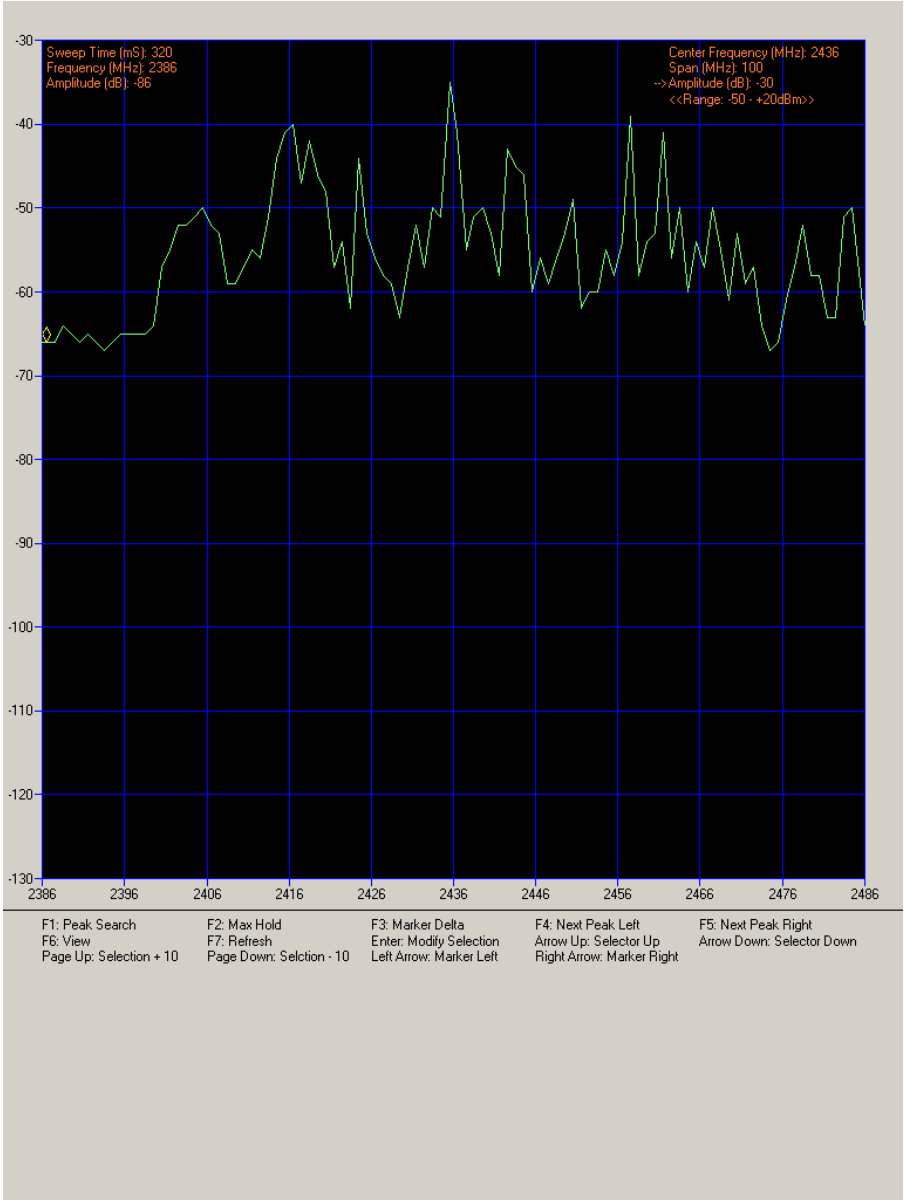
The file formats supplied may be automatically read into NYI's own protocol analyzer such as Network General's sniffer.

Reading the Netstumbler log files:
The Netstumbler files can be loaded and reviewed for further analysis by using the Netstumbler utility. A free copy of the utility can be downloaded at www.netstumbler.com

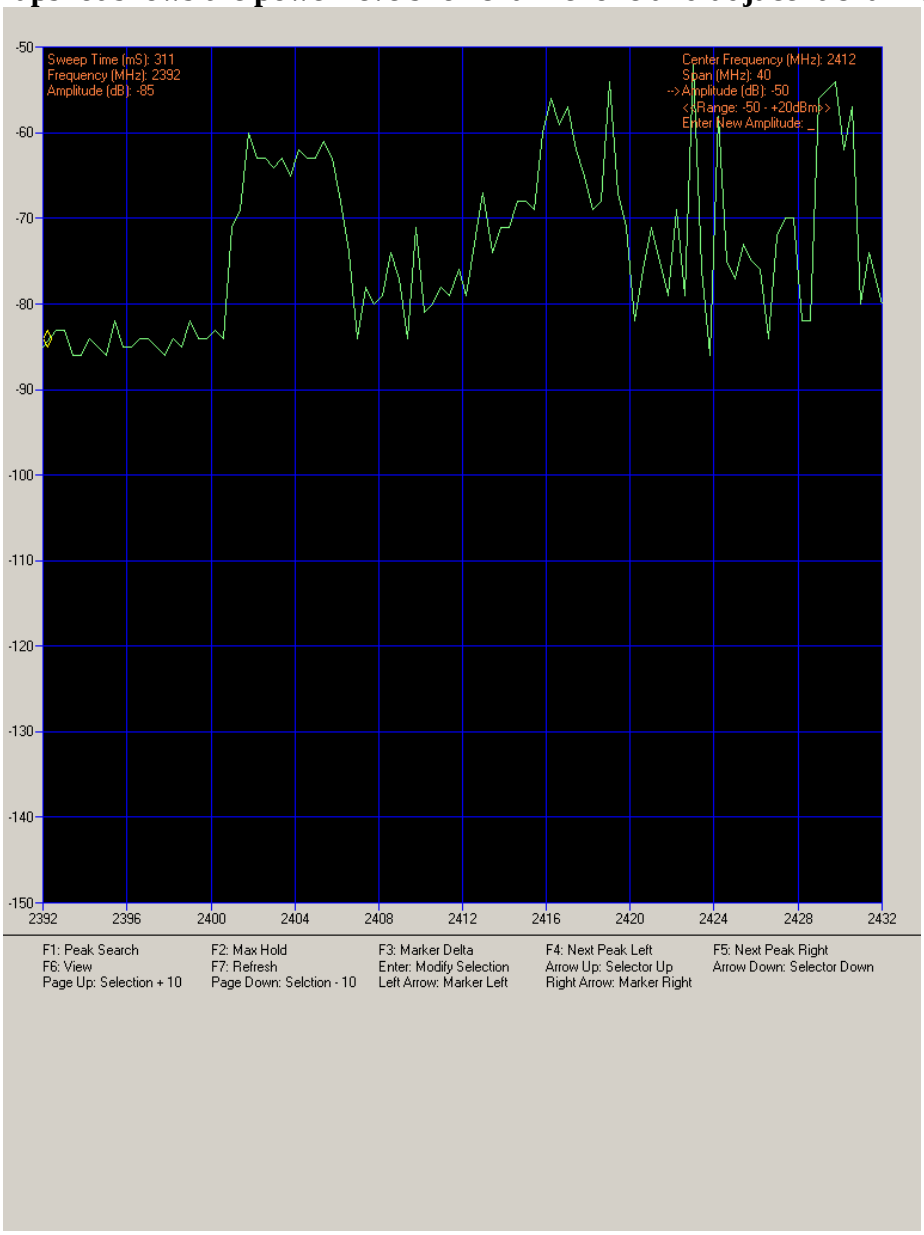
7.0 Spectral analysis

Since AMI did not have the NYI 11th floor specific APs and Channel numbers to focus its efforts for spectral channel utilization and coverage points, a general spectral analysis was conducted from the 10th floor to determine the power levels of the most prevalent channels observed(1,6 and 11) plus a full 2.4-2.5gHz sweep was conducted. AMI walked the 10th floor several times per scan to record maximum peak power levels observed. The following snapshots show what was observed by walking across the entire floor and not one particular location. It should be noted that the following graphs will be skewed due to the radiated power from Ad-hoc radios and neighbor radios from the other floors and outside the building. The spectral analysis was conducted using a 2.4ghz Spectrum Analyzer from Aerocomm.

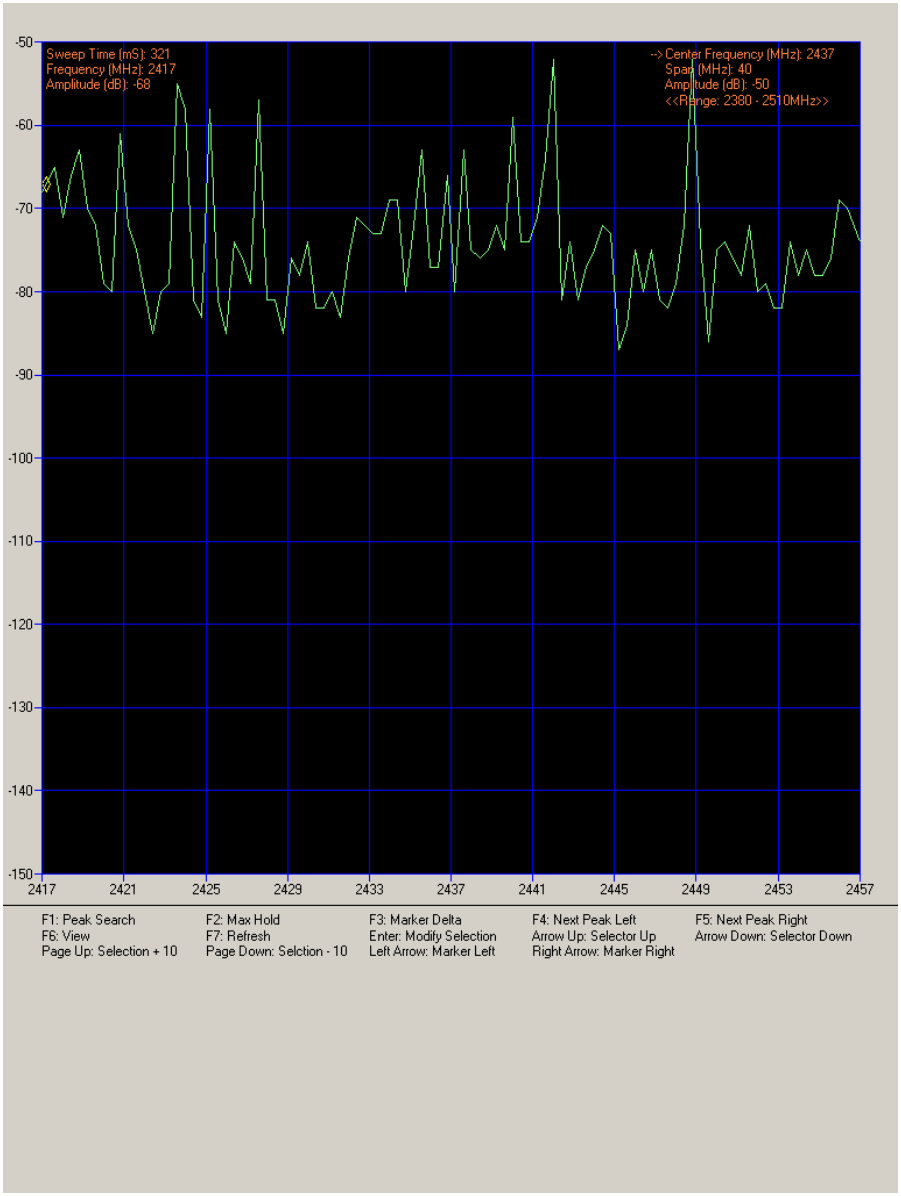
Below is the output of a scan of the full 2.4gHz range, channels 1, 6 and 11 are a little more pronounced than the others.



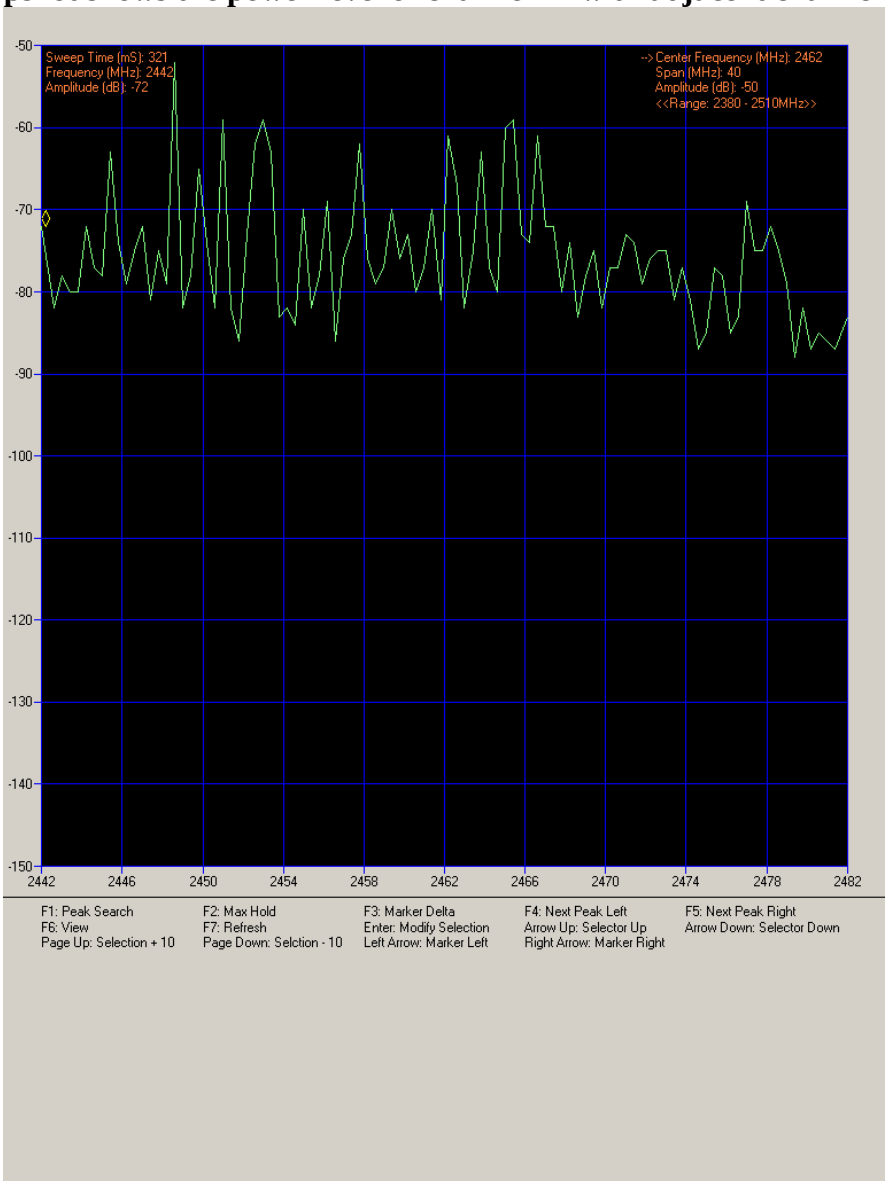
This snapshot shows the power levels for channel one and adjacent channel two.



This snapshot shows channel six and the adjacent channels on either side.



This snapshot shows the power level of channel 11 with adjacent channel activity.



8.0 Summary

Securing a wireless network by controlling its RF cell size is a challenging task due to the physics of RF and the environmental makeup of the office area. NYI's NYIIM access points were observed on other non NYIIM floors as well as various Ad-hoc networks, and other potential unsecured NYI APs in operation. This analysis report outlined what NYI and non NYI wireless devices were present around the 10th, 11th and the tenant floor of 12. This report listed the devices emanating from the NYI building outside at the street level and listed a series of issues and recommendations for NYI management and engineering personnel to review. AMI is available to answer any questions about this report or any questions in general relating to wireless networks and network security. AMI would like to thank NYI for the opportunity to conduct this wireless audit for NYIIM.