MacLab Session LT

Running Your Wireless Network Safely & Reliably - Tips on Best Tools

Wednesday, January 7, 2009 1:00 PM - 3:00 PM Room North 111

Dr. Bill Wiecking
wiecking@mac.com

Introductions: Who are we? What do we need to cover here?

8 Modules:

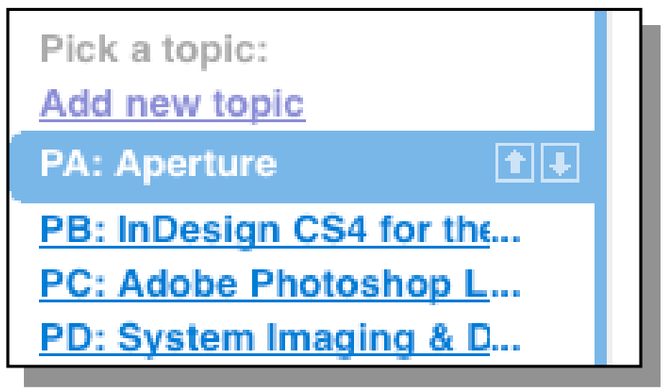
1. Wireless scanning 1: Active stumblers-iStumbler
2. Wireless scanning 2: Passive scanning-Kismac
3. Wireless scanning 3: Physical interference-WiSpy
4. Security 1: Packet sniffing-interarchy, IPnetmonitor, kismac
5. Security 2: AirPort setup-access control tools
6. Security 3: VPN-setup, issues, solutions
7. Client configuration: Setup, issues, solutions
8. Advanced topics: Rogue APs, logging, mapping

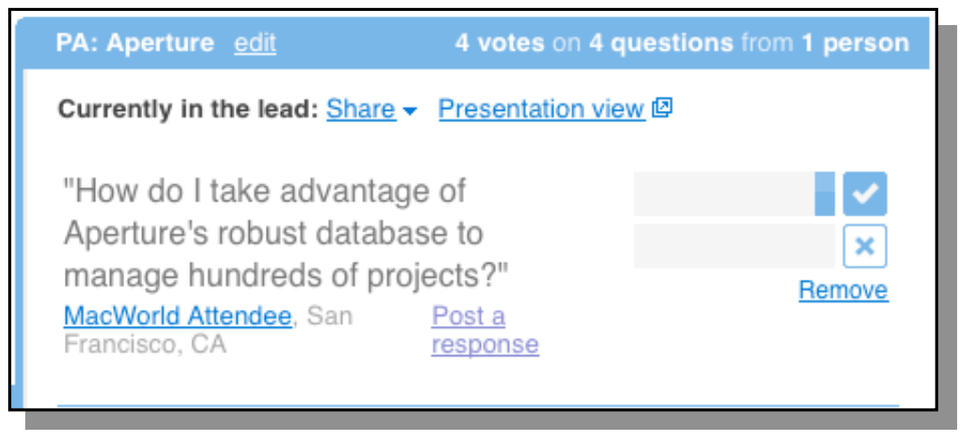
Questions---

Q&A - Users Conference

We are using Google Moderator to take questions for this session.

1. Go to http://tinyurl.com/5t55h2
2. Pick the topic that matches this session MacLab Session LT
3. Sign in using a Google Account
   User Name: macworldexpo09
   Password: macworld09
4. Submit the questions you want to ask
5. Vote on others' questions you want answered





Module 1: Wireless scanning 1: Active stumblers-iStumbler

Concepts:

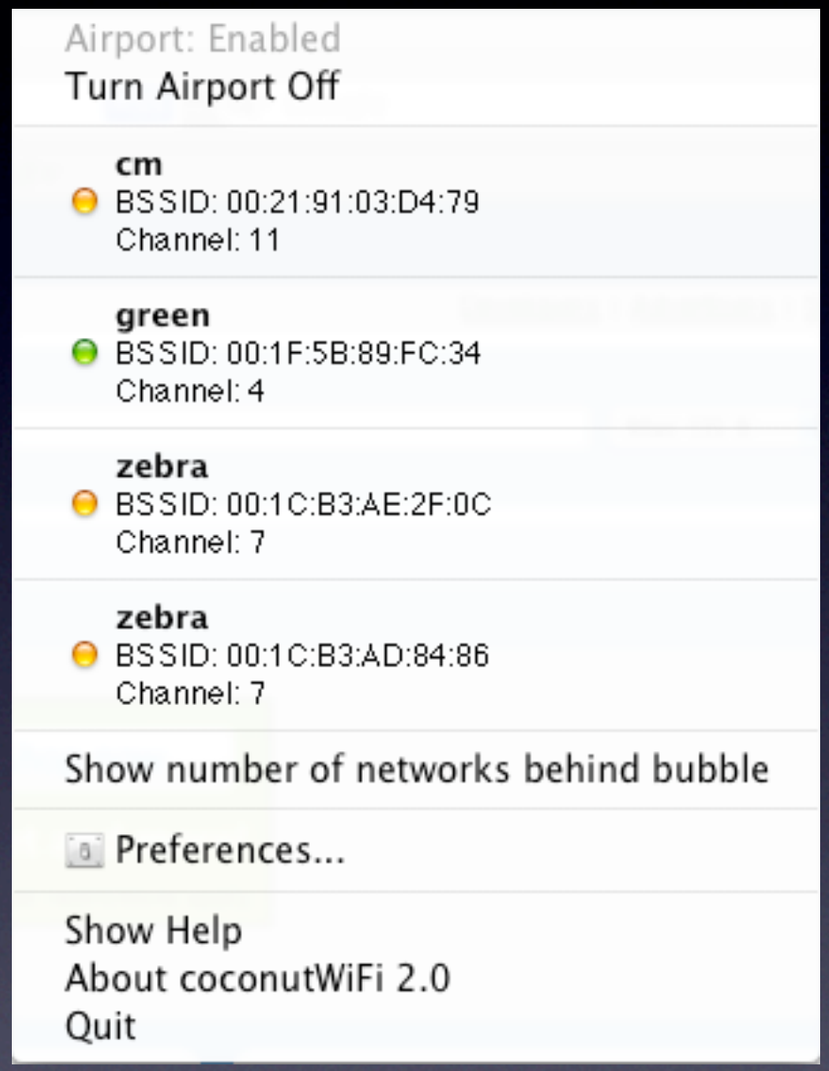
- Active only scans
- Sees only broadcasting networks
- No packet sniffing
- Completely legal
- Most common wireless scanning practice
- Beware of consultants who use only this toolset

Tools

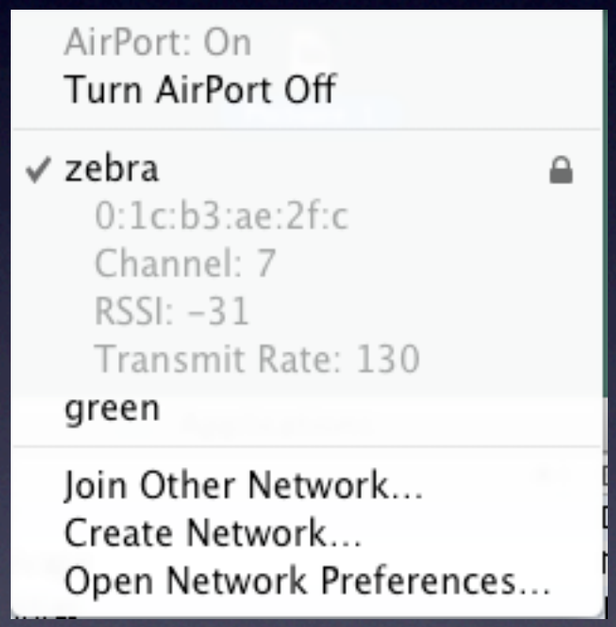
- Coconut wifi 2.0
- iStumbler 98

Try this:

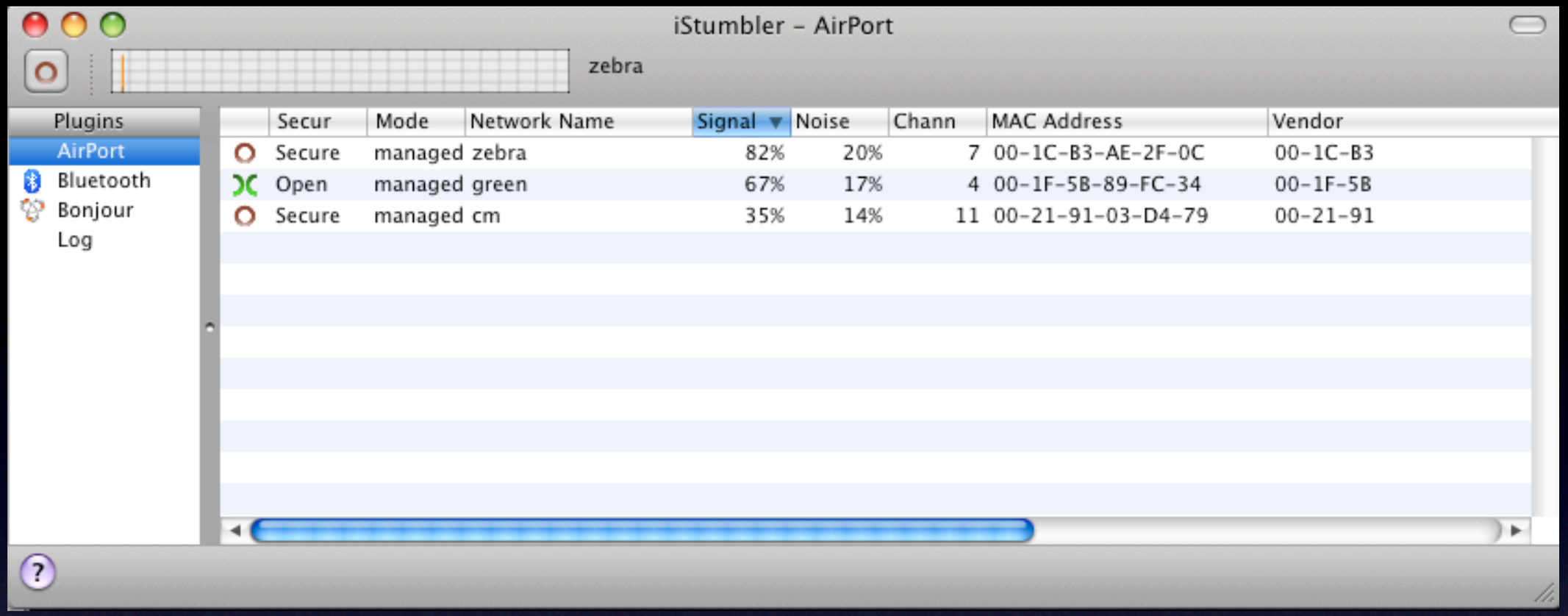
- Note signal to noise ratio (may be just signal on some scanners)
- Can you determine the direction of the source? How?
- Can this be used with external antennas/amps?



Coconut Wifi
Pull-down menu



Airport pull-down menu hold option click



iStumbler 98

Module 2: Wireless scanning 2: Passive scanning-Kismac

Concepts:

- Passive scans, you do not have to join the network to sniff
- This is done by using "promiscuous mode" which inactivates normal active wireless use for the interface
- Detects all logical networks: tunnels, hidden/closed networks, ad hoc networks and some others
- Very useful for determining SNR, aiming antennas etc.
- Also useful for packet sniffing
- Channel cycles, or you can choose one channel (for sniffing, SNR analysis)
- Works using internal wireless interface or USB interfaces
- Illegal in Germany

Tools

- Kismac R319

Try this:

- Note signal to noise ratio
- Look for more nets than you found the first time
- Note packet capture selections
- Note also WEP and WPA cracking tools included
- How could this help in setting up/diagnosing a wireless network problem?

KisMAC

KisMAC 0.21a

#	Ch	SSID	BSSID	Enc	Type	Signal	Avg	Max	Packets	Data	Last Seen	Ch/Re
0	8	green	00:1F:5B:89:FC:34	NO	managed	6	31	50	1999	465.48KiB	2009-01-02 14:53:56 -1	
1	8	zebra	00:1C:B3:AE:2F:0C	WPA	managed	60	43	68	3385	0.80MiB	2009-01-02 14:53:56 -1	
2	7	zebra	00:1C:B3:AD:84:86	WPA	managed	0	5	12	362	88.01KiB	2009-01-02 14:53:54 -1	
3	1	attic	00:1D:4F:A8:15:69	WPA	managed	0	3	4	264	29.11KiB	2009-01-02 14:53:54 -1	
4	9	cm	00:21:91:03:D4:79	WPA	managed	0	8	13	12	3.38KiB	2009-01-02 14:52:46 -1	

KisMAC

KisMAC 0.21a

Bytes | 15 sec | ?

40.60 kbps

zebra
green
zebra
attic

0 bps

6.21 kbps

Stop Scan

Property	Setting
SSID	green
BSSID	00:1F:5B:89:FC:34
Vendor	Apple, Inc.
First Seen	2009-01-02 14:47:59 -1000
Last Seen	2009-01-02 14:54:47 -1000
Channel	6
Main Channel	4
Supported Rates	1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54
Signal	30
MaxSignal	50
AvgSignal	30
Type	managed
Encryption	disabled
Packets	2287
Data Packets	0
Unique IVs	0
Inj. Packets	0
Bytes	532.70KiB
Key	
ASCII Key	
LastIV	00:00:00
Latitude	
Longitude	
Elevation	

KisMac r319

Module 3: Wireless scanning 3: Physical interference-WiSpy

Concepts:

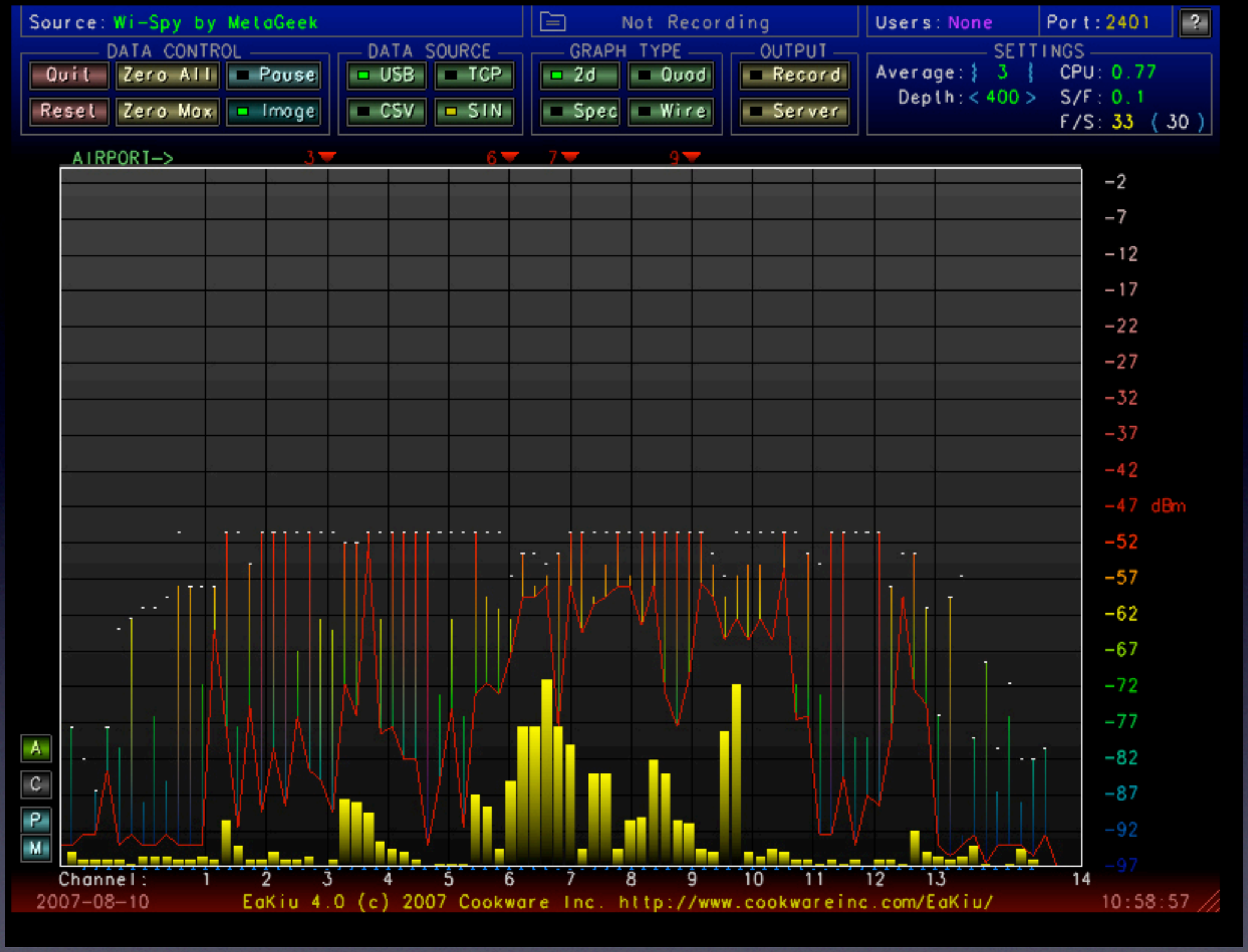
• Physical interference is anything not generated by a wireless device, so has no ID info, no packets, no channel ID, no data at all
• May be innocuous items you have installed without knowing they would interfere with your wireless networks
• May be intermittent (e.g. phones, microwave ovens) or constant (e.g. lighting, video units)
• May also be random noise, not associated with a specific device or source (e.g. background noise)
• Sources: microwave ovens, radar, cordless phones, video receivers, satellite dishes, compact fluorescent bulbs

Tools

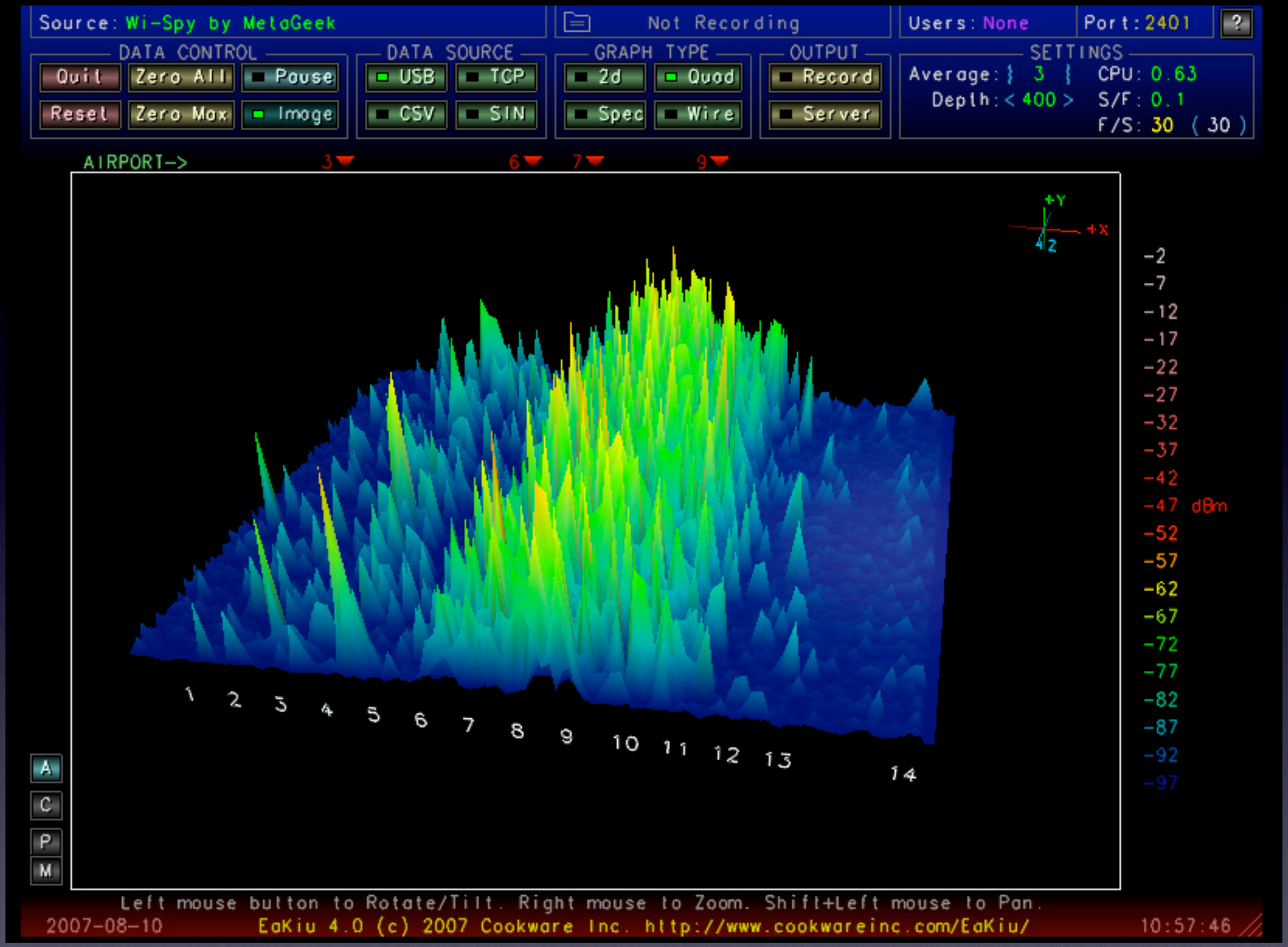
•Eakiu WiSpy

Try this:

• Note noise spectra
• How could you use this to triangulate on a source?
• How could this be used as a tripwire for rogue access points?


Source: Wi-Spy by MetaGeek
Not Recording
Users: None
Port: 2401
?
DATA CONTROL
Quit
Zero All
Pause
Reset
Zero Max
Image
DATA SOURCE
USB
TCP
CSV
SIN
GRAPH TYPE
2d
Quad
Spec
Wire
OUTPUT
Record
Server
SETTINGS
Average: 3
Depth: 400
CPU: 0.77
S/F: 0.1
F/S: 33 (30)
AIRPORT->
3
6
7
9
-2
-7
-12
-17
-22
-27
-32
-37
-42
-47 dBm
-52
-57
-62
-67
-72
-77
-82
-87
-92
-97
A
C
P
M
Channel: 1 2 3 4 5 6 7 8 9 10 11 12 13 14
2007-08-10
EaKiu 4.0 (c) 2007 Cookware Inc. http://www.cookwareinc.com/EaKiu/
10:58:57

Eakiu Wi-Spy


Source: Wi-Spy by MetaGeek
Not Recording
Users: None
Port: 2401
?
DATA CONTROL
Quit
Zero All
Pause
Reset
Zero Max
Image
DATA SOURCE
USB
TCP
CSV
SIN
GRAPH TYPE
2d
Quad
Spec
Wire
OUTPUT
Record
Server
SETTINGS
Average: 3
Depth: 400
CPU: 0.63
S/F: 0.1
F/S: 30 (30)
AIRPORT->
3
6
7
9
+Y
+X
+Z
-2
-7
-12
-17
-22
-27
-32
-37
-42
-47 dBm
-52
-57
-62
-67
-72
-77
-82
-87
-92
-97
1 2 3 4 5 6 7 8 9 10 11 12 13 14
A
C
P
M
Left mouse button to Rotate/Tilt. Right mouse to Zoom. Shift+Left mouse to Pan.
2007-08-10
EaKiu 4.0 (c) 2007 Cookware Inc. http://www.cookwareinc.com/EaKiu/
10:57:46

Eakiu Wi-Spy

Module 4: Security 1: Packet sniffing-interarchy, IPnetmonitor, kismac

Concepts:

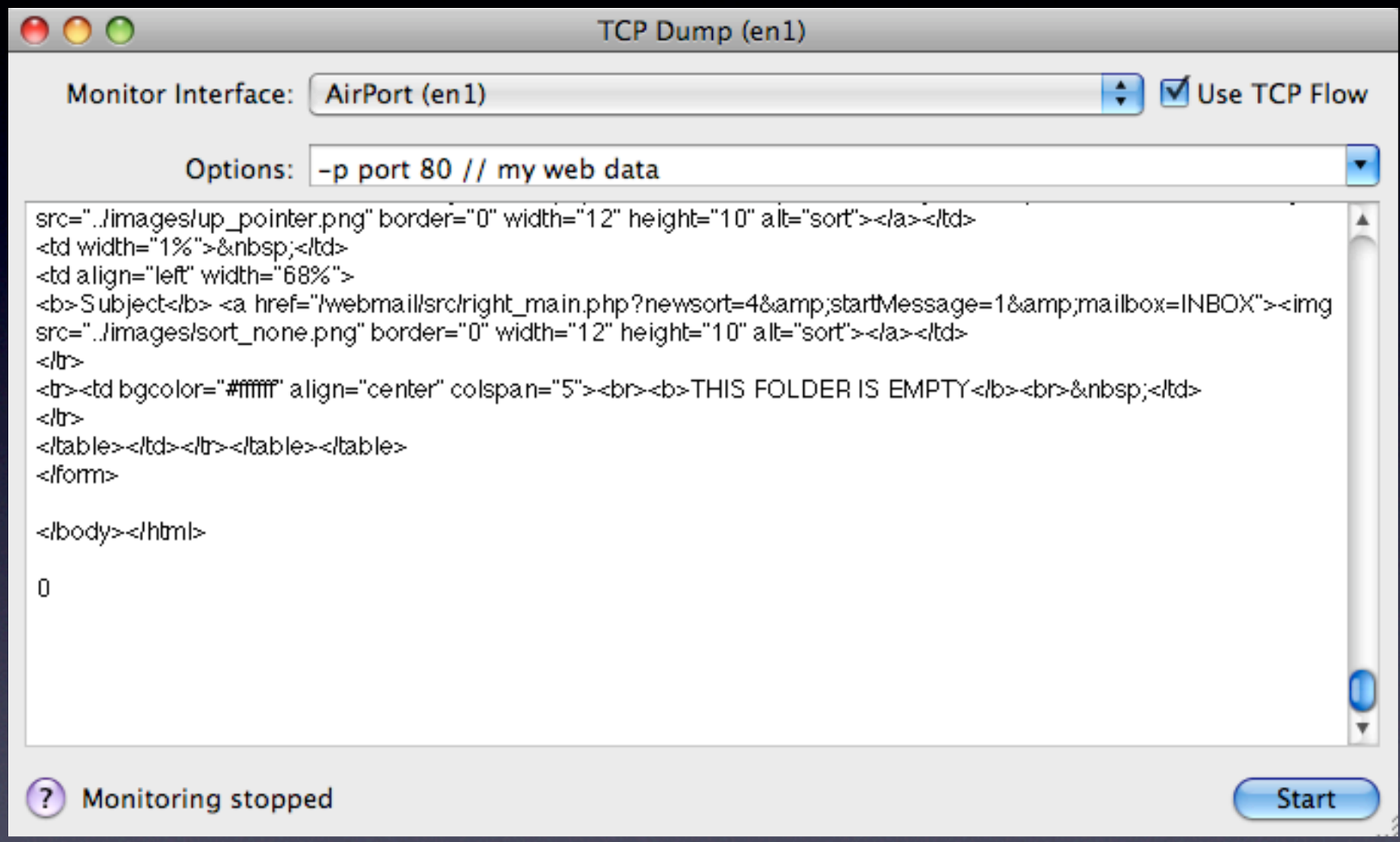
- If you have joined a network, packet sniffing is very easy, using IP netmonitor, interarchy or certain terminal commands
- If you cannot join, then passive scanning can be done using kismac
- Open unencrypted traffic includes FTP, webmail, mail (non APOP), retrospect backups and many more
- All SSL and VPN traffic is encrypted

Tools

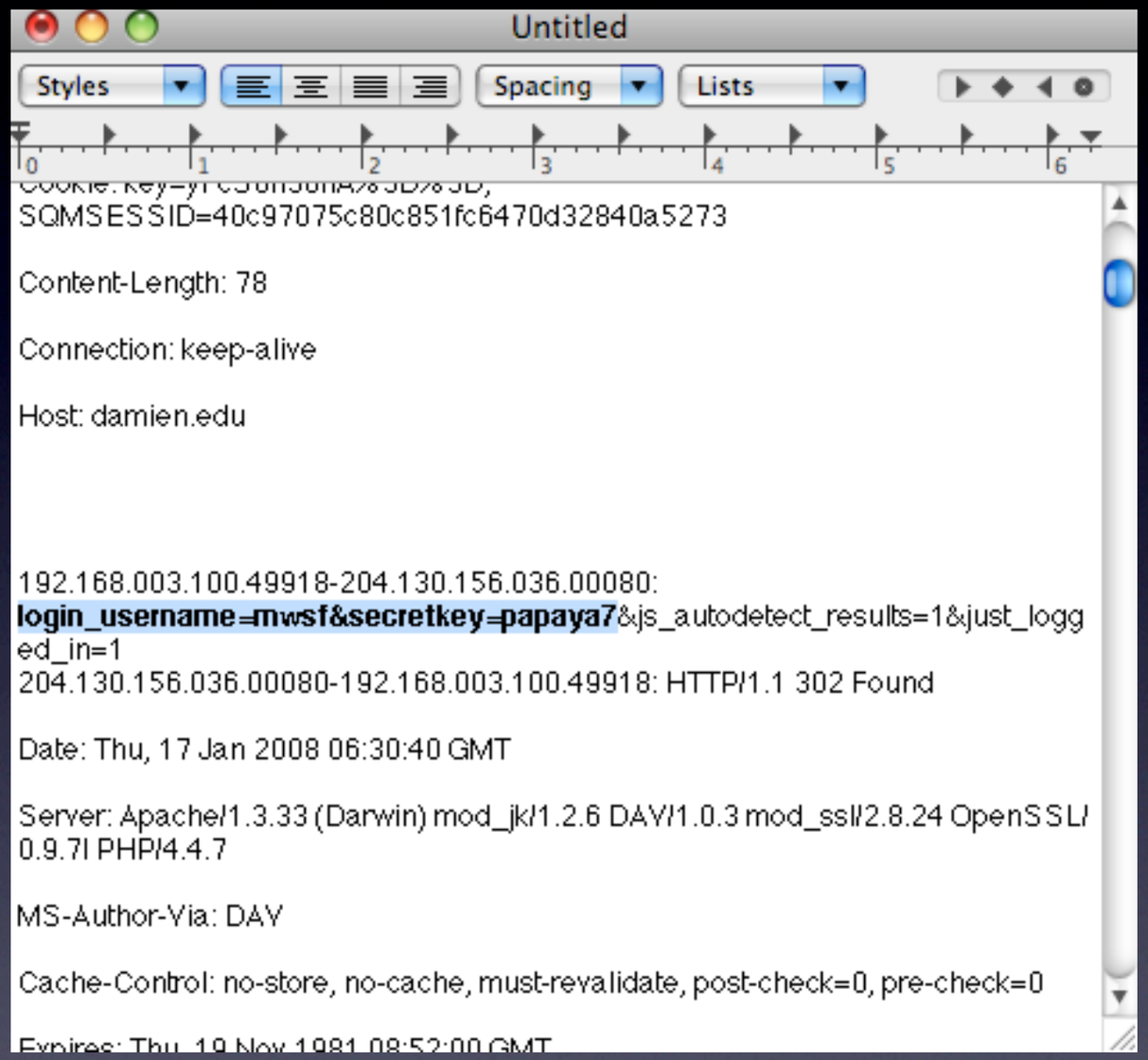
- IP net monitor 2.3
- Interarchy 8.5.4 (old version)
- Kismac r319

Try this:

- Capture packets on wireless network you have joined
- Browse a web page, note traffic decoded as clear text
- Login to your webmail account, note login and password (you can capture text and use find command in text edit)
- Repeat with VPN, APOP mail or SSL text/pages
- Try this with iPhone, both in wireless mode and in ad hoc mode


TCP Dump (en1)
Monitor Interface:
AirPort (en1)
Use TCP Flow
Options:
-p port 80 // my web data
src="../images/up_pointer.png" border="0" width="12" height="10" alt="sort"></td>
<td width="1%"> </td>
<td align="left" width="68%">
Subject <img
src="../images/sort_none.png" border="0" width="12" height="10" alt="sort"></td>
</tr>
<tr><td bgcolor="#ffffff" align="center" colspan="5">
THIS FOLDER IS EMPTY
 </td>
</tr>
</table></td></tr></table></table>
</form>
</body></html>
0
Monitoring stopped
Start

TCP dump


Untitled
Styles
Spacing
Lists
0
1
2
3
4
5
6
SQMSESSID=40c97075c80c851fc6470d32840a5273
Content-Length: 78
Connection: keep-alive
Host: damien.edu
192.168.003.100.49918-204.130.156.036.00080:
login_username=mwsf&secretkey=papaya7&js_autodetect_results=1&just_logged_in=1
204.130.156.036.00080-192.168.003.100.49918: HTTP/1.1 302 Found
Date: Thu, 17 Jan 2008 06:30:40 GMT
Server: Apache/1.3.33 (Darwin) mod_jk/1.2.6 DAV/1.0.3 mod_ssl/2.8.24 OpenSSL/0.9.7l PHP/4.4.7
MS-Author-Via: DAV
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

TCP dump

Module 5: Security 2: Airport setup-access control tools

Concepts:

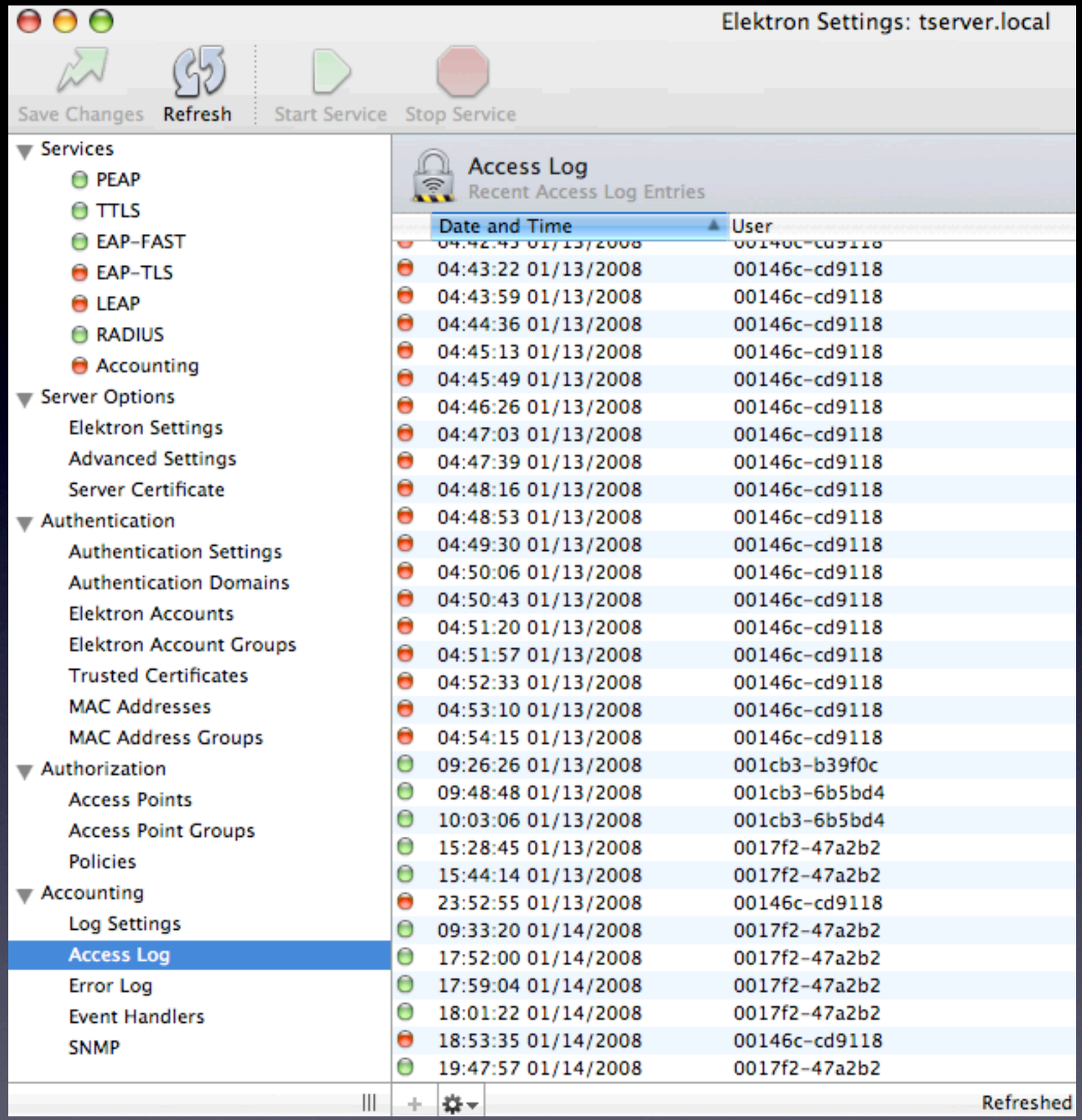
- Access control blocks certain folks from joining your network
- This does not stop them from passively sniffing your network
- Access control is the best first in keeping nosy folks off of your network
- On many networks, once wireless access is granted, wired assets become vulnerable to attack, sniffing, DOS etc.
- Using Apple AirPort Extreme (version 7 in this case) you can enforce the following access control measures:
  - WEP-bad, keys can be easily broken
  - Hardware access control lists (HWACL)-bad can be spoofed using ethernet utilities
  - WPA2-our best best these days, changes keys, assures data integrity, blocks man in the middle attacks

Tools

- Apple airport extreme
- Apple airport utility
- ChangeMac 1.5.1
- Elektron

Try this:

- Setup WEP on an Airport extreme station, try to gain access
- Note you can crack this using kismac
- Setup HWACL on AE unit, note your ethernet address, and try access
- Note you can change your ethernet address using ChangeMac 1.5.1
- Repeat above using WPA2
- Combinations of the above are also useful
- Elektron or Mac OSX leopard server can be used to administer many access points using HWACL, WPA2 enterprise and 802.11i



Elektron server

ChangeMac

With this you can defeat HW ACL on any network, wired or wireless

Module 6: Security 3: VPN-setup, issues, solutions

Concepts:

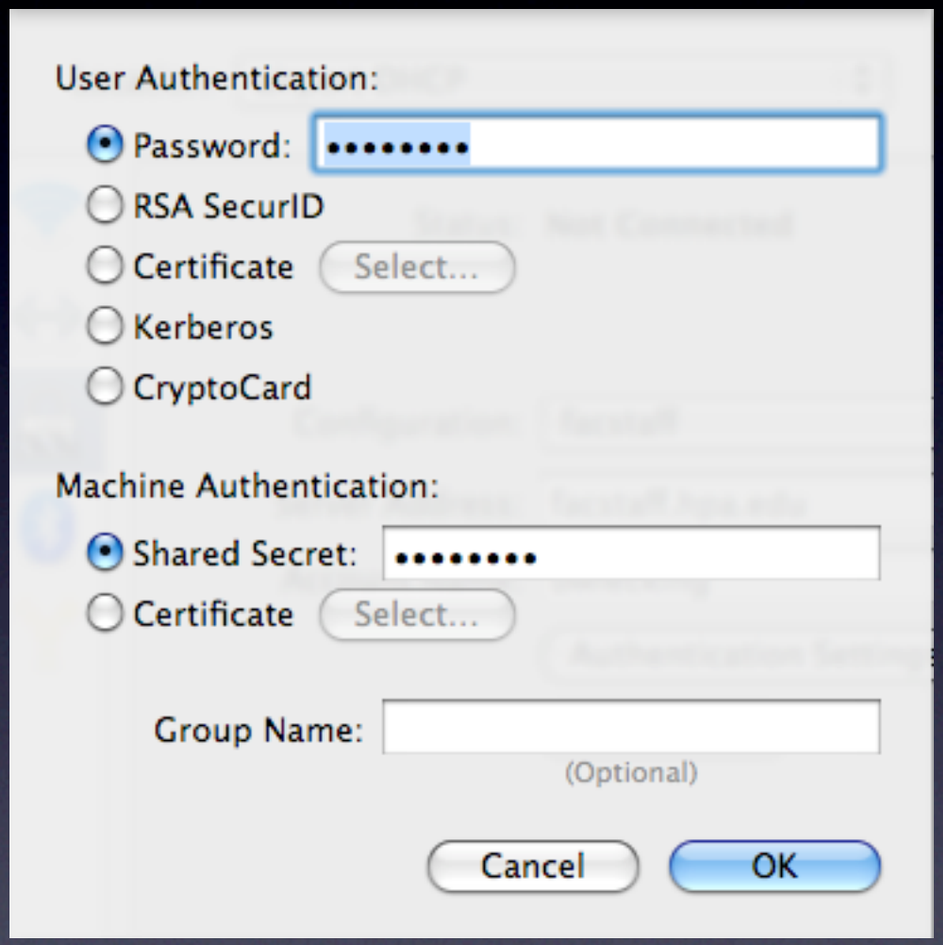
- Even if you believe you are secure in your access practices, your traffic can be passively gathered
- Encrypted traffic is relatively useless to hackers (exceptions: business, military, government)
- VPN creates a secure "tunnel" between your client and whatever VPN endpoint you are connected to
- Data can be all encrypted or only to certain destinations (see network prefs screen)
- Can be used as a remote content filter, or as a remote help desk using timbuktu or apple remote desktop
- VPN config files can be posted on web sites or emailed to clients for one-click setup

Tools

- Apple network preferences screen
- Apple OSX leopard server

Try this:

- Using one of the active packet sniffers (interarchy or IPNM) watch web traffic to a client on your network
- Have the client join a VPN tunnel, repeat
- How did the data you gathered change?
- n.b. watch the client config, it is easy to connect to the VPN and yet have traffic not encrypted



VPN client config

n.b. shared secret must be 8 characters or more

Module 7: Client configuration: Setup, issues, solutions

Concepts:

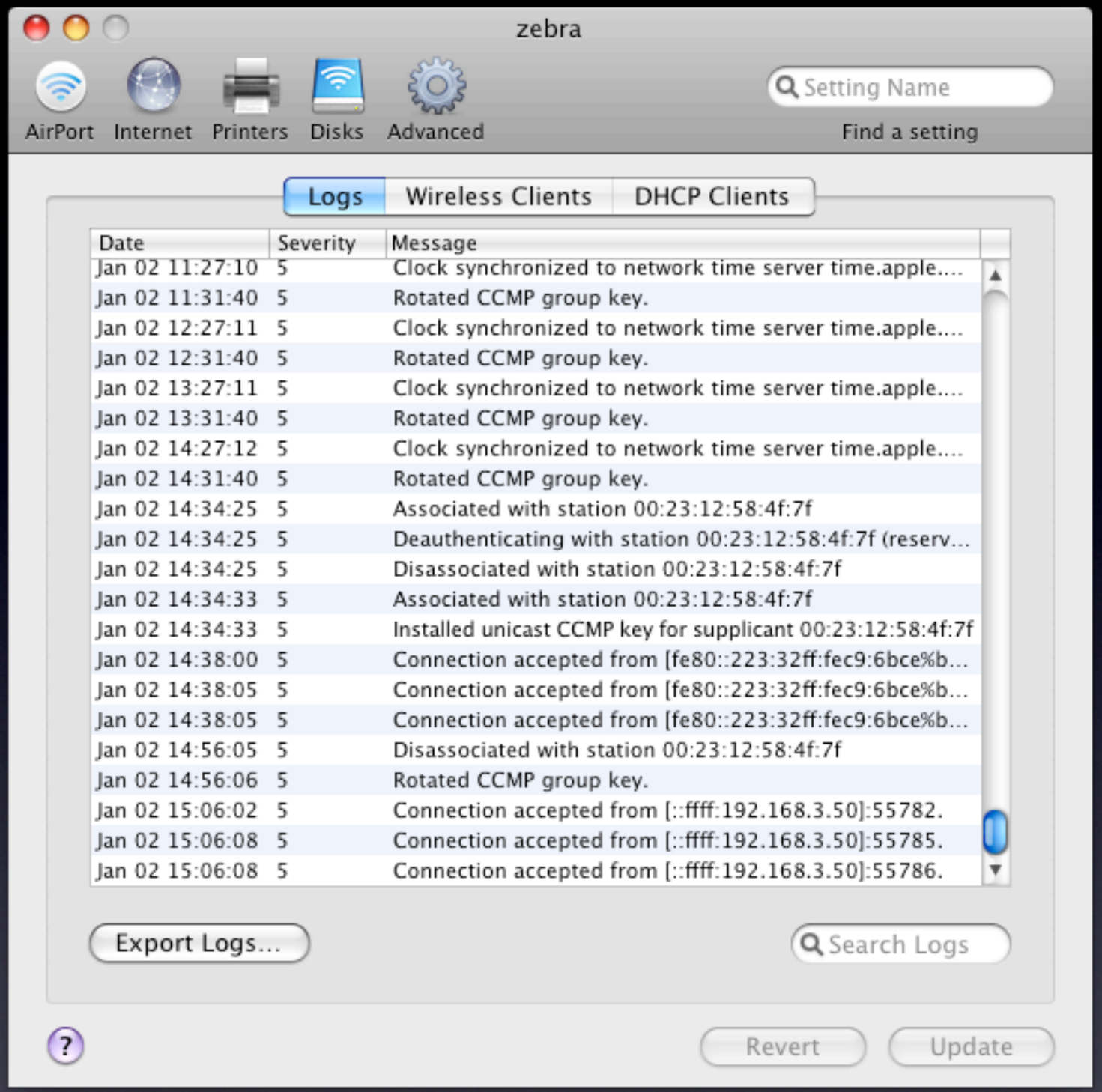
- Clients may be wireless laptops or desktops
- You may have to support guests (sandbox tips)
- You may have to support roaming clients over many of your Access Points
- DHCP: yes or no and where?
- Open or closed networks: why?
- Minimizing client confusion
- Clever tricks to determine hardware addresses

Tools

- Apple network preferences screen
- Apple AirPort Utility

Try this:

- Using AirPort utility, determine wireless ethernet address of anonymous client
- Notice the system logs and signal strength meters- useful for AP placement



AirPort log page

Module 8: Advanced topics: Rogue APs, logging, mapping

Concepts:

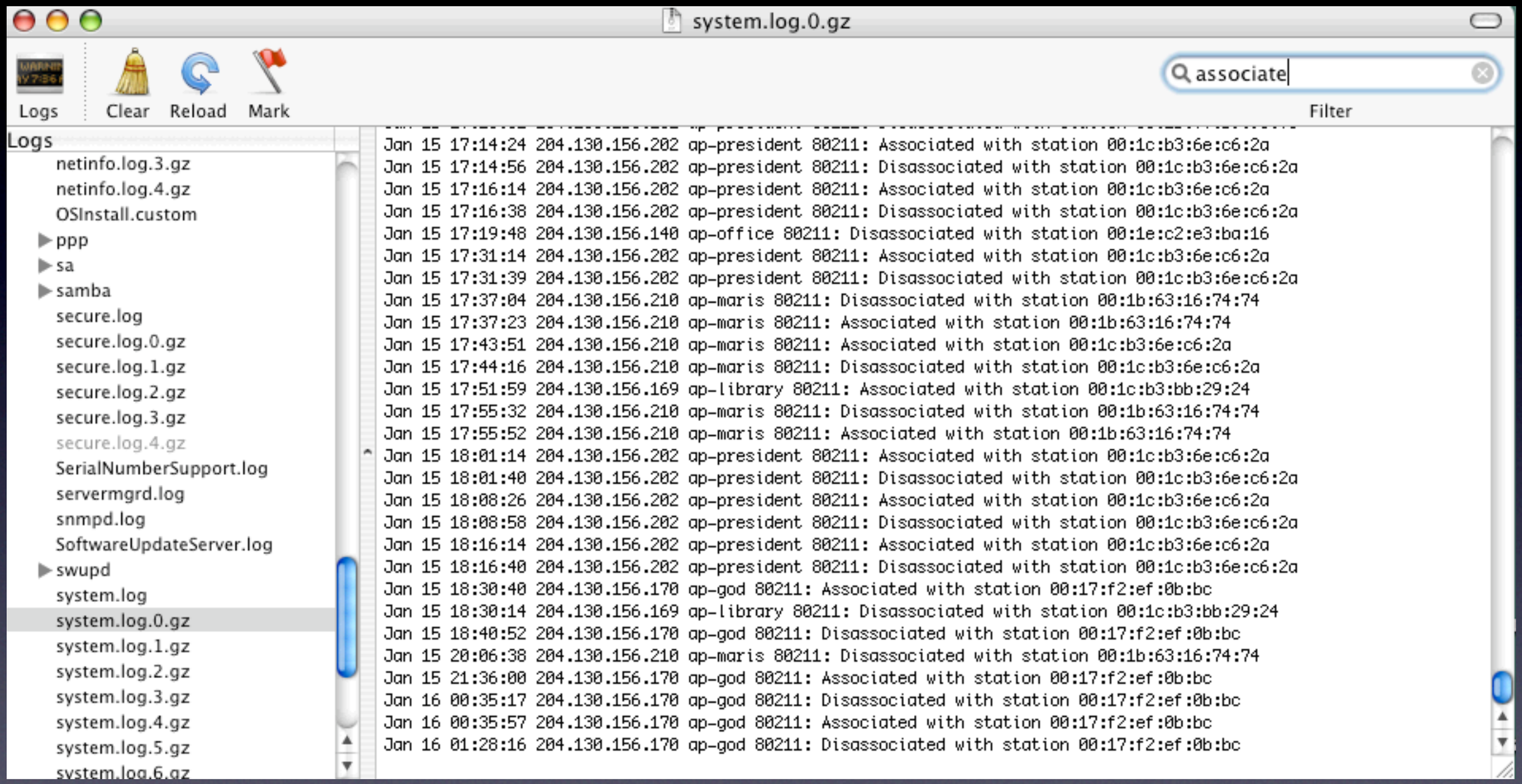
- Beginning with the AirPort Utility, note system logs
- syslogd can be setup on panther/tiger/leopard server to log access and refusals on all APs at once- great for intruder detection
- InterMapper can be used to monitor SNR dynamically over your network for AP placement and location of local noise sources
- Also helpful for mapping out traffic patterns, failover plans
- Use CyberGauge to monitor traffic in off-times, spot hackers
- Regular passive scans and/or Eakiu can be used to monitor and locate rogue APs, or serve as tripwires/honeypots
- Consider using HWACL on wired managed switches, which is an easy way to block rogue APs

Tools

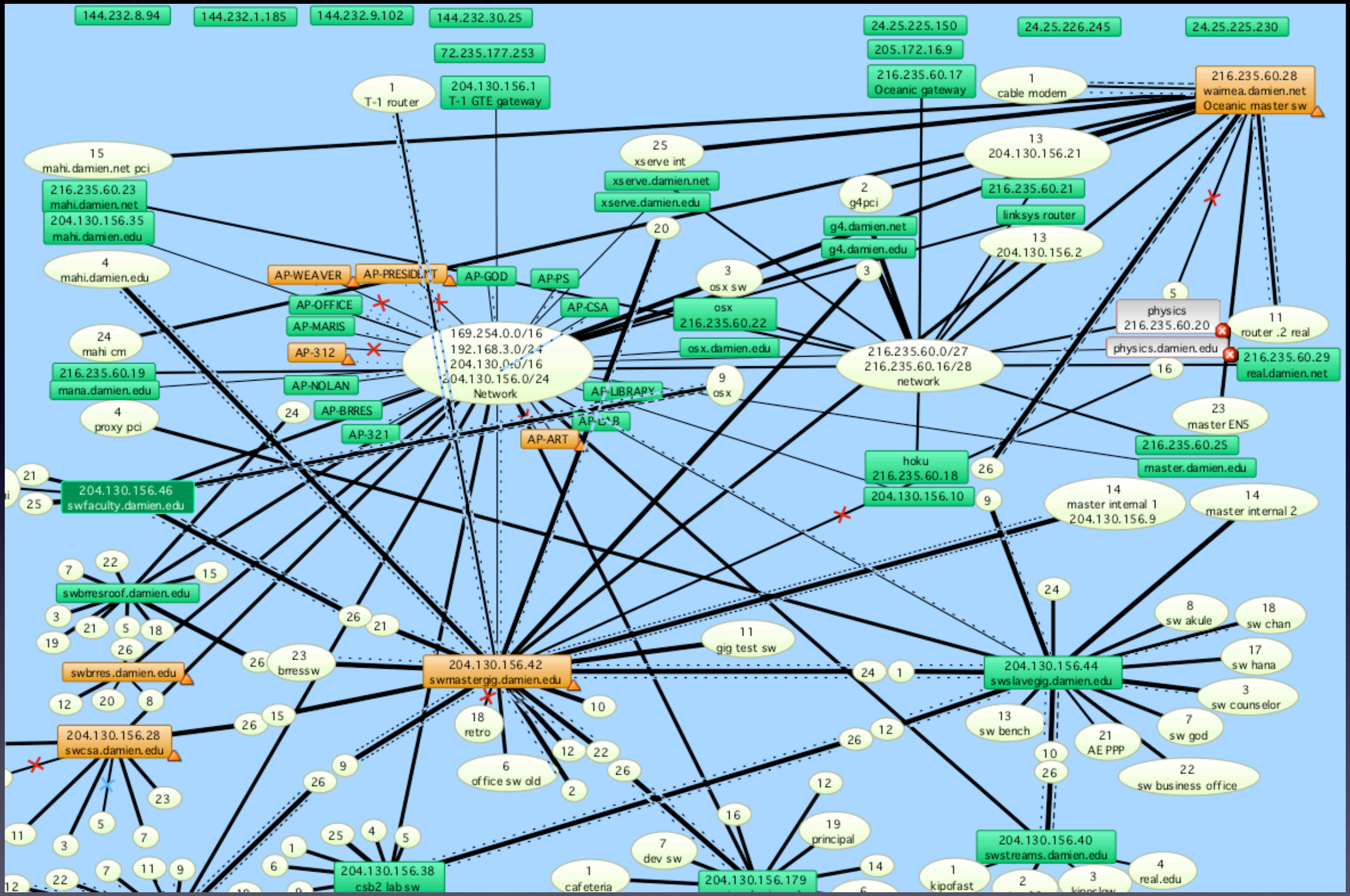
- Apple network preferences screen
- Apple AirPort Utility
- InterMapper 5

Try this:

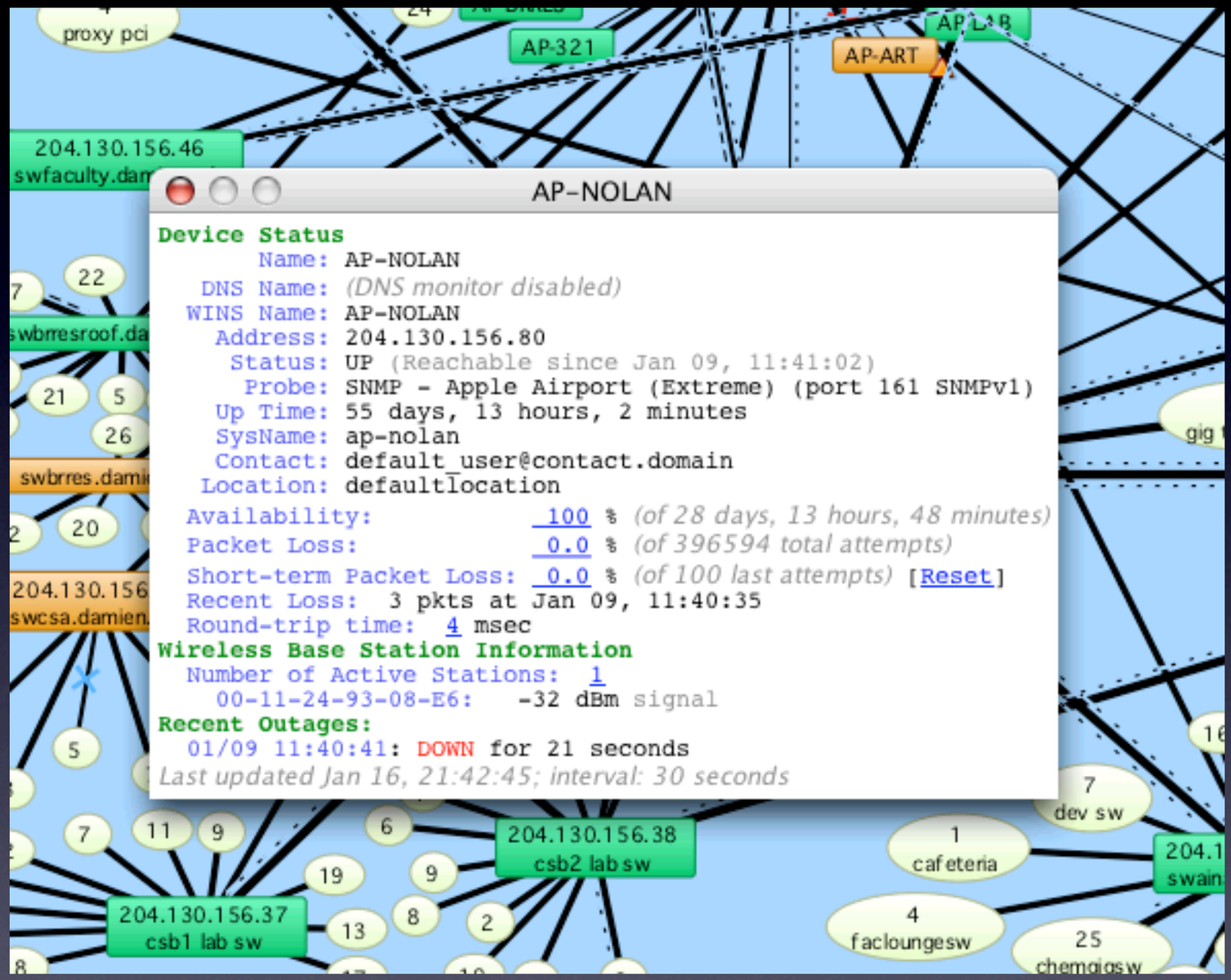
- Using AirPort utility, notice log activity as you login, logout, change security policies



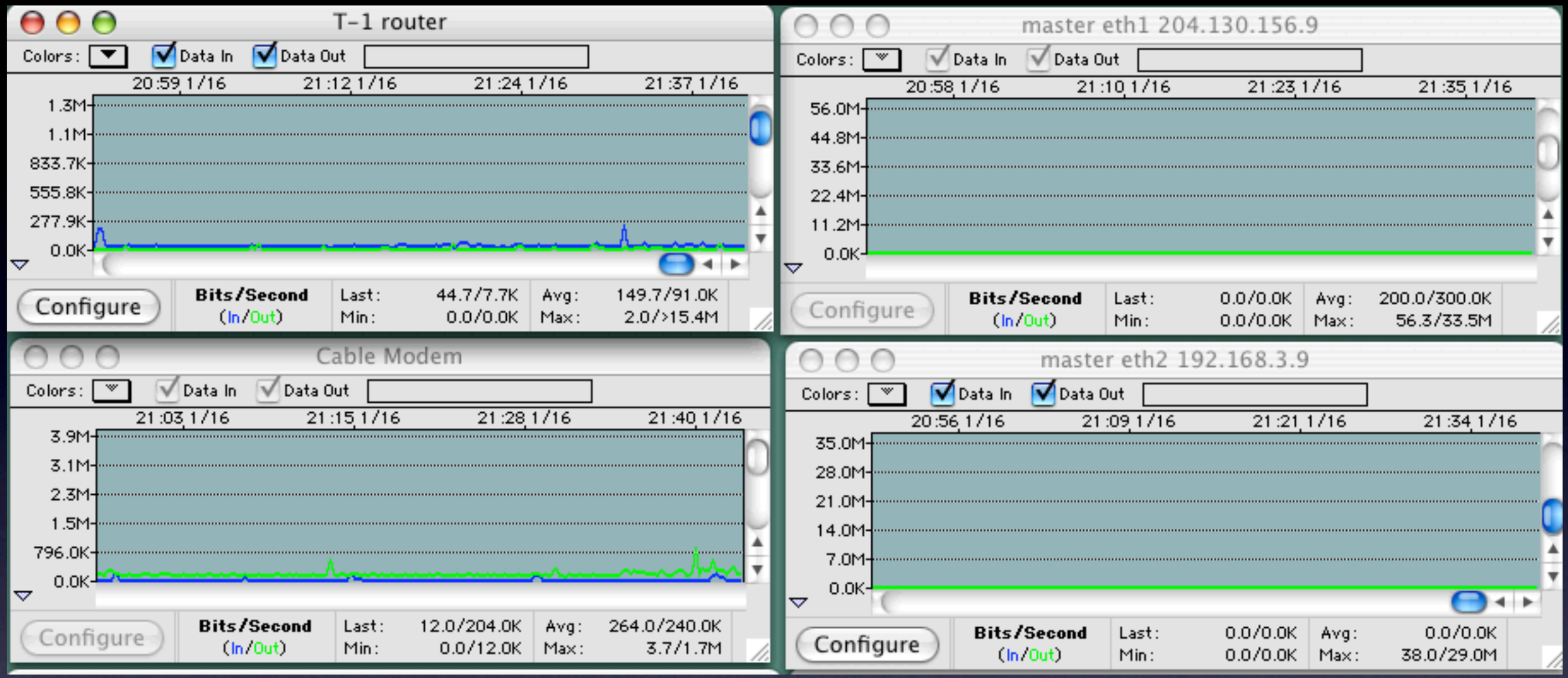
syslogd running on Mac OSX Tiger Server



InterMapper



InterMapper


T-1 router
Colors:
Data In
Data Out
20:59 1/16
21:12 1/16
21:24 1/16
21:37 1/16
1.3M
1.1M
833.7K
555.8K
277.9K
0.0K
Configure
Bits/Second
(In/Out)
Last: 44.7/7.7K
Min: 0.0/0.0K
Avg: 149.7/91.0K
Max: 2.0/>15.4M
master eth1 204.130.156.9
Colors:
Data In
Data Out
20:58 1/16
21:10 1/16
21:23 1/16
21:35 1/16
56.0M
44.8M
33.6M
22.4M
11.2M
0.0K
Configure
Bits/Second
(In/Out)
Last: 0.0/0.0K
Min: 0.0/0.0K
Avg: 200.0/300.0K
Max: 56.3/33.5M
Cable Modem
Colors:
Data In
Data Out
21:03 1/16
21:15 1/16
21:28 1/16
21:40 1/16
3.9M
3.1M
2.3M
1.5M
796.0K
0.0K
Configure
Bits/Second
(In/Out)
Last: 12.0/204.0K
Min: 0.0/12.0K
Avg: 264.0/240.0K
Max: 3.7/1.7M
master eth2 192.168.3.9
Colors:
Data In
Data Out
20:56 1/16
21:09 1/16
21:21 1/16
21:34 1/16
35.0M
28.0M
21.0M
14.0M
7.0M
0.0K
Configure
Bits/Second
(In/Out)
Last: 0.0/0.0K
Min: 0.0/0.0K
Avg: 0.0/0.0K
Max: 38.0/29.0M

CyberGauge

What we've learned

- Wireless networks are made up of channels 1-11, but there is considerable overlap
- Simple stumbler applications can locate active named networks, but not passive ones
- Packet sniffing can be done easily if access to the network is gained
- Even without access, Kismac can intercept traffic
- Solutions: VPN makes traffic encrypted, WPA2 keeps bad folks off your network
- RADIUS and WPA2 can be centrally administered using Leopard Server or Elektron on both the wireless network and the wired network for a comprehensive solution
- Syslog, intermapper and cybergauge can help monitor network health
- Antennas and amplifiers both increase range, antennas increase SNR, amplifiers boost both noise and signal, adding some noise of their own (raising the noise floor)

Questions

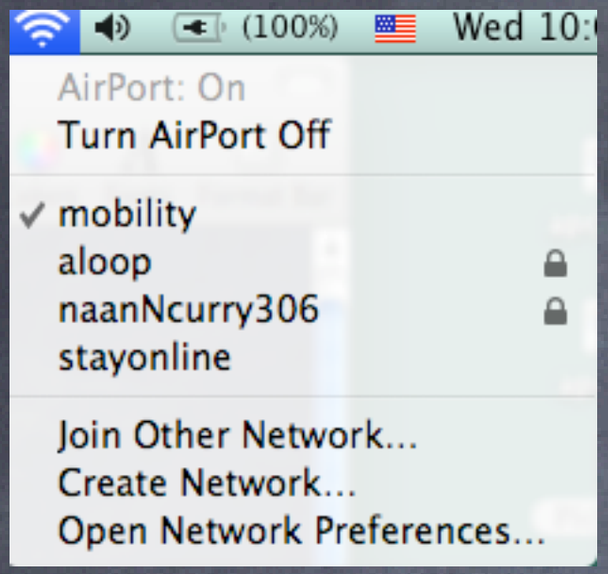
Download Session Presentations

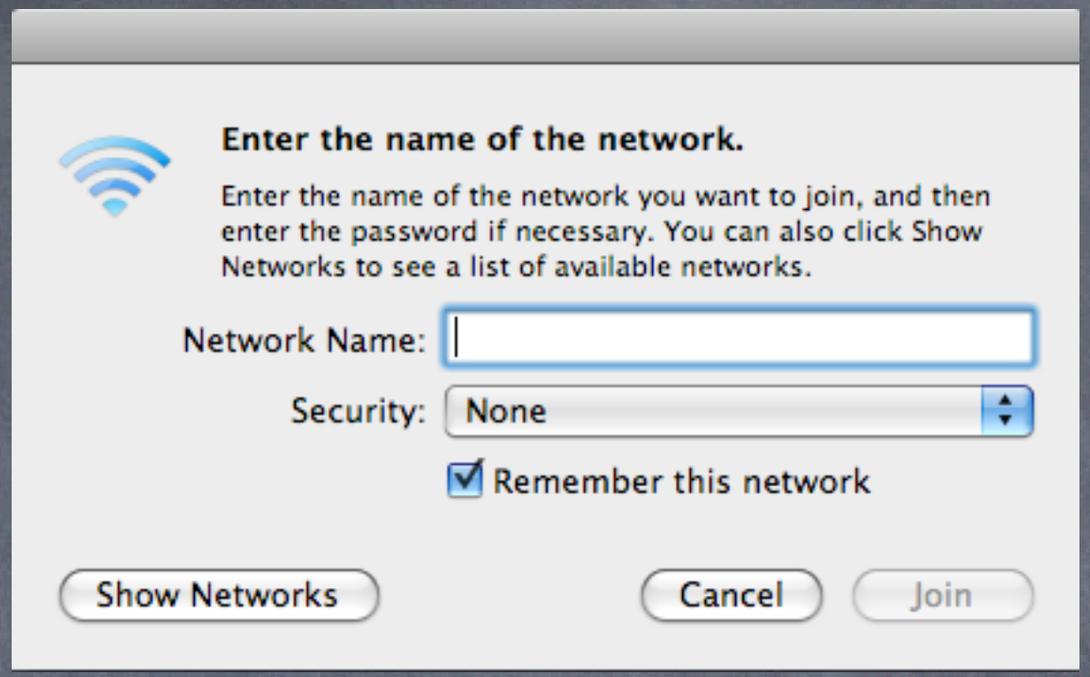
http://macpres09.shownets.net

All registered conference attendees can go to http://macpres09.shownets.net to access the presentations for sessions they want to download. Each conference program will have a folder, with the corresponding presentations included that speakers have posted. Please refer to the sign outside the conference room if you need information about the Conference Name & Session Number.

Fin

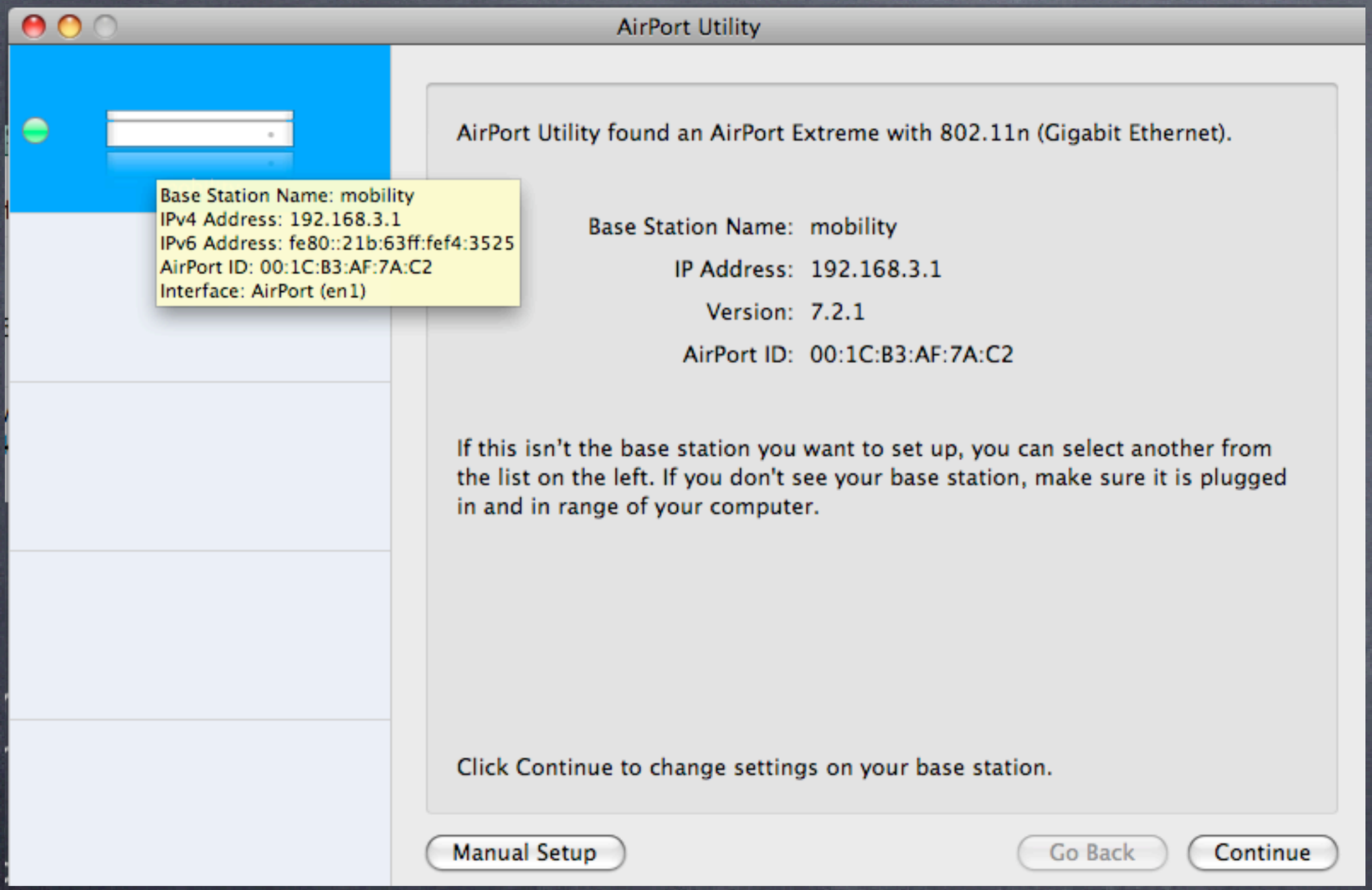
Reference: Leopard Wireless client setup





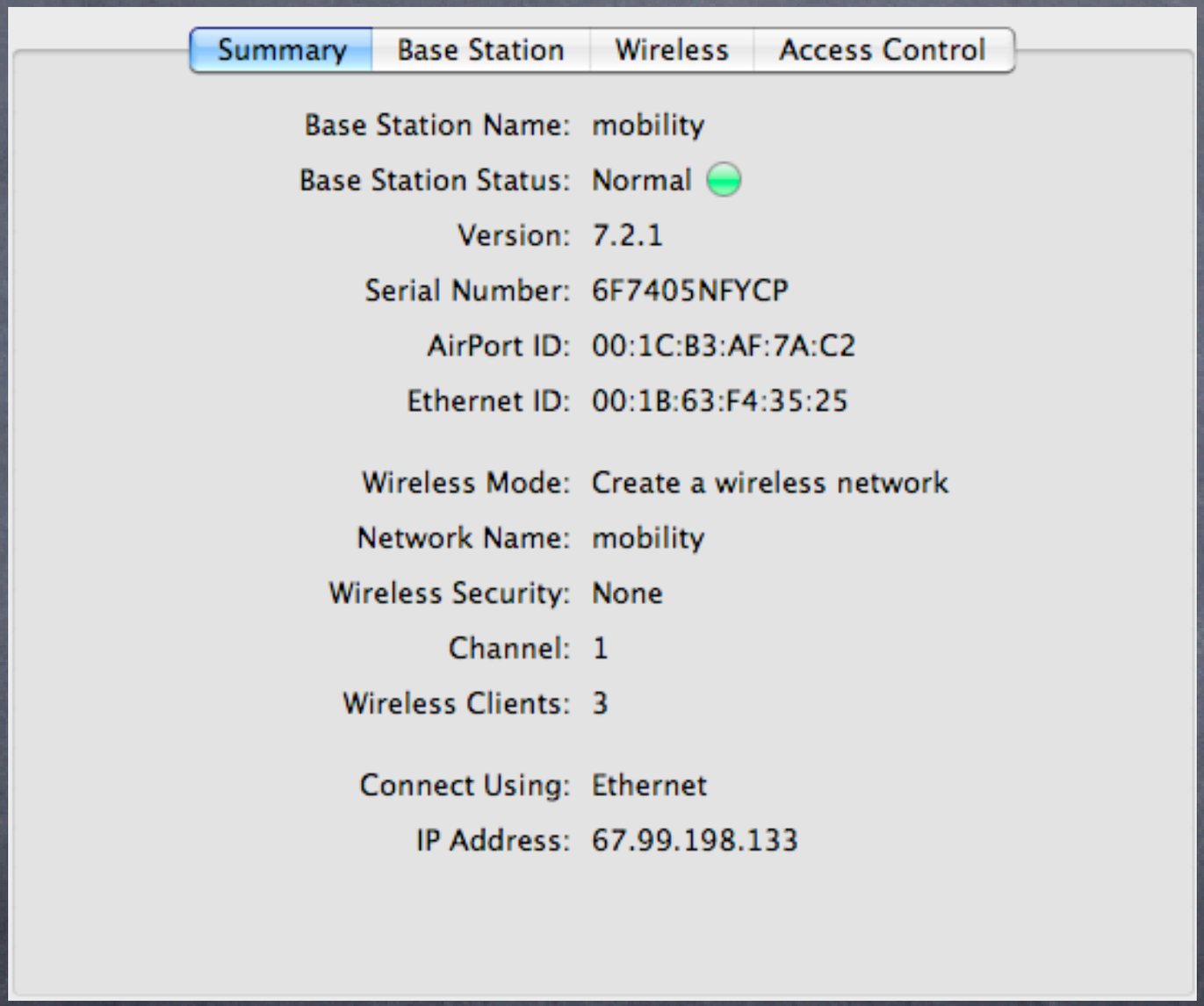
- Notice:
  - Open networks show as names
  - Closed networks must be added
  - If secure, this is where you add the options
  - More on security in a bit

Reference: Wireless Access point setup



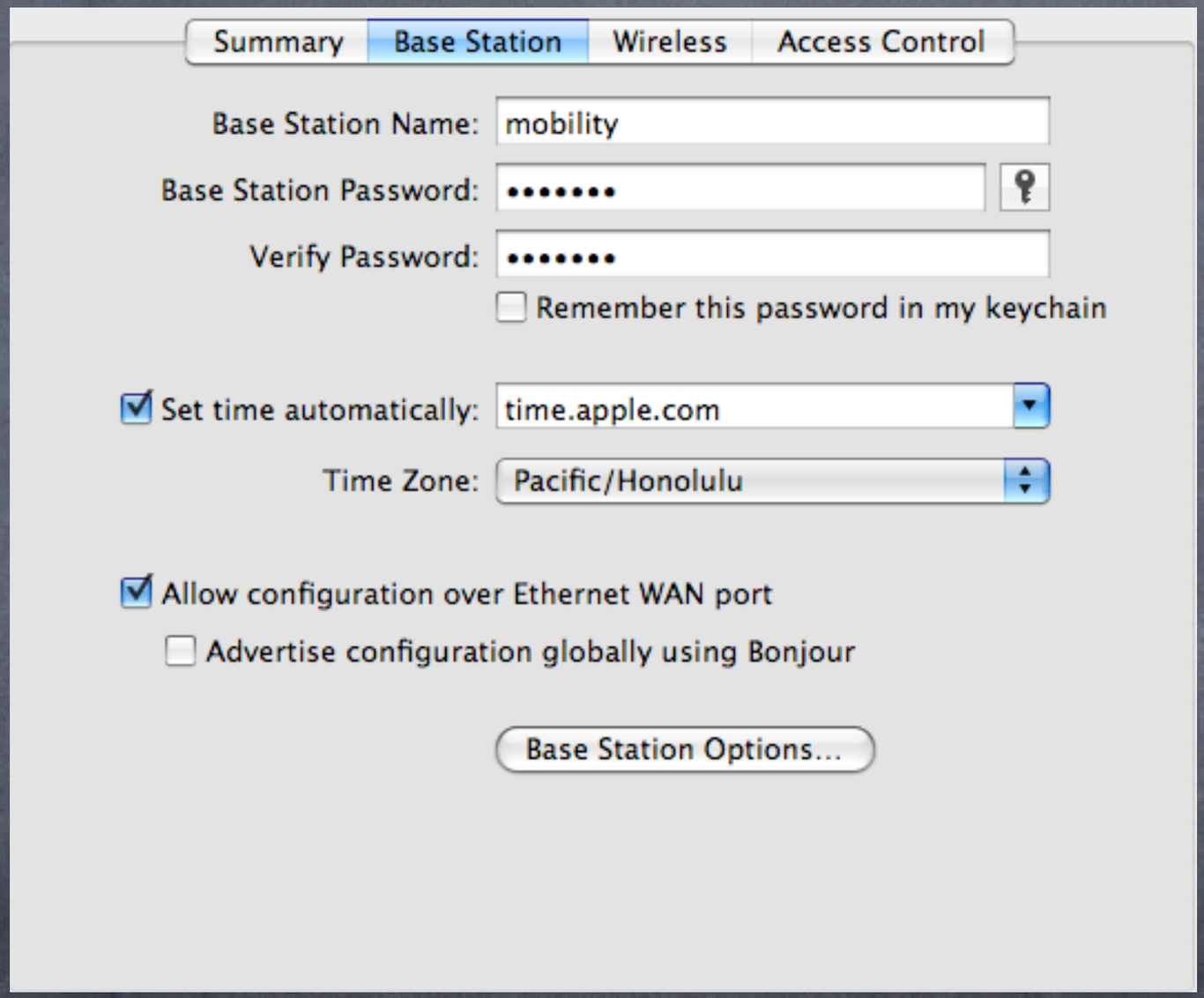
- Basic access screen, let's start here
- Go to manual setup

Basic Wireless Access point setup



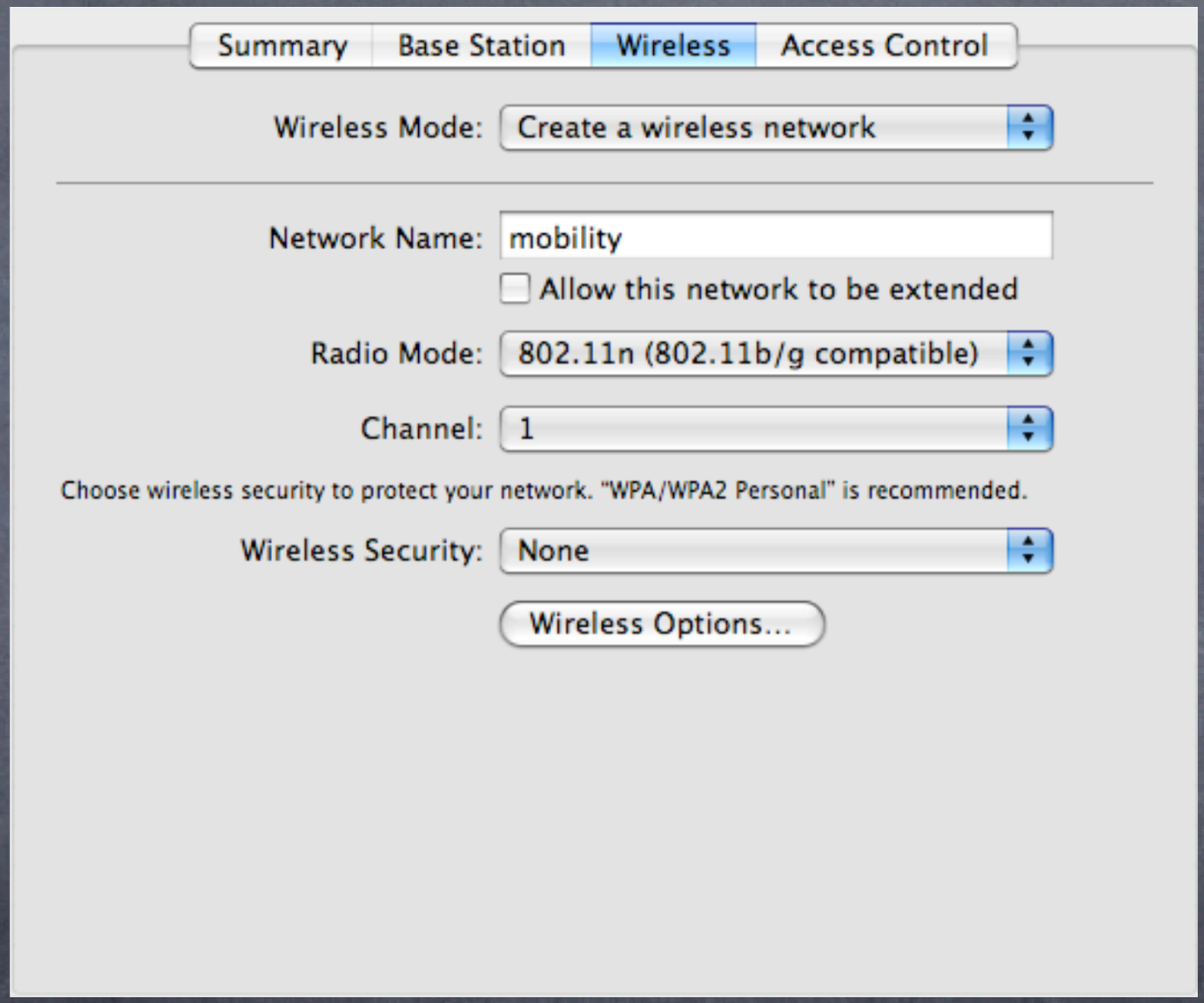
- Access Point identification information
- A good idea is to take a screen shot (apple-shift-4) for later reference

Basic Wireless Access point setup



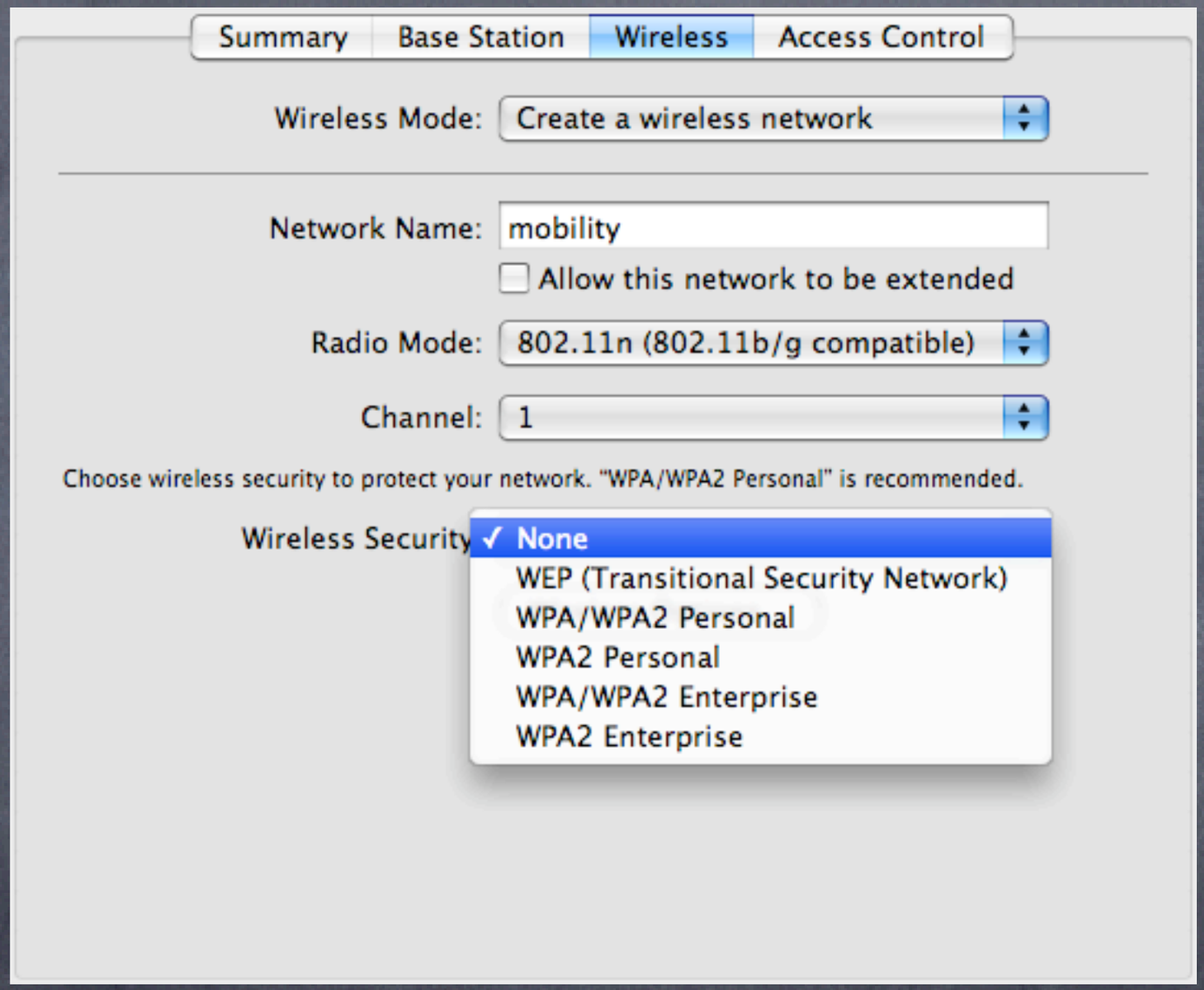
- Change the name and always change the password
- If you forget it, you can always reset it with a pencil in the back

Basic Wireless Access point setup



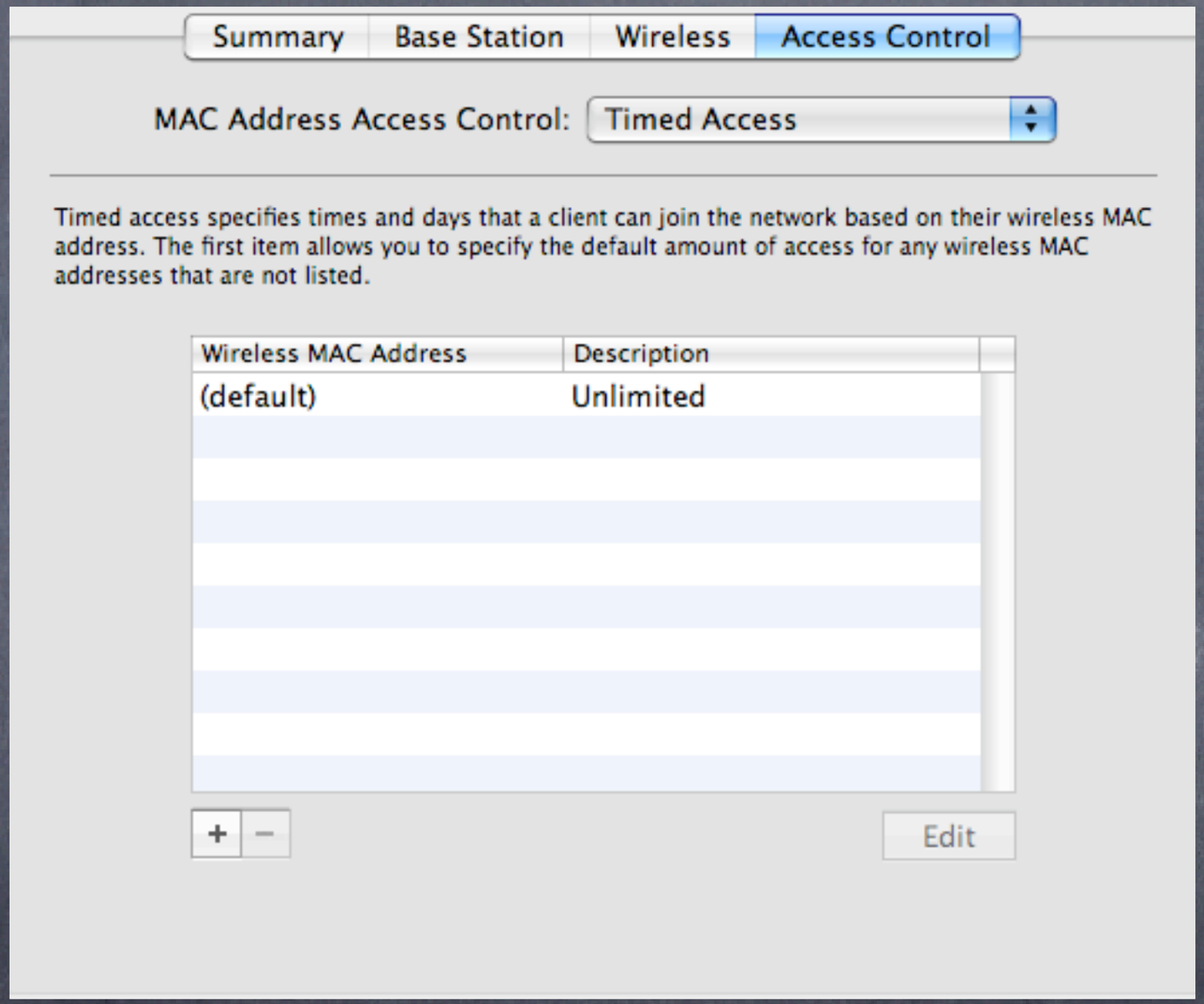
- Network name may be unique, or for roaming, make it the same as the others
- Note no security here

Basic Wireless Access point setup



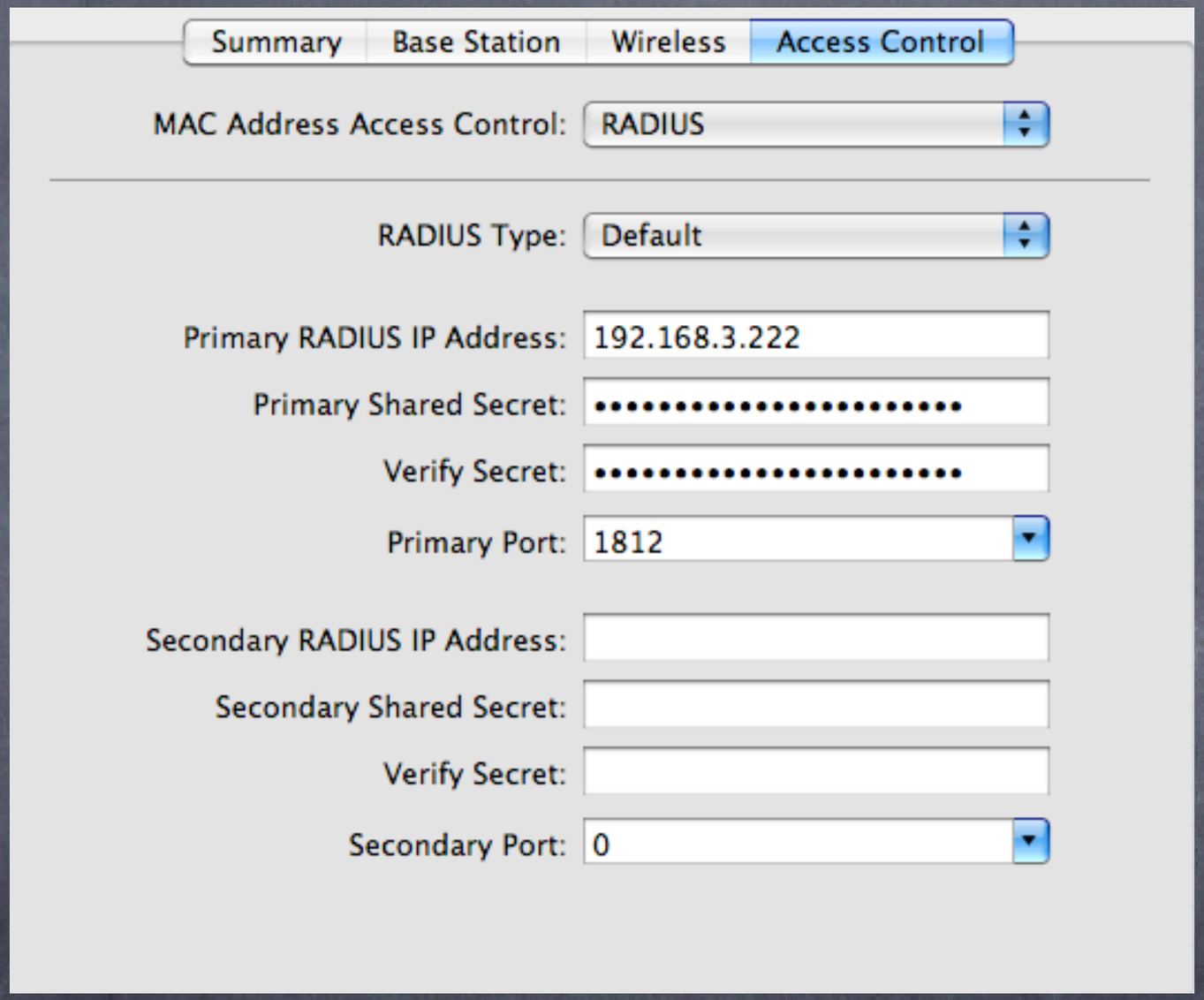
- Security options
- WEP is old school, not secure
- WPA2 is best
- Personal is between the client and the AP
- Enterprise uses a separate RADIUS server

Basic Wireless Access point setup



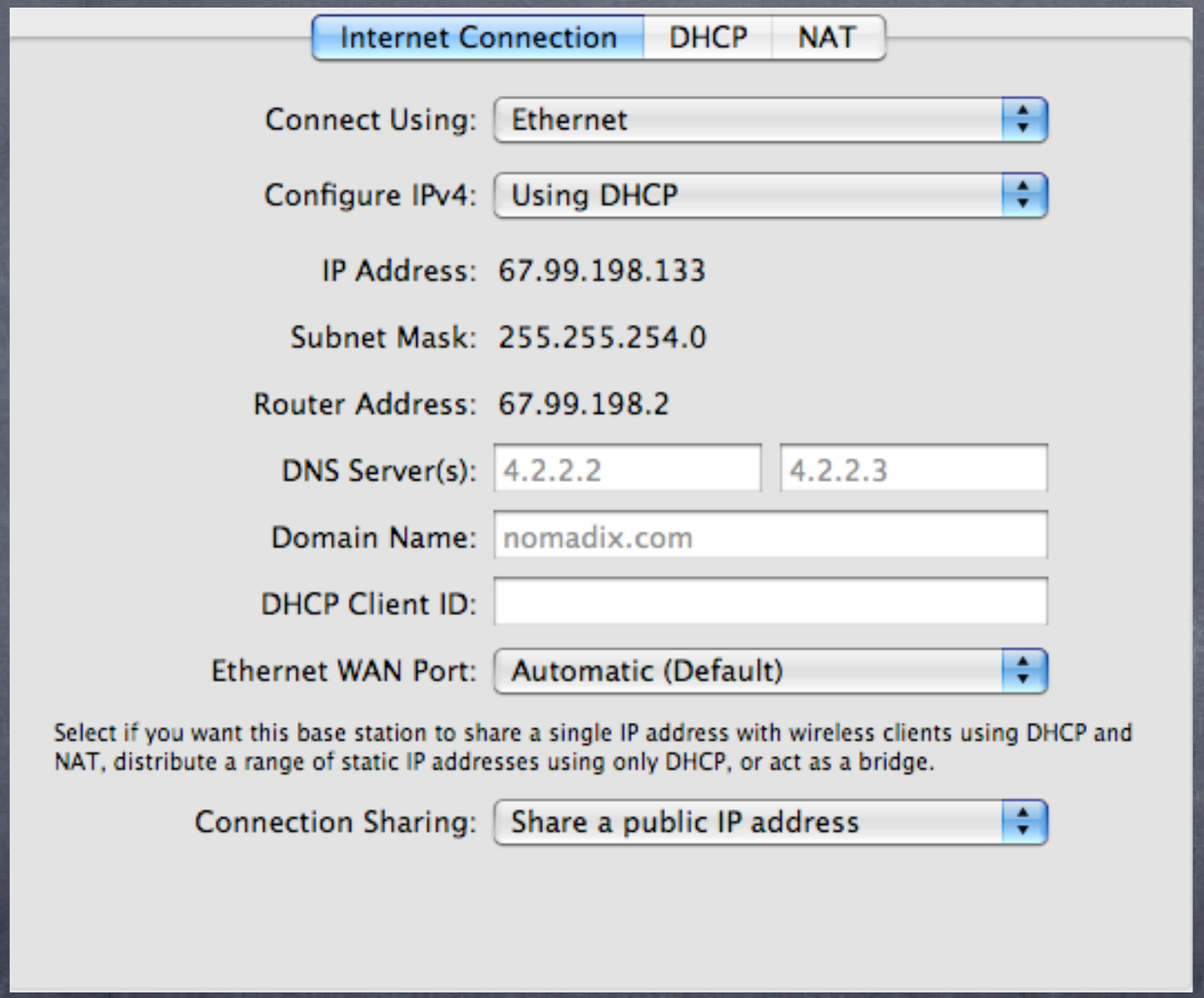
- Alternate security screen, based on MAC address of client radio
- Note default is all clients, all on

Basic Wireless Access point setup



- Central admin through a RADIUS server
- Much more elegant, and easier to manage multiple APs

Basic Wireless Access point setup

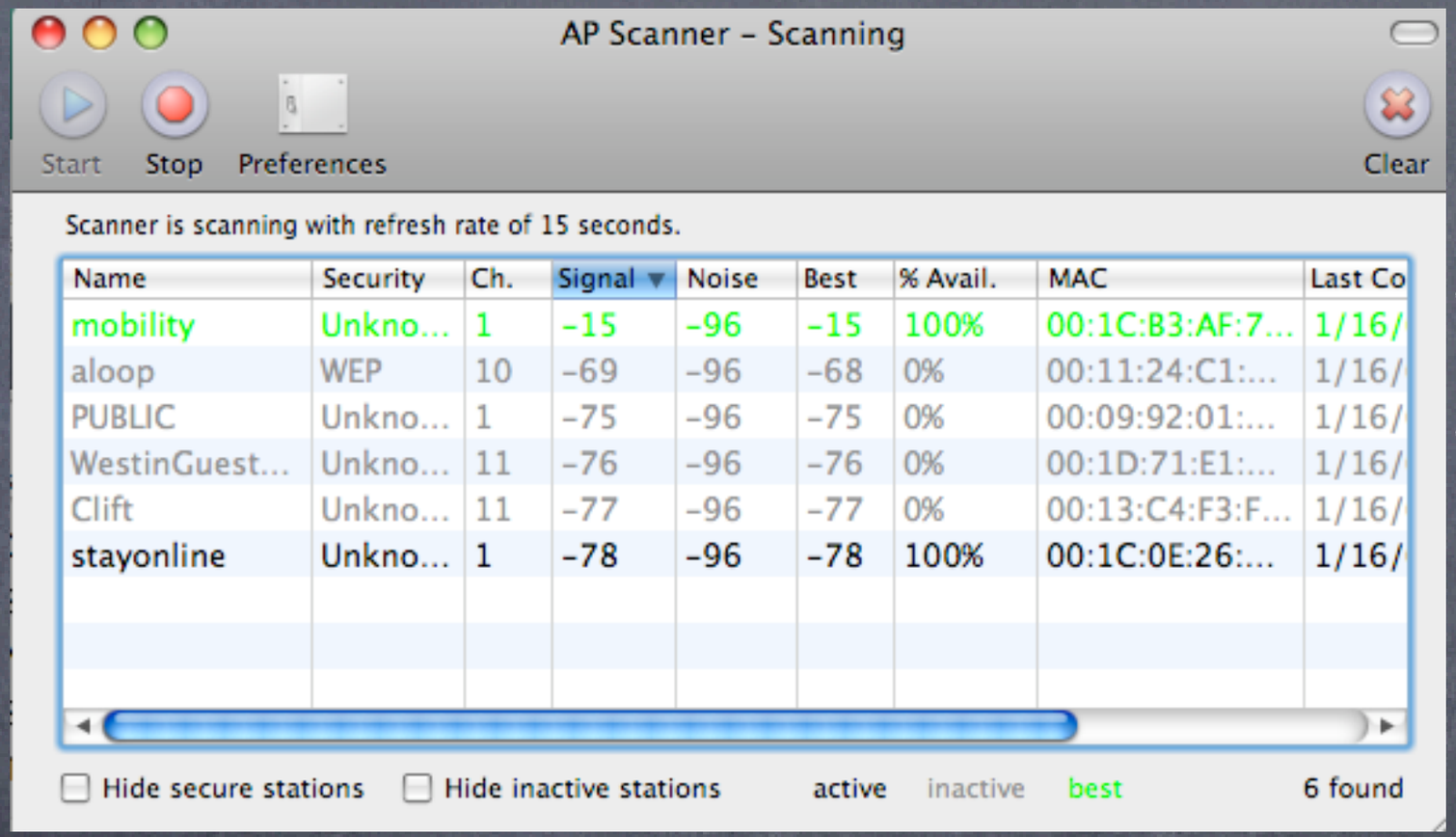


- Internet Connection info
- Most common is share
- Bridge is fine, always connect the outside to the circular icon, even if you plan on bridging local devices (e.g. printers)

Access Point testing: how good is my connection?

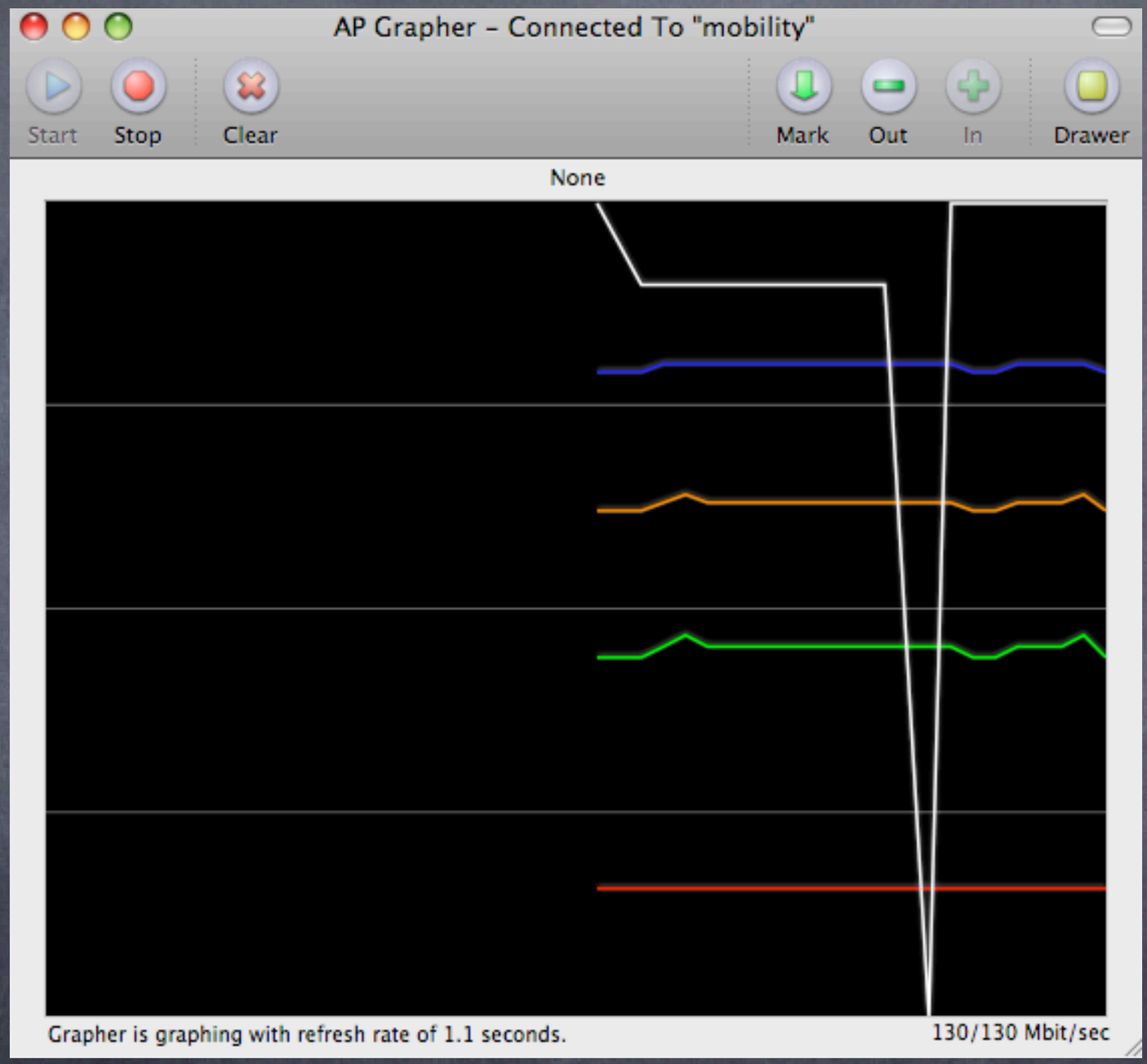
- Goal: Learn how to evaluate the signal and noise from an Access point using a client based application
- Tools: AP Grapher

Basic Wireless Access point setup



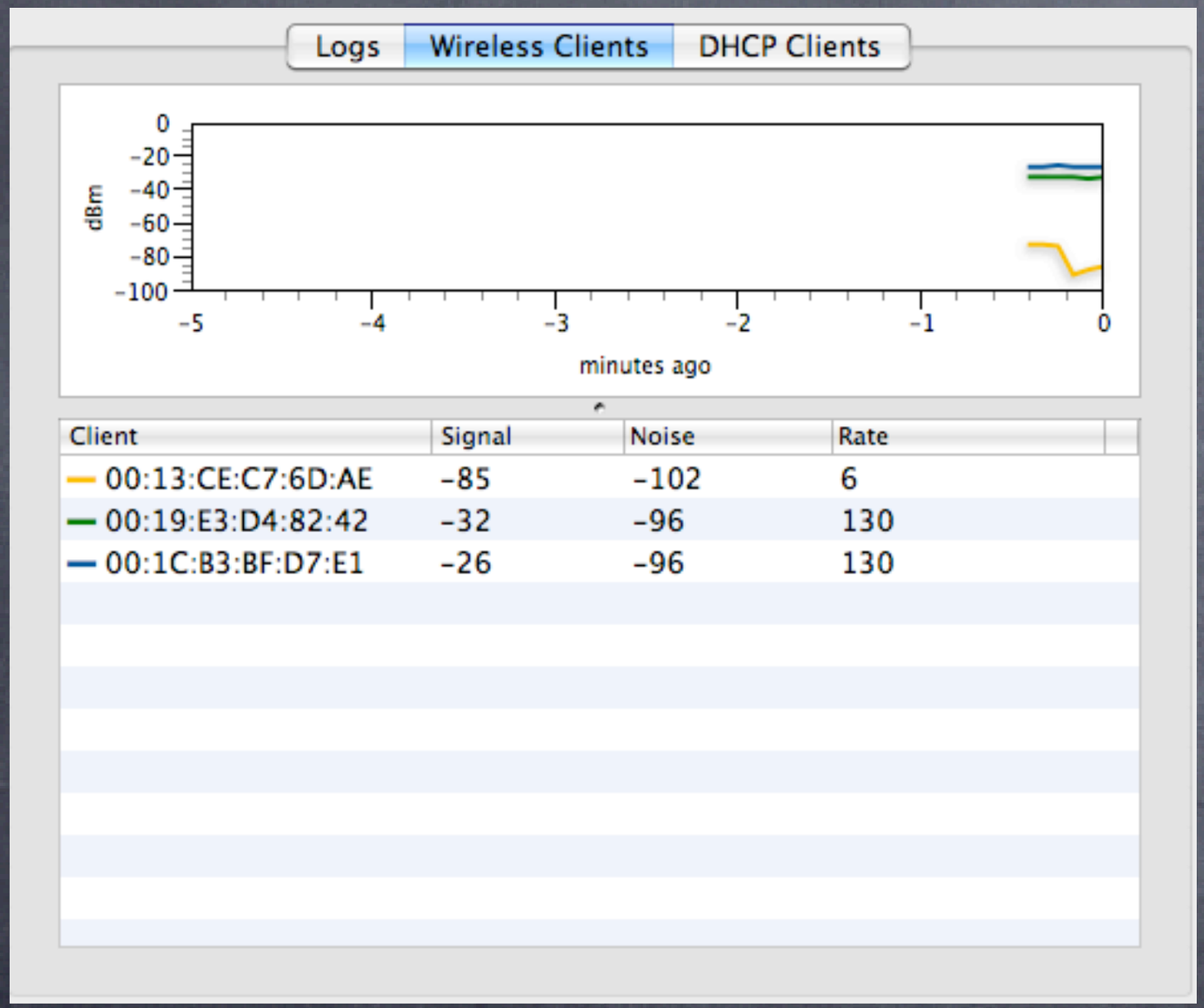
- Access point list
- Note all stats at once for comparison

Basic Wireless Access point setup



- Access point graph
- note speed and other stats

Basic Wireless Access point monitoring: take two



- Pretty graphs show client signals from the Access point perspective
- Very useful for AP placement