Hands-on Mac lab
Advanced Wireless

Diving into the black art of wireless and making it work for you and your organization

Dr. Bill Wiecking
Hawai'i Preparatory Academy
Apple Distinguished Educator
wiecking@mac.com

Assumptions:

- A basic understanding of wireless and wired networks
- Familiarity with basic setup on most Tiger and Leopard clients
- General knowledge of basic access point configuration

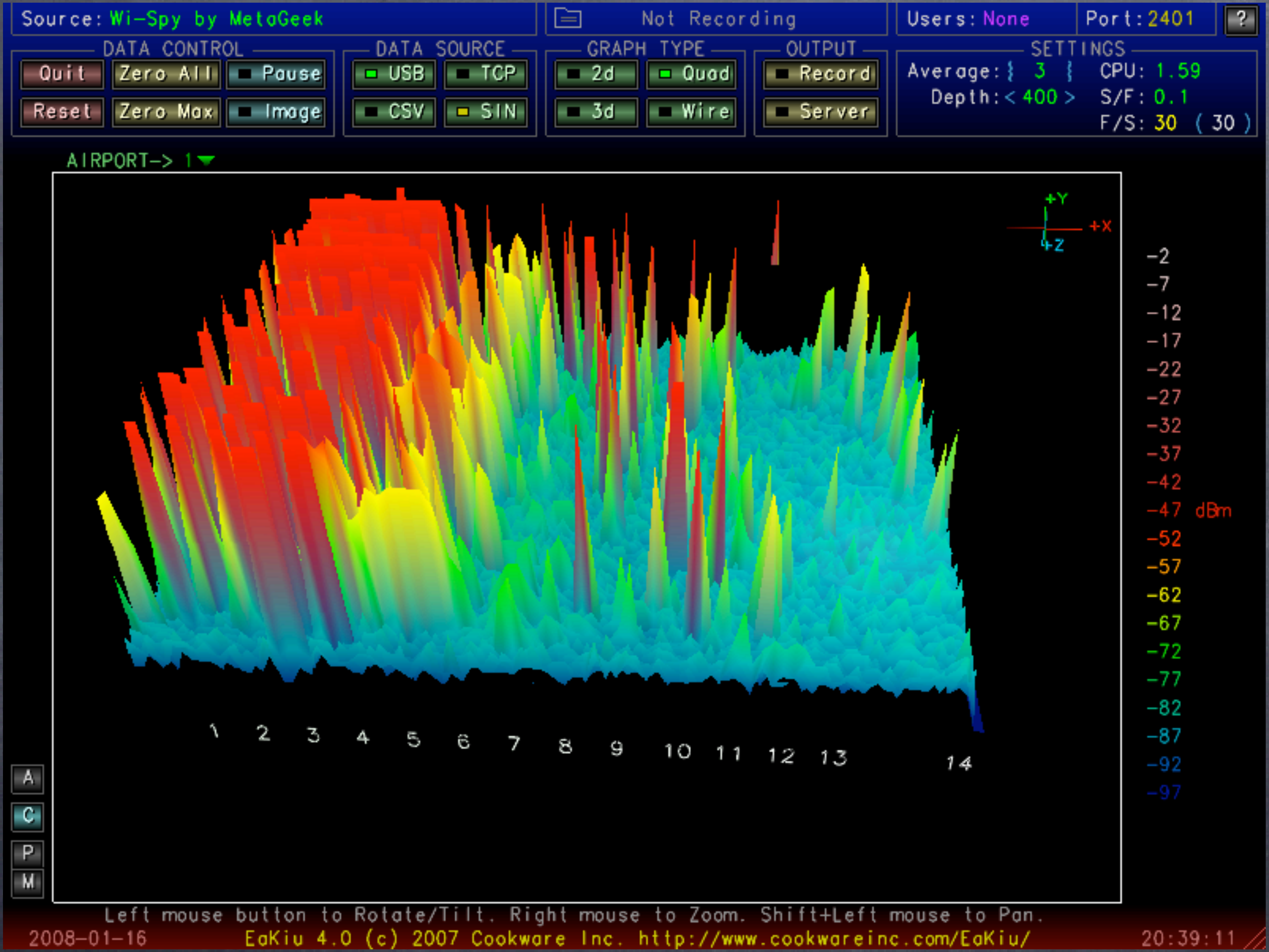
Goals:

- Broaden your knowledge of wireless networks, obvious and hidden
- Enable you to understand advanced security skills using software and hardware tools
- Learn how to manage complex wireless networks
- Learn how to extend wireless beyond the bounds of mere mortals

Wireless-what does it look like?

- Goal: to understand what wireless channels look like
- Tools: Eakiu and wi-spy

Wireless-what does it look like?



Source: Wi-Spy by MetaGeek

Not Recording

Users: None

Port: 2401

Average: { 3 }

Depth: < 400 >

CPU: 1.59

S/F: 0.1

F/S: 30 (30)

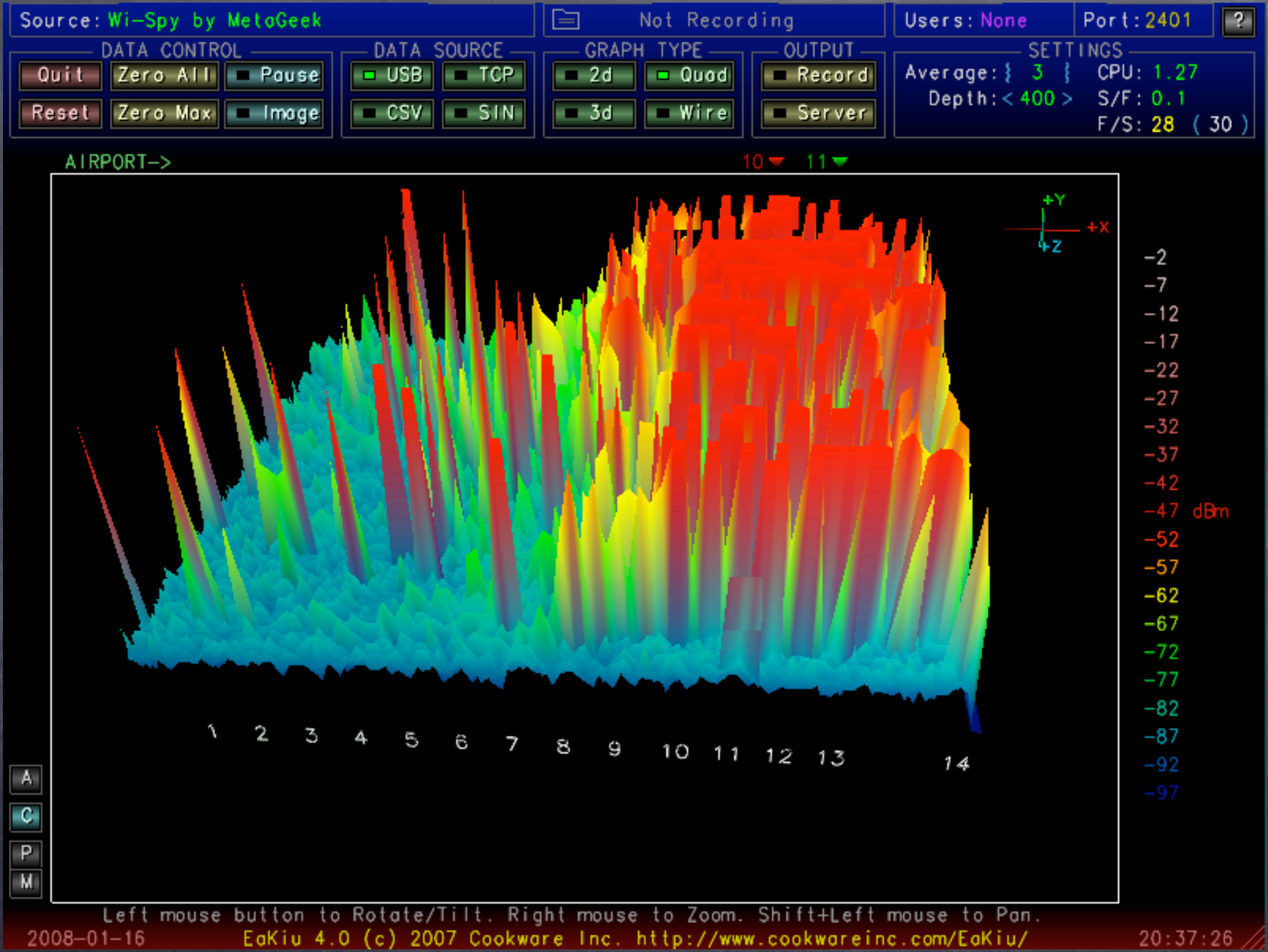
AIRPORT-> 1

Left mouse button to Rotate/Tilt. Right mouse to Zoom. Shift+Left mouse to Pan.

2008-01-16 EaKiu 4.0 (c) 2007 Cookware Inc. http://www.cookwareinc.com/EaKiu/ 20:39:11

On which channel is this access point broadcasting?

Wireless-what does it look like?



Source: Wi-Spy by MetaGeek

Not Recording

Users: None

Port: 2401

Average: { 3 }

Depth: < 400 >

CPU: 1.27

S/F: 0.1

F/S: 28 (30)

Left mouse button to Rotate/Tilt. Right mouse to Zoom. Shift+Left mouse to Pan.

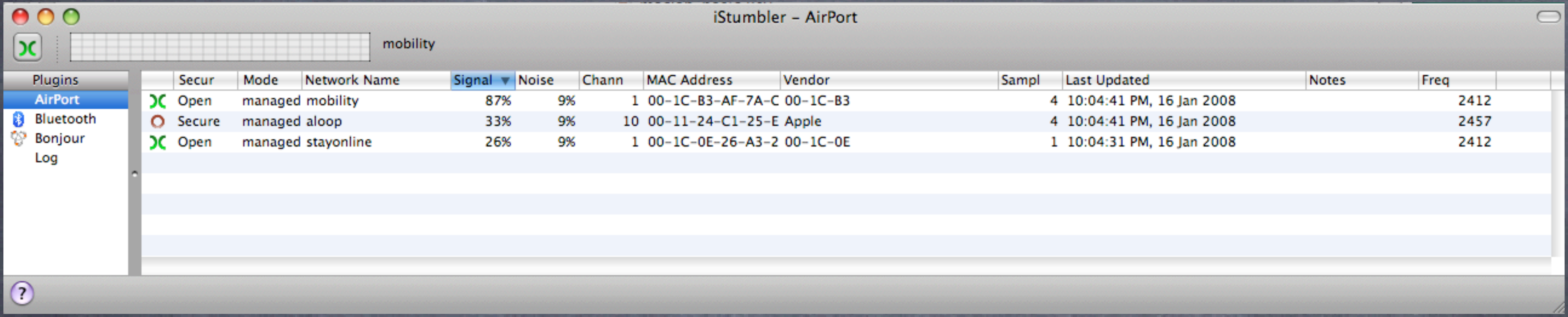
2008-01-16 EaKiu 4.0 (c) 2007 Cookware Inc. http://www.cookwareinc.com/EaKiu/ 20:37:26

On which channel is this access point broadcasting?

iStumbler: now you try

- Goal: Using a software stumbler, have a look at the local active wireless neighborhood
- Tools: iStumbler v.98
- Note: only active network show up

iStumbler: now you try



	Secur	Mode	Network Name	Signal ▼	Noise	Chann	MAC Address	Vendor	Sampl	Last Updated	Notes	Freq
)(	Open	managed	mobility	87%	9%	1	00-1C-B3-AF-7A-C	00-1C-B3	4	10:04:41 PM, 16 Jan 2008		2412
○	Secure	managed	aloop	33%	9%	10	00-11-24-C1-25-E	Apple	4	10:04:41 PM, 16 Jan 2008		2457
)(	Open	managed	stayonline	26%	9%	1	00-1C-0E-26-A3-2	00-1C-0E	1	10:04:31 PM, 16 Jan 2008		2412

- Notice:
  - security
  - modes
  - signal/noise
  - MAC address
  - signal graph
  - war chalking signs

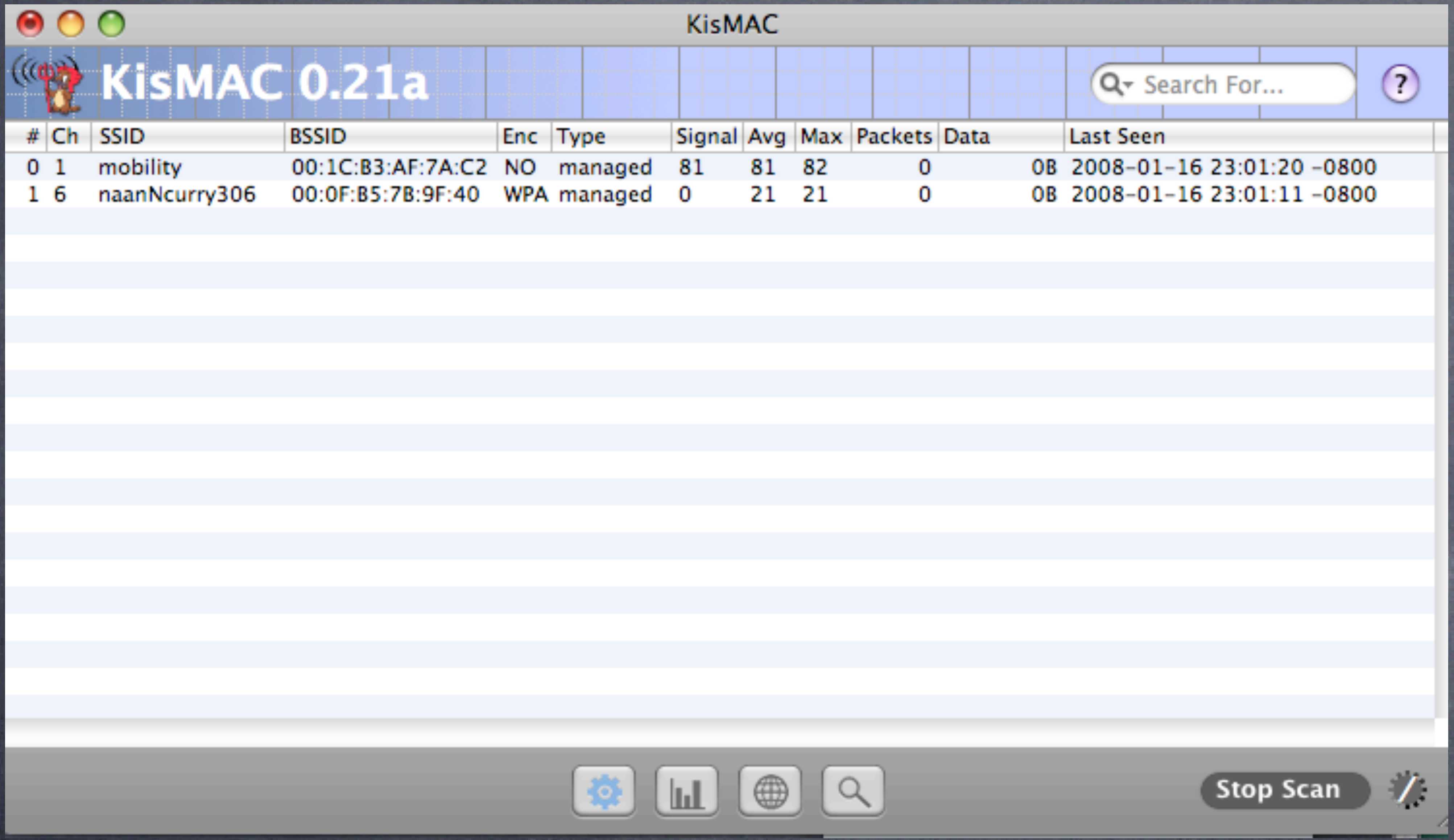
Security 101: Kismac

- Goal: Learn how to monitor even secured and closed networks using Kismac
- Tools: Kismac, USB wireless adapters (Prism2 chipset, passive mode)
- What to do:
  - Start Kismac on your computer
  - Under preferences (apple-,) select airport extreme, active mode
  - Start, notice active networks
  - Now go back to prefs, and unload the active mode, and repeat with a USB adapter in passive mode (see above)
  - Note data gathered (dumped) and even closed networks show up
  - Data can be collected for later analysis

Basic Wireless client setup

- Goal: Learn how to configure Leopard or Tiger to join open and closed networks
- Tools: Tiger or Leopard client

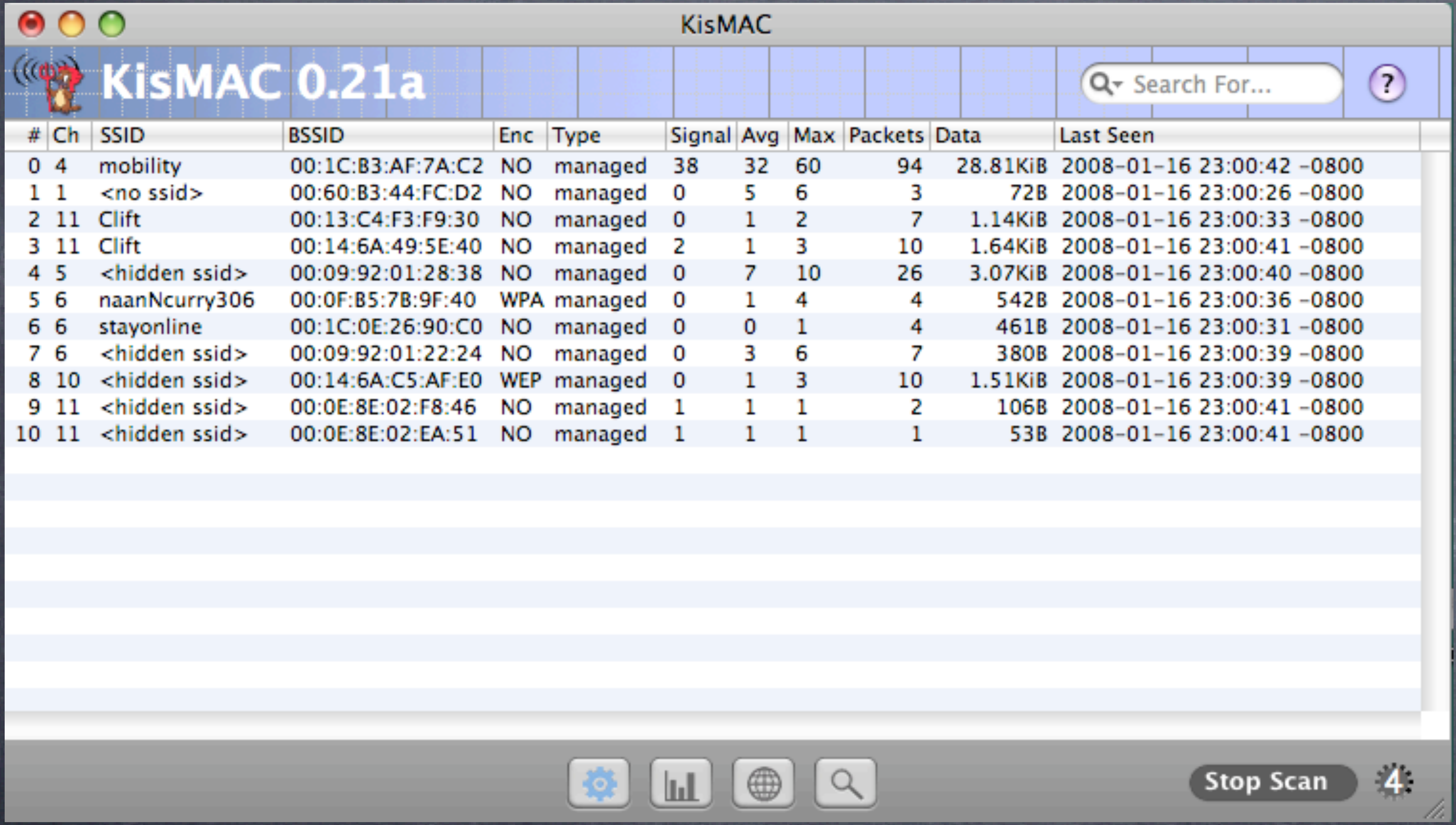
Kismac: active mode



#	Ch	SSID	BSSID	Enc	Type	Signal	Avg	Max	Packets	Data	Last Seen
0	1	mobility	00:1C:B3:AF:7A:C2	NO	managed	81	81	82	0	0B	2008-01-16 23:01:20 -0800
1	6	naanNcurry306	00:0F:B5:7B:9F:40	WPA	managed	0	21	21	0	0B	2008-01-16 23:01:11 -0800

- Notice number of networks
- no packets listed or data collected
- client can still use the airport interface

Kismac: passive mode



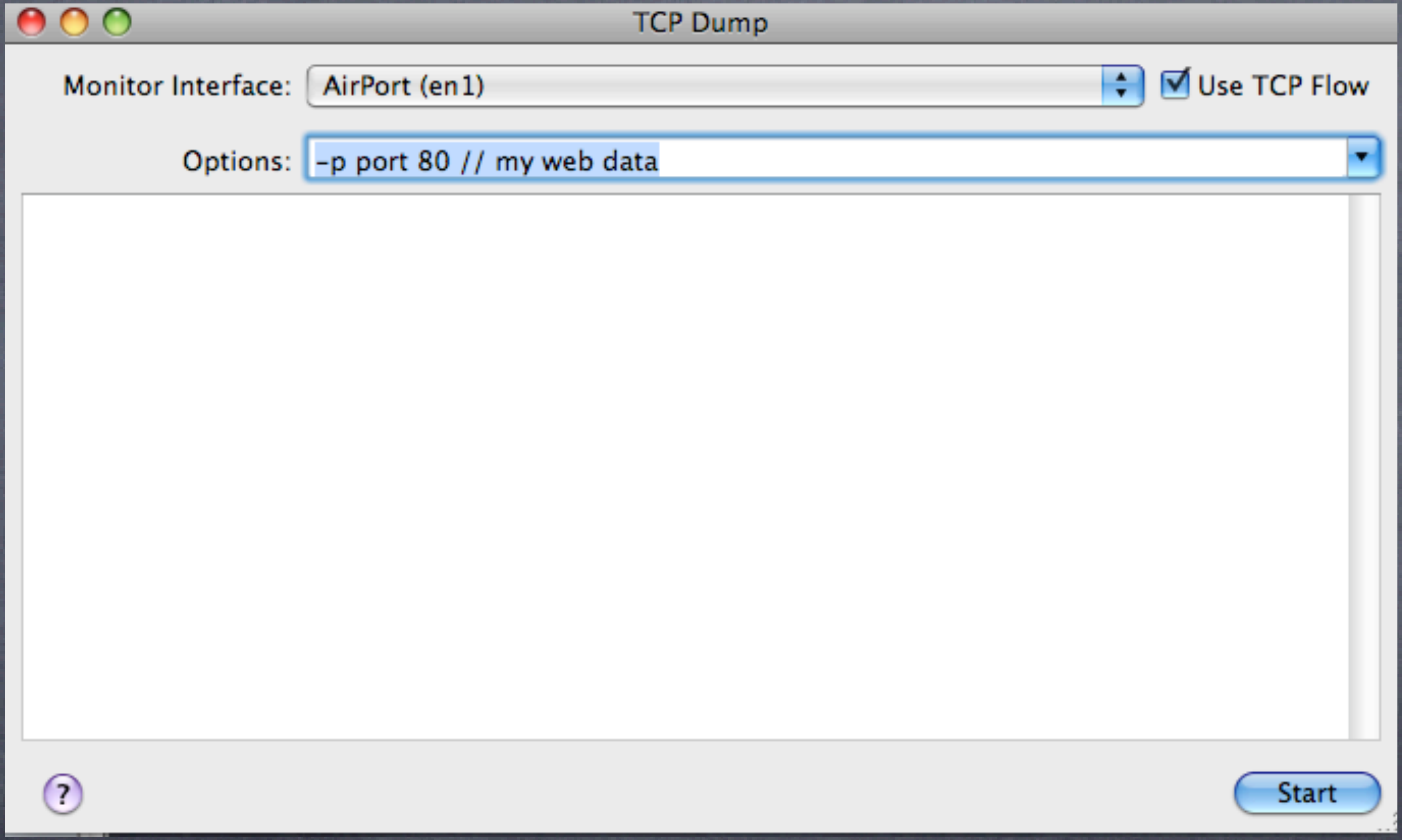
#	Ch	SSID	BSSID	Enc	Type	Signal	Avg	Max	Packets	Data	Last Seen
0	4	mobility	00:1C:B3:AF:7A:C2	NO	managed	38	32	60	94	28.81KiB	2008-01-16 23:00:42 -0800
1	1	<no ssid>	00:60:B3:44:FC:D2	NO	managed	0	5	6	3	72B	2008-01-16 23:00:26 -0800
2	11	Clift	00:13:C4:F3:F9:30	NO	managed	0	1	2	7	1.14KiB	2008-01-16 23:00:33 -0800
3	11	Clift	00:14:6A:49:5E:40	NO	managed	2	1	3	10	1.64KiB	2008-01-16 23:00:41 -0800
4	5	<hidden ssid>	00:09:92:01:28:38	NO	managed	0	7	10	26	3.07KiB	2008-01-16 23:00:40 -0800
5	6	naanNcurry306	00:0F:B5:7B:9F:40	WPA	managed	0	1	4	4	542B	2008-01-16 23:00:36 -0800
6	6	stayonline	00:1C:0E:26:90:C0	NO	managed	0	0	1	4	461B	2008-01-16 23:00:31 -0800
7	6	<hidden ssid>	00:09:92:01:22:24	NO	managed	0	3	6	7	380B	2008-01-16 23:00:39 -0800
8	10	<hidden ssid>	00:14:6A:C5:AF:E0	WEP	managed	0	1	3	10	1.51KiB	2008-01-16 23:00:39 -0800
9	11	<hidden ssid>	00:0E:8E:02:F8:46	NO	managed	1	1	1	2	106B	2008-01-16 23:00:41 -0800
10	11	<hidden ssid>	00:0E:8E:02:EA:51	NO	managed	1	1	1	1	53B	2008-01-16 23:00:41 -0800

- Notice number of networks
- note packets listed and data collected
- client can no longer use the airport interface, unless passive device is USB (as in this case)

Security 101: packet sniffing

- Goal: Learn how insecure network are once joined
- Tools: IP Net Monitor (sustworks.com)

Security 101: packet sniffing



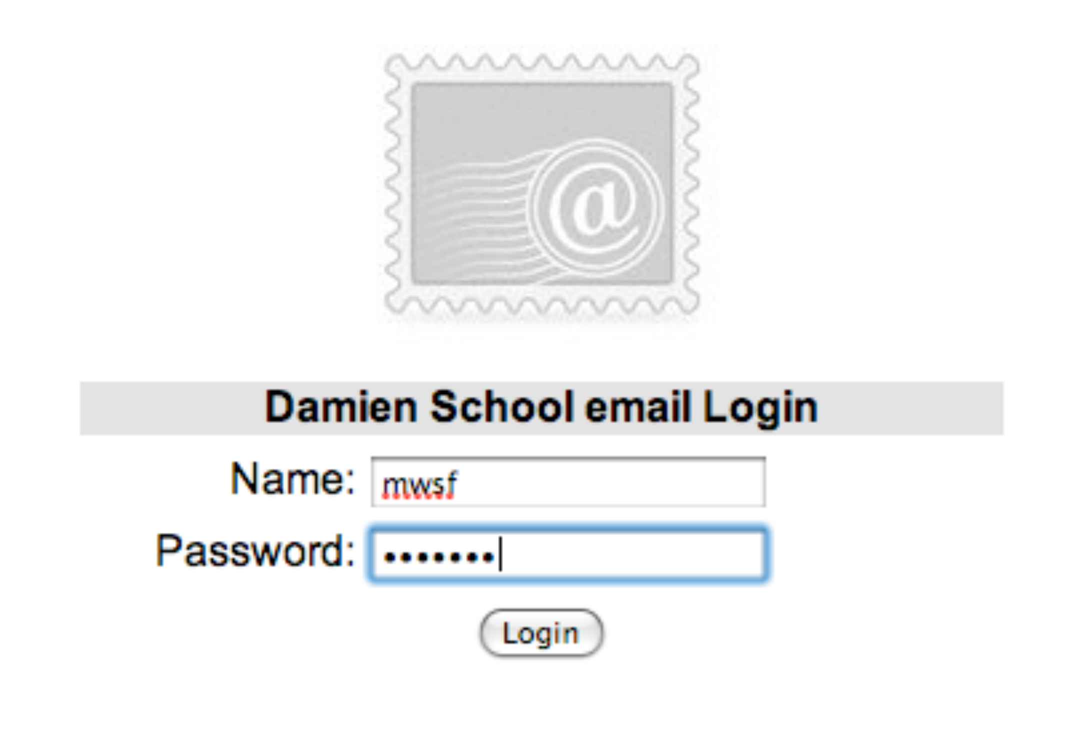
Monitor Interface: AirPort (en1)

☑ Use TCP Flow

Options: -p port 80 // my web data

IP Net Monitor TCPdump console

Security 101: packet sniffing



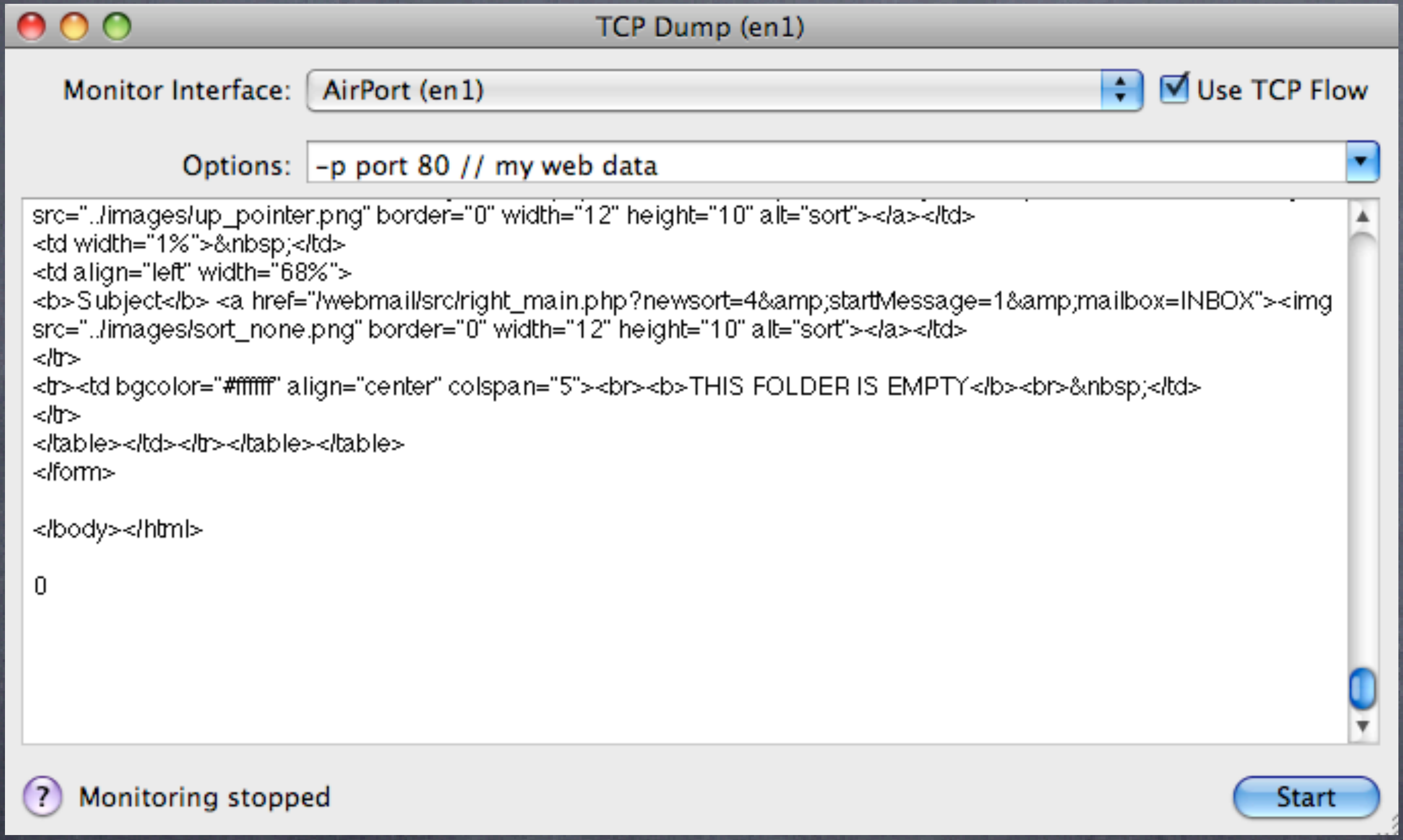
Damien School email Login

Name: mwsf

Password: ••••••••

Login to webmail or other app

Security 101: packet sniffing



TCP Dump (en1)

Monitor Interface: AirPort (en1) ☑ Use TCP Flow

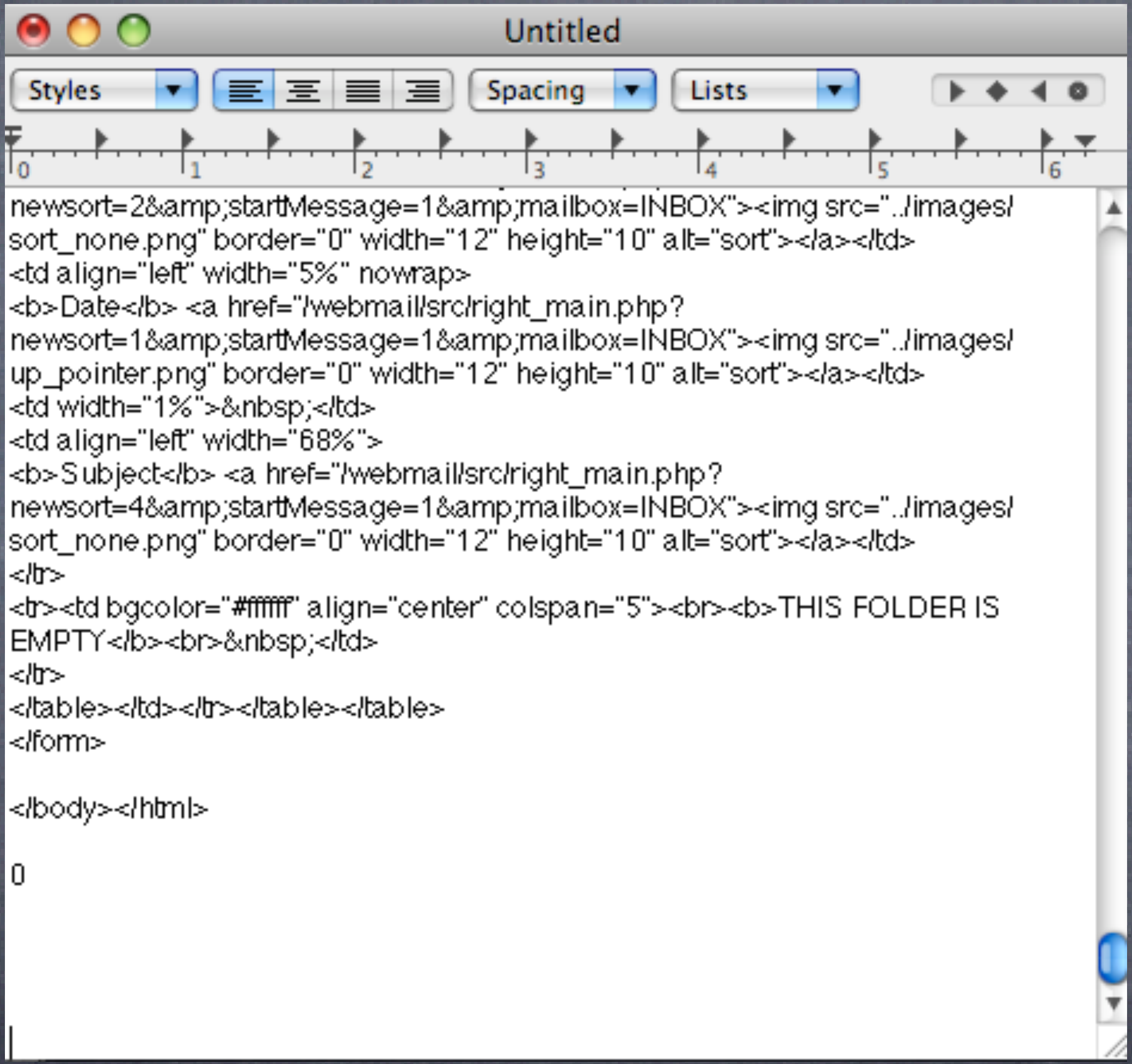
Options: -p port 80 // my web data

```
src="../images/up_pointer.png" border="0" width="12" height="10" alt="sort"></a></td>
<td width="1%">&nbsp;</td>
<td align="left" width="68%">
<b>Subject</b> <a href="/webmail/src/right_main.php?newsort=4&amp;startMessage=1&amp;mailbox=INBOX"><img
src="../images/sort_none.png" border="0" width="12" height="10" alt="sort"></a></td>
</tr>
<tr><td bgcolor="#ffffff" align="center" colspan="5"><br><b>THIS FOLDER IS EMPTY</b><br>&nbsp;</td>
</tr>
</table></td></tr></table></table>
</form>

</body></html>

0
```

Monitoring stopped

start, then check email

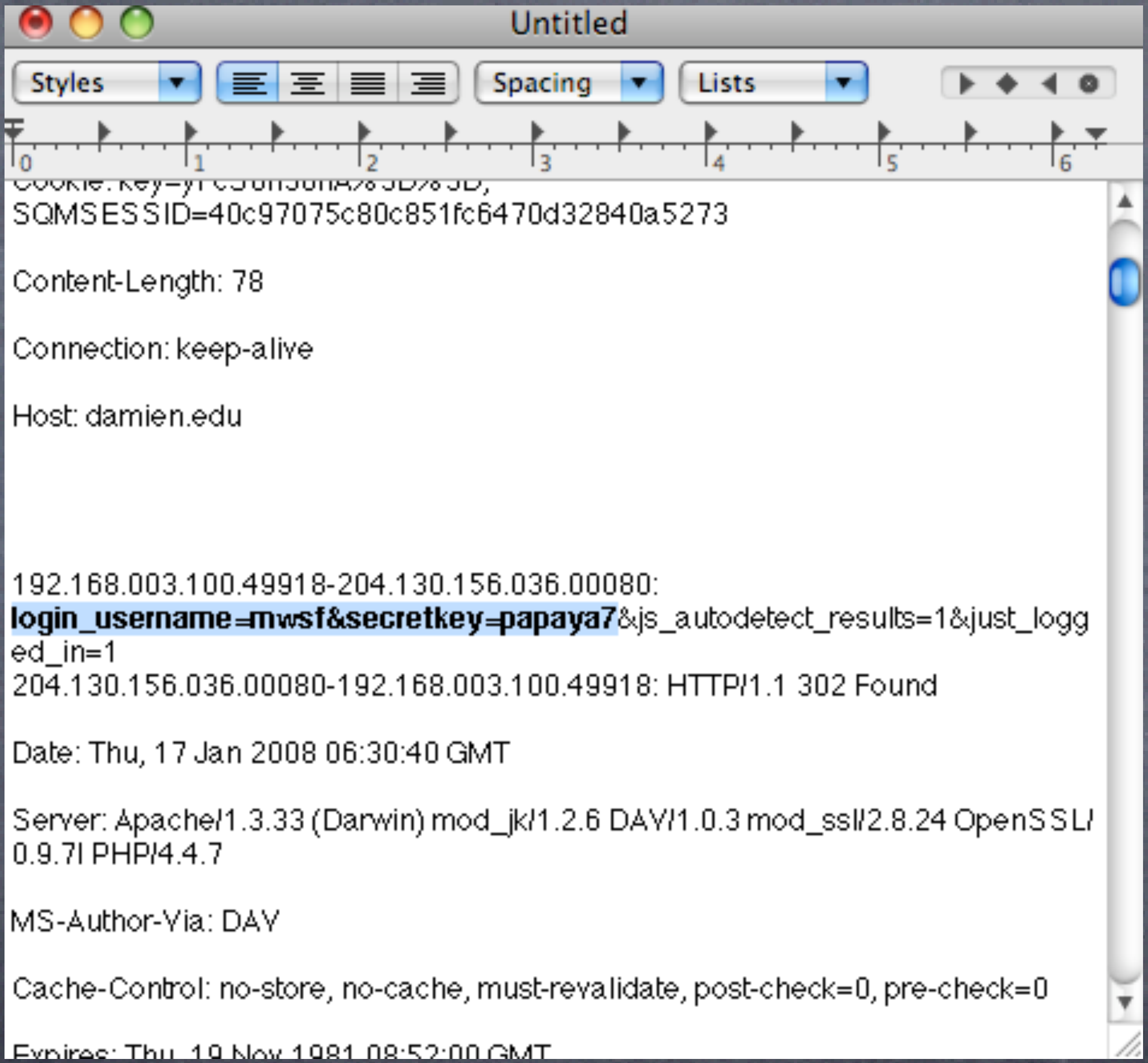
Security 101: packet sniffing



```
newsort=2&amp;startMessage=1&amp;mailbox=INBOX"><img src="../images/
sort_none.png" border="0" width="12" height="10" alt="sort"></a></td>
<td align="left" width="5%" nowrap>
<b>Date</b> <a href="/webmail/src/right_main.php?
newsort=1&amp;startMessage=1&amp;mailbox=INBOX"><img src="../images/
up_pointer.png" border="0" width="12" height="10" alt="sort"></a></td>
<td width="1%">&nbsp;</td>
<td align="left" width="68%">
<b>Subject</b> <a href="/webmail/src/right_main.php?
newsort=4&amp;startMessage=1&amp;mailbox=INBOX"><img src="../images/
sort_none.png" border="0" width="12" height="10" alt="sort"></a></td>
</tr>
<tr><td bgcolor="#ffffff" align="center" colspan="5"><br><b>THIS FOLDER IS
EMPTY</b><br>&nbsp;</td>
</tr>
</table></td></tr></table></table>
</form>

</body></html>

0
```

copy all from window into textedit

Security 101: packet sniffing



```
Cookie: key=yrCJUnJUnA%3D%3D;
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_logg
ed_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

Expires: Thu, 19 Nov 1981 08:52:00 GMT
```

do a find for USER or PASS

The client experience: basic setups

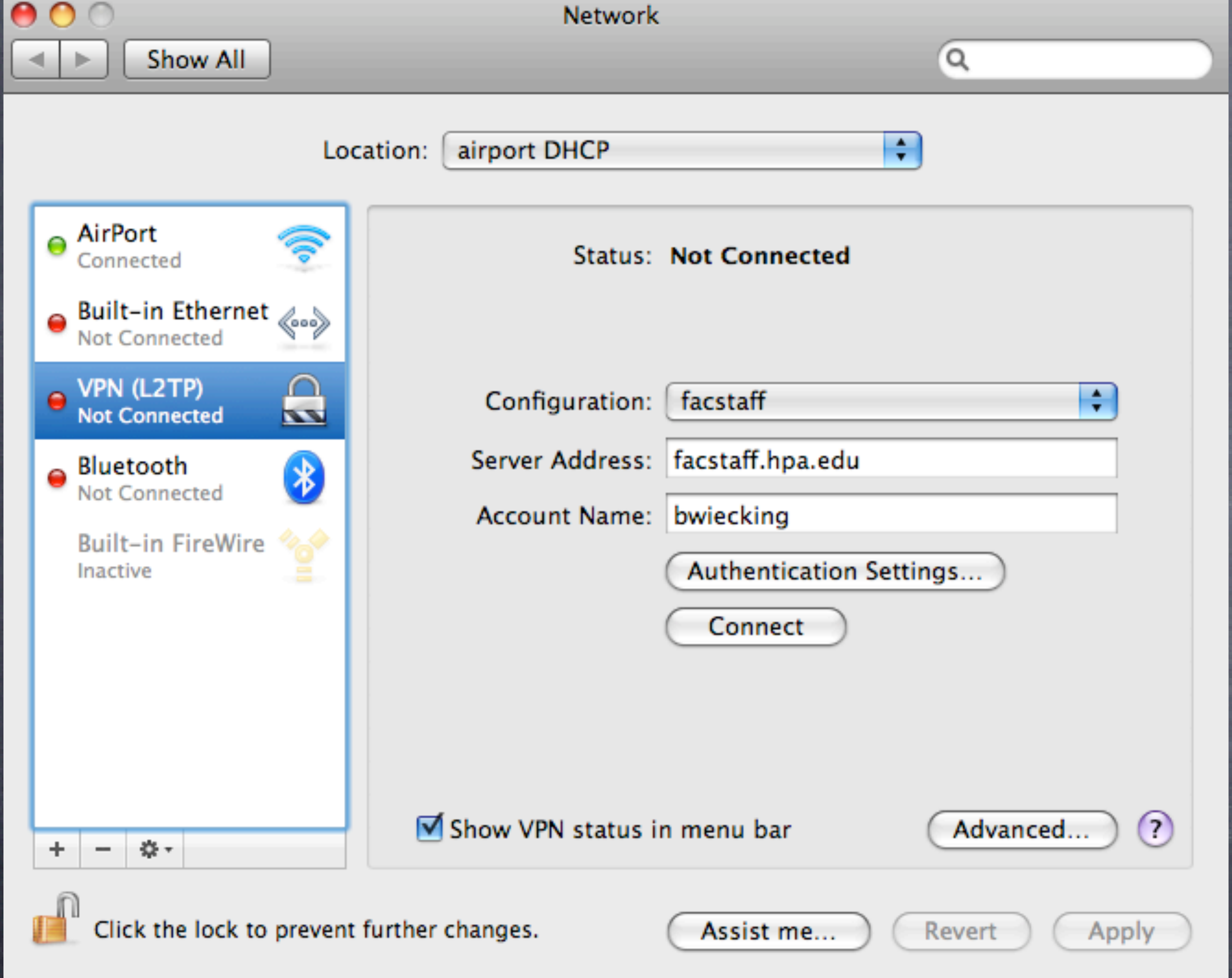
- Goal: Learn how to setup wireless services on Leopard client
- Tools: Leopard client

Advanced Security: VPN and WPA2 to the rescue

- Two main concerns:
  - integrity/security of the data passing on the network
  - access to the network

- Solutions
  - VPN for secure tunnel
  - 802.1x/WPA2 for encrypted authentication

VPN client setup



Network

Location: airport DHCP

AirPort
Connected

Built-in Ethernet
Not Connected

VPN (L2TP)
Not Connected

Bluetooth
Not Connected

Built-in FireWire
Inactive

Status: **Not Connected**

Configuration: facstaff

Server Address: facstaff.hpa.edu

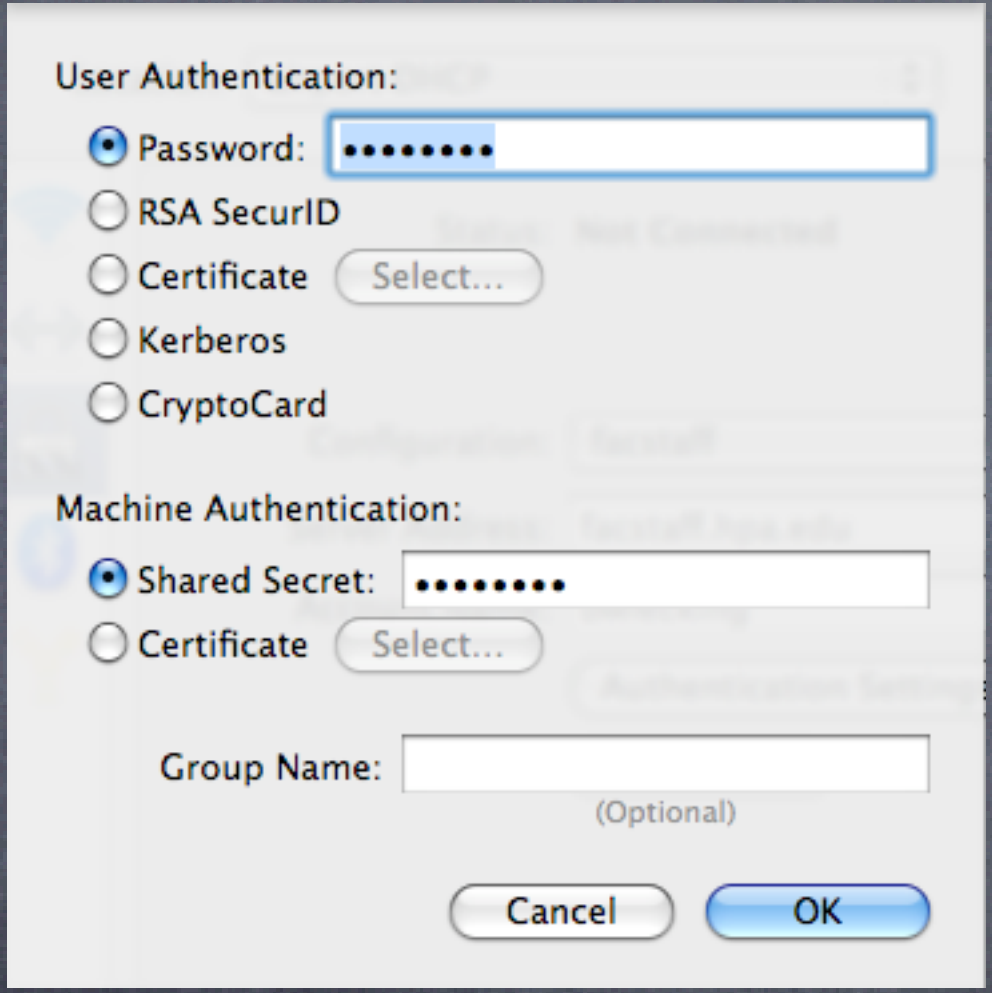
Account Name: bwiecking

☑ Show VPN status in menu bar

Click the lock to prevent further changes.

- Requires a VPN server or endpoint
- Can be Panther, Tiger or Leopard Server
- Free with the server

Client VPN setup



User Authentication:

● Password: •••••••••

○ RSA SecurID

○ Certificate

○ Kerberos

○ CryptoCard

Machine Authentication:

● Shared Secret: •••••••••

○ Certificate

Group Name: (Optional)

- password can be any number of characters
- shared secret must be 8 or more characters

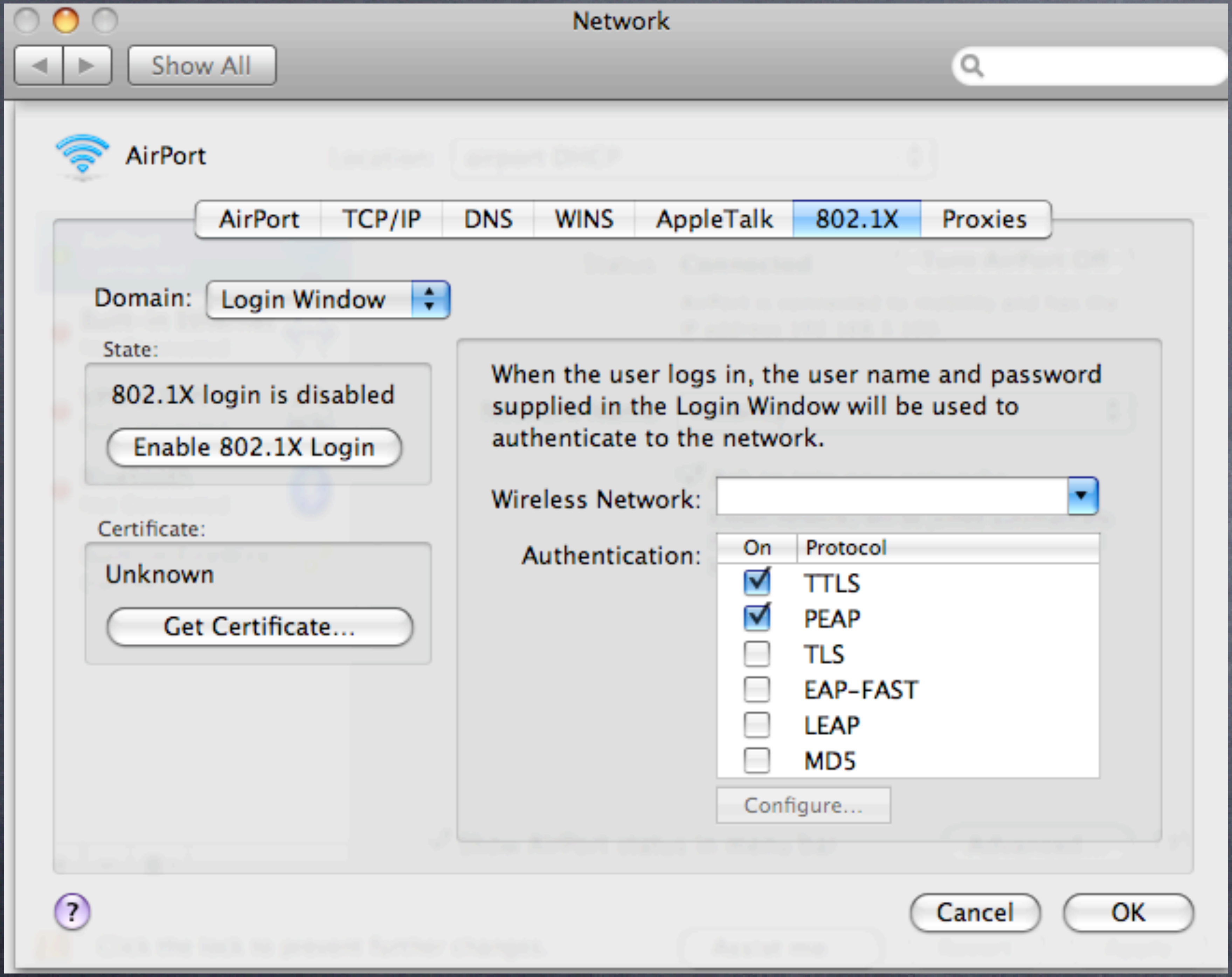
VPN demonstration

- Login to listed VPN servers with login, password and shared secret
- Notice user interface, timer and traffic indicators
- If you dare, try repeating the packet sniffing from before on another person's VPN

iPhone VPN demonstration

- If you have an iPhone, repeat the VPN demonstration above with the iPhone
- Try packet sniffing the conversation

Client WPA2 setup



Domain: Login Window

State:

802.1X login is disabled

Certificate:

Unknown

When the user logs in, the user name and password supplied in the Login Window will be used to authenticate to the network.

Wireless Network:

Authentication:

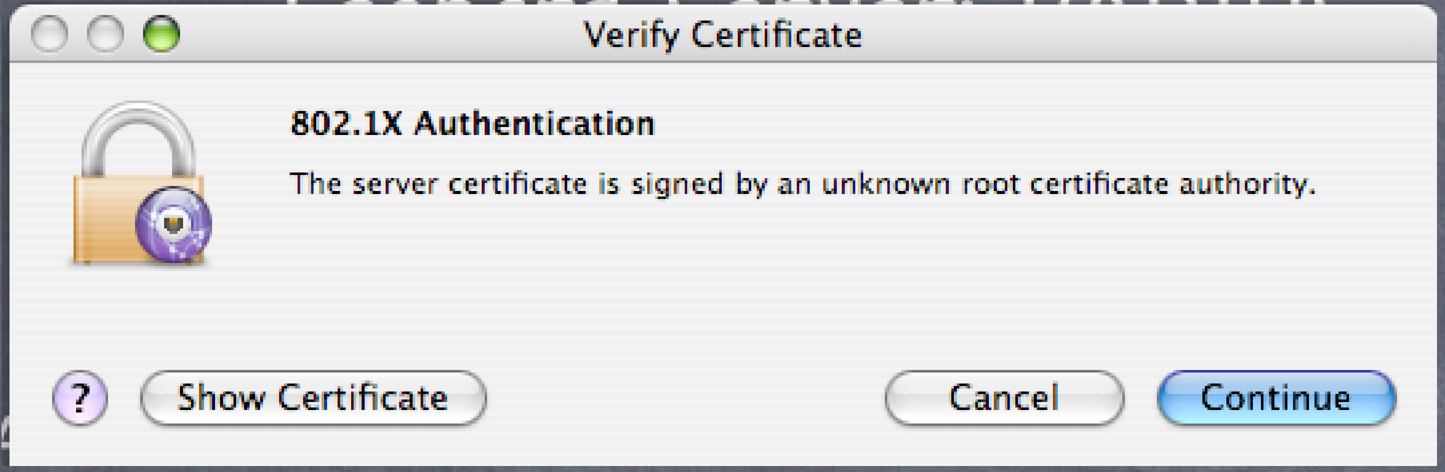
On	Protocol
☑	TTLS
☑	PEAP
□	TLS
□	EAP-FAST
□	LEAP
□	MD5

- Found under system prefs, network settings, and advanced settings
- Provides excellent user authentication to the network

WPA2 demonstration

- Change access on one of the access points to WPA2 personal
- Notice login interface transparency, and inability of others to join the network
- If possible, use the Leopard RADIUS server to enable WPA2 enterprise
- Test and evaluate, particularly looking at the logs

Leopard Server: RADIUS
Exported Internet Connect file



Verify Certificate

802.1X Authentication

The server certificate is signed by an unknown root certificate authority.

Client view: Note very limited user intervention

Authentication: Elektron vs. Leopard Server

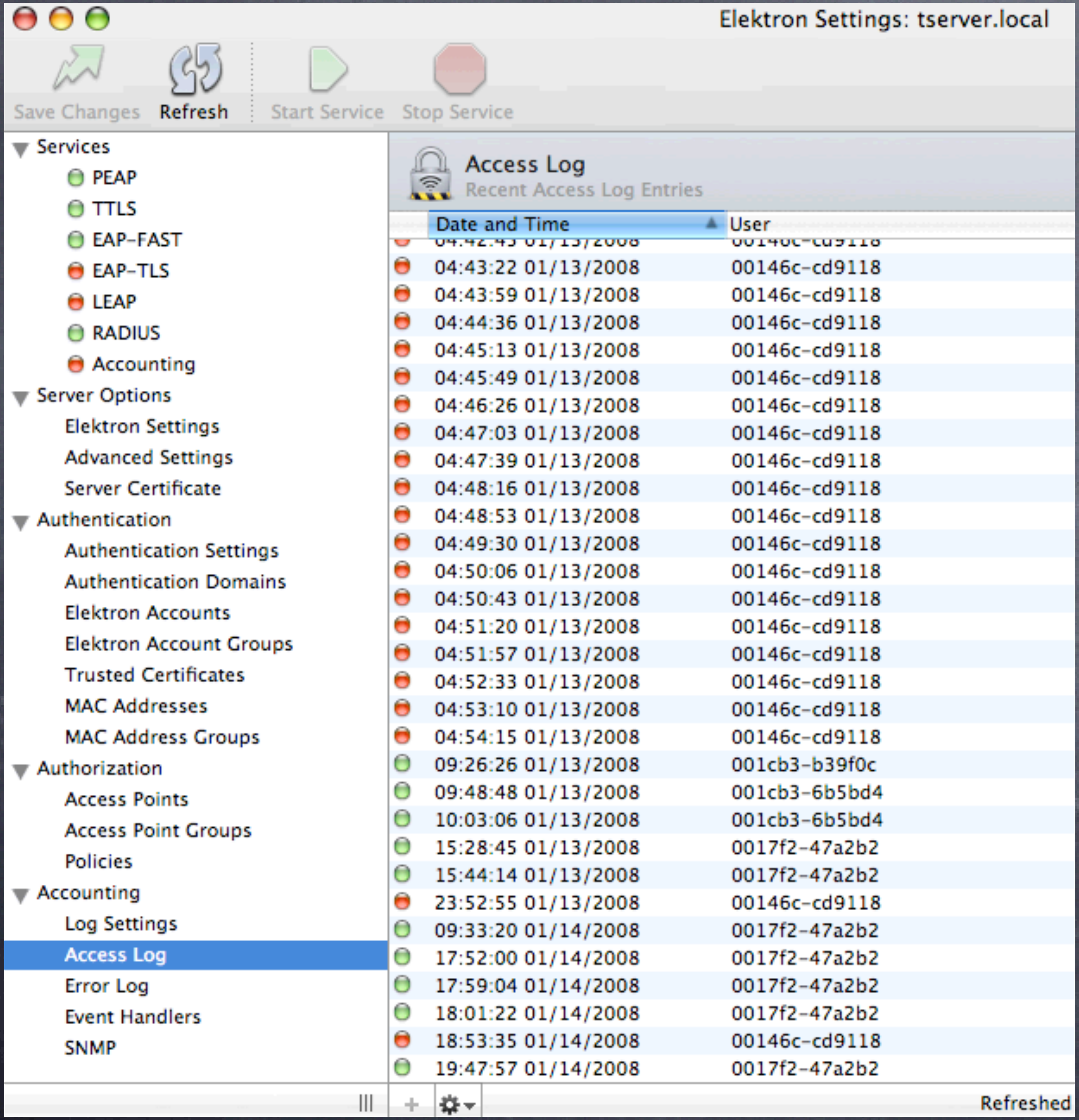
Elektron:

- Cheaper
- Runs on client, not server
- More flexible (MAC ACL and/or WPA2)
- Unlimited user database
- Integrates with Open Directory
- Can export certificates for mac, pc users

Leopard Server:

- Point and click simplicity
- When integrated into Tiger/Leopard client, very easy for users
- Exports internet connect file for one click client setup (can be stored on a server with password protection for all users, or emailed to certain users)
- Fine user access control

Elektron RADIUS/WPA2 server



Access Log

Recent Access Log Entries

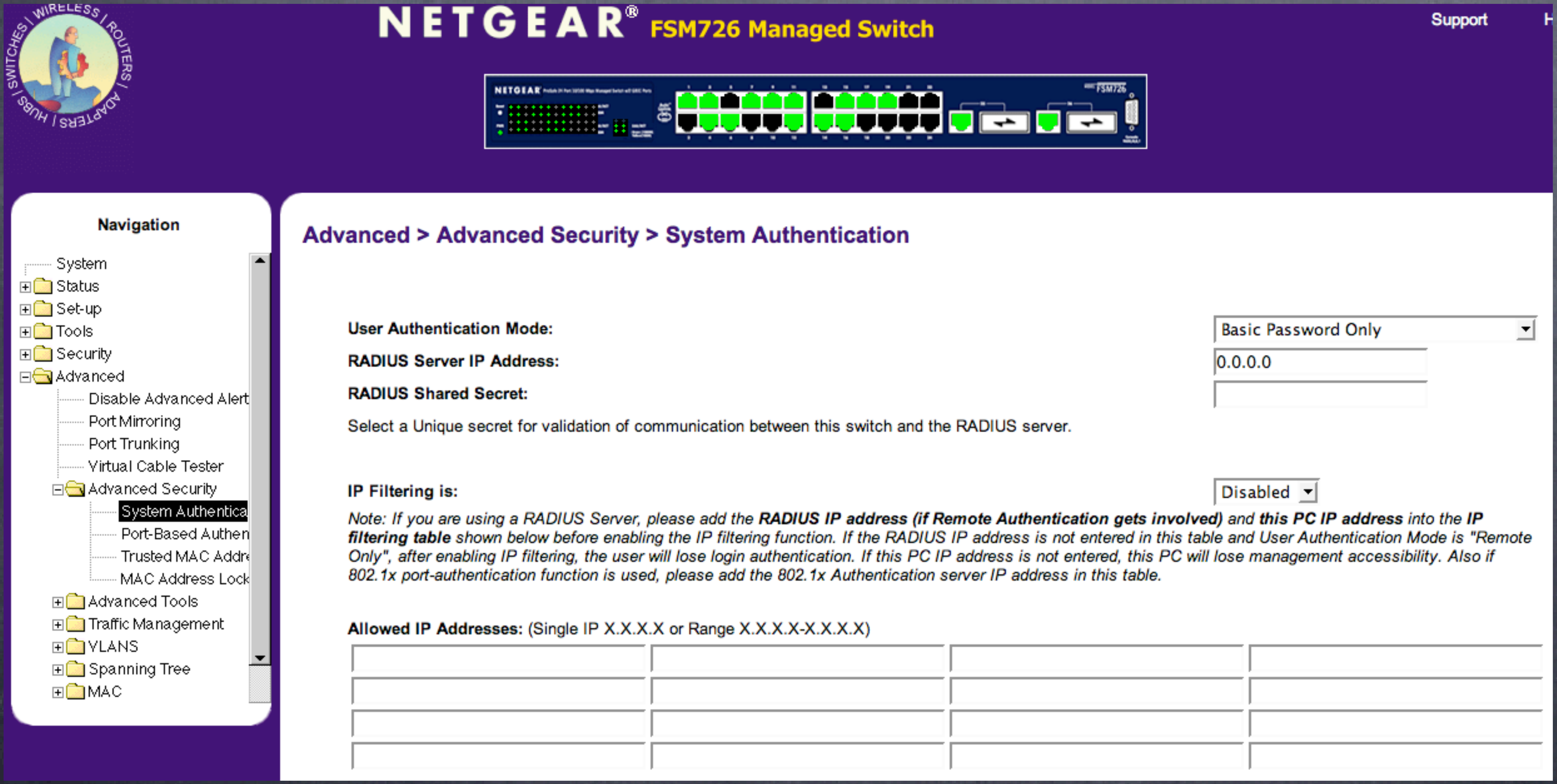
	Date and Time	User
🔴	04:42:45 01/13/2008	00146c-cd9118
🔴	04:43:22 01/13/2008	00146c-cd9118
🔴	04:43:59 01/13/2008	00146c-cd9118
🔴	04:44:36 01/13/2008	00146c-cd9118
🔴	04:45:13 01/13/2008	00146c-cd9118
🔴	04:45:49 01/13/2008	00146c-cd9118
🔴	04:46:26 01/13/2008	00146c-cd9118
🔴	04:47:03 01/13/2008	00146c-cd9118
🔴	04:47:39 01/13/2008	00146c-cd9118
🔴	04:48:16 01/13/2008	00146c-cd9118
🔴	04:48:53 01/13/2008	00146c-cd9118
🔴	04:49:30 01/13/2008	00146c-cd9118
🔴	04:50:06 01/13/2008	00146c-cd9118
🔴	04:50:43 01/13/2008	00146c-cd9118
🔴	04:51:20 01/13/2008	00146c-cd9118
🔴	04:51:57 01/13/2008	00146c-cd9118
🔴	04:52:33 01/13/2008	00146c-cd9118
🔴	04:53:10 01/13/2008	00146c-cd9118
🔴	04:54:15 01/13/2008	00146c-cd9118
🟢	09:26:26 01/13/2008	001cb3-b39f0c
🟢	09:48:48 01/13/2008	001cb3-6b5bd4
🟢	10:03:06 01/13/2008	001cb3-6b5bd4
🟢	15:28:45 01/13/2008	0017f2-47a2b2
🟢	15:44:14 01/13/2008	0017f2-47a2b2
🔴	23:52:55 01/13/2008	00146c-cd9118
🟢	09:33:20 01/14/2008	0017f2-47a2b2
🟢	17:52:00 01/14/2008	0017f2-47a2b2
🟢	17:59:04 01/14/2008	0017f2-47a2b2
🟢	18:01:22 01/14/2008	0017f2-47a2b2
🔴	18:53:35 01/14/2008	00146c-cd9118
🟢	19:47:57 01/14/2008	0017f2-47a2b2

- Access log
- Note red dots are unauthorized attempts
- Green dots are OK connections
- Can be used to determine MAC address

Wireless network management

- Central RADIUS simplifies network access and intervention
- Can be integrated into wired switches for a comprehensive security solution (MAC address, 802.1x or both)
- Syslog server integration with all access points is very helpful
- Intermapper network mapping uses SNMP information to determine wireless network health
- Cybergauge uses similar information to monitor network traffic at access points, to spot anomalous users

Managed Switches: MAC address access control



Advanced > Advanced Security > System Authentication

User Authentication Mode: Basic Password Only

RADIUS Server IP Address: 0.0.0.0

RADIUS Shared Secret:

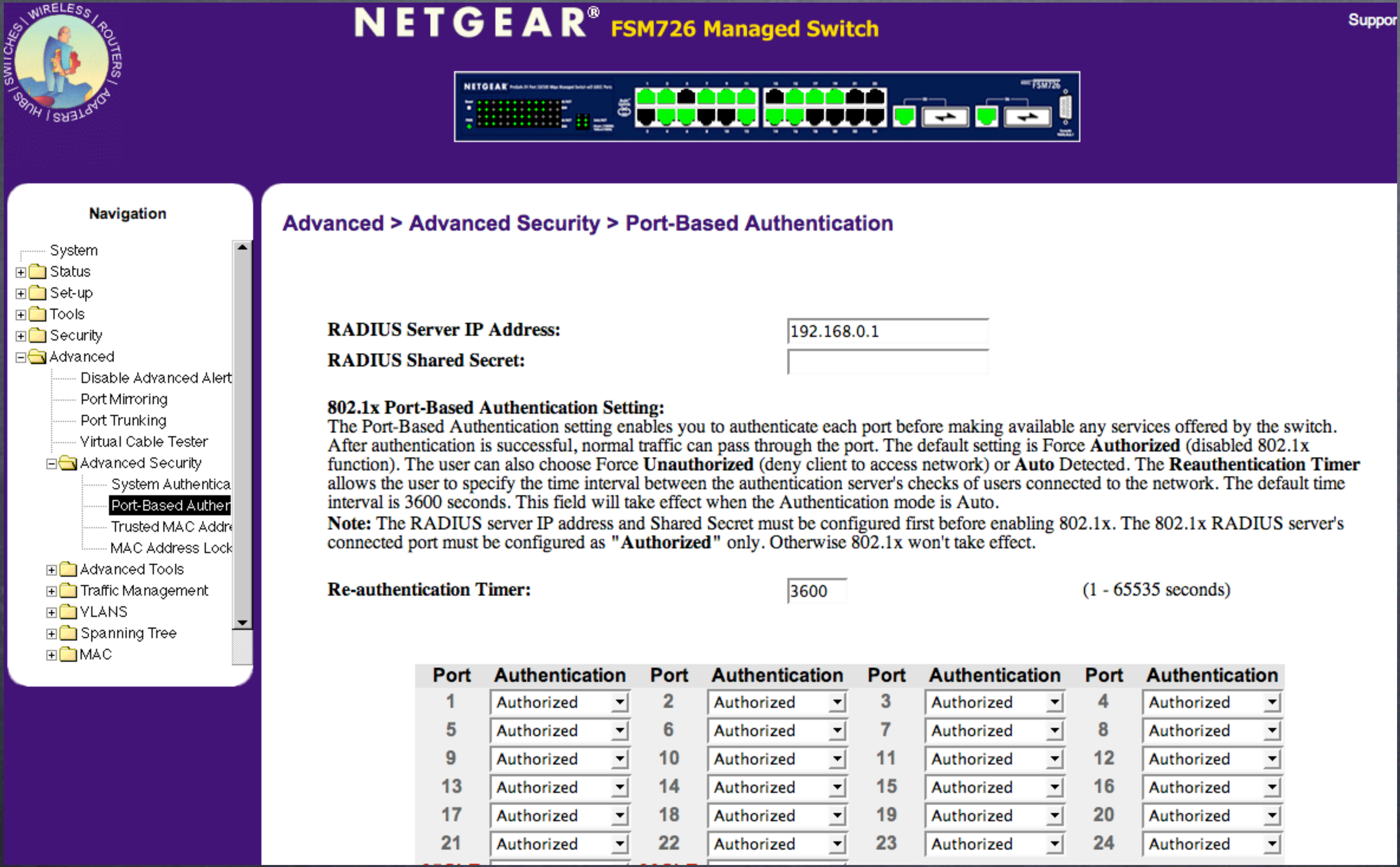
Select a Unique secret for validation of communication between this switch and the RADIUS server.

IP Filtering is: Disabled

Note: If you are using a RADIUS Server, please add the ***RADIUS IP address (if Remote Authentication gets involved)*** *and* ***this PC IP address*** *into the* ***IP filtering table*** *shown below before enabling the IP filtering function. If the RADIUS IP address is not entered in this table and User Authentication Mode is "Remote Only", after enabling IP filtering, the user will lose login authentication. If this PC IP address is not entered, this PC will lose management accessibility. Also if 802.1x port-authentication function is used, please add the 802.1x Authentication server IP address in this table.*

Allowed IP Addresses: (Single IP X.X.X.X or Range X.X.X.X-X.X.X.X)

Managed Switches: 802.1x access control



Advanced > Advanced Security > Port-Based Authentication

RADIUS Server IP Address: 192.168.0.1

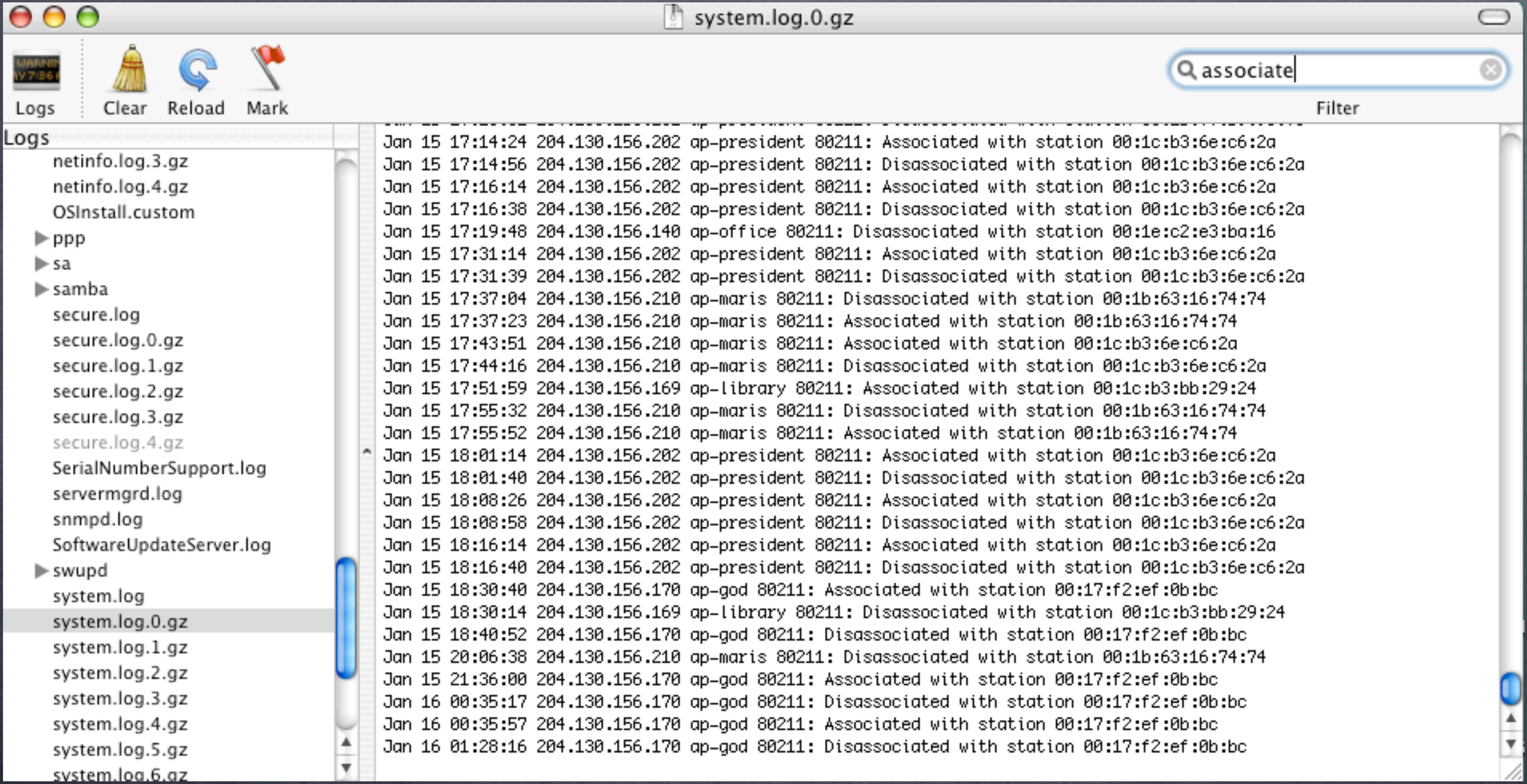
RADIUS Shared Secret:

802.1x Port-Based Authentication Setting:
The Port-Based Authentication setting enables you to authenticate each port before making available any services offered by the switch. After authentication is successful, normal traffic can pass through the port. The default setting is Force **Authorized** (disabled 802.1x function). The user can also choose Force **Unauthorized** (deny client to access network) or **Auto** Detected. The **Reauthentication Timer** allows the user to specify the time interval between the authentication server's checks of users connected to the network. The default time interval is 3600 seconds. This field will take effect when the Authentication mode is Auto.
Note: The RADIUS server IP address and Shared Secret must be configured first before enabling 802.1x. The 802.1x RADIUS server's connected port must be configured as "**Authorized**" only. Otherwise 802.1x won't take effect.

Re-authentication Timer: 3600 (1 - 65535 seconds)

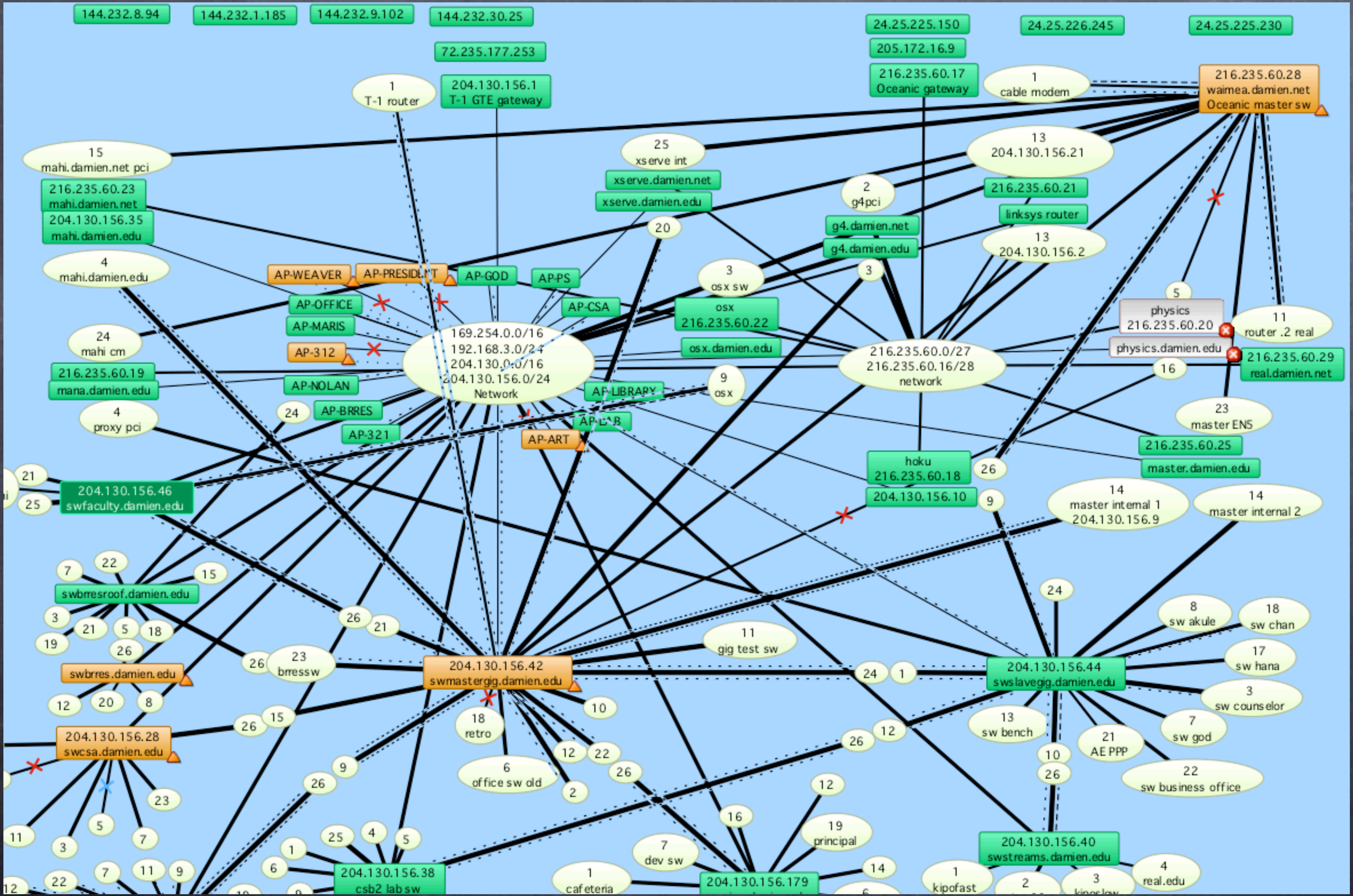
Port	Authentication	Port	Authentication	Port	Authentication	Port	Authentication
1	Authorized	2	Authorized	3	Authorized	4	Authorized
5	Authorized	6	Authorized	7	Authorized	8	Authorized
9	Authorized	10	Authorized	11	Authorized	12	Authorized
13	Authorized	14	Authorized	15	Authorized	16	Authorized
17	Authorized	18	Authorized	19	Authorized	20	Authorized
21	Authorized	22	Authorized	23	Authorized	24	Authorized

syslogd on xserve: note association records

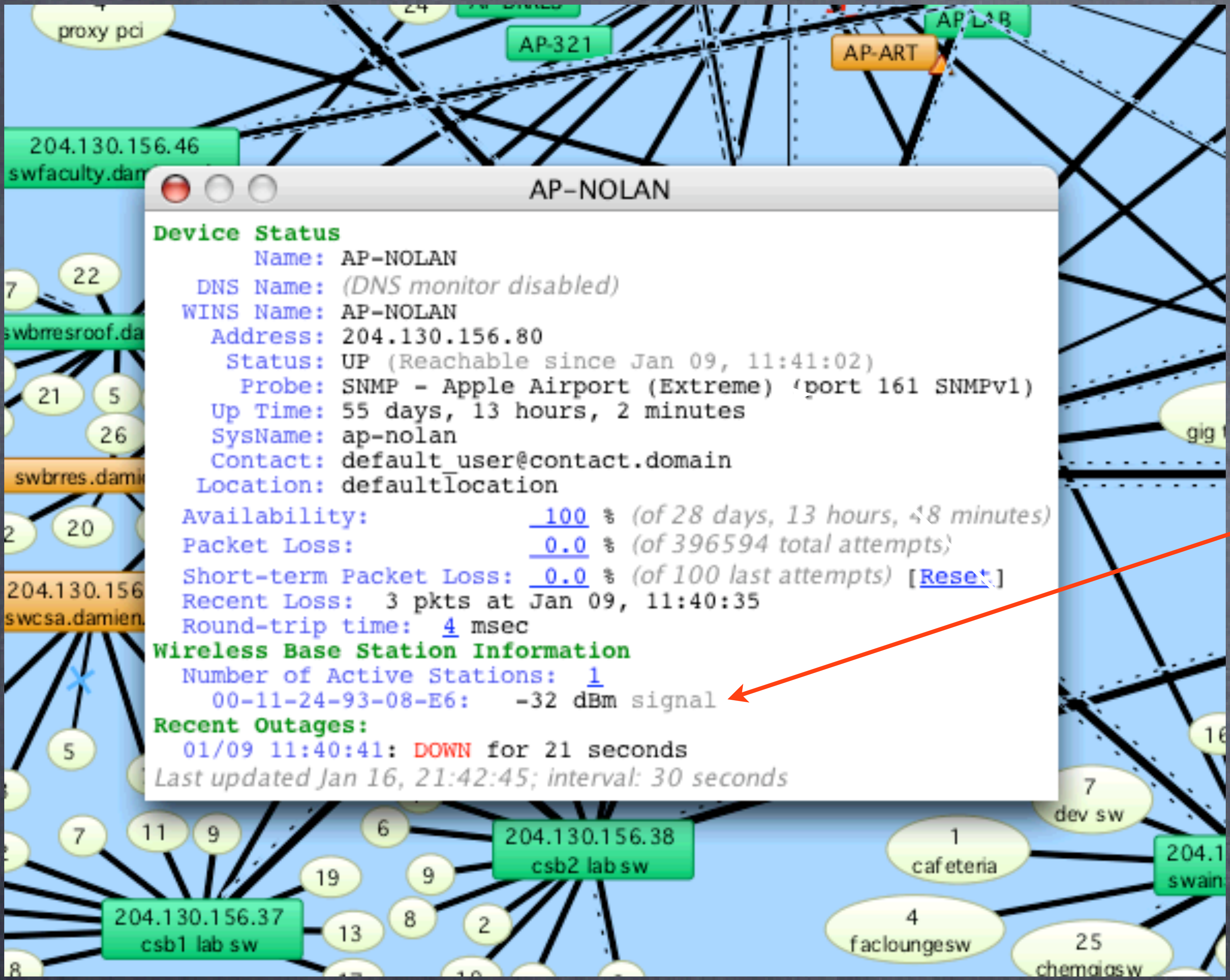


```
Jan 15 17:14:24 204.130.156.202 ap-president 80211: Associated with station 00:1c:b3:6e:c6:2a
Jan 15 17:14:56 204.130.156.202 ap-president 80211: Disassociated with station 00:1c:b3:6e:c6:2a
Jan 15 17:16:14 204.130.156.202 ap-president 80211: Associated with station 00:1c:b3:6e:c6:2a
Jan 15 17:16:38 204.130.156.202 ap-president 80211: Disassociated with station 00:1c:b3:6e:c6:2a
Jan 15 17:19:48 204.130.156.140 ap-office 80211: Disassociated with station 00:1e:c2:e3:ba:16
Jan 15 17:31:14 204.130.156.202 ap-president 80211: Associated with station 00:1c:b3:6e:c6:2a
Jan 15 17:31:39 204.130.156.202 ap-president 80211: Disassociated with station 00:1c:b3:6e:c6:2a
Jan 15 17:37:04 204.130.156.210 ap-maris 80211: Disassociated with station 00:1b:63:16:74:74
Jan 15 17:37:23 204.130.156.210 ap-maris 80211: Associated with station 00:1b:63:16:74:74
Jan 15 17:43:51 204.130.156.210 ap-maris 80211: Associated with station 00:1c:b3:6e:c6:2a
Jan 15 17:44:16 204.130.156.210 ap-maris 80211: Disassociated with station 00:1c:b3:6e:c6:2a
Jan 15 17:51:59 204.130.156.169 ap-library 80211: Associated with station 00:1c:b3:bb:29:24
Jan 15 17:55:32 204.130.156.210 ap-maris 80211: Disassociated with station 00:1b:63:16:74:74
Jan 15 17:55:52 204.130.156.210 ap-maris 80211: Associated with station 00:1b:63:16:74:74
Jan 15 18:01:14 204.130.156.202 ap-president 80211: Associated with station 00:1c:b3:6e:c6:2a
Jan 15 18:01:40 204.130.156.202 ap-president 80211: Disassociated with station 00:1c:b3:6e:c6:2a
Jan 15 18:08:26 204.130.156.202 ap-president 80211: Associated with station 00:1c:b3:6e:c6:2a
Jan 15 18:08:58 204.130.156.202 ap-president 80211: Disassociated with station 00:1c:b3:6e:c6:2a
Jan 15 18:16:14 204.130.156.202 ap-president 80211: Associated with station 00:1c:b3:6e:c6:2a
Jan 15 18:16:40 204.130.156.202 ap-president 80211: Disassociated with station 00:1c:b3:6e:c6:2a
Jan 15 18:30:40 204.130.156.170 ap-god 80211: Associated with station 00:17:f2:ef:0b:bc
Jan 15 18:30:14 204.130.156.169 ap-library 80211: Disassociated with station 00:1c:b3:bb:29:24
Jan 15 18:40:52 204.130.156.170 ap-god 80211: Disassociated with station 00:17:f2:ef:0b:bc
Jan 15 20:06:38 204.130.156.210 ap-maris 80211: Disassociated with station 00:1b:63:16:74:74
Jan 15 21:36:00 204.130.156.170 ap-god 80211: Associated with station 00:17:f2:ef:0b:bc
Jan 16 00:35:17 204.130.156.170 ap-god 80211: Disassociated with station 00:17:f2:ef:0b:bc
Jan 16 00:35:57 204.130.156.170 ap-god 80211: Associated with station 00:17:f2:ef:0b:bc
Jan 16 01:28:16 204.130.156.170 ap-god 80211: Disassociated with station 00:17:f2:ef:0b:bc
```

Intermapper interface



Intermapper interface

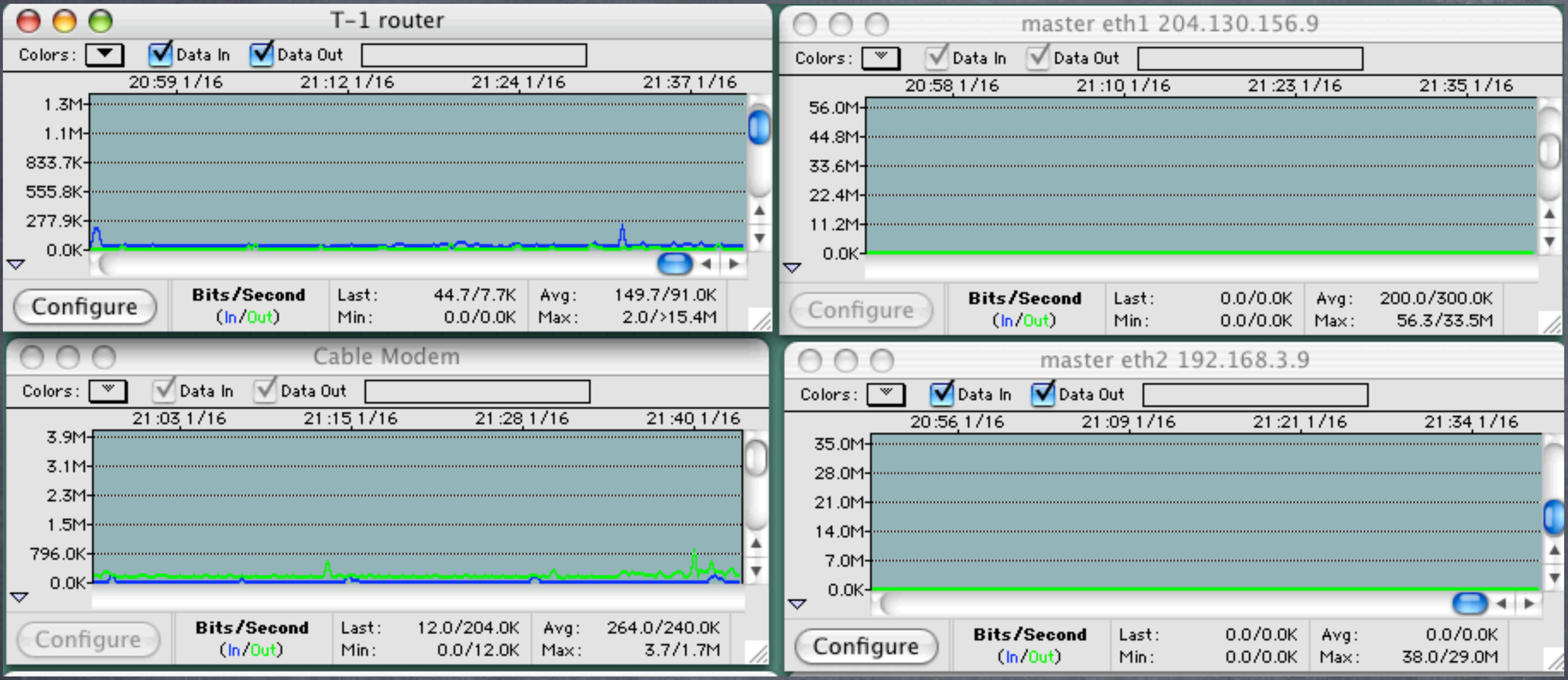


AP-NOLAN

```
Device Status
        Name: AP-NOLAN
    DNS Name: (DNS monitor disabled)
   WINS Name: AP-NOLAN
     Address: 204.130.156.80
      Status: UP (Reachable since Jan 09, 11:41:02)
       Probe: SNMP - Apple Airport (Extreme) (port 161 SNMPv1)
     Up Time: 55 days, 13 hours, 2 minutes
     SysName: ap-nolan
     Contact: default_user@contact.domain
    Location: defaultlocation
  Availability:            100 % (of 28 days, 13 hours, 48 minutes)
  Packet Loss:             0.0 % (of 396594 total attempts)
  Short-term Packet Loss:  0.0 % (of 100 last attempts) [Reset]
  Recent Loss:   3 pkts at Jan 09, 11:40:35
  Round-trip time:  4 msec
Wireless Base Station Information
  Number of Active Stations:  1
    00-11-24-93-08-E6:    -32 dBm signal
Recent Outages:
  01/09 11:40:41: DOWN for 21 seconds
Last updated Jan 16, 21:42:45; interval: 30 seconds
```

- Notice wireless client information gathered from SNMP data

Cybergauge interface



T-1 router

Colors: ☑ Data In ☑ Data Out

Bits/Second (In/Out) Last: 44.7/7.7K Avg: 149.7/91.0K
Min: 0.0/0.0K Max: 2.0/>15.4M

master eth1 204.130.156.9

Colors: ☑ Data In ☑ Data Out

Bits/Second (In/Out) Last: 0.0/0.0K Avg: 200.0/300.0K
Min: 0.0/0.0K Max: 56.3/33.5M

Cable Modem

Colors: ☑ Data In ☑ Data Out

Bits/Second (In/Out) Last: 12.0/204.0K Avg: 264.0/240.0K
Min: 0.0/12.0K Max: 3.7/1.7M

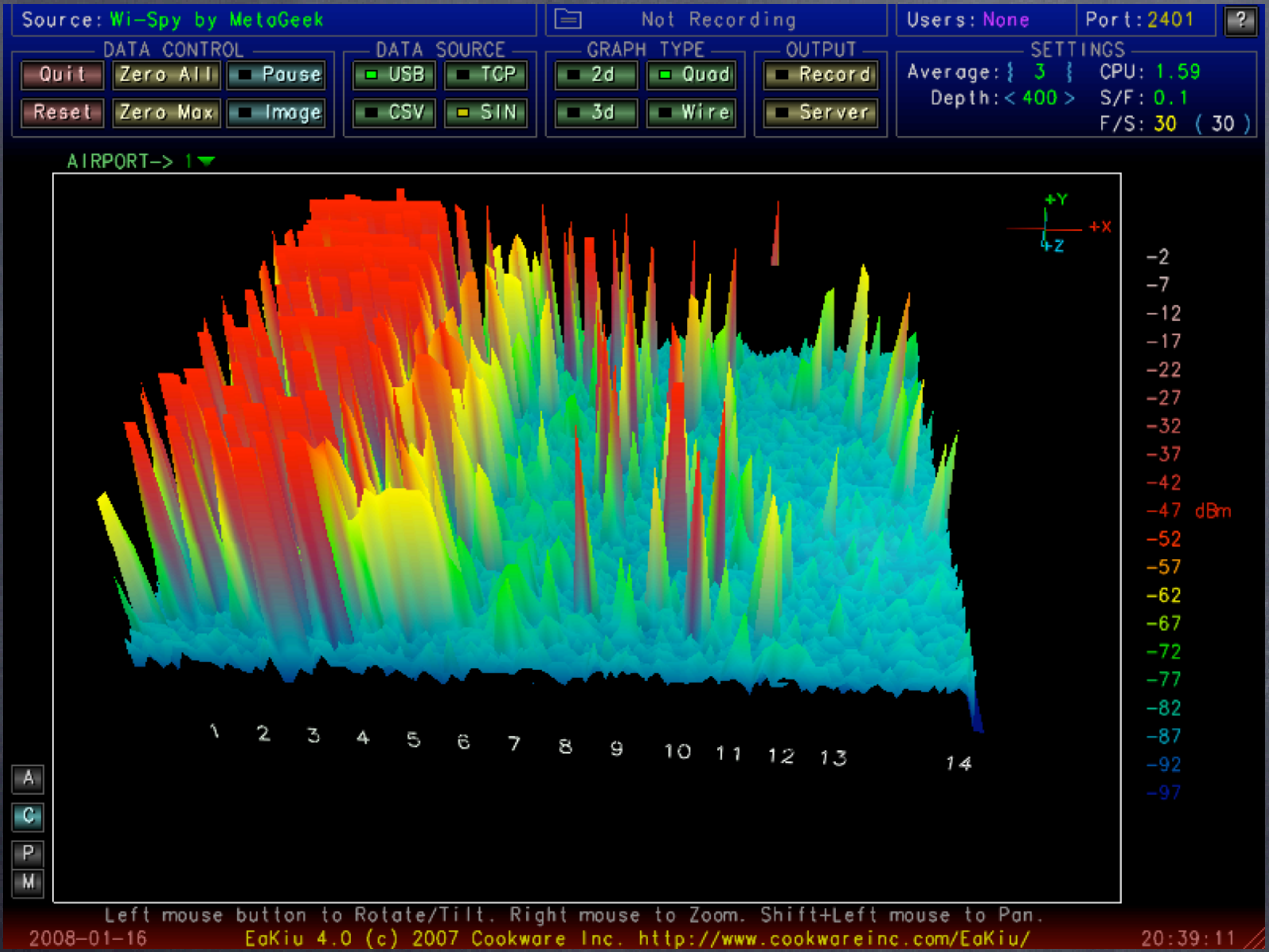
master eth2 192.168.3.9

Colors: ☑ Data In ☑ Data Out

Bits/Second (In/Out) Last: 0.0/0.0K Avg: 0.0/0.0K
Min: 0.0/0.0K Max: 38.0/29.0M

- Notice traffic in and out, monitors and alarms on anomalous traffic at off hours

Antennas and amplifiers



Source: Wi-Spy by MetaGeek

Not Recording

Users: None

Port: 2401

Average: { 3 }

Depth: < 400 >

CPU: 1.59

S/F: 0.1

F/S: 30 (30)

AIRPORT-> 1

Left mouse button to Rotate/Tilt. Right mouse to Zoom. Shift+Left mouse to Pan.

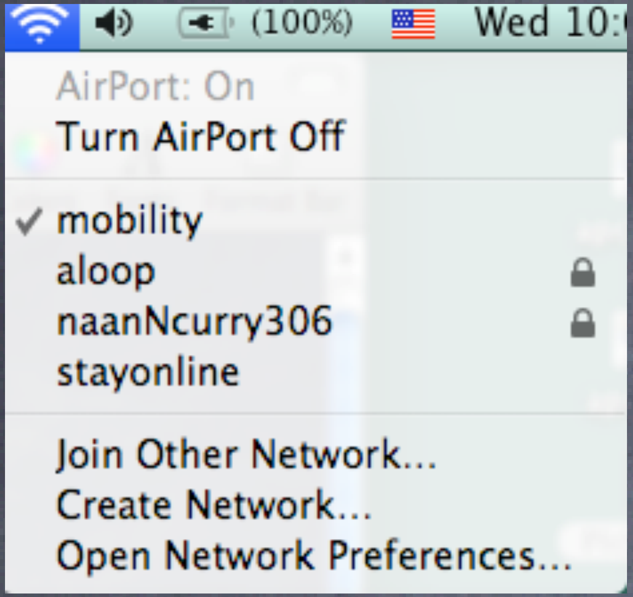
2008-01-16 EaKiu 4.0 (c) 2007 Cookware Inc. http://www.cookwareinc.com/EaKiu/ 20:39:11

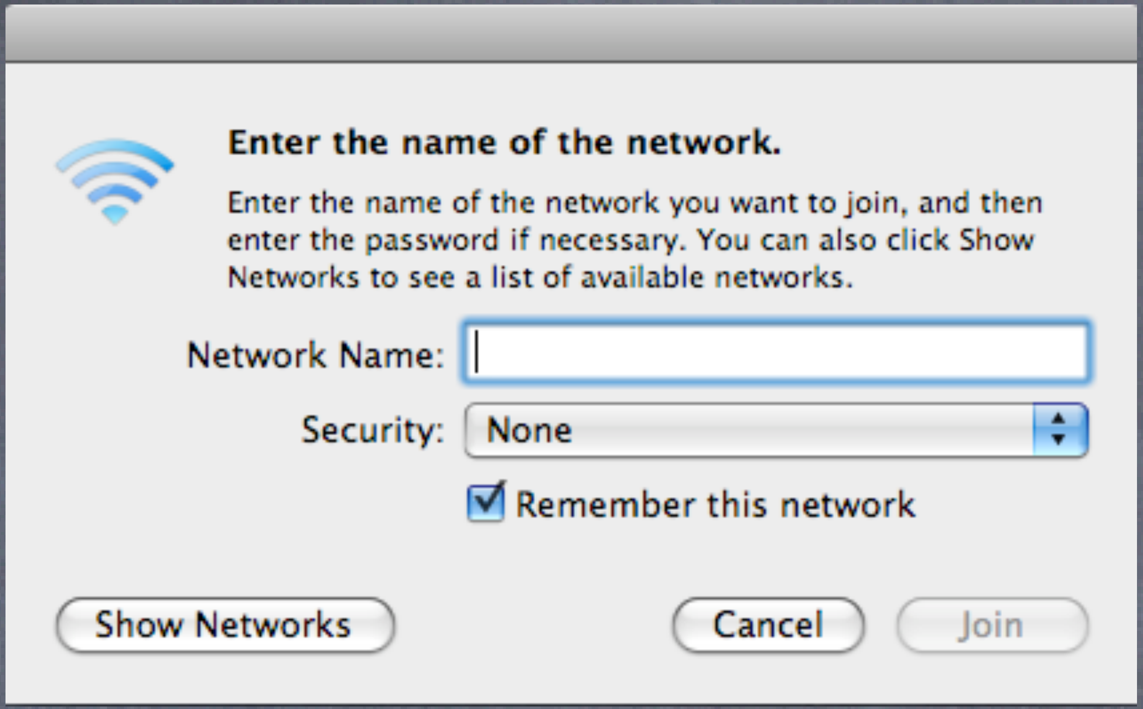
- Repeat wispy test with antennas and amplifiers
- Notice that antennas increase SNR, amplifiers raise the noise floor

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)

Reference: Leopard Wireless client setup





Enter the name of the network.

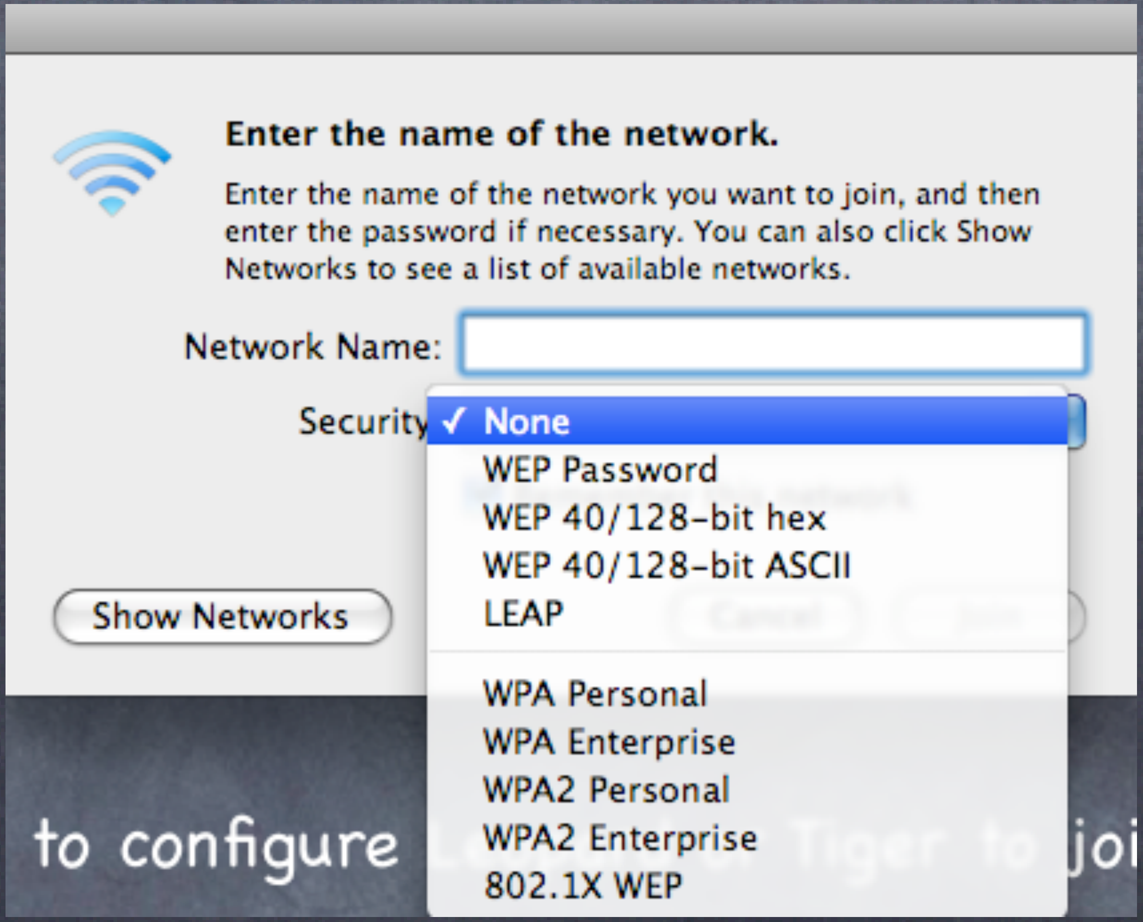
Enter the name of the network you want to join, and then enter the password if necessary. You can also click Show Networks to see a list of available networks.

Network Name:

Security: None

☑ Remember this network

- 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



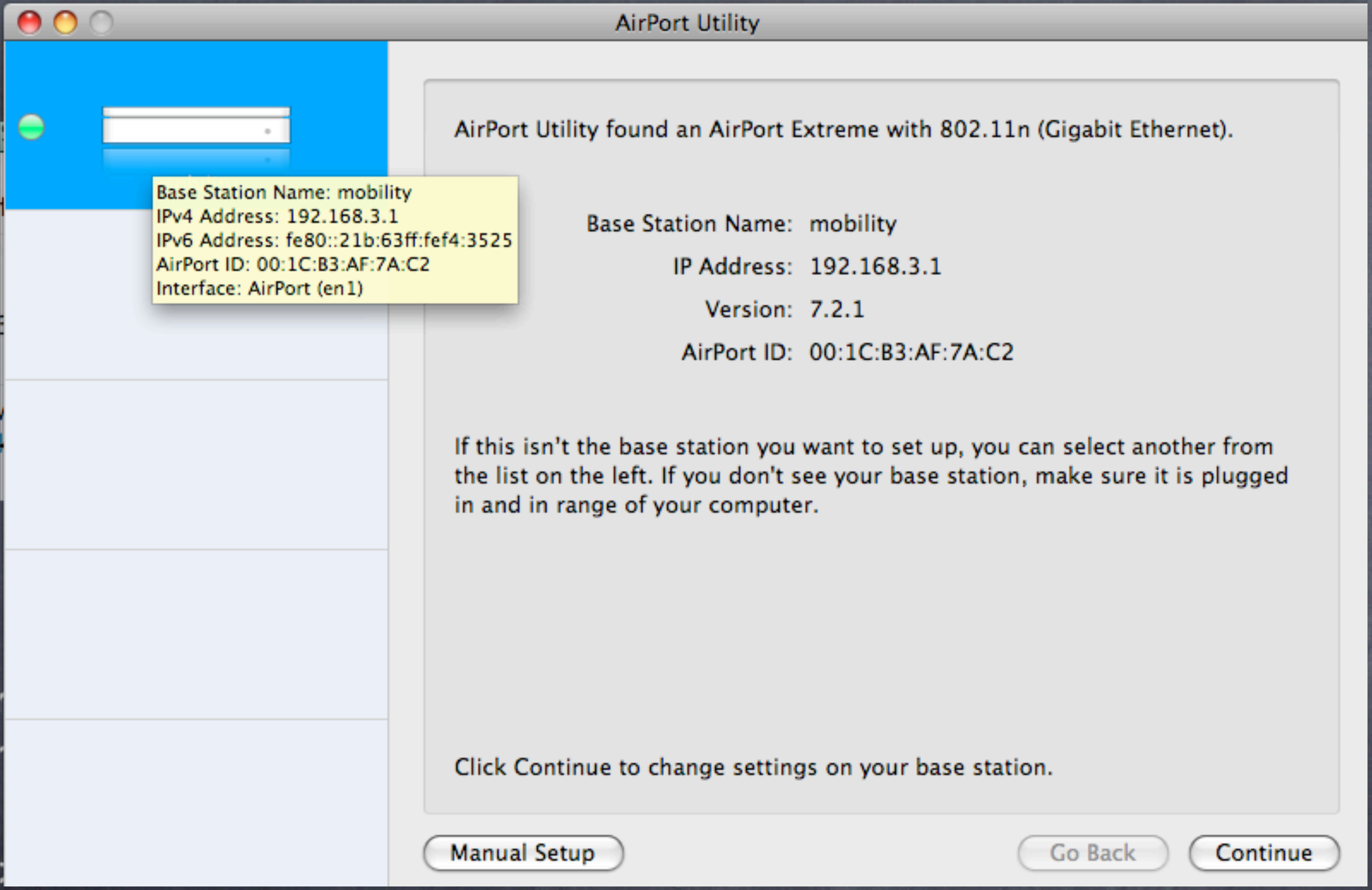
Enter the name of the network.

Enter the name of the network you want to join, and then enter the password if necessary. You can also click Show Networks to see a list of available networks.

Network Name:

Security: ✓ None

Reference: Wireless Access point setup



AirPort Utility

Base Station Name: mobility
IPv4 Address: 192.168.3.1
IPv6 Address: fe80::21b:63ff:fef4:3525
AirPort ID: 00:1C:B3:AF:7A:C2
Interface: AirPort (en1)

AirPort Utility found an AirPort Extreme with 802.11n (Gigabit Ethernet).

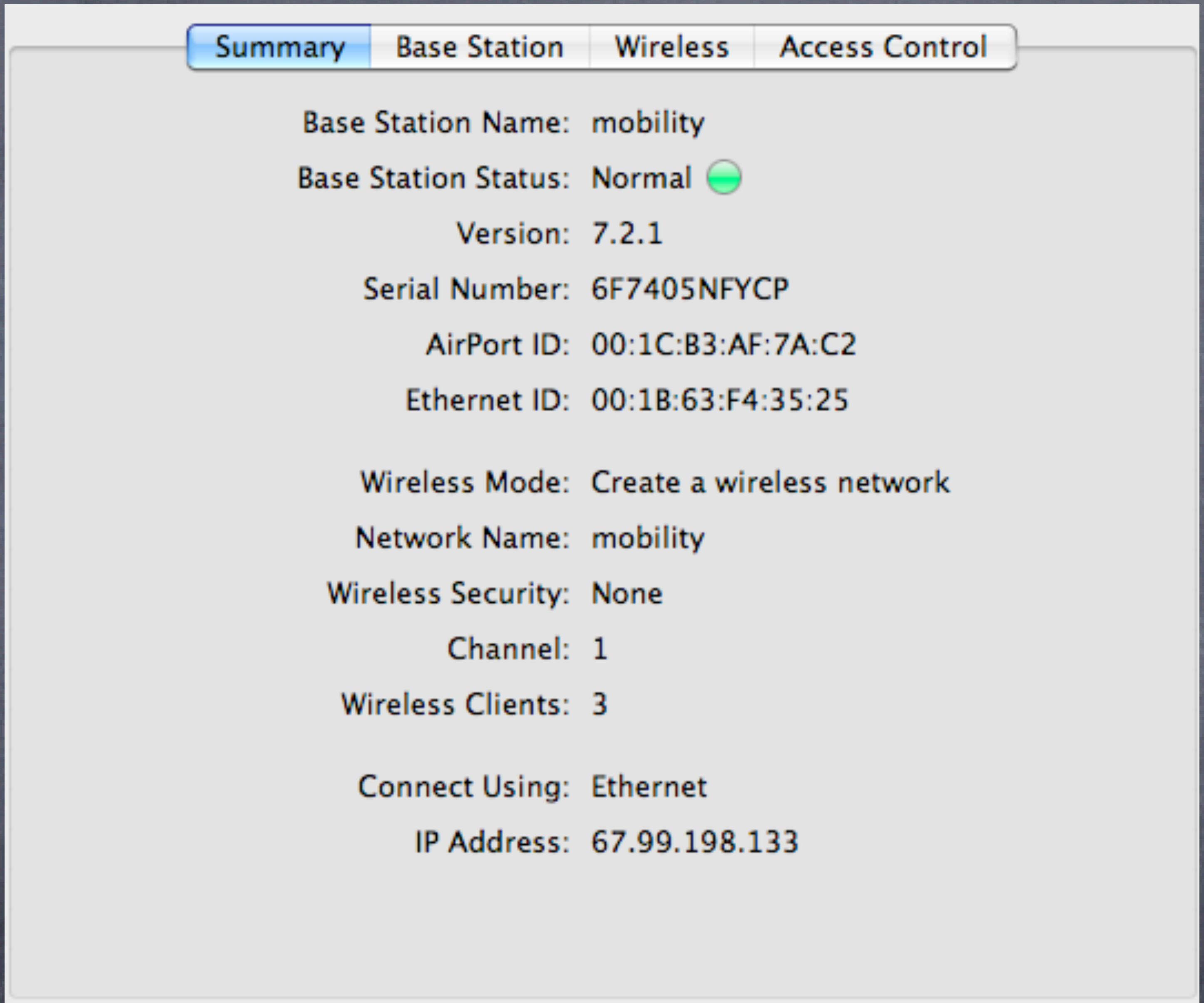
Base Station Name: mobility
IP Address: 192.168.3.1
Version: 7.2.1
AirPort ID: 00:1C:B3:AF:7A:C2

If this isn't the base station you want to set up, you can select another from the list on the left. If you don't see your base station, make sure it is plugged in and in range of your computer.

Click Continue to change settings on your base station.

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

Basic Wireless Access point setup



Base Station Name: mobility

Base Station Status: Normal 🟢

Version: 7.2.1

Serial Number: 6F7405NFYCP

AirPort ID: 00:1C:B3:AF:7A:C2

Ethernet ID: 00:1B:63:F4:35:25

Wireless Mode: Create a wireless network

Network Name: mobility

Wireless Security: None

Channel: 1

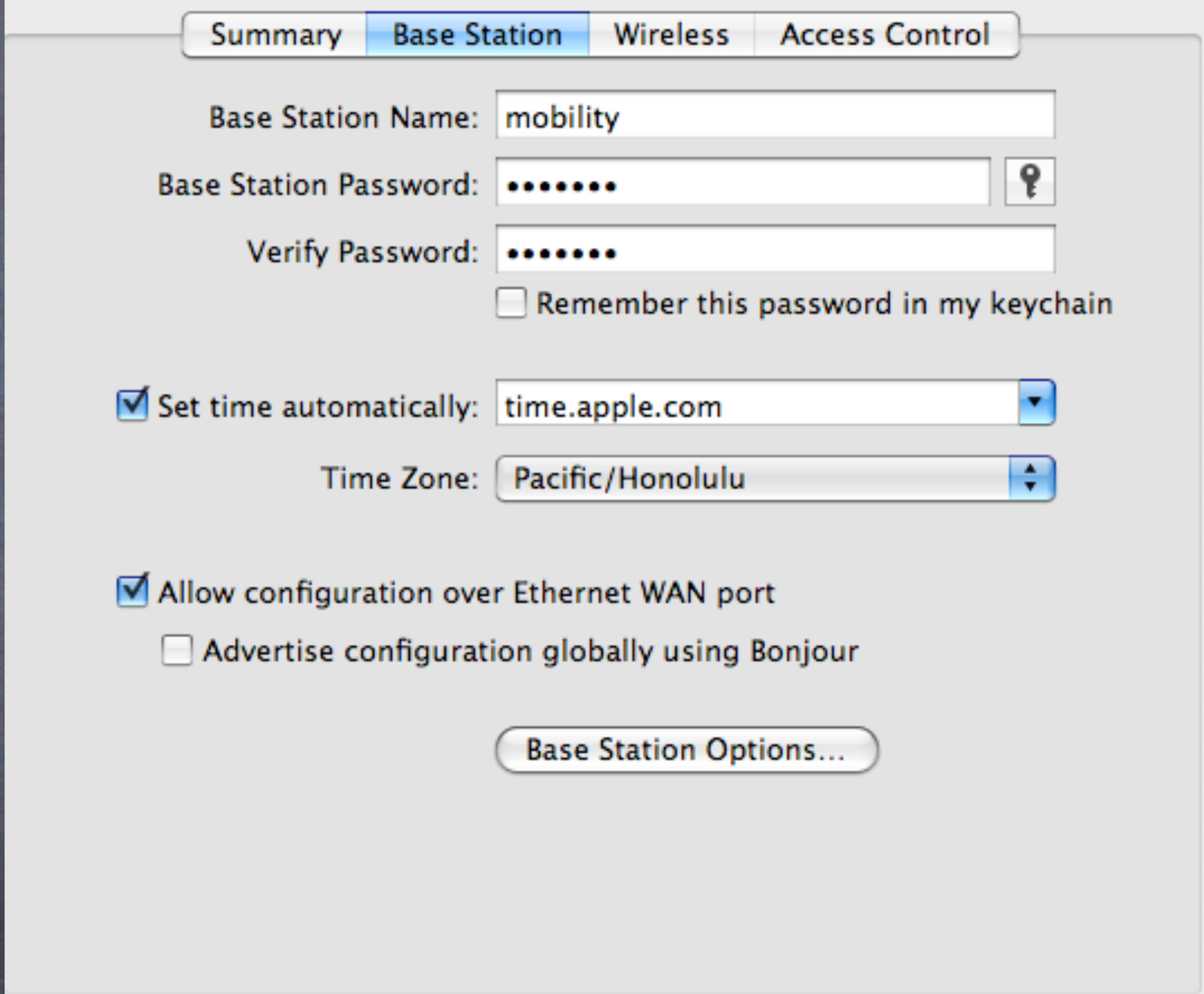
Wireless Clients: 3

Connect Using: Ethernet

IP Address: 67.99.198.133

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

Basic Wireless Access point setup



Base Station Name: mobility

Base Station Password: ••••••••

Verify Password: ••••••••

□ Remember this password in my keychain

☑ Set time automatically: time.apple.com

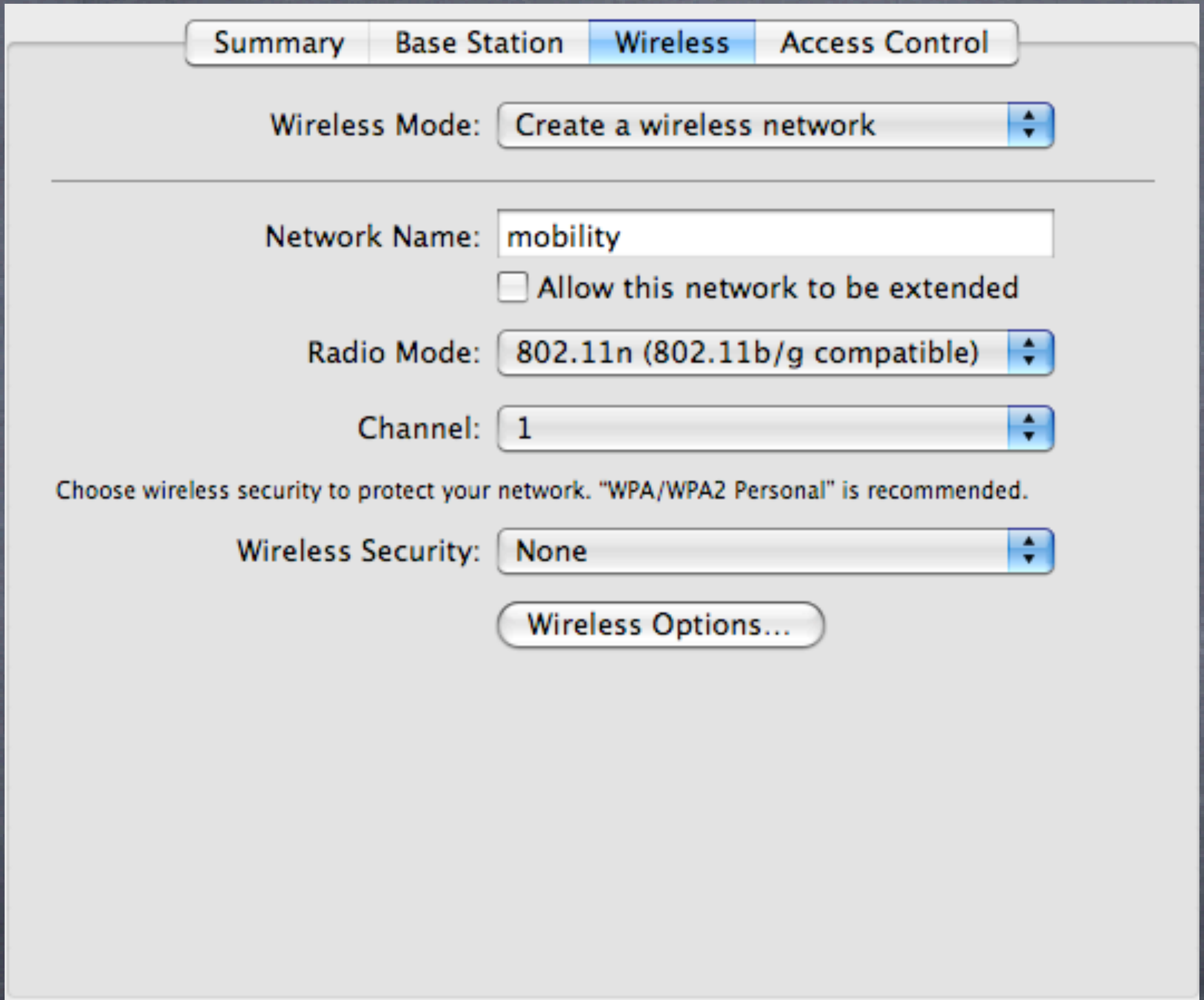
Time Zone: Pacific/Honolulu

☑ Allow configuration over Ethernet WAN port

□ Advertise configuration globally using Bonjour

- 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



Wireless Mode: Create a wireless network

Network Name: mobility

□ Allow this network to be extended

Radio Mode: 802.11n (802.11b/g compatible)

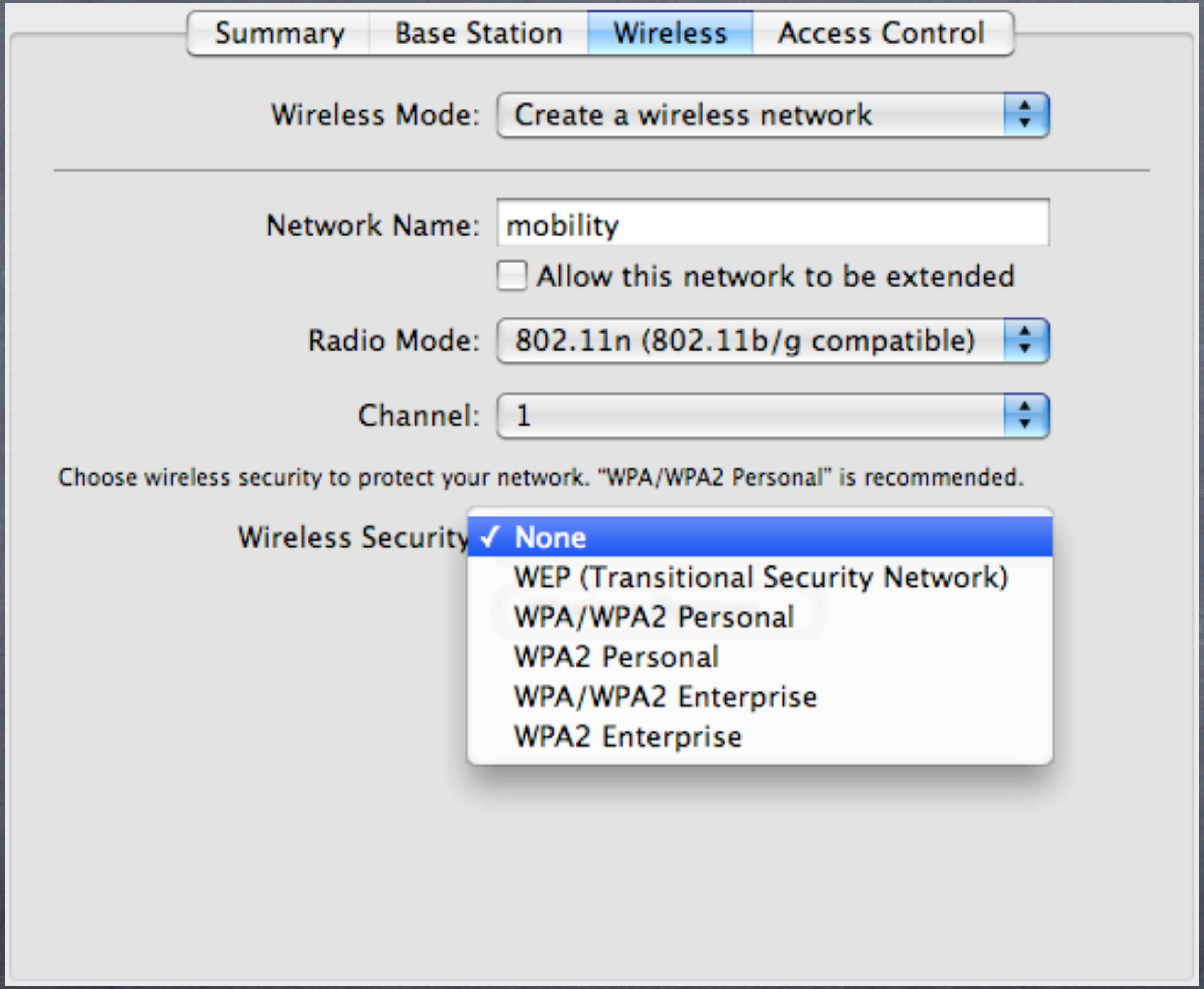
Channel: 1

Choose wireless security to protect your network. "WPA/WPA2 Personal" is recommended.

Wireless Security: None

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

Basic Wireless Access point setup



Wireless Mode: Create a wireless network

Network Name: mobility

□ Allow this network to be extended

Radio Mode: 802.11n (802.11b/g compatible)

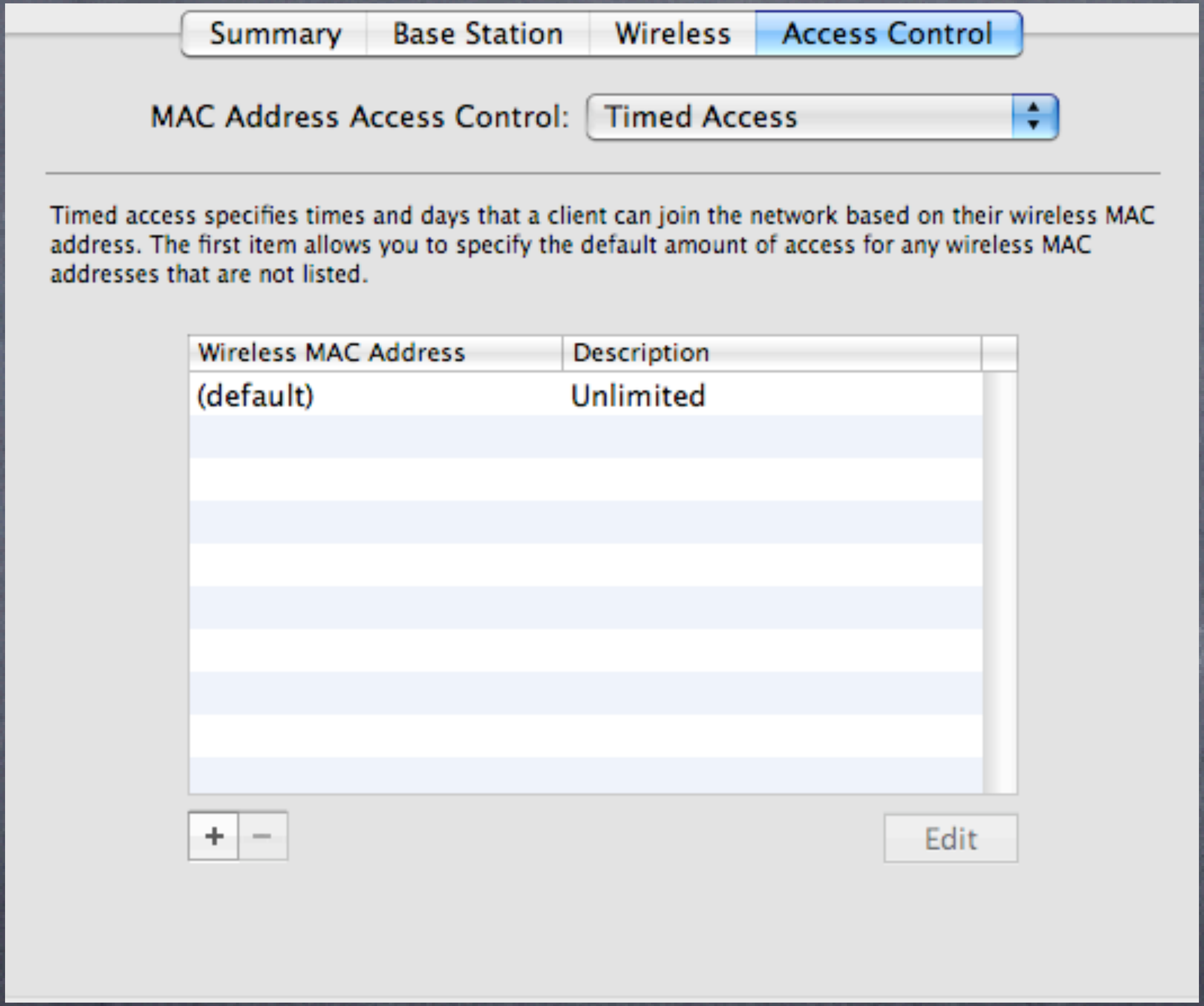
Channel: 1

Choose wireless security to protect your network. "WPA/WPA2 Personal" is recommended.

Wireless Security: ✓ None

- 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



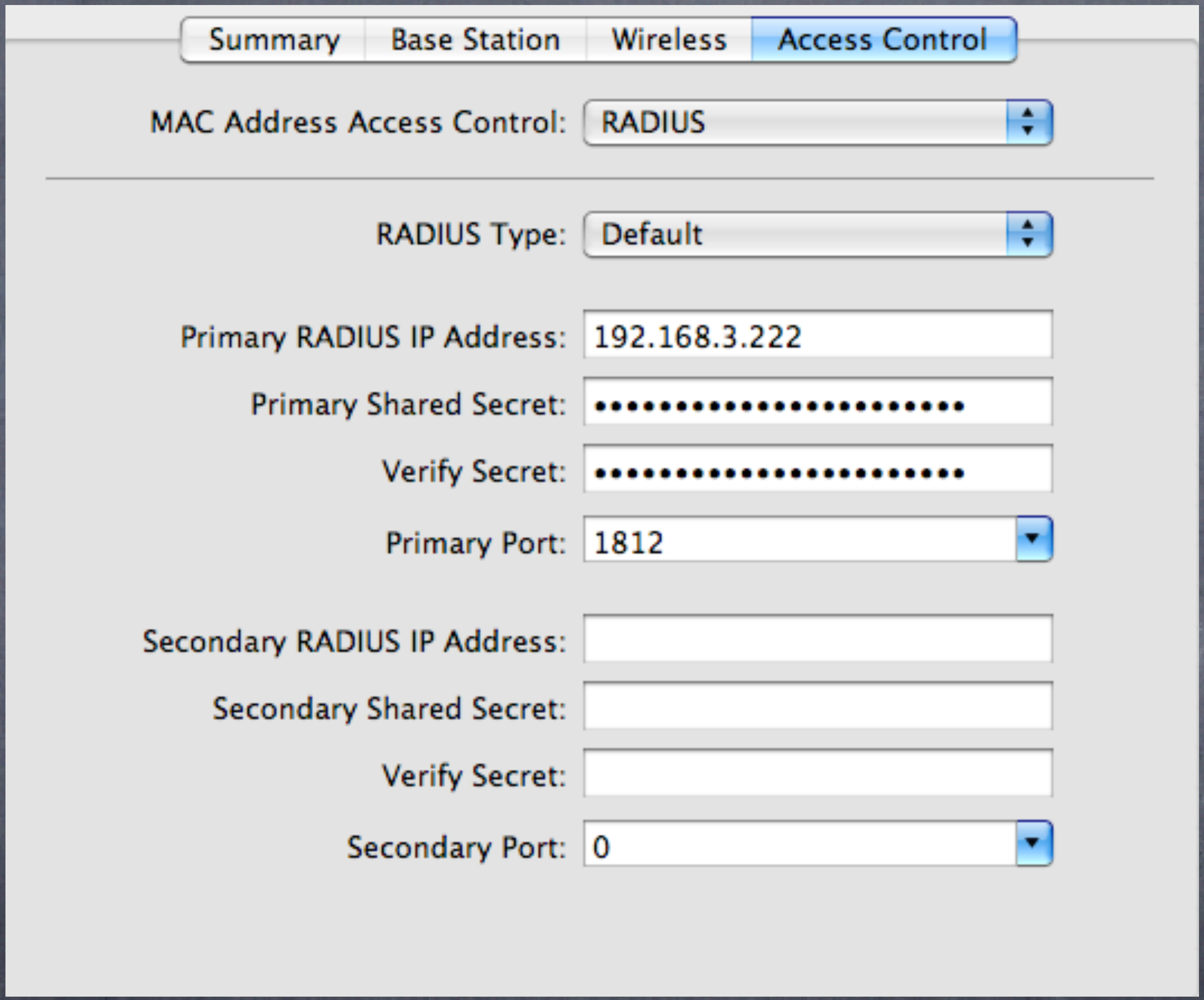
MAC Address Access Control: Timed Access

Timed access specifies times and days that a client can join the network based on their wireless MAC address. The first item allows you to specify the default amount of access for any wireless MAC addresses that are not listed.

Wireless MAC Address	Description
(default)	Unlimited

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

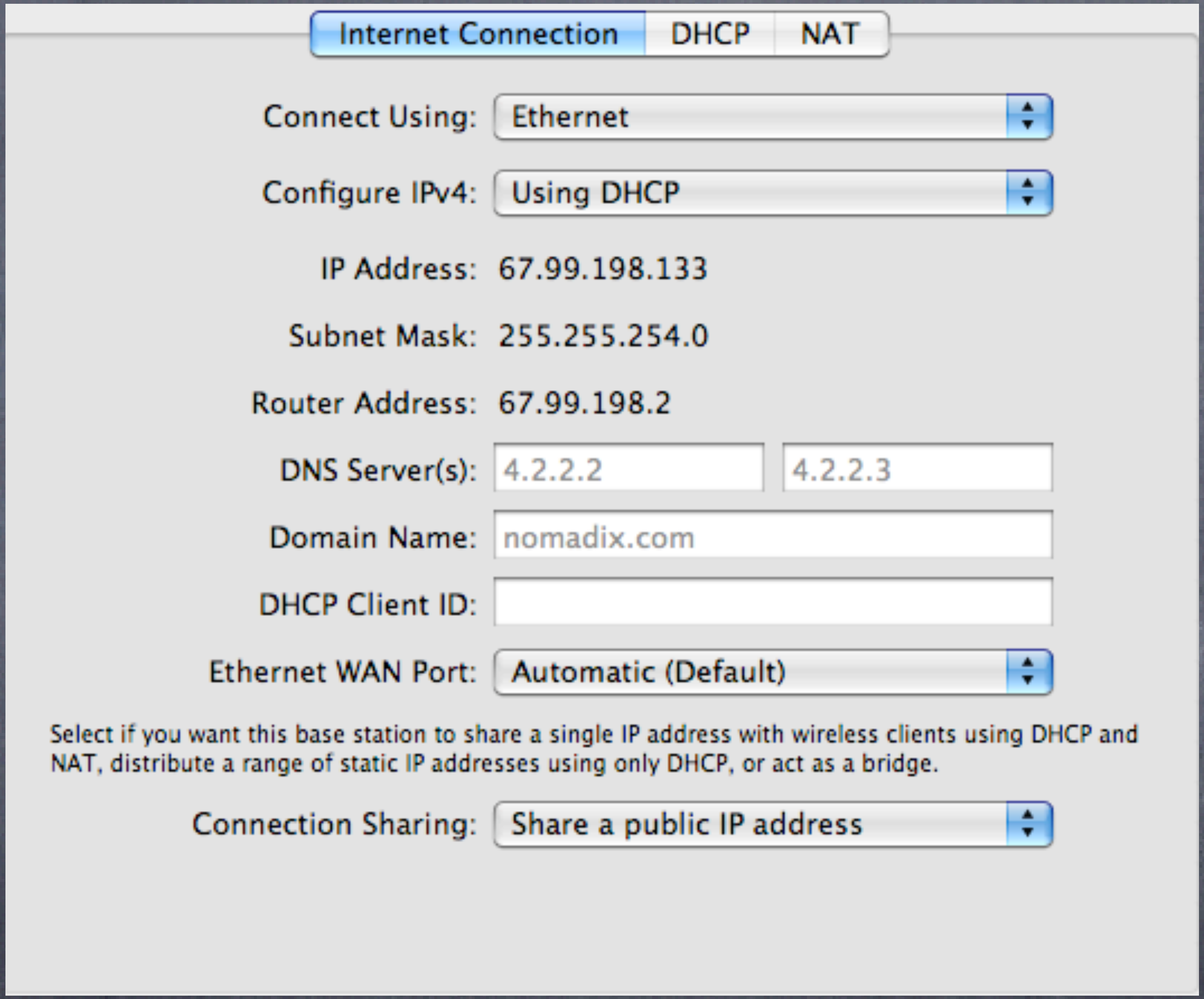
Basic Wireless Access point setup



MAC Address Access Control:	RADIUS
RADIUS Type:	Default
Primary RADIUS IP Address:	192.168.3.222
Primary Shared Secret:	••••••••••••••••••••••••
Verify Secret:	••••••••••••••••••••••••
Primary Port:	1812
Secondary RADIUS IP Address:	
Secondary Shared Secret:	
Verify Secret:	
Secondary Port:	0

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

Basic Wireless Access point setup



Connect Using: Ethernet

Configure IPv4: Using DHCP

IP Address: 67.99.198.133

Subnet Mask: 255.255.254.0

Router Address: 67.99.198.2

DNS Server(s): 4.2.2.2 4.2.2.3

Domain Name: nomadix.com

DHCP Client ID:

Ethernet WAN Port: Automatic (Default)

Select if you want this base station to share a single IP address with wireless clients using DHCP and NAT, distribute a range of static IP addresses using only DHCP, or act as a bridge.

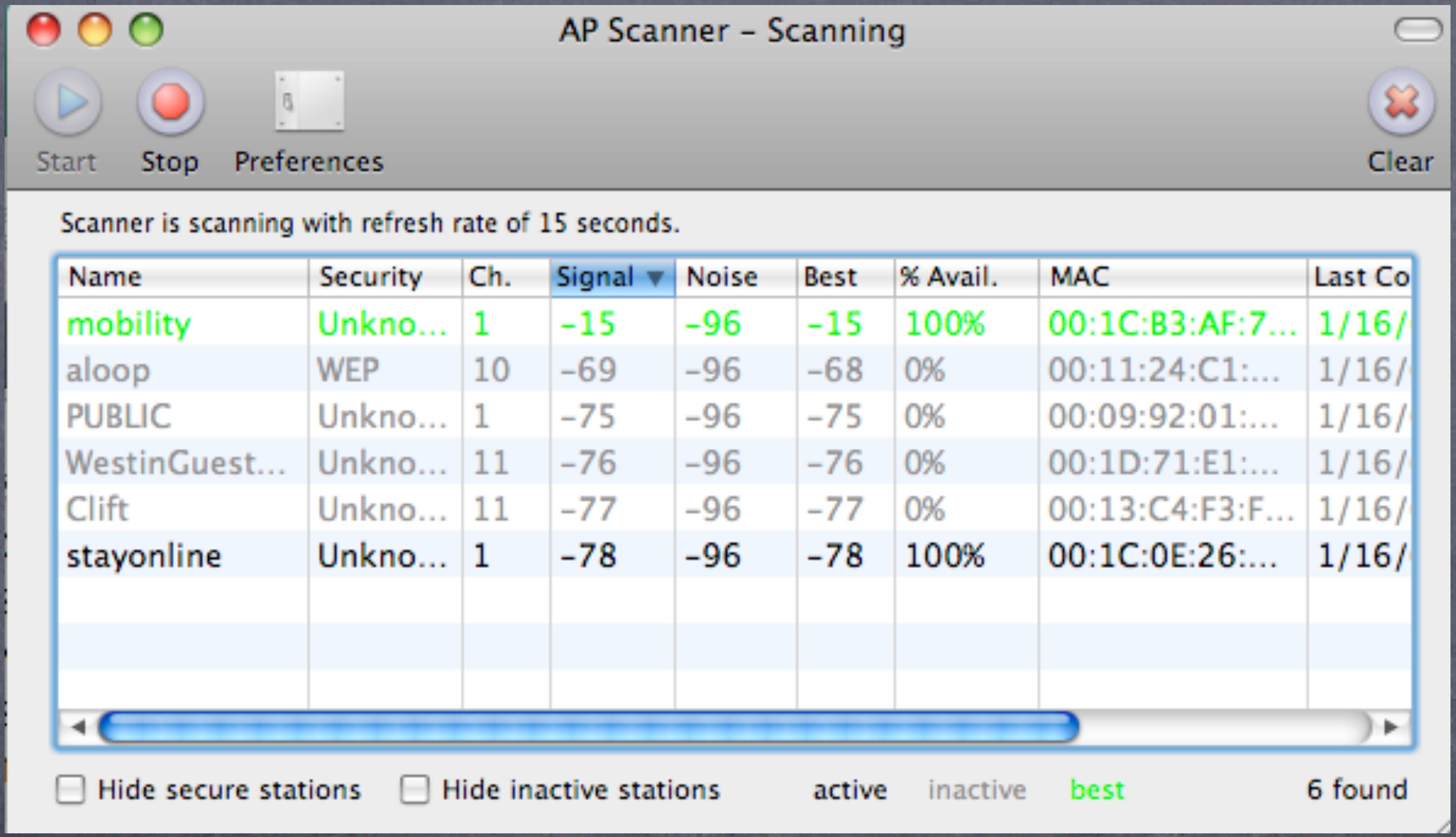
Connection Sharing: Share a public IP address

- 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



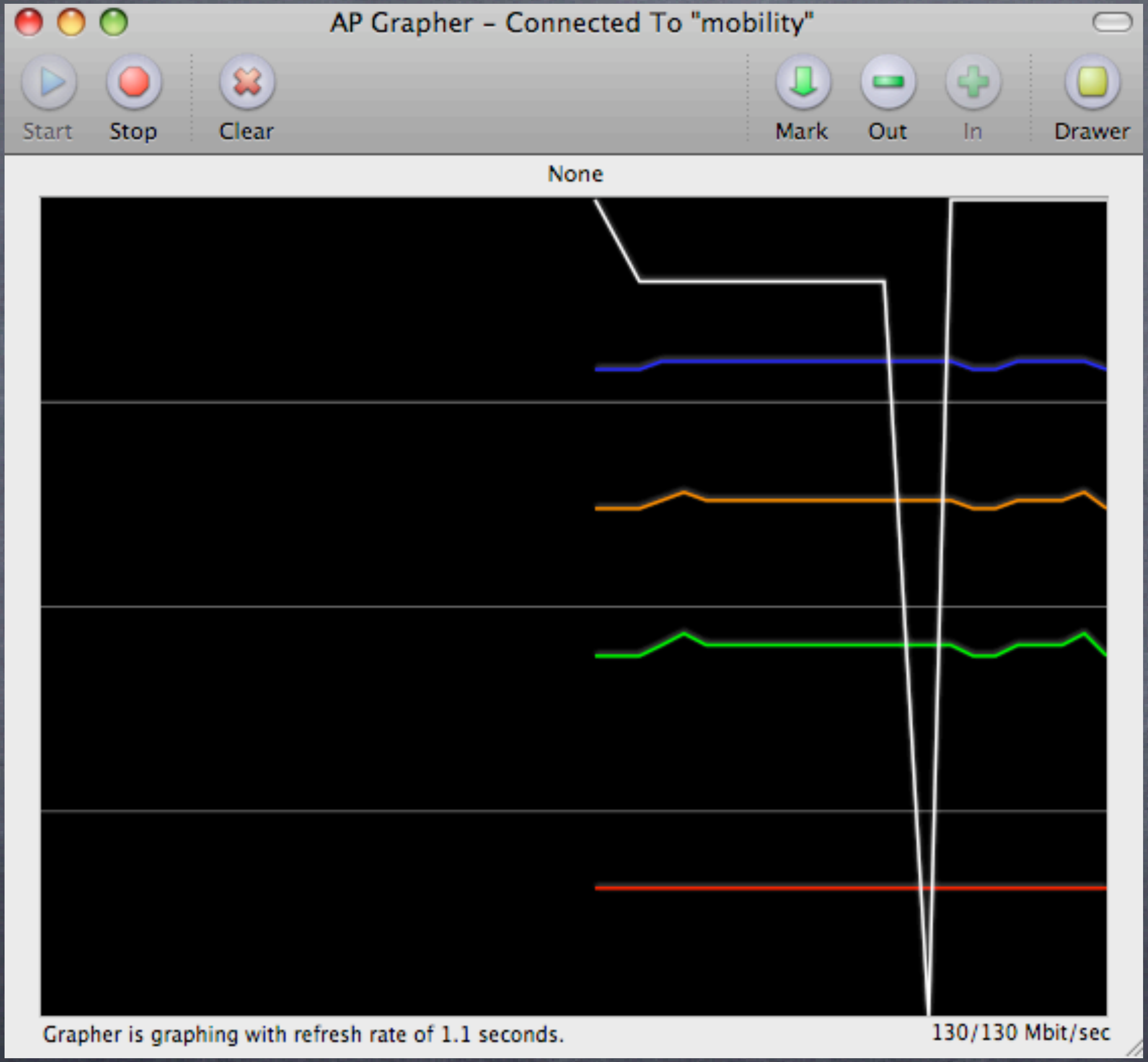
Scanner is scanning with refresh rate of 15 seconds.

Name	Security	Ch.	Signal ▾	Noise	Best	% Avail.	MAC	Last Co
mobility	Unkno...	1	-15	-96	-15	100%	00:1C:B3:AF:7...	1/16/
aloop	WEP	10	-69	-96	-68	0%	00:11:24:C1:...	1/16/
PUBLIC	Unkno...	1	-75	-96	-75	0%	00:09:92:01:...	1/16/
WestinGuest...	Unkno...	11	-76	-96	-76	0%	00:1D:71:E1:...	1/16/
Clift	Unkno...	11	-77	-96	-77	0%	00:13:C4:F3:F...	1/16/
stayonline	Unkno...	1	-78	-96	-78	100%	00:1C:0E:26:...	1/16/

☐ Hide secure stations ☐ Hide inactive stations active inactive best 6 found

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

Basic Wireless Access point setup

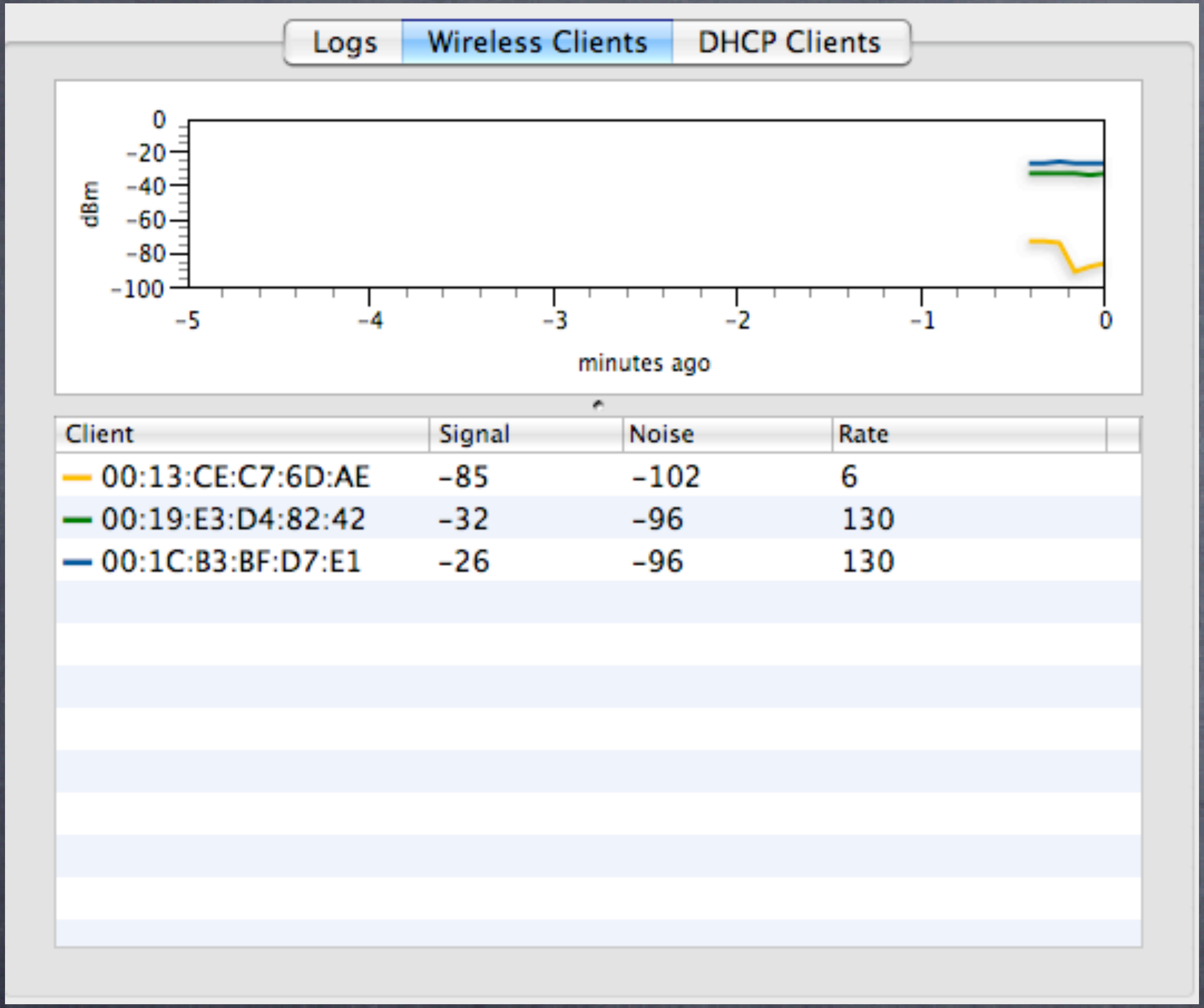


Grapher is graphing with refresh rate of 1.1 seconds.

130/130 Mbit/sec

- Access point graph
- note speed and other stats

Basic Wireless Access point monitoring: take two



Client	Signal	Noise	Rate
🟨 00:13:CE:C7:6D:AE	-85	-102	6
🟩 00:19:E3:D4:82:42	-32	-96	130
🟦 00:1C:B3:BF:D7:E1	-26	-96	130

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