Hands-on Mac lab
Wireless Basics

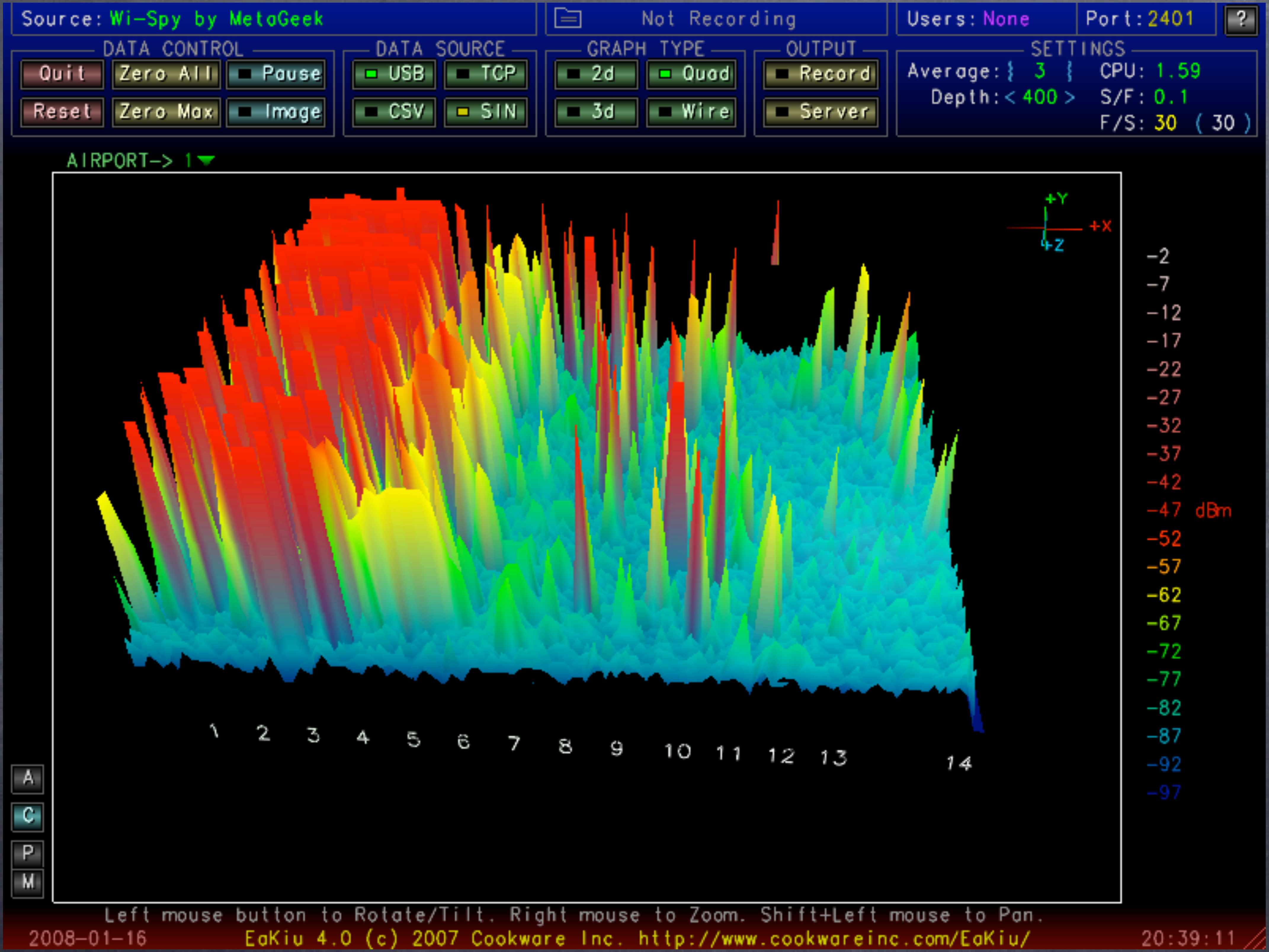
What you need to know to setup and use your wireless networks with safety and reliability

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

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 } CPU: 1.59

Depth: < 400 > S/F: 0.1

F/S: 30 (30)

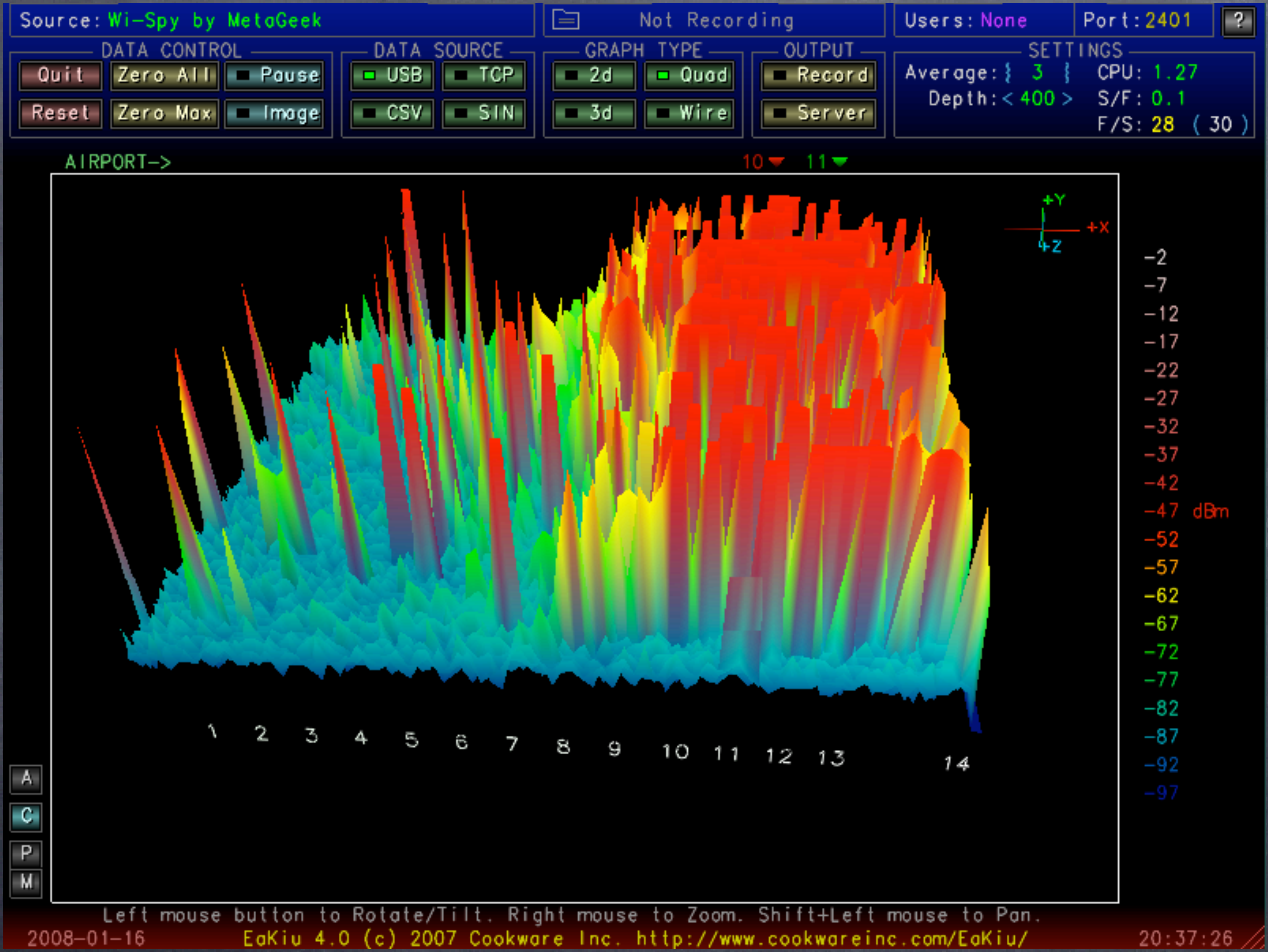
AIRPORT-> 1

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.

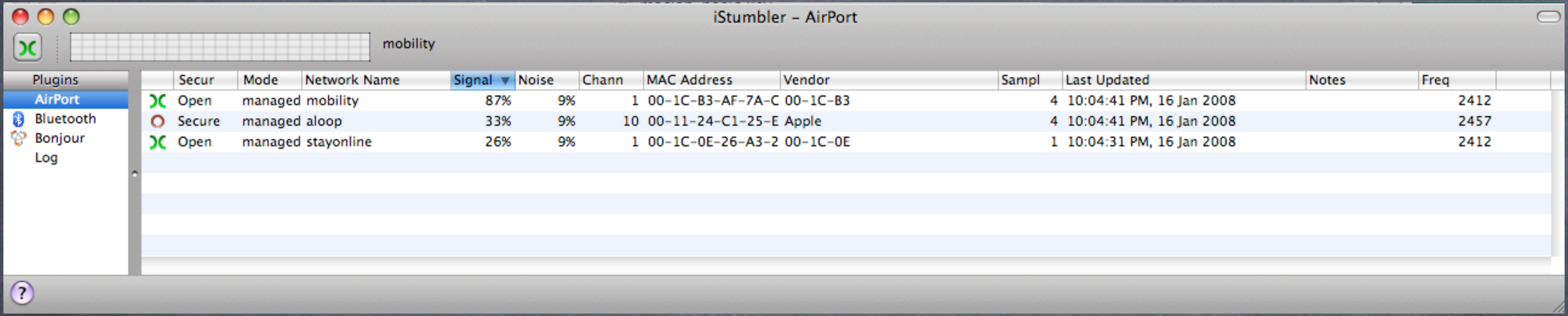
2008-01-16 EaKiu 4.0 (c) 2007 Cookware Inc. http://www.cookwareinc.com/EaKiu/ 20:37:26

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

iStumbler: now you try



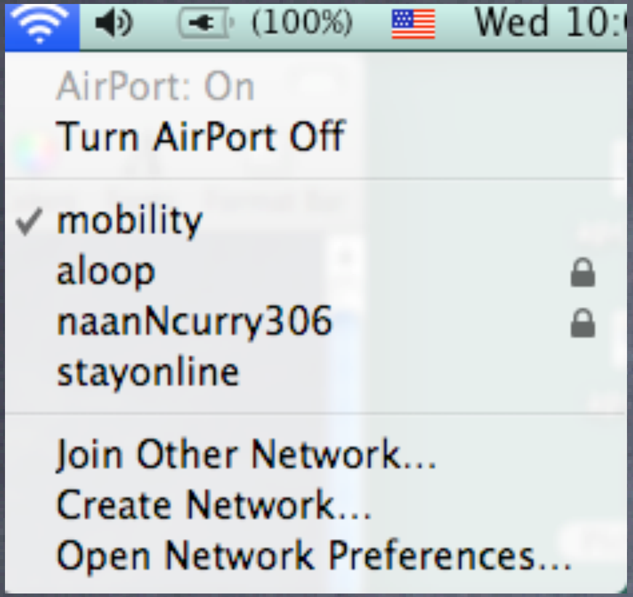
	Secur	Mode	Network Name	Signal ▼	Noise	Chann	MAC Address	Vendor	Sampl	Last Updated	Notes	Freq
)(	Open	managed	mobility	87%	9%	1	00-1C-B3-AF-7A-C	00-1C-B3	4	10:04:41 PM, 16 Jan 2008		2412
○	Secure	managed	aloop	33%	9%	10	00-11-24-C1-25-E	Apple	4	10:04:41 PM, 16 Jan 2008		2457
)(	Open	managed	stayonline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

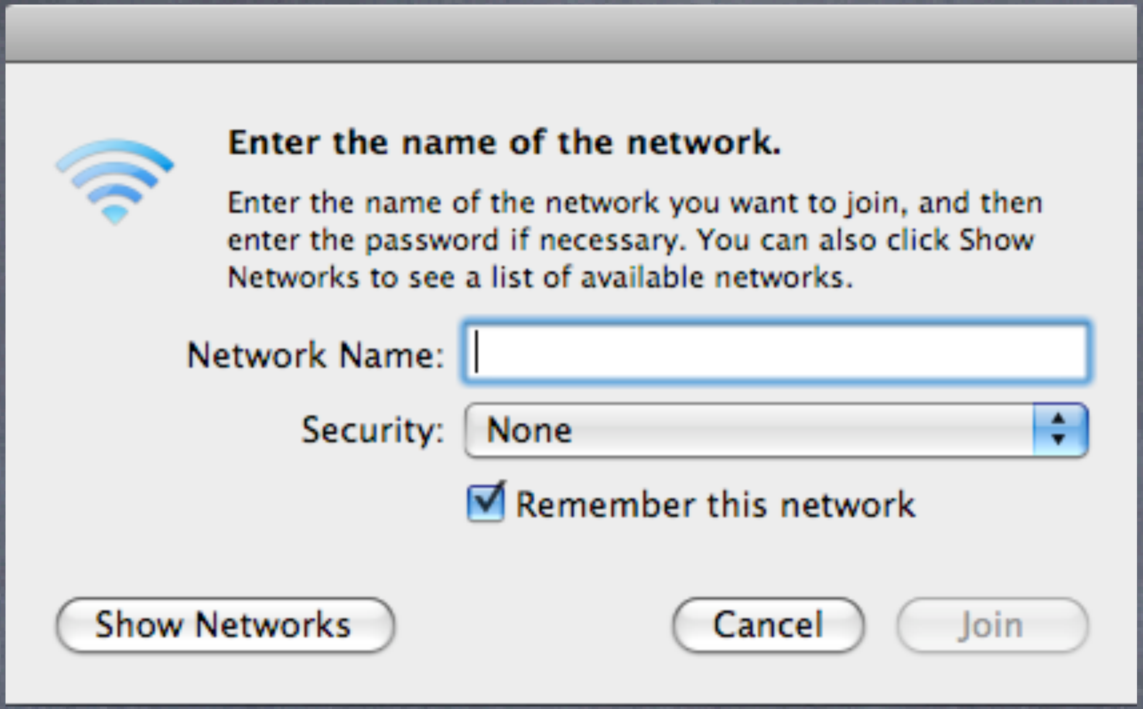
- Notice:
    - security
    - modes
    - signal/noise
    - MAC address
    - signal graph
    - war chalking signs

Basic Wireless client setup

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

Basic Wireless client setup





Enter the name of the network.

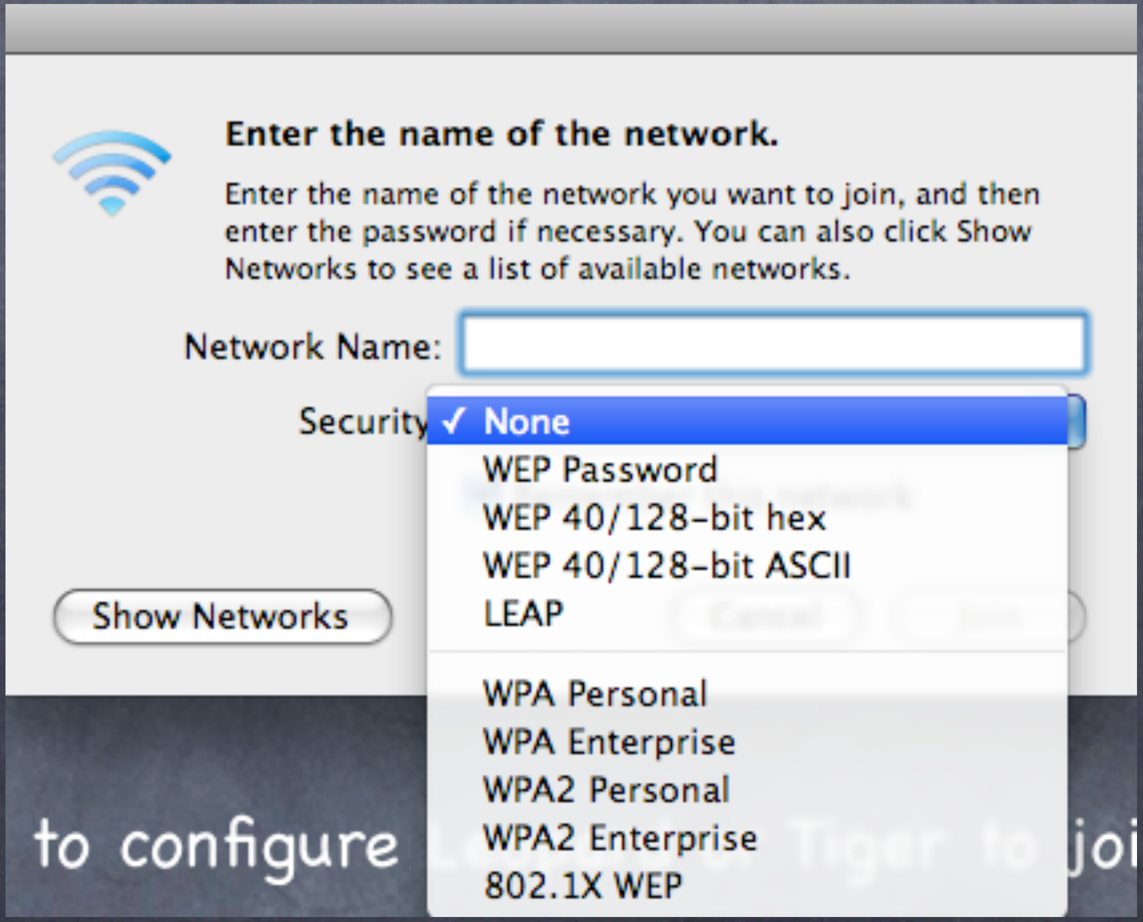
Enter the name of the network you want to join, and then enter the password if necessary. You can also click Show Networks to see a list of available networks.

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



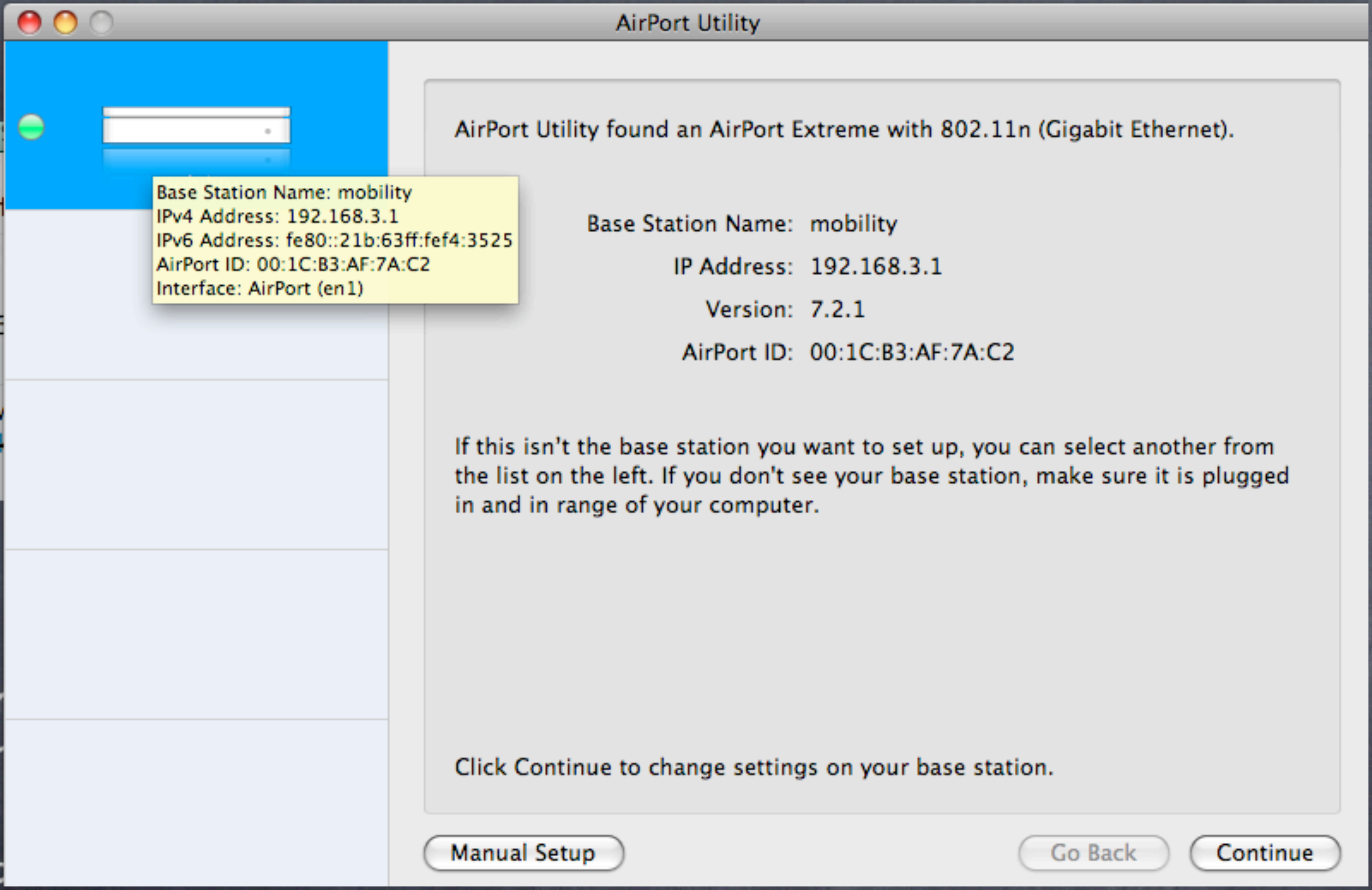
Enter the name of the network.

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

Basic Wireless Access point setup



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).

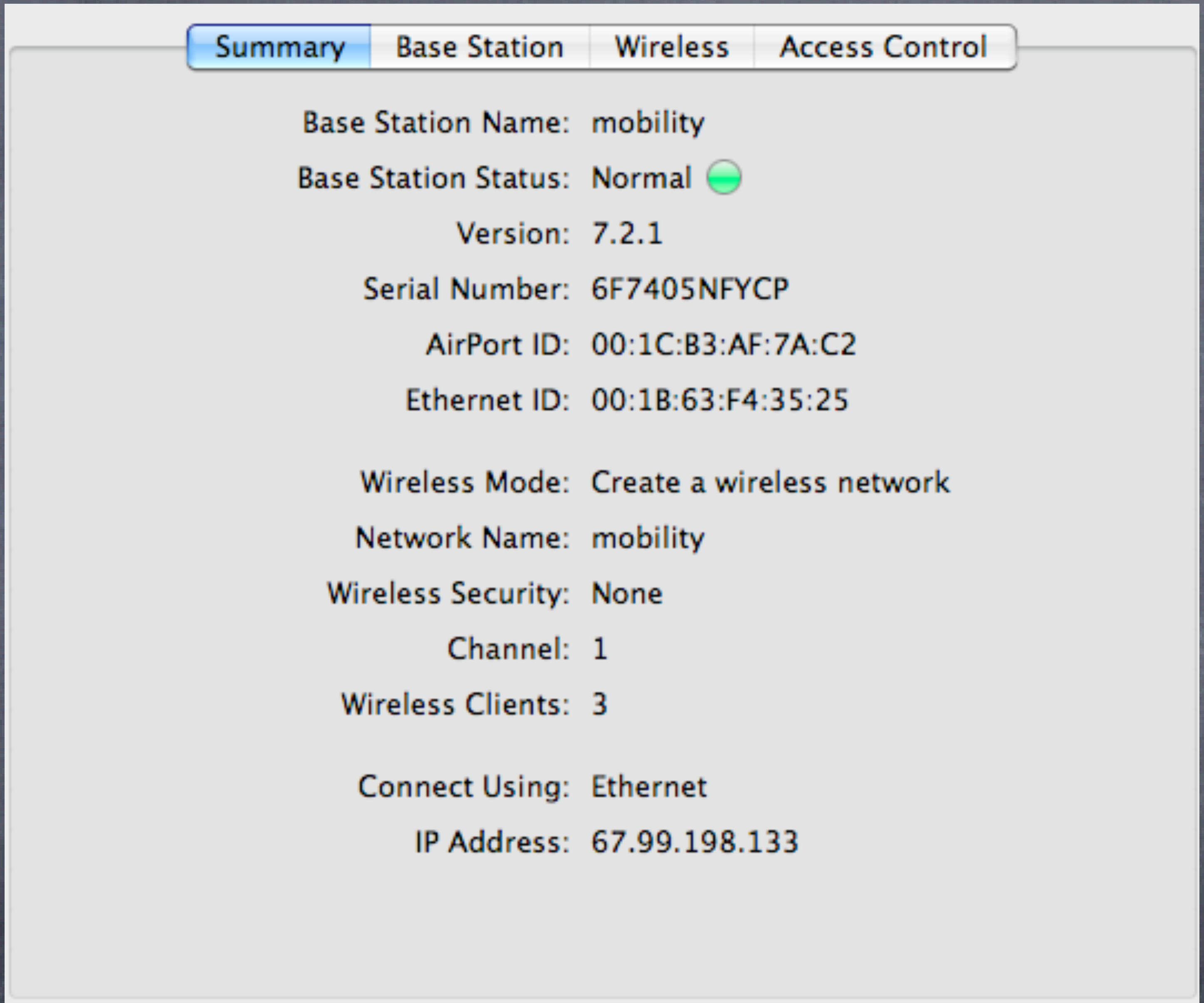
Base Station Name: mobility
IP Address: 192.168.3.1
Version: 7.2.1
AirPort ID: 00:1C:B3:AF:7A:C2

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



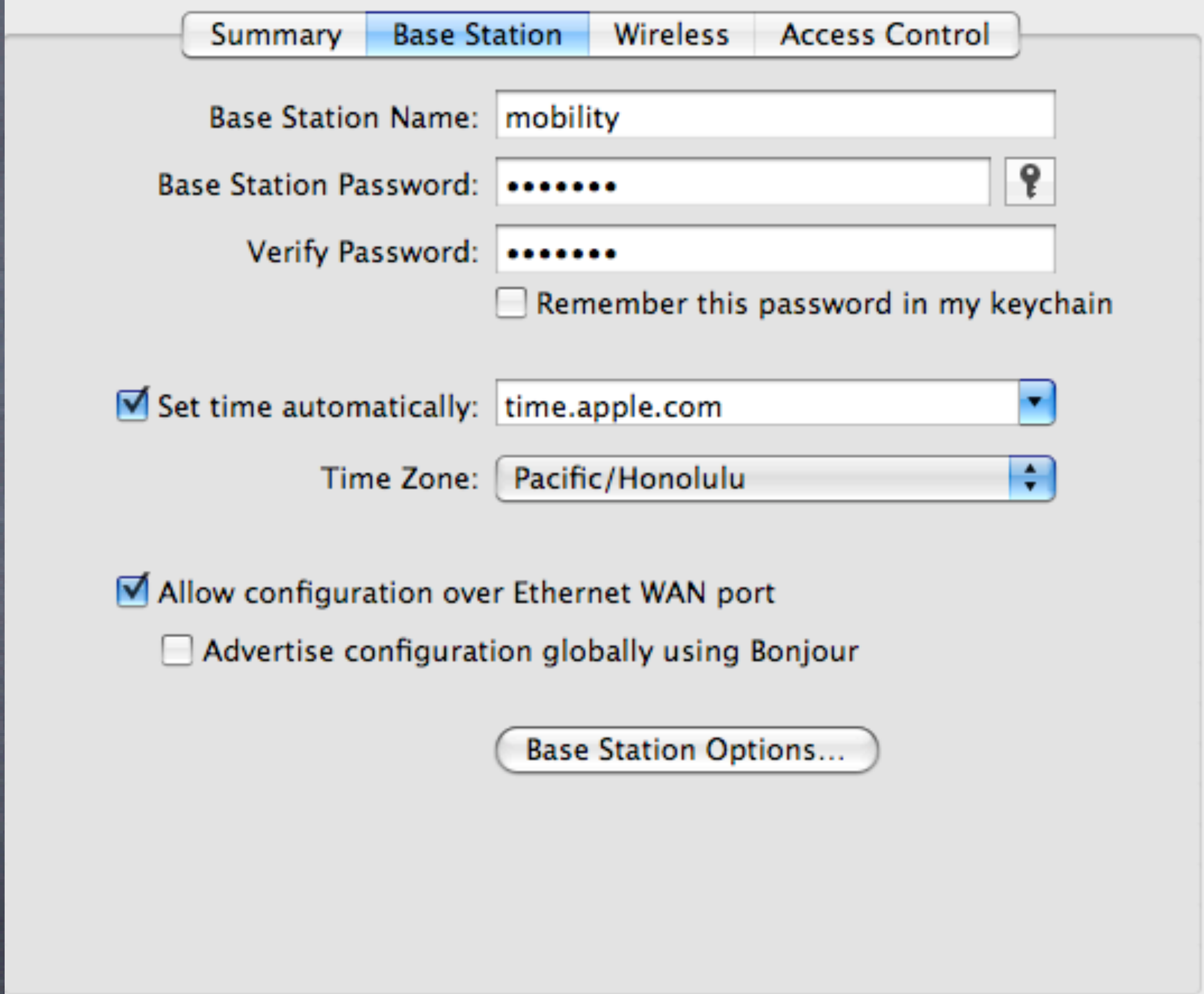
Base Station Name: mobility
Base Station Status: Normal ●
Version: 7.2.1
Serial Number: 6F7405NFYCP
AirPort ID: 00:1C:B3:AF:7A:C2
Ethernet ID: 00:1B:63:F4:35:25

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

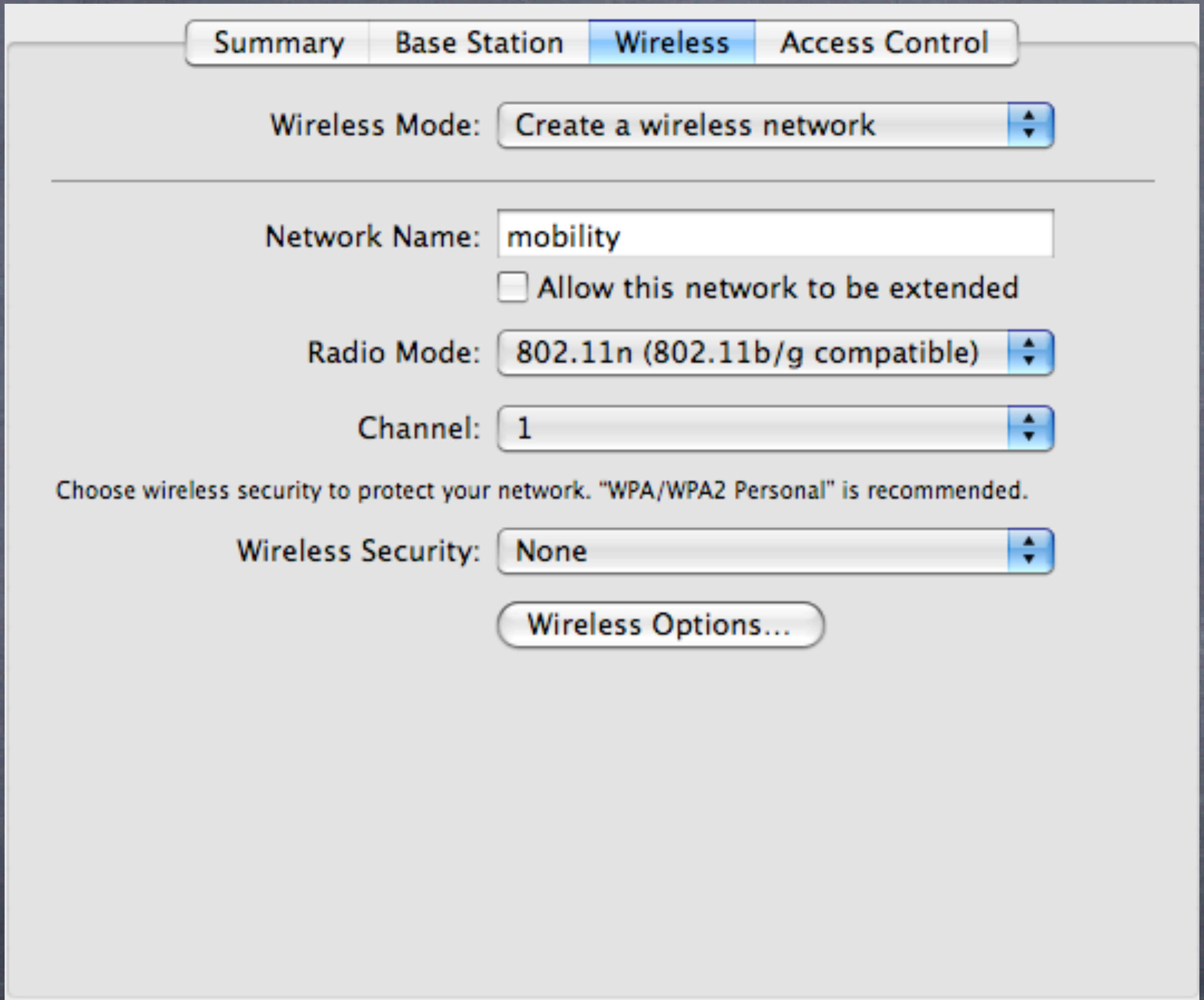
Time Zone: Pacific/Honolulu

☑ 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)

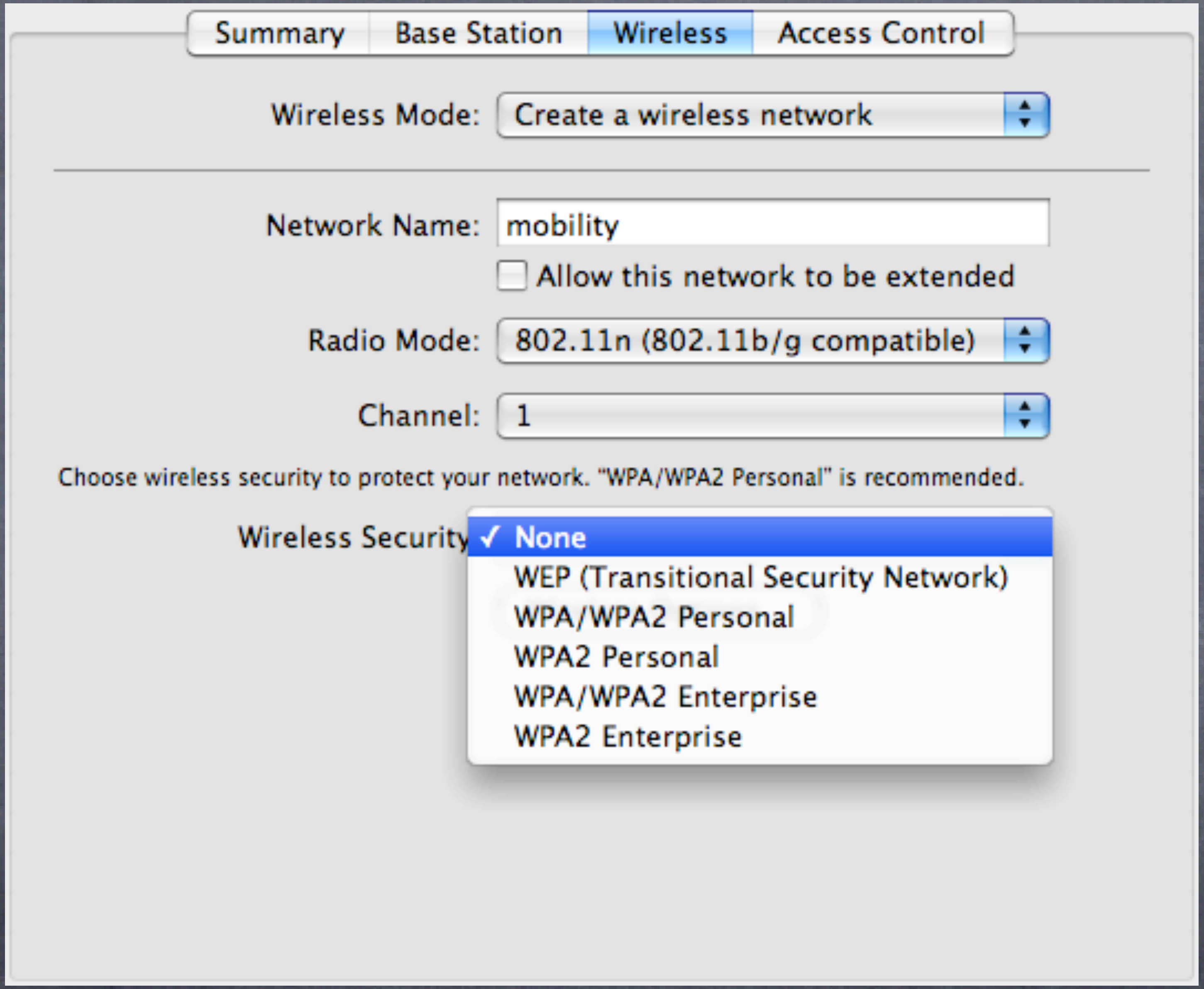
Channel: 1

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)

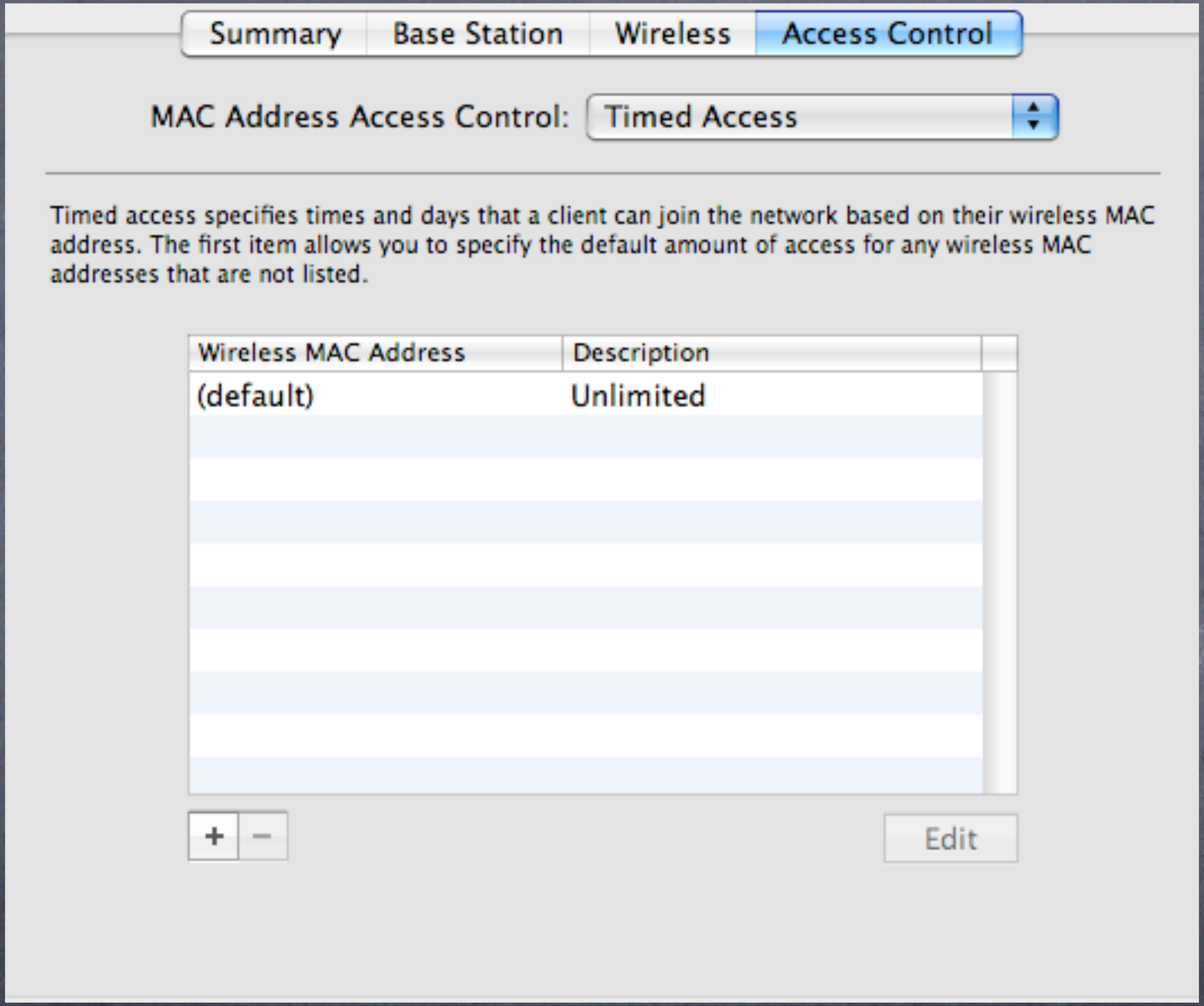
Channel: 1

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



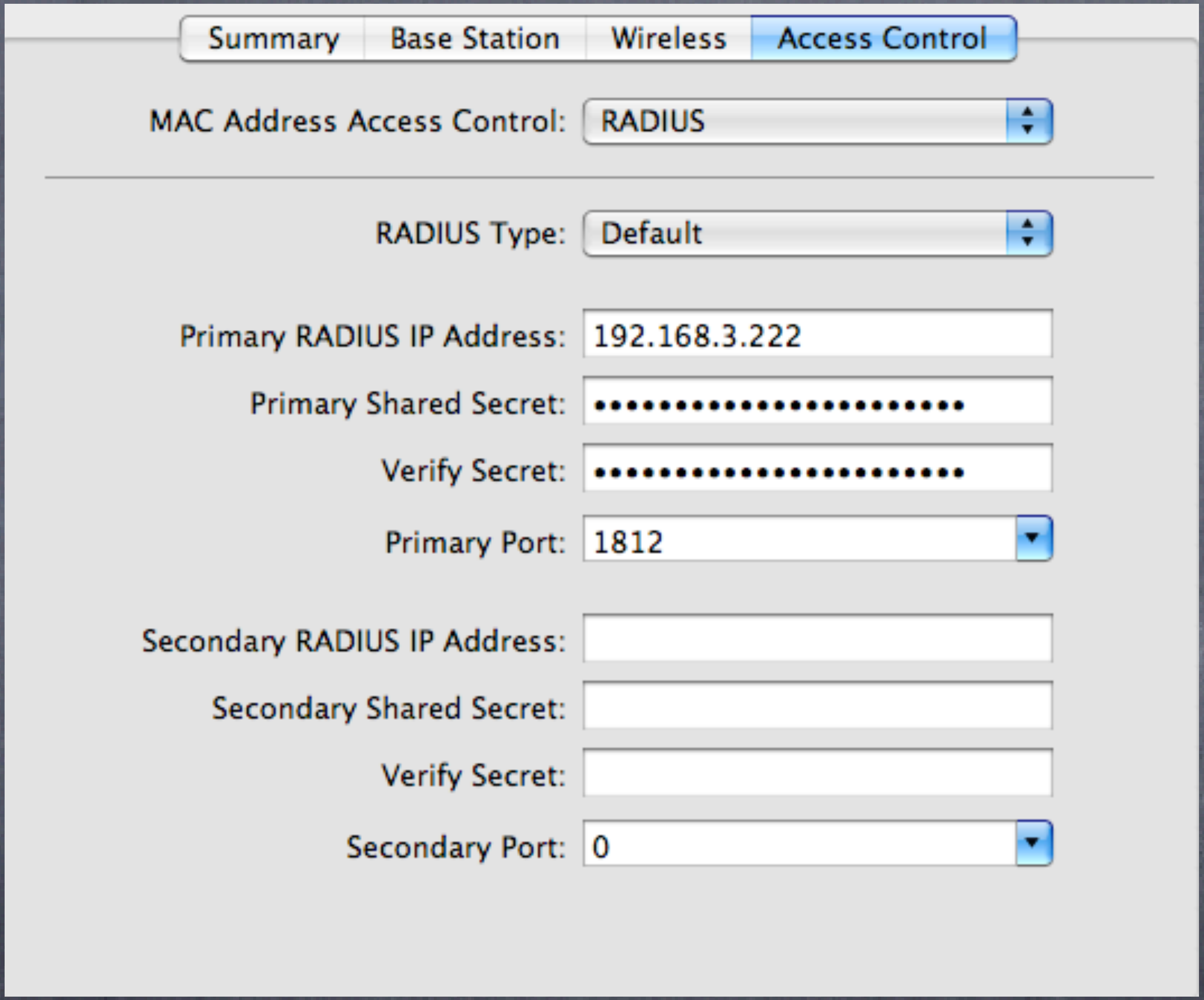
MAC Address Access Control: Timed Access

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:

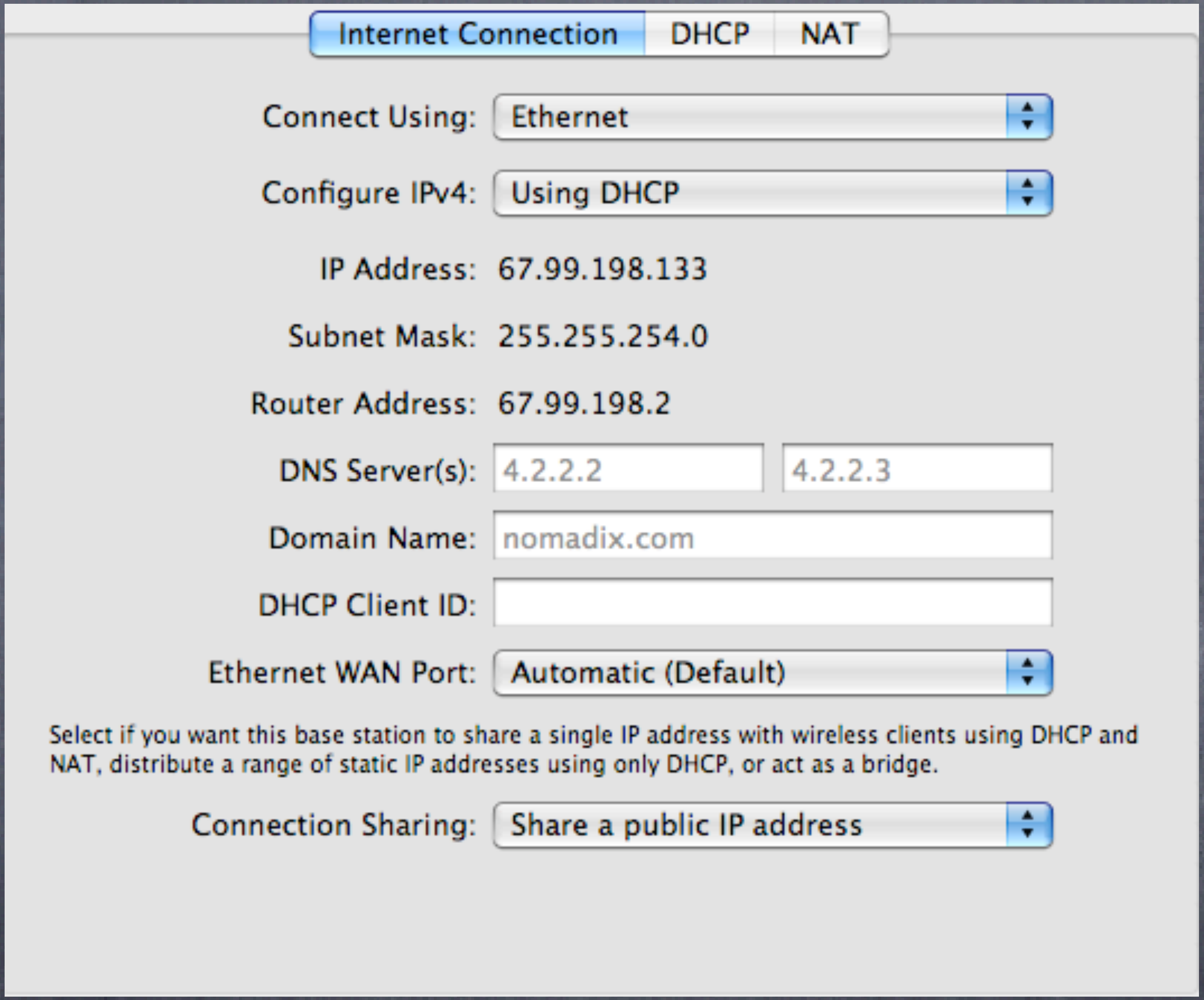
Secondary Shared Secret:

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.

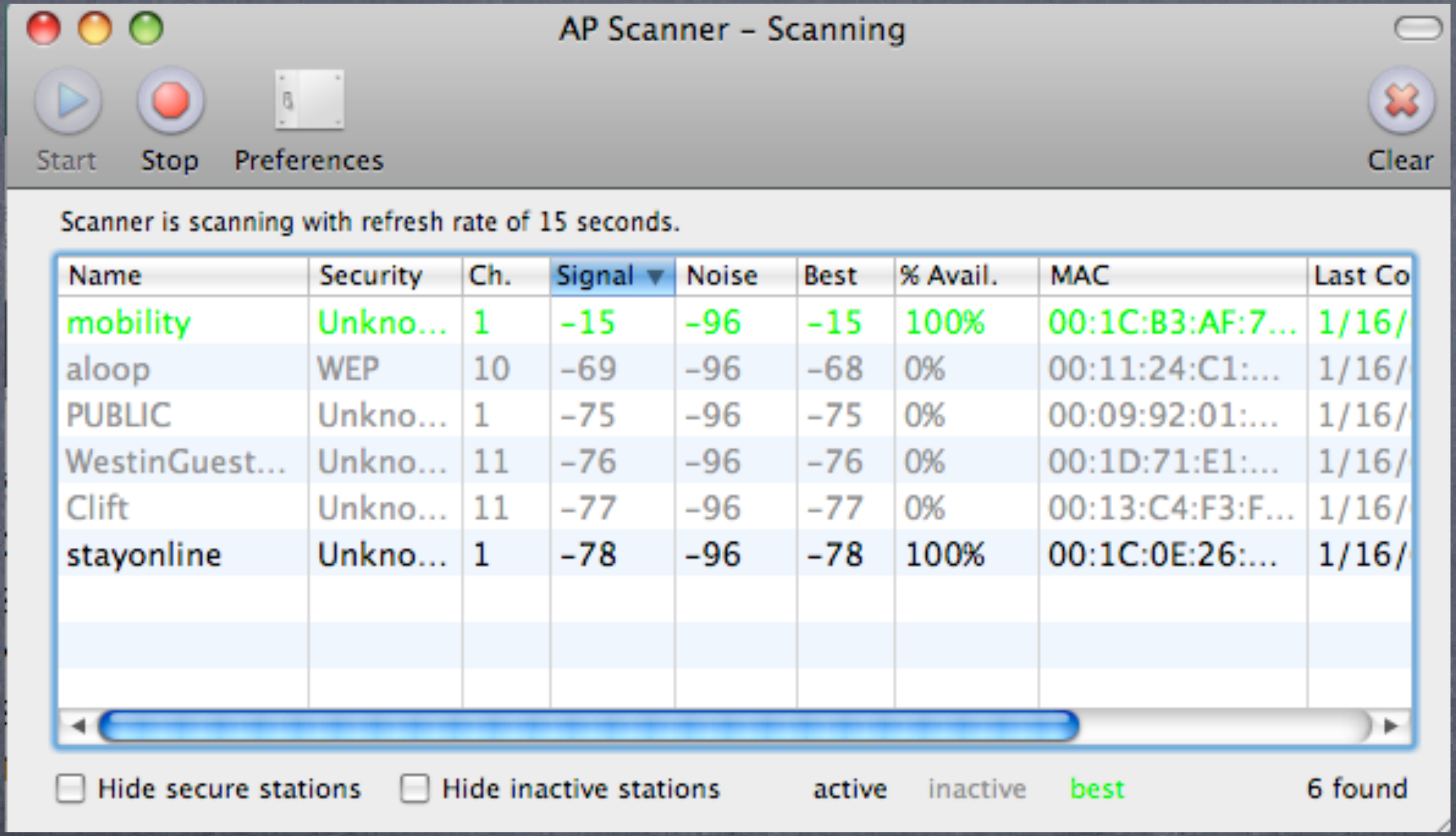
Connection Sharing: Share a public IP address

- 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



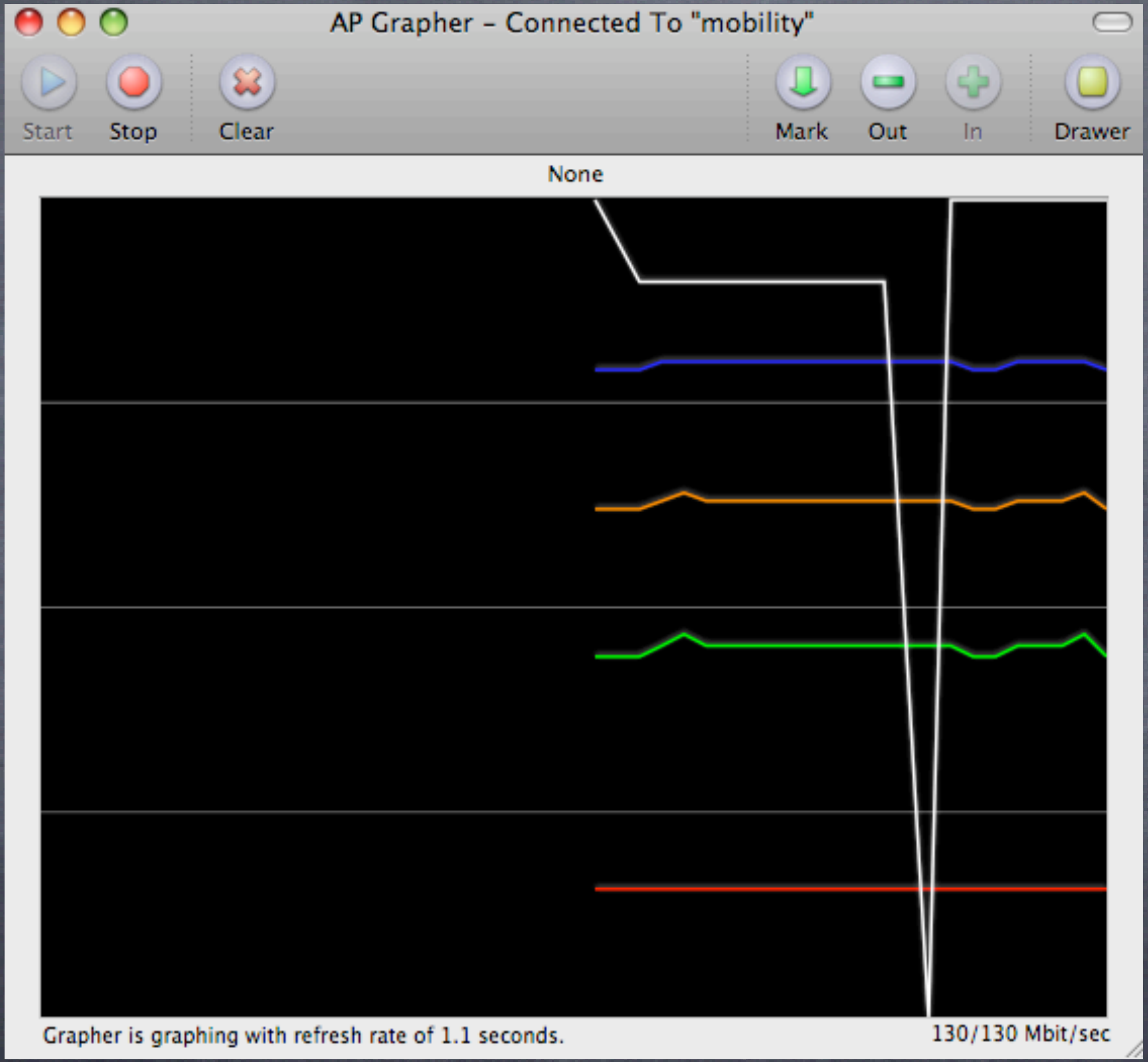
Scanner is scanning with refresh rate of 15 seconds.

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

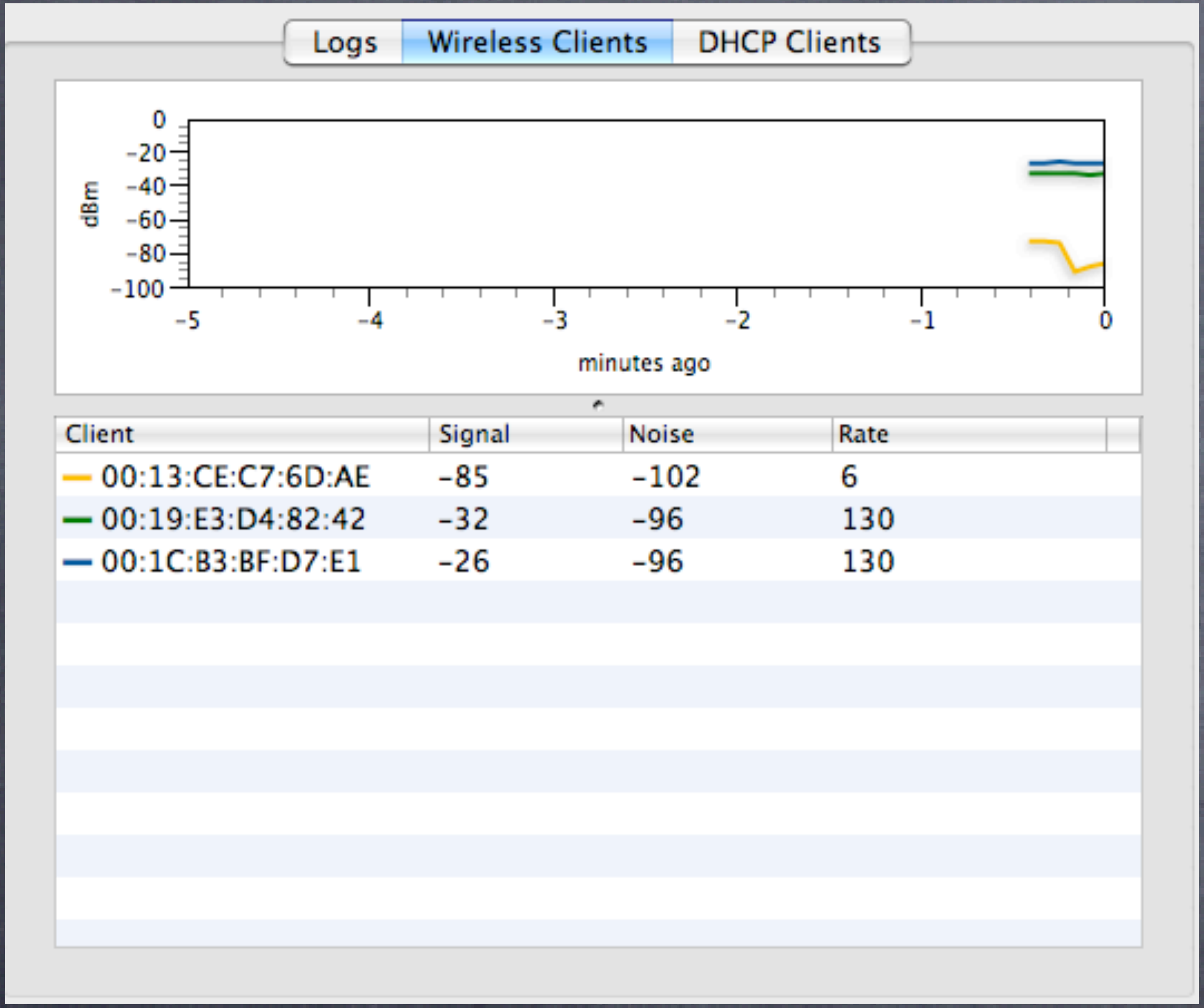


Grapher is graphing with refresh rate of 1.1 seconds.

130/130 Mbit/sec

- Access point graph
- note speed and other stats

Basic Wireless Access point monitoring: take two



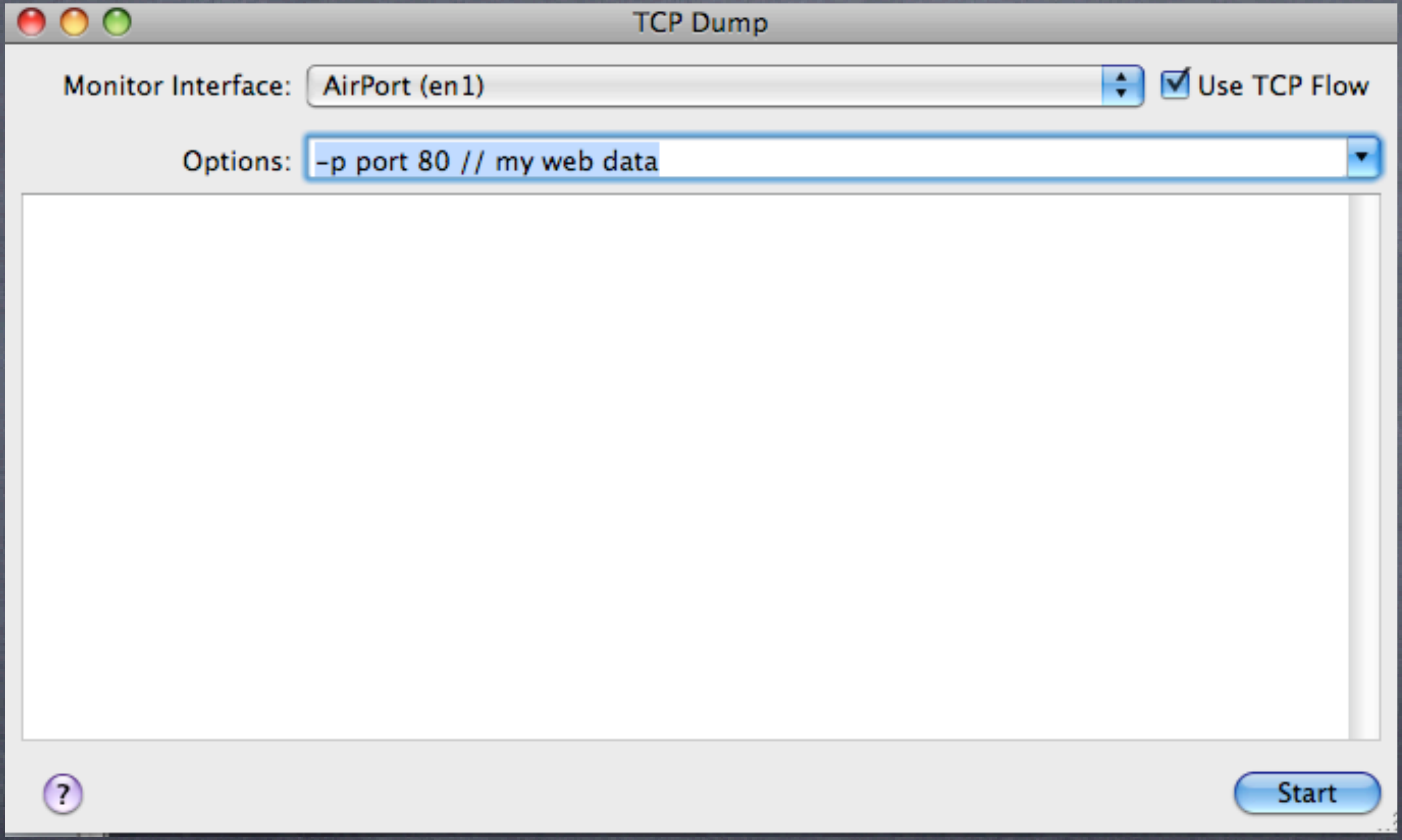
Client	Signal	Noise	Rate
🟨 00:13:CE:C7:6D:AE	-85	-102	6
🟩 00:19:E3:D4:82:42	-32	-96	130
🟦 00:1C:B3:BF:D7:E1	-26	-96	130

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

Security 101: packet sniffing

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

Security 101: packet sniffing



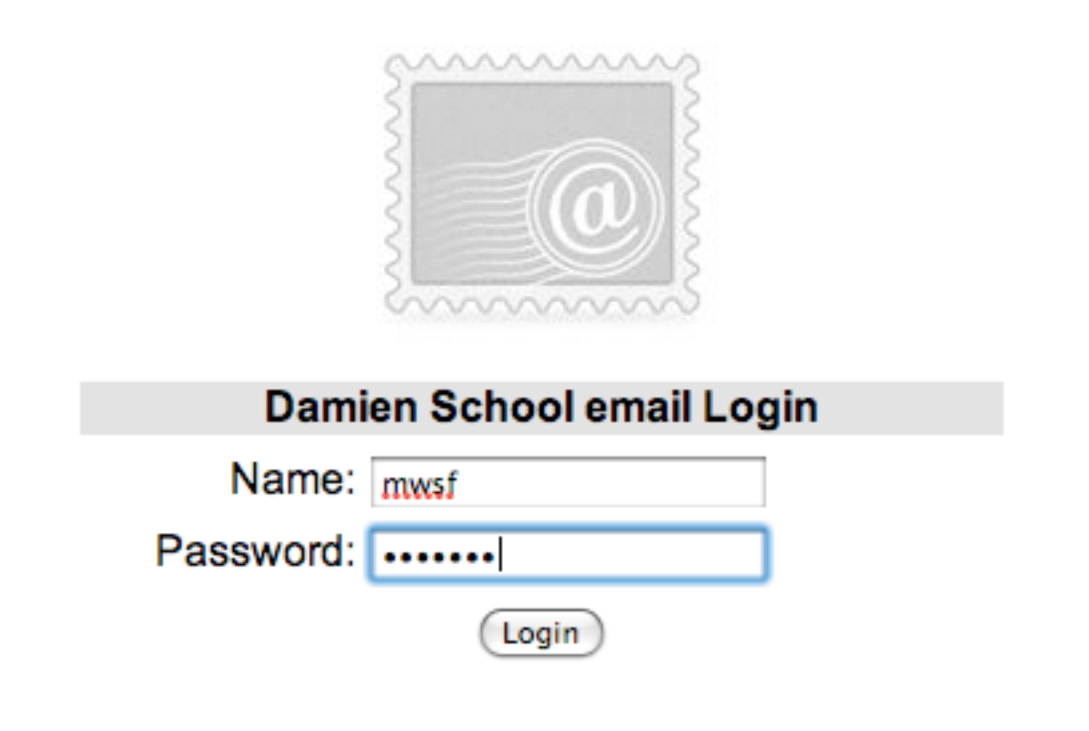
Monitor Interface: AirPort (en1)

☑ Use TCP Flow

Options: -p port 80 // my web data

IP Net Monitor TCPdump console

Security 101: packet sniffing



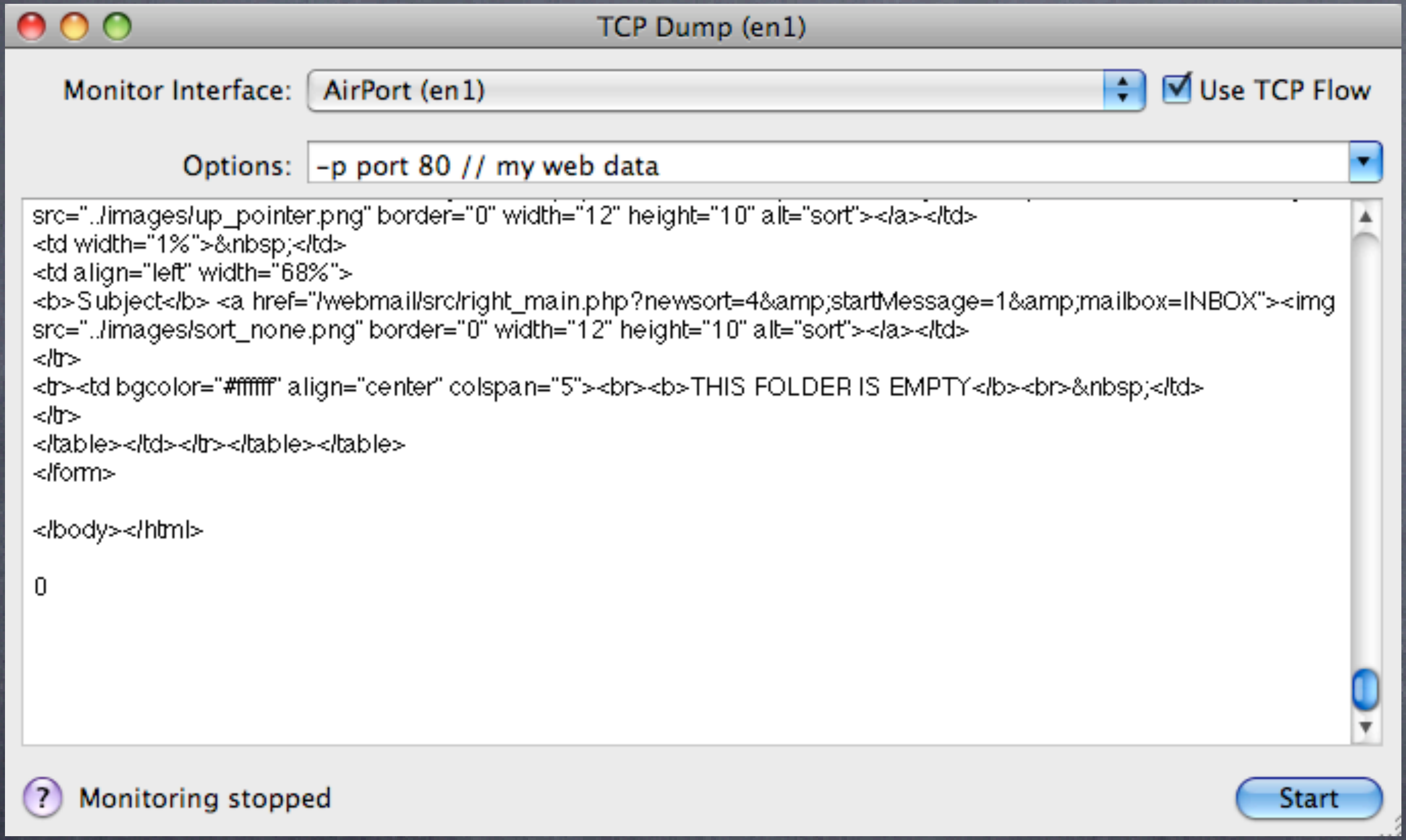
Damien School email Login

Name: mwsf

Password: •••••••

Login to webmail or other app

Security 101: packet sniffing



Monitor Interface: AirPort (en1)

☑ Use TCP Flow

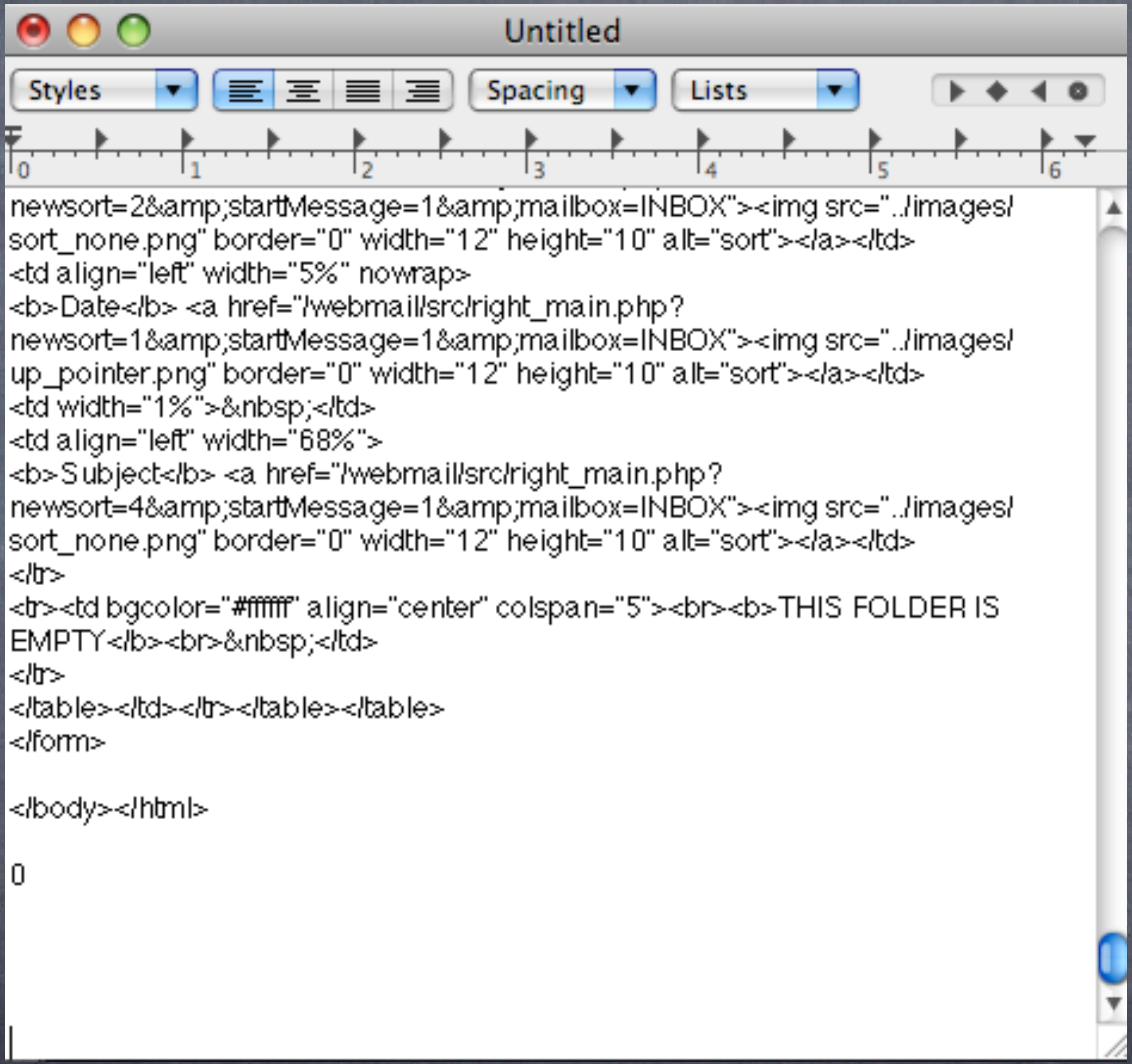
Options: -p port 80 // my web data

```
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

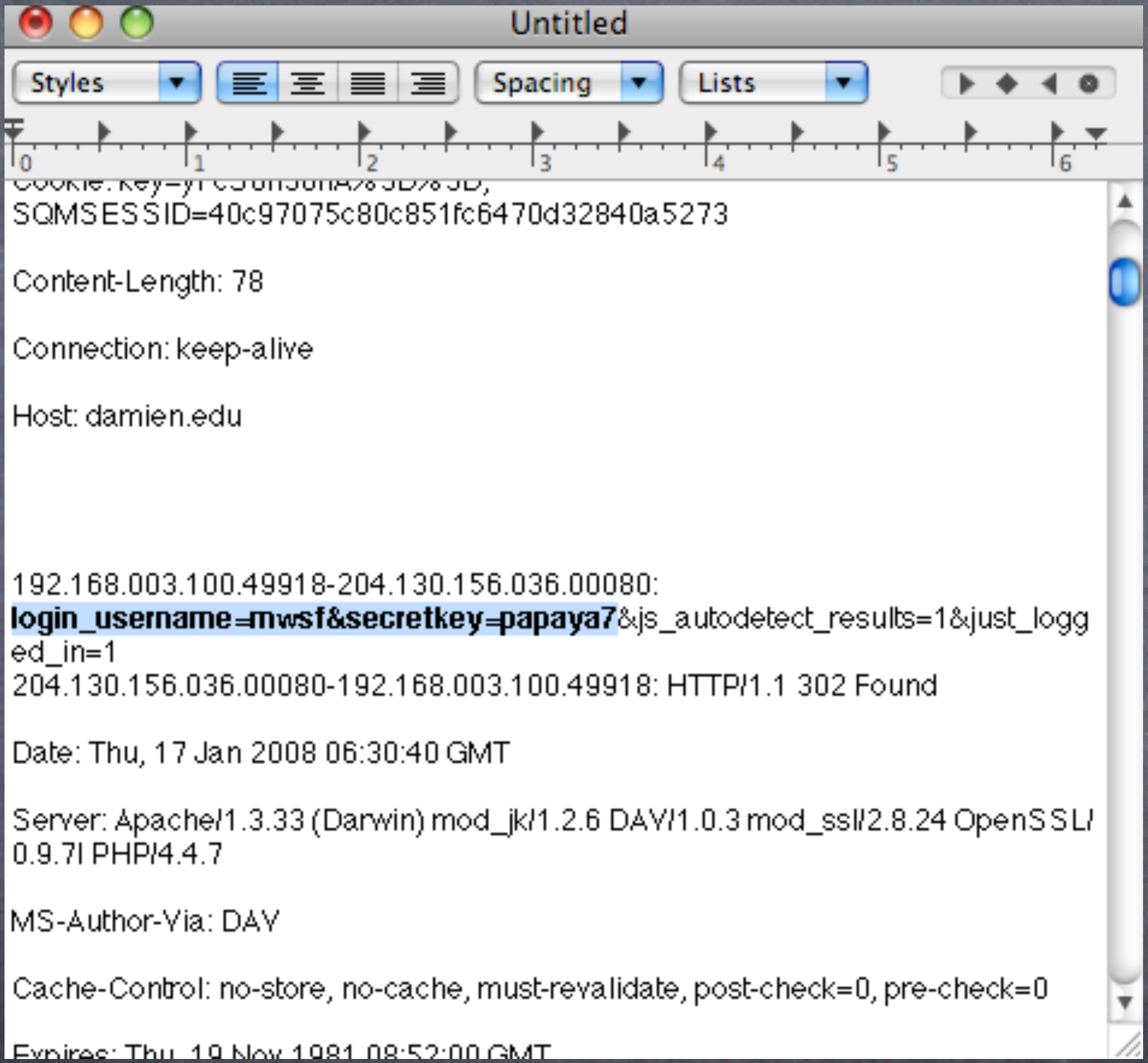
Security 101: packet sniffing



```
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=yPc5un5unA%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

Security 101: packet sniffing

Yikes!

...but it gets worse...

Imagine you could do this without joining the network...

from 12 miles away...

enter **Kismac**

Security 102: Kismac

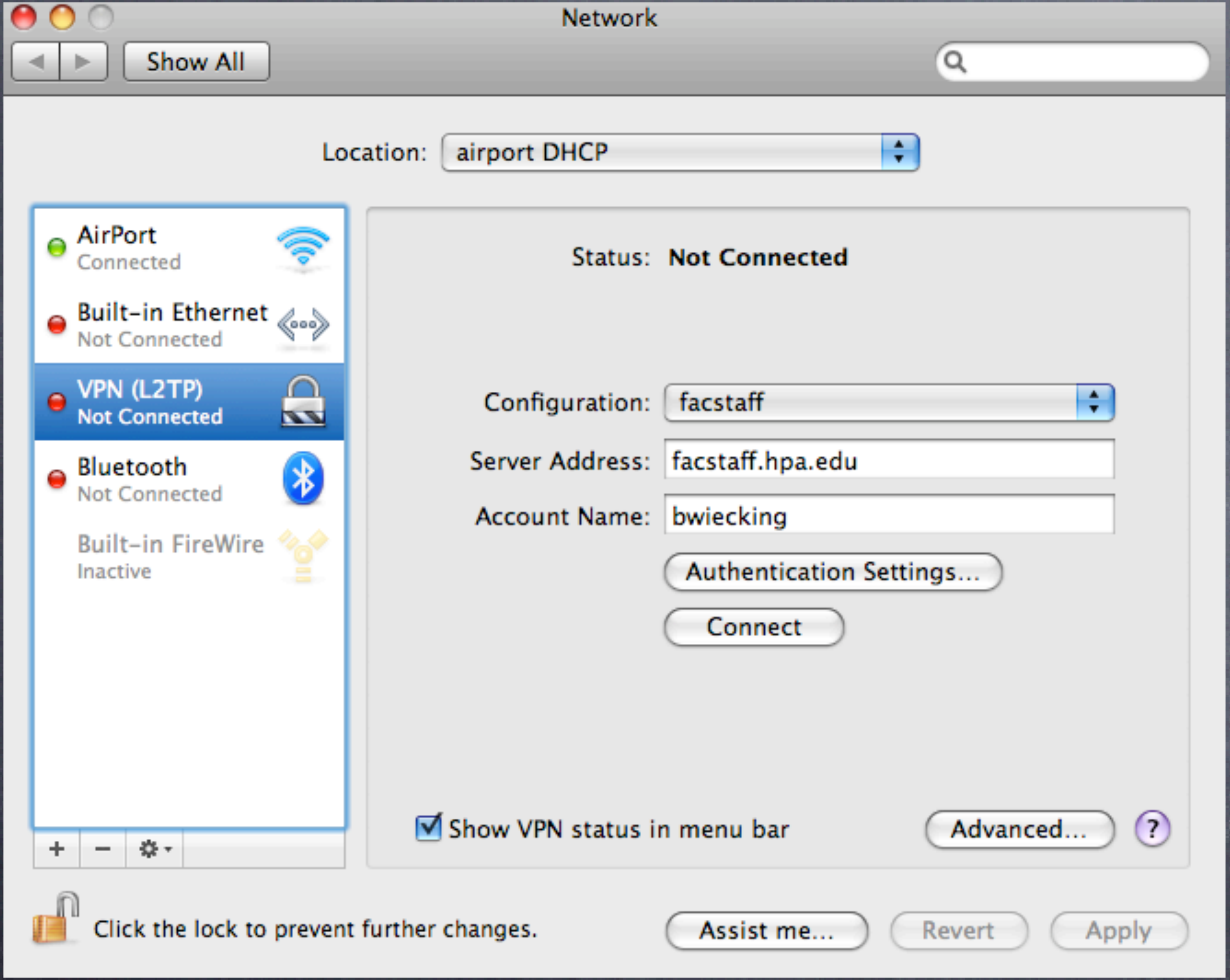
- Goal: Learn how to monitor even secured networks using Kismac
- Tools: Kismac, USB wireless adapters (Prism2 chipset, passive mode)
- What to do:
  - Start Kismac on your computer
  - Under preferences (apple-,) select airport extreme, active mode
  - Start, notice active networks
  - Now go back to 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

Security 103: 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

Security 103: VPN setup



Location: airport DHCP

Status: Not Connected

Configuration: facstaff

Server Address: facstaff.hpa.edu

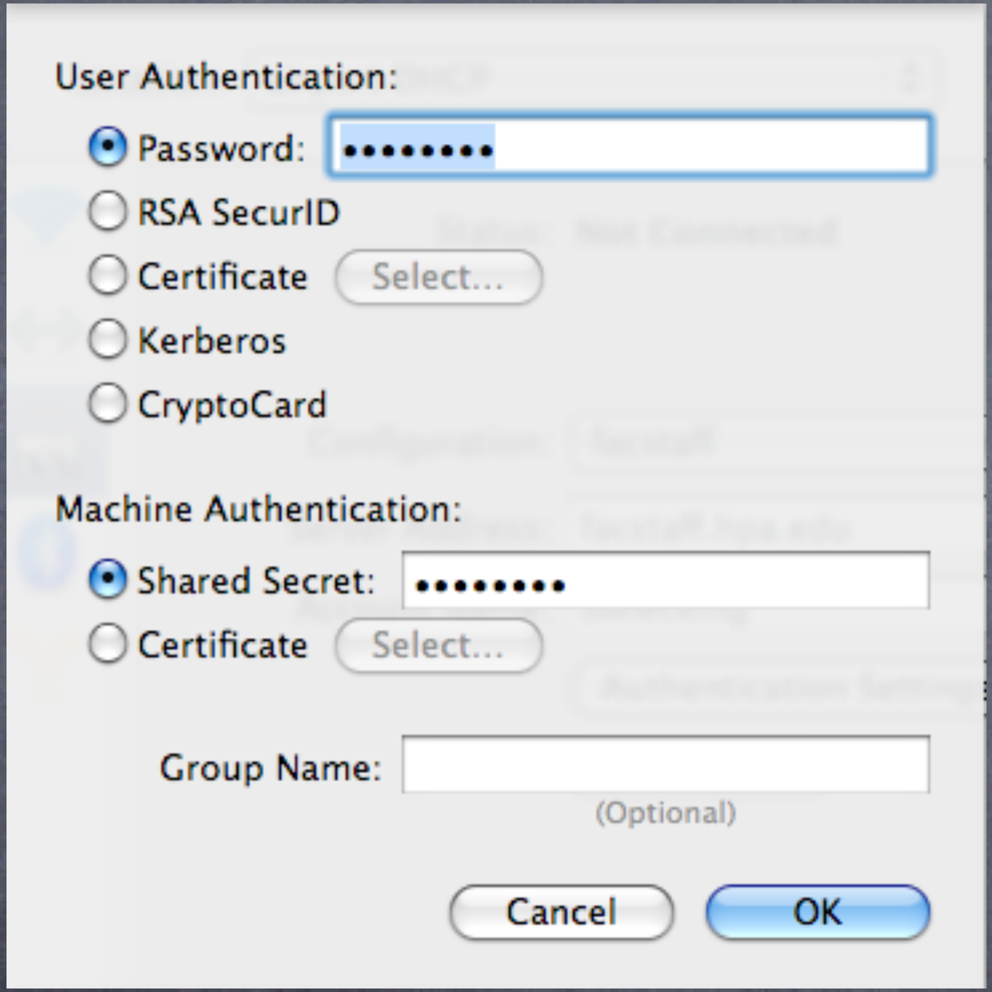
Account Name: bwiecking

☑ 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

Security 103: VPN setup



User Authentication:

- ● Password: •••••••••
- ○ RSA SecurID
- ○ Certificate
- ○ Kerberos
- ○ CryptoCard

Machine Authentication:

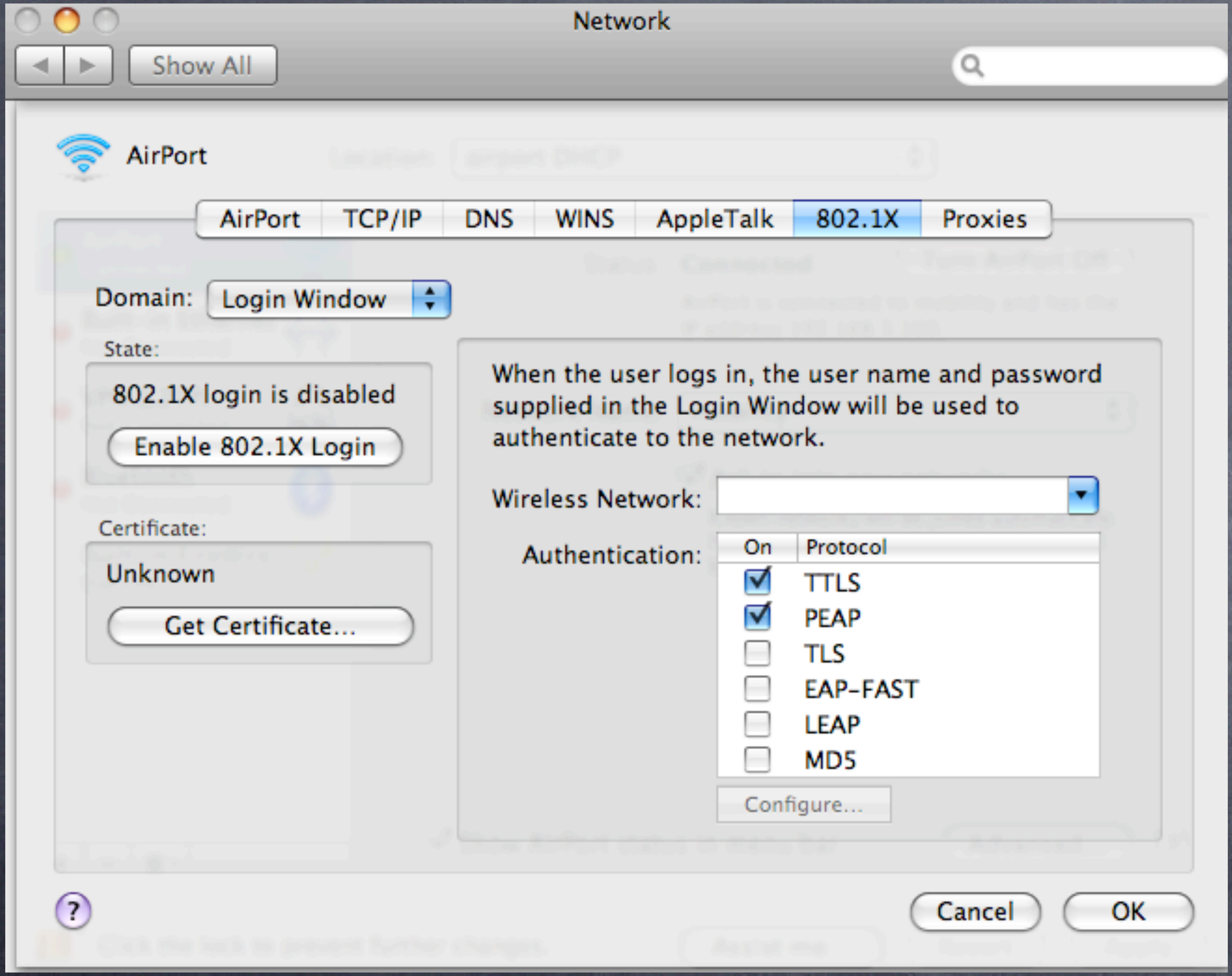
- ● Shared Secret: •••••••••
- ○ Certificate

Group Name:

(Optional)

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

Security 103: 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:

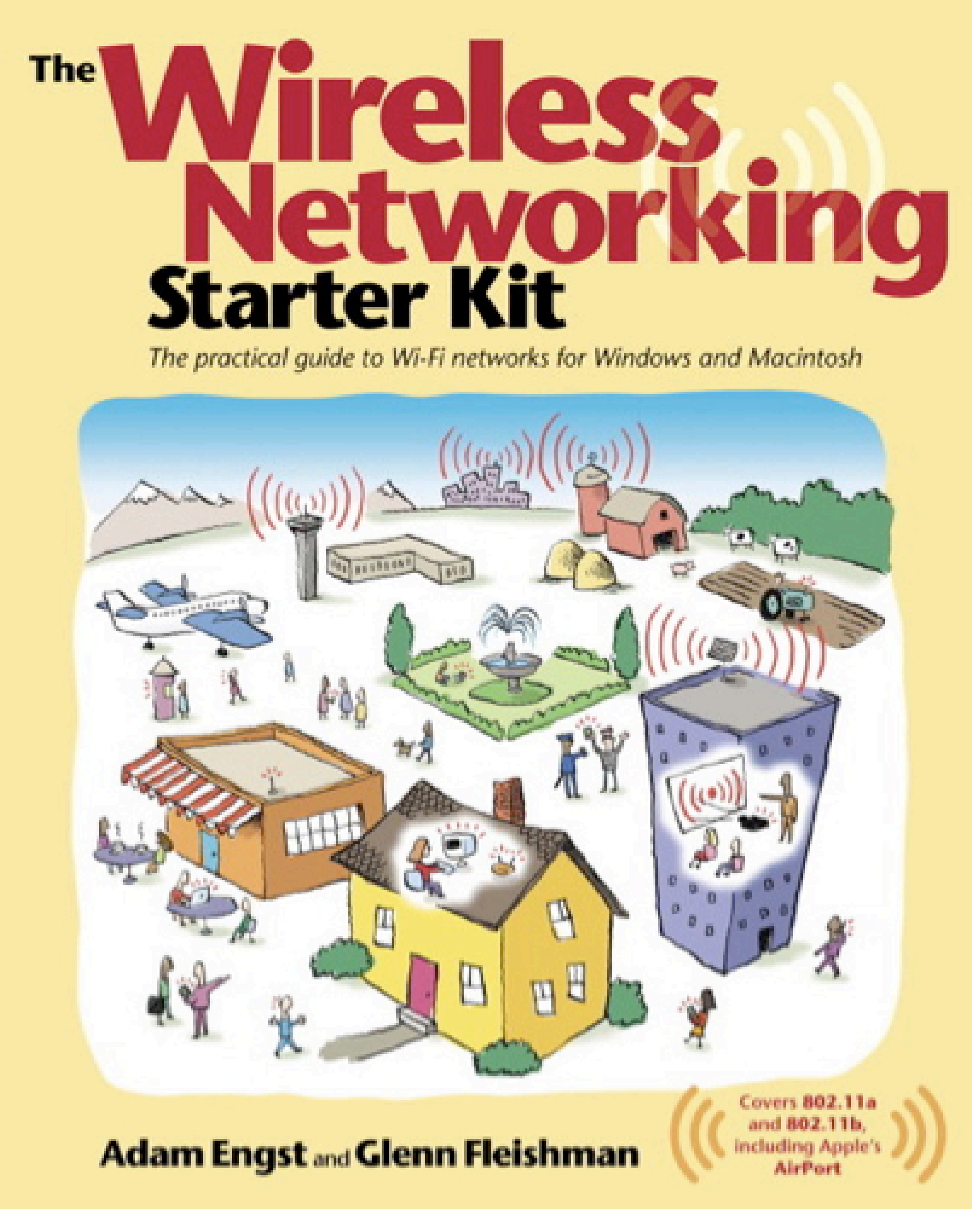
On	Protocol
☑	TTLS
☑	PEAP
□	TLS
□	EAP-FAST
□	LEAP
□	MD5

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

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
- Basic Access point setups are straightforward when done with care
- Access Point stats can be derived locally on the client, or on the Access Point if you are the admin
- 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

Helpful References

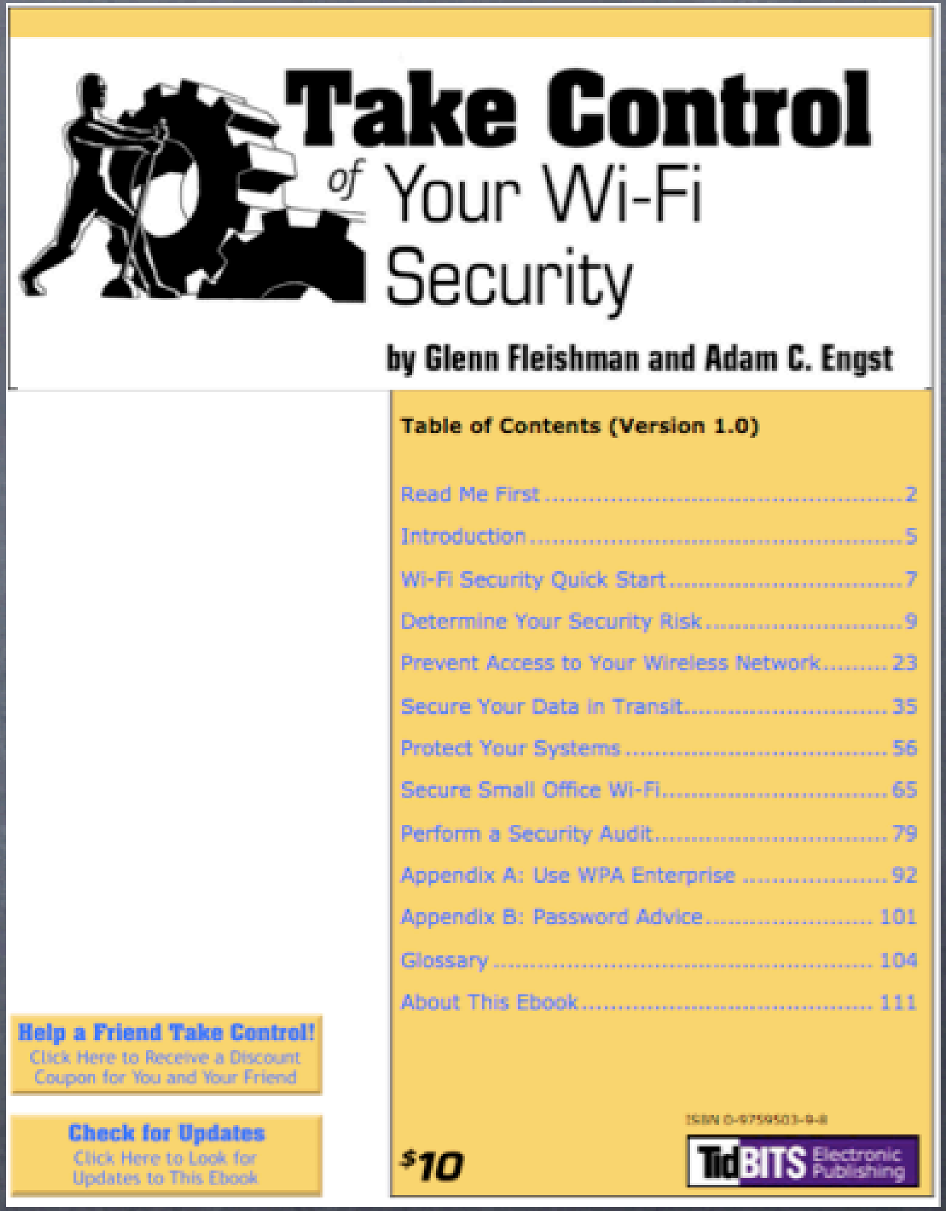


The Wireless Networking Starter Kit

The practical guide to Wi-Fi networks for Windows and Macintosh

Adam Engst and Glenn Fleishman

Covers 802.11a and 802.11b, including Apple's AirPort



Take Control of Your Wi-Fi Security

by Glenn Fleishman and Adam C. Engst

Table of Contents (Version 1.0)

Help a Friend Take Control!
Click Here to Receive a Discount Coupon for You and Your Friend

Check for Updates
Click Here to Look for Updates to This Ebook

ISBN 0-9759503-9-8

$10

TidBITS Electronic Publishing