# Mobility:
# Work away from work

Dr. Bill Wiecking
Volcano Wireless Networks
Apple Distinguished Educator
wiecking@mac.com

# Workshop Goals

- Learn how to access and use resources while mobile
- Learn about security risks and solutions
- Integration and collaboration while mobile
- Learn about new tools/strategies

# Agenda

Day One:

- Introductions
- Case Studies: who are we?
- Virtual Presence: being where you are not
- Infrastructure: yours and theirs

Day Two:

- Security: as guest and as host
- Integration: putting it all together, iPhone
- Collaboration: working better while away

# Introductions

# Section 1: Case studies
# Who are we?

- Road Warriors
- Tele-commuters
- Students
- SOHO users
- System Administrators

# Road Warriors

- Access dependent on location
- Must carry your tools with you
- Very transient
- Home support may vary
- Need reliable/secure access to resources
- Latest: hybrid tools, e.g. iPhone, laptop

# Road Warriors

- Power: Batteries, adapters, inverters
- wireless enhancement (antennas, amplifiers), wireless scanners
- Repair tools on the road: USB/FW jump drives
- Timbuktu and VPN basics
- iChat, skype, skype out, softphones
- How safe is my connection? Demo: Interarchy, webmail
- Webmail, dotmac facilities are ideal support

# Tele-commuter

- Ideal: same experience as while at work
- Remote control options
- Often a friendly location: security, power, backups, access
- Issues: security, speed, access, residential poaching, “where is my data”?

# Tele-commuter

- May not be a laptop, so data may have to be portable (hard drives, jump drives, network drives)
- May be fixed or variable IP address: some services can be hosted at home (Timbuktu, file sharing)
- ISP issues: Cable Modem, DSL, dialup, satellite
- May be able to setup permanent VPN to the office
- IP Net Monitor to check local CM users
- Secure file transfers
- LPR printing to office
- iChatAV/Skype for office presence
- VPN and TB2 for reverse help desk

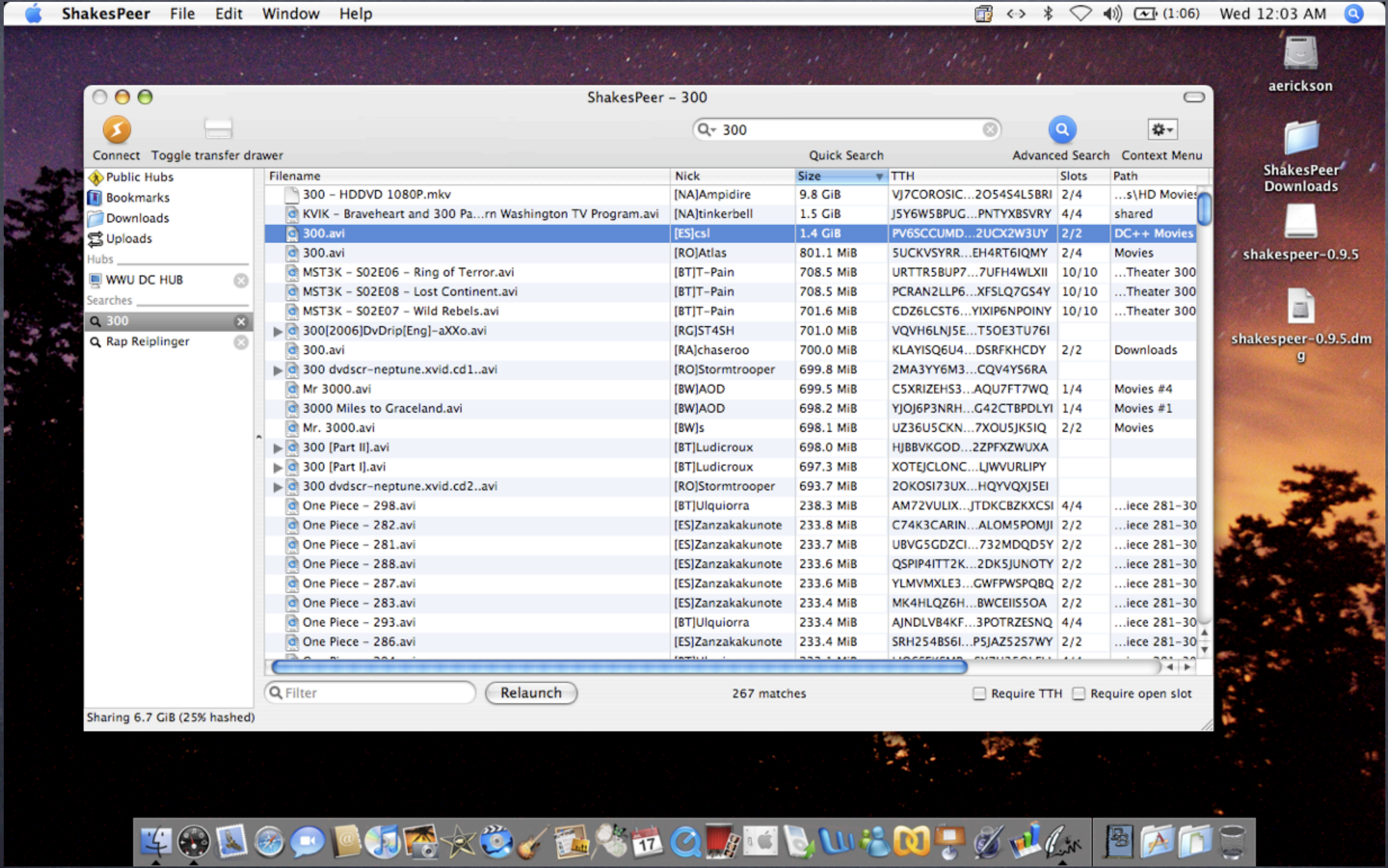
# Student user

- Dorm, classroom, home, bench outside: Give me speed and access
- Functions: IM, chat, mail, online courses, access to documents, collaboration
- Security? What me worry?
- Usually limited budget
- Some support at school

# Student user

- Limited budget
- Need space (mp3, videos, lectures)
- Need speed, access
- Often file sharing
- Hybrid wireless/wired: often wireless coverage issues
- Security not a priority (but should be)
- Admin may need service access (privacy issues)
- Roaming wireless issues
- Peer sharing: Shakespeer

# Student user: ShakesPeer



| Filename | Nick | Size | TTH | Slots | Path |
|---|---|---|---|---|---|
| 300 – HDDVD 1080P.mkv | [NA]Ampidire | 9.8 GiB | VJ7COROSIC…2O54S4L5BRI | 2/4 | …s\HD Movies |
| KVIK – Braveheart and 300 Pa…rn Washington TV Program.avi | [NA]tinkerbell | 1.5 GiB | J5Y6W5BPUG…PNTYXBSVRY | 4/4 | shared |
| 300.avi | [ES]csl | 1.4 GiB | PV6SCCUMD…2UCX2W3UY | 2/2 | DC++ Movies |
| 300.avi | [RO]Atlas | 801.1 MiB | 5UCKVSYRR…EH4RT6IQMY | 2/4 | Movies |
| MST3K – S02E06 – Ring of Terror.avi | [BT]T-Pain | 708.5 MiB | URTTR5BUP7…7UFH4WLXII | 10/10 | …Theater 300 |
| MST3K – S02E08 – Lost Continent.avi | [BT]T-Pain | 708.5 MiB | PCRAN2LLP6…XFSLQ7GS4Y | 10/10 | …Theater 300 |
| MST3K – S02E07 – Wild Rebels.avi | [BT]T-Pain | 701.6 MiB | CDZ6LCST6…YIXIP6NPOINY | 10/10 | …Theater 300 |
| ▶ 300[2006]DvDrip[Eng]-aXXo.avi | [RG]ST4SH | 701.0 MiB | VQVH6LNJ5E…T5OE3TU76I | | |
| 300.avi | [RA]chaseroo | 700.0 MiB | KLAYISQ6U4…DSRFKHCDY | 2/2 | Downloads |
| ▶ 300 dvdscr-neptune.xvid.cd1..avi | [RO]Stormtrooper | 699.8 MiB | 2MA3YY6M3…CQV4YS6RA | | |
| Mr 3000.avi | [BW]AOD | 699.5 MiB | C5XRIZEHS3…AQU7FT7WQ | 1/4 | Movies #4 |
| 3000 Miles to Graceland.avi | [BW]AOD | 698.2 MiB | YJOJ6P3NRH…G42CTBPDLYI | 1/4 | Movies #1 |
| Mr. 3000.avi | [BW]s | 698.1 MiB | UZ36U5CKN…7XOU5JK5IQ | 2/2 | Movies |
| ▶ 300 [Part II].avi | [BT]Ludicroux | 698.0 MiB | HJBBVKGOD…2ZPFXZWUXA | | |
| ▶ 300 [Part I].avi | [BT]Ludicroux | 697.3 MiB | XOTEJCLONC…LJWVURLIPY | | |
| ▶ 300 dvdscr-neptune.xvid.cd2..avi | [RO]Stormtrooper | 693.7 MiB | 2OKOSI73UX…HQYVQXJ5EI | | |
| One Piece – 298.avi | [BT]Ulquiorra | 238.3 MiB | AM72VULIX…JTDKCBZKXCSI | 4/4 | …iece 281-30 |
| One Piece – 282.avi | [ES]Zanzakakunote | 233.8 MiB | C74K3CARIN…ALOM5POMJI | 2/2 | …iece 281-30 |
| One Piece – 281.avi | [ES]Zanzakakunote | 233.7 MiB | UBVG5GDZCI…732MDQD5Y | 2/2 | …iece 281-30 |
| One Piece – 288.avi | [ES]Zanzakakunote | 233.6 MiB | QSPIP4ITT2K…2DK5JUNOTY | 2/2 | …iece 281-30 |
| One Piece – 287.avi | [ES]Zanzakakunote | 233.6 MiB | YLMVMXLE3…GWFPWSPQBQ | 2/2 | …iece 281-30 |
| One Piece – 283.avi | [ES]Zanzakakunote | 233.4 MiB | MK4HLQZ6H…BWCEIIS5OA | 2/2 | …iece 281-30 |
| One Piece – 293.avi | [BT]Ulquiorra | 233.4 MiB | AJNDLVB4KF…3POTRZESNQ | 4/4 | …iece 281-30 |
| One Piece – 286.avi | [ES]Zanzakakunote | 233.4 MiB | SRH254BS6I…P5JAZ52S7WY | 2/2 | …iece 281-30 |

Filter  Relaunch  267 matches  □ Require TTH  □ Require open slot

Sharing 6.7 GiB (25% hashed)

# SOHO user

- Residential/hybrid users
- Small group of known users
- Easy to access clients for maintenance/upgrades/ security policies
- Limited support staff (may be you)
- Often must host visitors/transient workers
- Security is and should be an issue (HIPAA)
- Neighbors may be poaching
- Corporate/business security?
- ISP options: DSL/Cable Modem
- Services at SOHO office may support other mobile users

# System Administrator/Support staff

- Support all above users
- Security issues: social engineering: are you who we are paid to support?
- Help!--"Where are you?"
- Some users in office, others at home
- Wireless issues come with the territory
- VPN and Timbuktu as reverse help desk
- How to support the office from home?

# Wireless access options:

- Best: the networks you setup yourself
- Hotels: wired or wireless, usually with a captive portal page (billing to your room)
- Coffee shops: T-mobile etc. : Captive portal with RADIUS backend (checks to see if you have paid)
- Some are free for iTunes sales
- “Free” open networks: NoCat nets, residences

# Wireless access cautions:

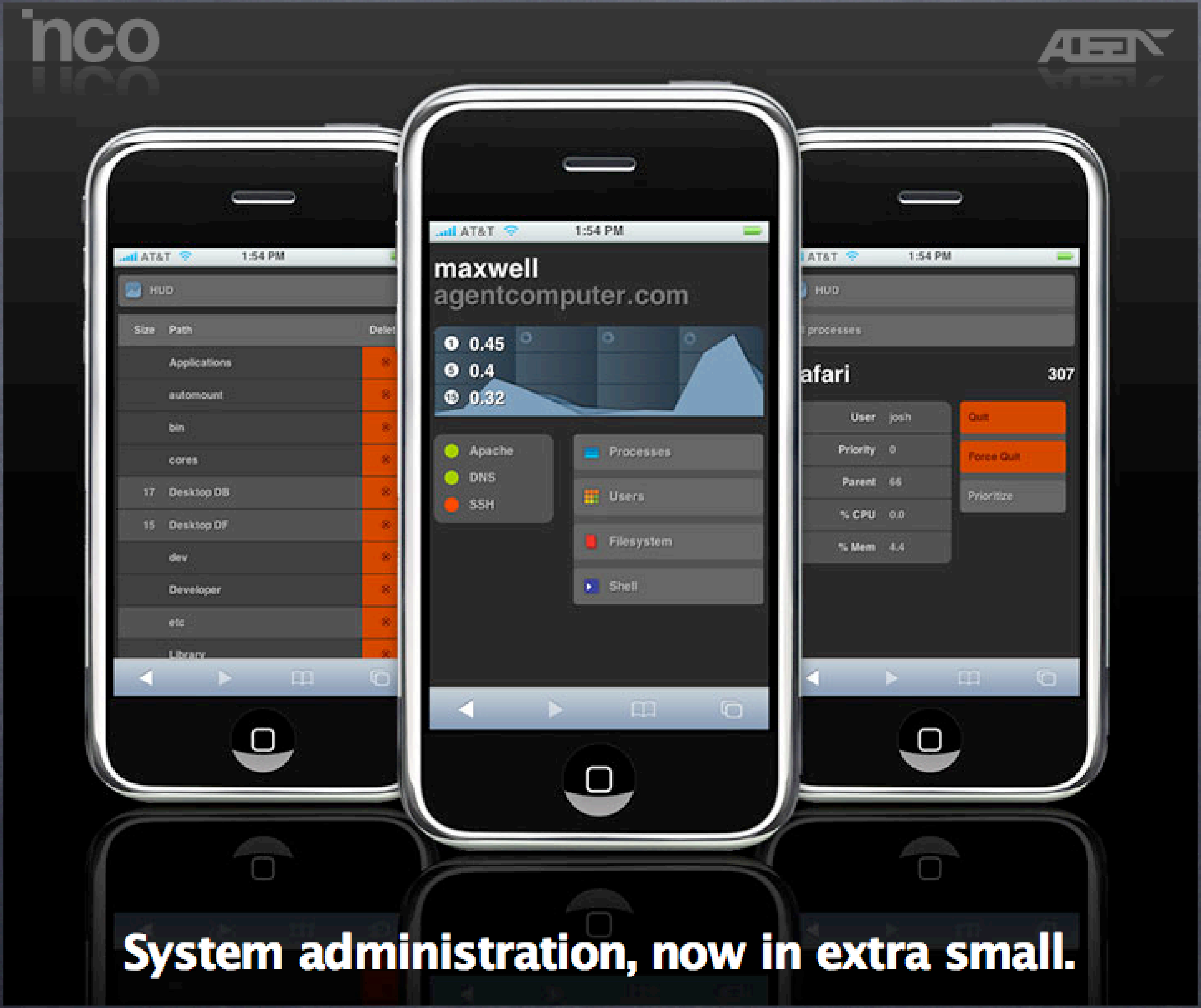
- Some networks are free with the intent of gaining your secure information
- Most are just open due to lack of care/interest on the part of the host/
- Much more on this soon when we cover wireless setups

# Hands-on: What’s out there?

- Using your laptop, connect to the network named alpha
- How can you tell if there are other networks?
  - Answer: Kismac
- Look for all networks in the area, and find the second network

# Section2

# Office 2.0: the office extended



# Remote Control

"Wherever you go, there you are"
-Buckaroo Banzai

- Best tool for remote presence is Timbuktu (an extremely remote town in Mali)
- Can allow secure connections, file transfers, remote control
- Can be used in your direction or to your direction (reverse help desk)
- Cross platform: control PCs or Macs
- Other variants: Apple Remote Desktop, VNC

# Timbuktu, ARD and VNC

- Timbuktu is one-to-one experience, not good for lab or mass control
- Best for admin of labs is Apple Remote Desktop (ARD)
- Free version of remote control is VNC
- Command Line Interface commands can be done remotely as well using ssh
- Can create ssh tunnels to host as well

# Timbuktu: best tricks

- You can setup one machine inside any firewall with inbound port mapping (port 407 on the mac, others on the PC)
- Once you have a pied a terre, you can jump to other machines
- On fast networks, you can jump up to 4 times
- Backup: always make sure you can ssh and shutdown -r if the system stalls
- Timbuktu 8.7 is Leopard compatible
- Timbuktu 8.x can be installed remotely using SSH

# ARD: Best tricks

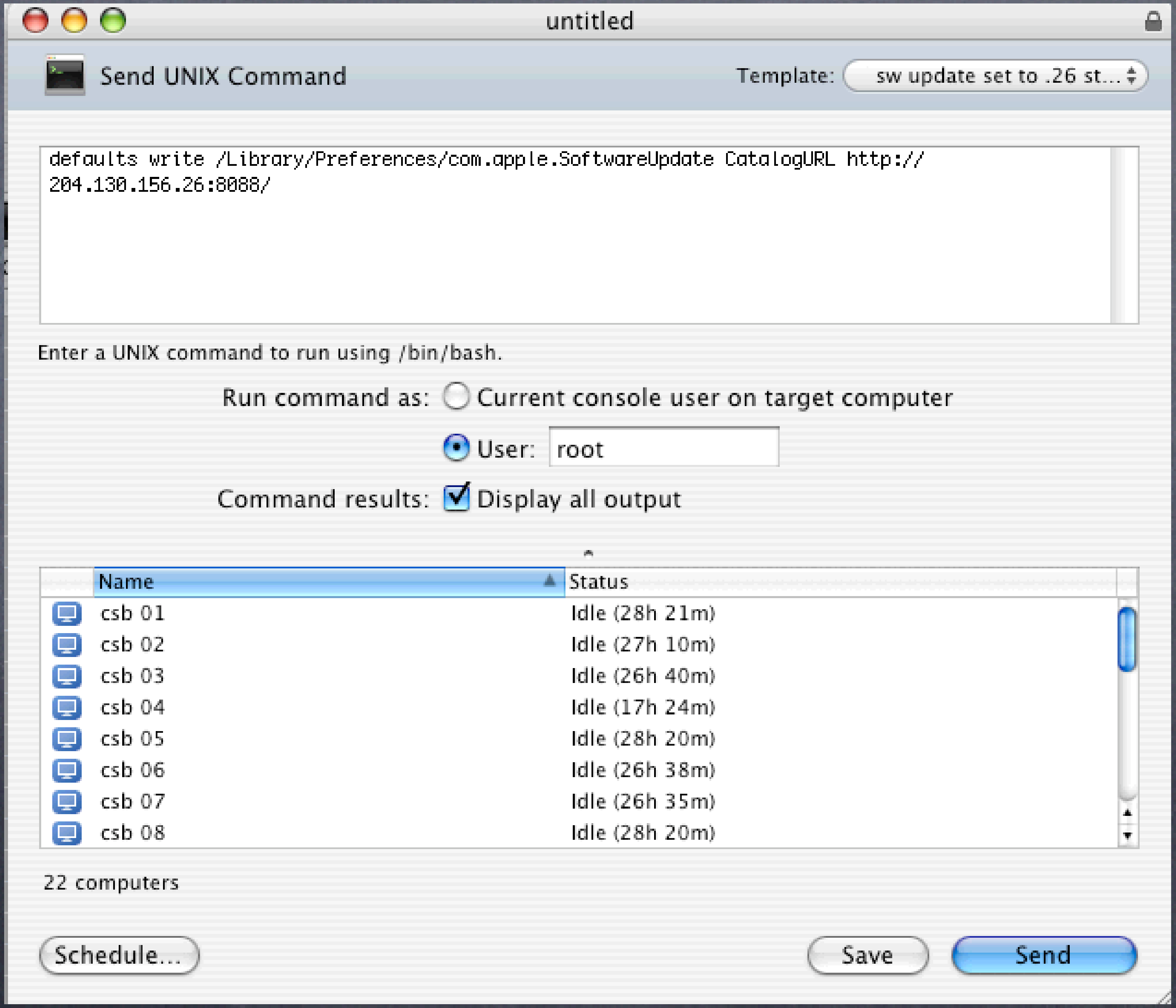
- ARD is slow for mass copies of files, but extremely fast for mass CLI (command line interface) commands
- Example: **Software update**

```
defaults write /Library/Preferences/com.apple.SoftwareUpdate
CatalogURL http://10.2.250.2:8088/

sudo defaults write /private/var/root/Library/Preferences/
com.apple.SoftwareUpdate CatalogURL http://10.2.250.2:8088/

sudo softwareupdate -i -a
```

# ARD: Best tricks



Template: sw update set to .26 st...

```
defaults write /Library/Preferences/com.apple.SoftwareUpdate CatalogURL http://
204.130.156.26:8088/
```

Enter a UNIX command to run using /bin/bash.

Run command as: ○ Current console user on target computer

● User: root

Command results: ☑ Display all output

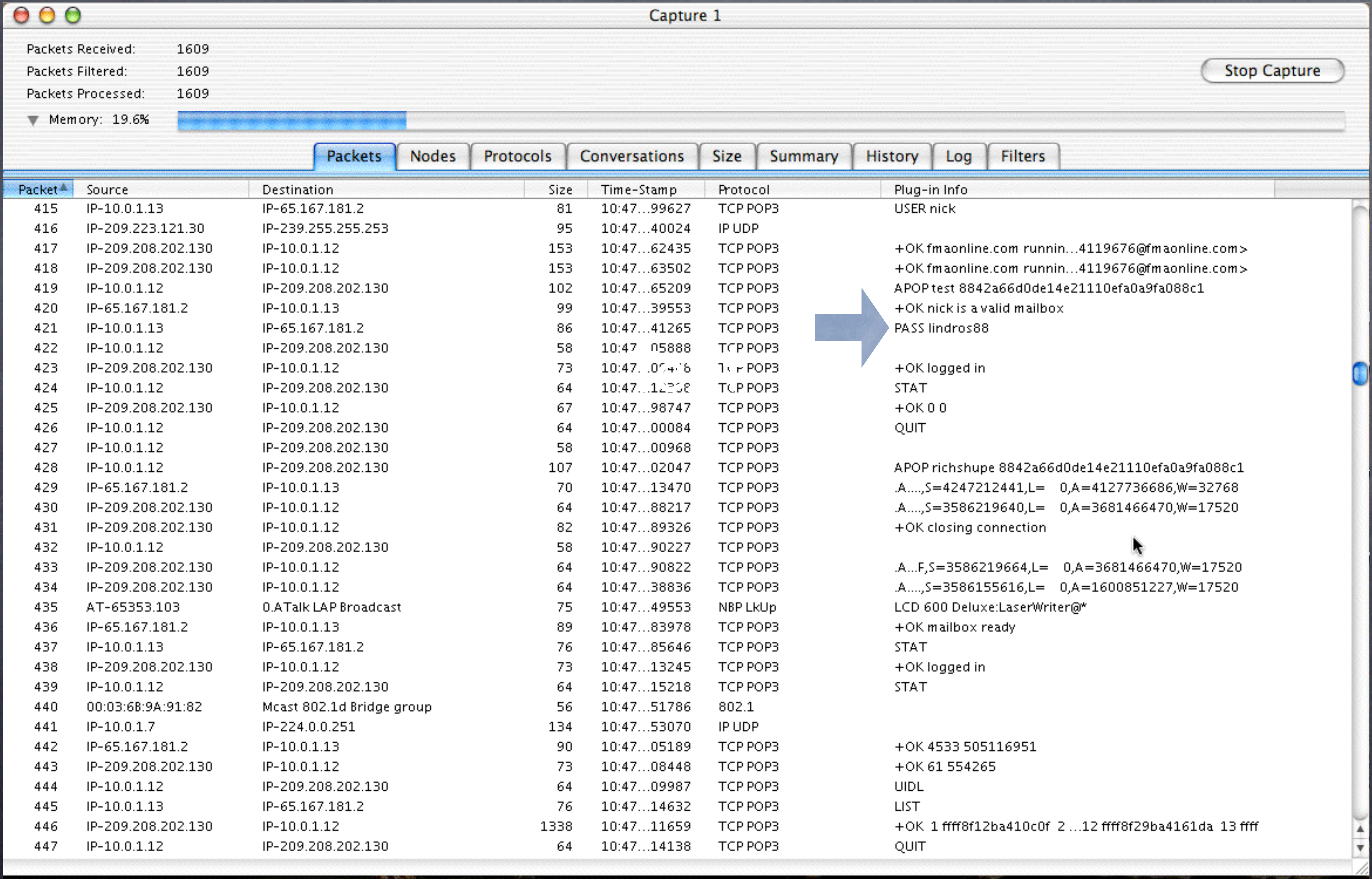
```
Name      Status
csb 01    Idle (28h 21m)
csb 02    Idle (27h 10m)
csb 03    Idle (26h 40m)
csb 04    Idle (17h 24m)
csb 05    Idle (28h 20m)
csb 06    Idle (26h 38m)
csb 07    Idle (26h 35m)
csb 08    Idle (28h 20m)
```

22 computers

# A note on security

- ARD and Timbuktu sessions can be encrypted
- Watch the next screen of a webmail login, then think of why you would need an encrypted session
- Other packet sniffing examples follow

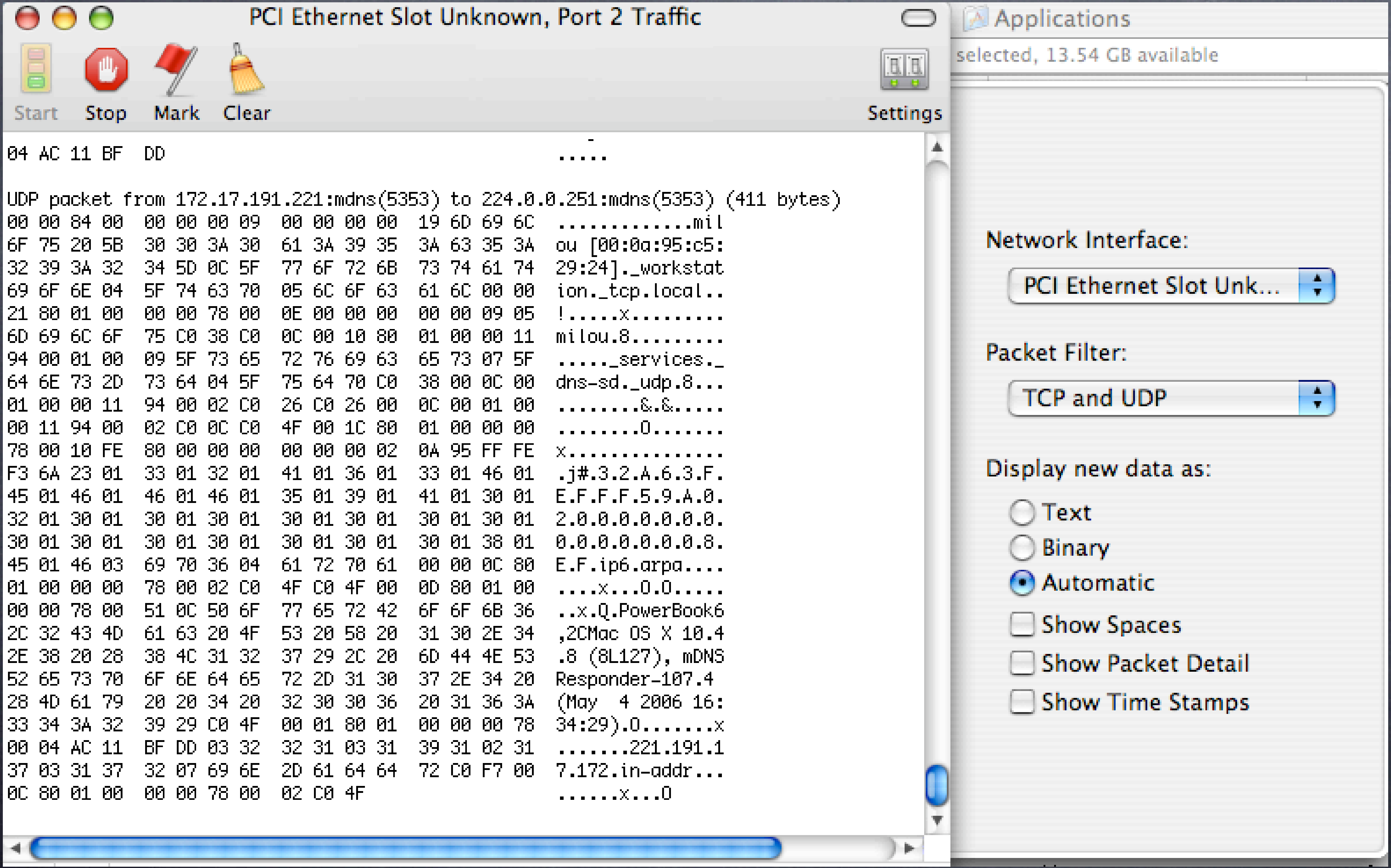
# EtherPeek Password Capture example



Packets Received: 1609
Packets Filtered: 1609
Packets Processed: 1609
Memory: 19.6%

| Packet | Source | Destination | Size | Time-Stamp | Protocol | Plug-in Info |
|---|---|---|---|---|---|---|
| 415 | IP-10.0.1.13 | IP-65.167.181.2 | 81 | 10:47...99627 | TCP POP3 | USER nick |
| 416 | IP-209.223.121.30 | IP-239.255.255.253 | 95 | 10:47...40024 | IP UDP | |
| 417 | IP-209.208.202.130 | IP-10.0.1.12 | 153 | 10:47...62435 | TCP POP3 | +OK fmaonline.com runnin...4119676@fmaonline.com> |
| 418 | IP-209.208.202.130 | IP-10.0.1.12 | 153 | 10:47...63502 | TCP POP3 | +OK fmaonline.com runnin...4119676@fmaonline.com> |
| 419 | IP-10.0.1.12 | IP-209.208.202.130 | 102 | 10:47...65209 | TCP POP3 | APOP test 8842a66d0de14e21110efa0a9fa088c1 |
| 420 | IP-65.167.181.2 | IP-10.0.1.13 | 99 | 10:47...39553 | TCP POP3 | +OK nick is a valid mailbox |
| 421 | IP-10.0.1.13 | IP-65.167.181.2 | 86 | 10:47...41265 | TCP POP3 | PASS lindros88 |
| 422 | IP-10.0.1.12 | IP-209.208.202.130 | 58 | 10:47...05888 | TCP POP3 | |
| 423 | IP-209.208.202.130 | IP-10.0.1.12 | 73 | 10:47...0[illegible]6 | TCP POP3 | +OK logged in |
| 424 | IP-10.0.1.12 | IP-209.208.202.130 | 64 | 10:47...12[illegible] | TCP POP3 | STAT |
| 425 | IP-209.208.202.130 | IP-10.0.1.12 | 67 | 10:47...98747 | TCP POP3 | +OK 0 0 |
| 426 | IP-10.0.1.12 | IP-209.208.202.130 | 64 | 10:47...00084 | TCP POP3 | QUIT |
| 427 | IP-10.0.1.12 | IP-209.208.202.130 | 58 | 10:47...00968 | TCP POP3 | |
| 428 | IP-10.0.1.12 | IP-209.208.202.130 | 107 | 10:47...02047 | TCP POP3 | APOP richshupe 8842a66d0de14e21110efa0a9fa088c1 |
| 429 | IP-65.167.181.2 | IP-10.0.1.13 | 70 | 10:47...13470 | TCP POP3 | .A....,S=4247212441,L= 0,A=4127736686,W=32768 |
| 430 | IP-209.208.202.130 | IP-10.0.1.12 | 64 | 10:47...88217 | TCP POP3 | .A....,S=3586219640,L= 0,A=3681466470,W=17520 |
| 431 | IP-209.208.202.130 | IP-10.0.1.12 | 82 | 10:47...89326 | TCP POP3 | +OK closing connection |
| 432 | IP-10.0.1.12 | IP-209.208.202.130 | 58 | 10:47...90227 | TCP POP3 | |
| 433 | IP-209.208.202.130 | IP-10.0.1.12 | 64 | 10:47...90822 | TCP POP3 | .A...F,S=3586219664,L= 0,A=3681466470,W=17520 |
| 434 | IP-209.208.202.130 | IP-10.0.1.12 | 64 | 10:47...38836 | TCP POP3 | .A....,S=3586155616,L= 0,A=1600851227,W=17520 |
| 435 | AT-65353.103 | 0.ATalk LAP Broadcast | 75 | 10:47...49553 | NBP LkUp | LCD 600 Deluxe:LaserWriter@* |
| 436 | IP-65.167.181.2 | IP-10.0.1.13 | 89 | 10:47...83978 | TCP POP3 | +OK mailbox ready |
| 437 | IP-10.0.1.13 | IP-65.167.181.2 | 76 | 10:47...85646 | TCP POP3 | STAT |
| 438 | IP-209.208.202.130 | IP-10.0.1.12 | 73 | 10:47...13245 | TCP POP3 | +OK logged in |
| 439 | IP-10.0.1.12 | IP-209.208.202.130 | 64 | 10:47...15218 | TCP POP3 | STAT |
| 440 | 00:03:6B:9A:91:82 | Mcast 802.1d Bridge group | 56 | 10:47...51786 | 802.1 | |
| 441 | IP-10.0.1.7 | IP-224.0.0.251 | 134 | 10:47...53070 | IP UDP | |
| 442 | IP-65.167.181.2 | IP-10.0.1.13 | 90 | 10:47...05189 | TCP POP3 | +OK 4533 505116951 |
| 443 | IP-209.208.202.130 | IP-10.0.1.12 | 73 | 10:47...08448 | TCP POP3 | +OK 61 554265 |
| 444 | IP-10.0.1.12 | IP-209.208.202.130 | 64 | 10:47...09987 | TCP POP3 | UIDL |
| 445 | IP-10.0.1.13 | IP-65.167.181.2 | 76 | 10:47...14632 | TCP POP3 | LIST |
| 446 | IP-209.208.202.130 | IP-10.0.1.12 | 1338 | 10:47...11659 | TCP POP3 | +OK 1 ffff8f12ba410c0f 2 ...12 ffff8f29ba4161da 13 ffff |
| 447 | IP-10.0.1.12 | IP-209.208.202.130 | 64 | 10:47...14138 | TCP POP3 | QUIT |

# Interarchy packet sniffing


PCI Ethernet Slot Unknown, Port 2 Traffic
Start
Stop
Mark
Clear
Settings
Applications
selected, 13.54 GB available

```
04 AC 11 BF  DD                                    .....

UDP packet from 172.17.191.221:mdns(5353) to 224.0.0.251:mdns(5353) (411 bytes)
00 00 84 00  00 00 00 09  00 00 00 00  19 6D 69 6C  .............mil
6F 75 20 5B  30 30 3A 30  61 3A 39 35  3A 63 35 3A  ou [00:0a:95:c5:
32 39 3A 32  34 5D 0C 5F  77 6F 72 6B  73 74 61 74  29:24]._workstat
69 6F 6E 04  5F 74 63 70  05 6C 6F 63  61 6C 00 00  ion._tcp.local..
21 80 01 00  00 00 78 00  0E 00 00 00  00 00 09 05  !.....x.........
6D 69 6C 6F  75 C0 38 C0  0C 00 10 80  01 00 00 11  milou.8.........
94 00 01 00  09 5F 73 65  72 76 69 63  65 73 07 5F  ....._services._
64 6E 73 2D  73 64 04 5F  75 64 70 C0  38 00 0C 00  dns-sd._udp.8...
01 00 00 11  94 00 02 C0  26 C0 26 00  0C 00 01 00  ........&.&.....
00 11 94 00  02 C0 0C C0  4F 00 1C 80  01 00 00 00  ........O.......
78 00 10 FE  80 00 00 00  00 00 00 02  0A 95 FF FE  x...............
F3 6A 23 01  33 01 32 01  41 01 36 01  33 01 46 01  .j#.3.2.A.6.3.F.
45 01 46 01  46 01 46 01  35 01 39 01  41 01 30 01  E.F.F.F.5.9.A.0.
32 01 30 01  30 01 30 01  30 01 30 01  30 01 30 01  2.0.0.0.0.0.0.0.
30 01 30 01  30 01 30 01  30 01 30 01  30 01 38 01  0.0.0.0.0.0.0.8.
45 01 46 03  69 70 36 04  61 72 70 61  00 00 0C 80  E.F.ip6.arpa....
01 00 00 00  78 00 02 C0  4F C0 4F 00  0D 80 01 00  ....x...O.O.....
00 00 78 00  51 0C 50 6F  77 65 72 42  6F 6F 6B 36  ..x.Q.PowerBook6
2C 32 43 4D  61 63 20 4F  53 20 58 20  31 30 2E 34  ,2CMac OS X 10.4
2E 38 20 28  38 4C 31 32  37 29 2C 20  6D 44 4E 53  .8 (8L127), mDNS
52 65 73 70  6F 6E 64 65  72 2D 31 30  37 2E 34 20  Responder-107.4
28 4D 61 79  20 20 34 20  32 30 30 36  20 31 36 3A  (May  4 2006 16:
33 34 3A 32  39 29 C0 4F  00 01 80 01  00 00 00 78  34:29).O.......x
00 04 AC 11  BF DD 03 32  32 31 03 31  39 31 02 31  .......221.191.1
37 03 31 37  32 07 69 6E  2D 61 64 64  72 C0 F7 00  7.172.in-addr...
0C 80 01 00  00 00 78 00  02 C0 4F                  ......x...O
```

Network Interface: PCI Ethernet Slot Unk…

Packet Filter: TCP and UDP

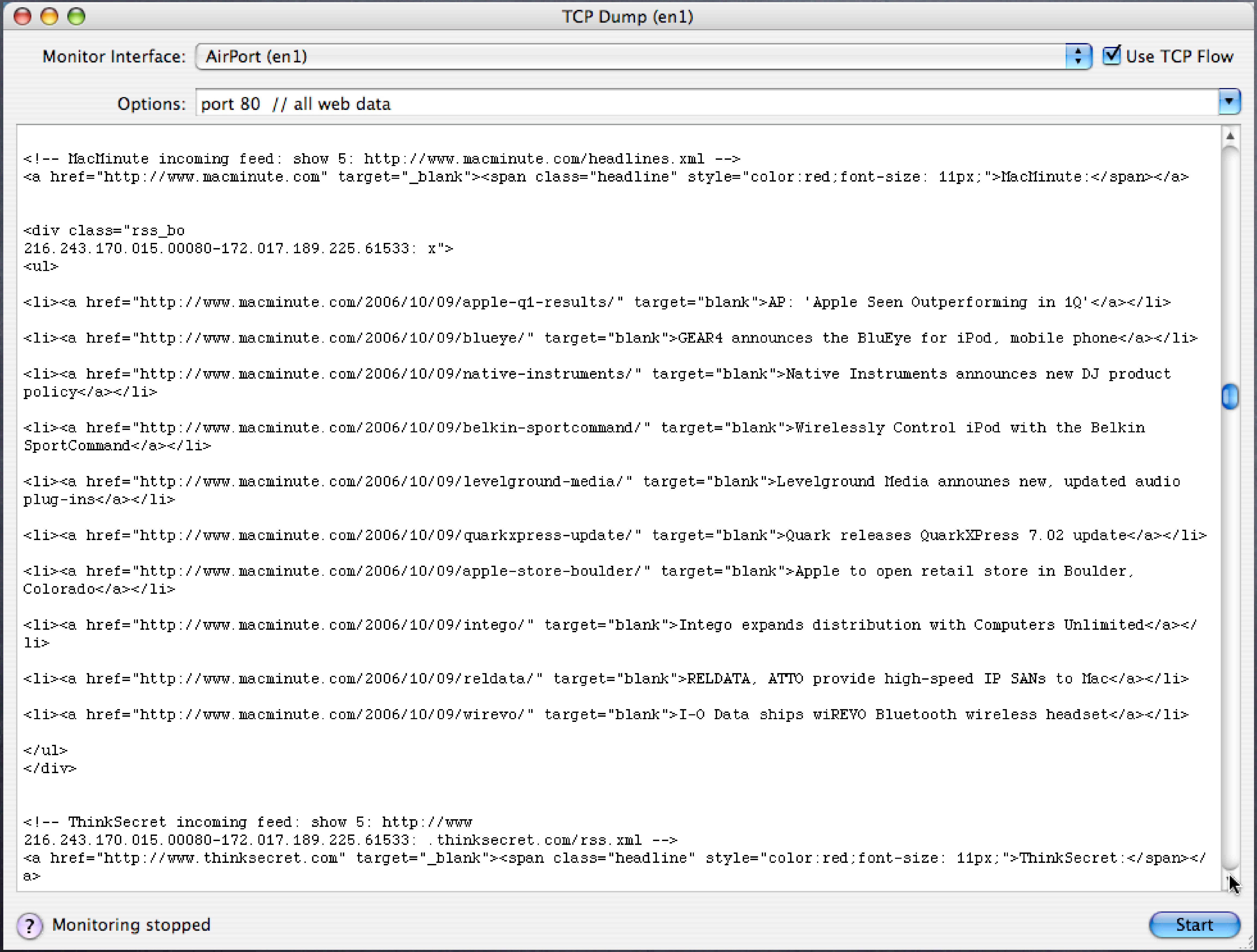
Display new data as:

○ Text
○ Binary
● Automatic

□ Show Spaces
□ Show Packet Detail
□ Show Time Stamps

# IPNetMonitor/TCPflow

- Can capture your packets, their packets, all sorts of packets
- Great for testing VPN security, for demonstrating security needs



Monitor Interface: AirPort (en1)

☑ Use TCP Flow

Options: port 80 // all web data

```
<!-- MacMinute incoming feed: show 5: http://www.macminute.com/headlines.xml -->
<a href="http://www.macminute.com" target="_blank"><span class="headline" style="color:red;font-size: 11px;">MacMinute:</span></a>


<div class="rss_bo
216.243.170.015.00080-172.017.189.225.61533: x">
<ul>

<li><a href="http://www.macminute.com/2006/10/09/apple-q1-results/" target="blank">AP: 'Apple Seen Outperforming in 1Q'</a></li>

<li><a href="http://www.macminute.com/2006/10/09/blueye/" target="blank">GEAR4 announces the BluEye for iPod, mobile phone</a></li>

<li><a href="http://www.macminute.com/2006/10/09/native-instruments/" target="blank">Native Instruments announces new DJ product
policy</a></li>

<li><a href="http://www.macminute.com/2006/10/09/belkin-sportcommand/" target="blank">Wirelessly Control iPod with the Belkin
SportCommand</a></li>

<li><a href="http://www.macminute.com/2006/10/09/levelground-media/" target="blank">Levelground Media announes new, updated audio
plug-ins</a></li>

<li><a href="http://www.macminute.com/2006/10/09/quarkxpress-update/" target="blank">Quark releases QuarkXPress 7.02 update</a></li>

<li><a href="http://www.macminute.com/2006/10/09/apple-store-boulder/" target="blank">Apple to open retail store in Boulder,
Colorado</a></li>

<li><a href="http://www.macminute.com/2006/10/09/intego/" target="blank">Intego expands distribution with Computers Unlimited</a></
li>

<li><a href="http://www.macminute.com/2006/10/09/reldata/" target="blank">RELDATA, ATTO provide high-speed IP SANs to Mac</a></li>

<li><a href="http://www.macminute.com/2006/10/09/wirevo/" target="blank">I-O Data ships wiREVO Bluetooth wireless headset</a></li>

</ul>
</div>


<!-- ThinkSecret incoming feed: show 5: http://www
216.243.170.015.00080-172.017.189.225.61533: .thinksecret.com/rss.xml -->
<a href="http://www.thinksecret.com" target="_blank"><span class="headline" style="color:red;font-size: 11px;">ThinkSecret:</span></
a>
```

Monitoring stopped

# Solution:VPN
# Virtual Private Network (tunnel)

Good

Secure data connection
Stops access to the data not the network
Transparent with Panther, Tiger, Leopard
Wired and wireless use (thwarts packet sniffers)
Included with Panther/Tiger/Leopard server

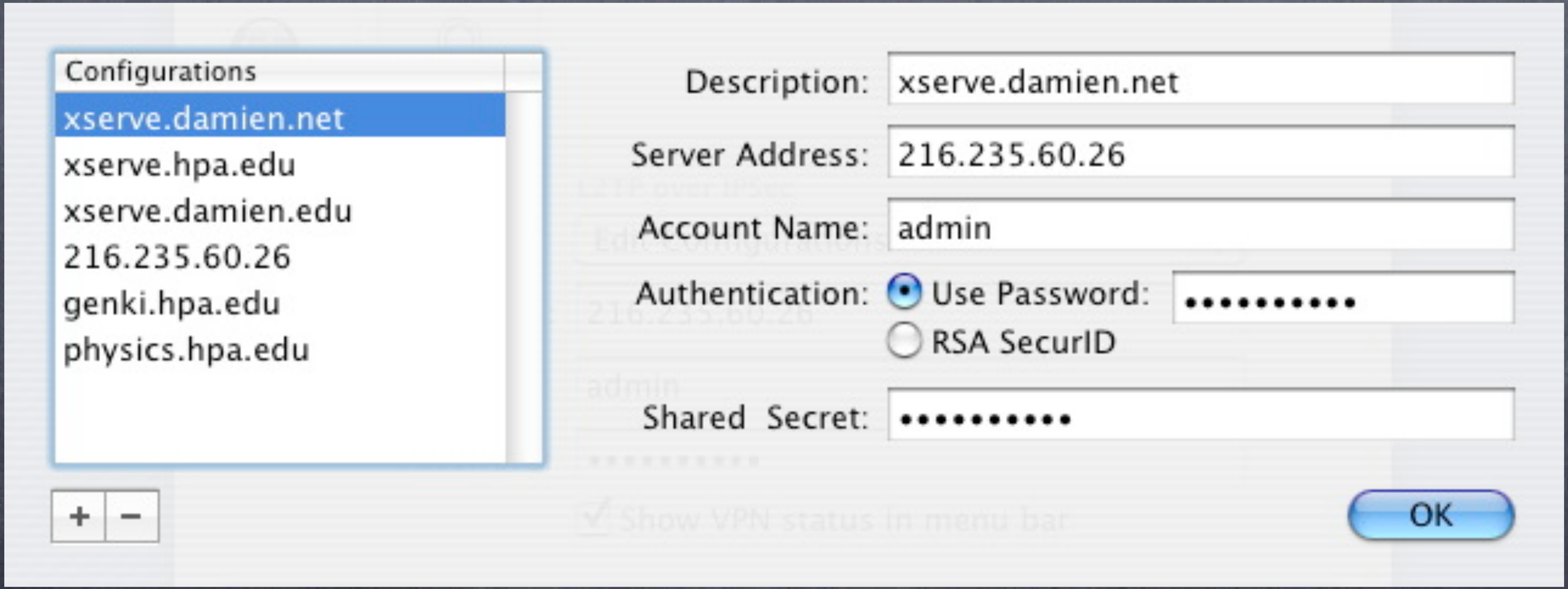
Bad

Server or VPN endpoint needed

# VPN: basics

- Uses either L2TP (Layer 2 transport protocol) or PPTP (point to point transfer protocol)
- A secure connection is established between the client and the VPN server
- Using Panther, Tiger or Leopard server (10.3, 10.4, 10.5), this connection can be tunneled into the internal network where the server lives
- Roaming users can then have an "encapsulated" communication
- This is the best way to ensure security over a wireless link, as any intercepted packets are gibberish without access to a supercomputer (an interesting DHS issue)
- When setting up the VPN, network routing is critical. To encrypt all traffic, make all routes private. For best speed, only make the internal traffic private
- Increases the speed of certain management tools (Timbuktu, Apple Remote Desktop)
- Can also be used for help desk to work with home users (reverse VPN)
- VPN client is built in to Internet Connect app in Tiger and Leopard, on-demand
- Shared Secret must be 8 characters or more

# VPN from OSX Panther/Tiger/Leopard



Configurations

- xserve.damien.net
- xserve.hpa.edu
- xserve.damien.edu
- 216.235.60.26
- genki.hpa.edu
- physics.hpa.edu

Description: xserve.damien.net

Server Address: 216.235.60.26

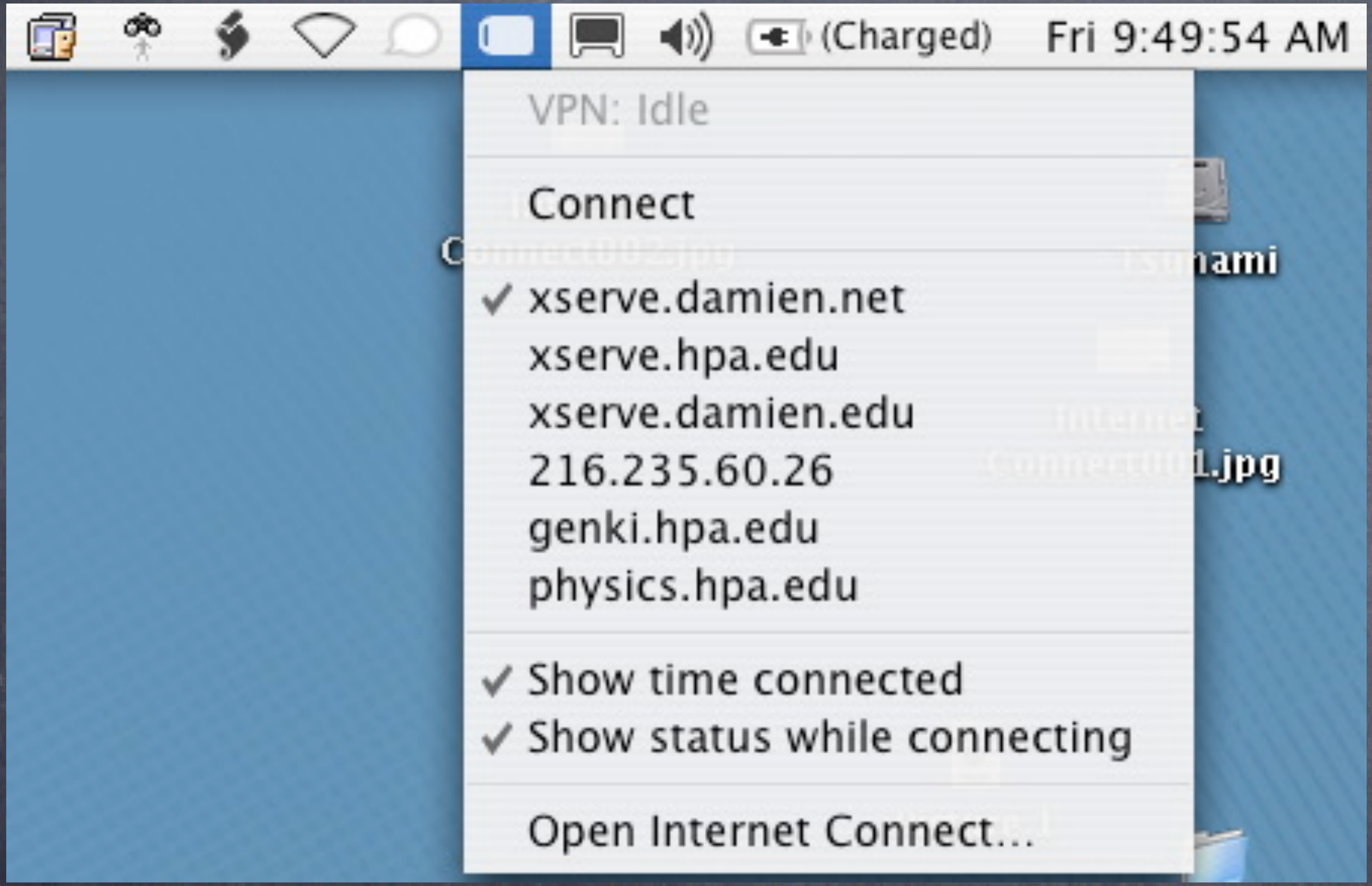
Account Name: admin

Authentication: ● Use Password: •••••••••••
○ RSA SecurID

Shared Secret: •••••••••••

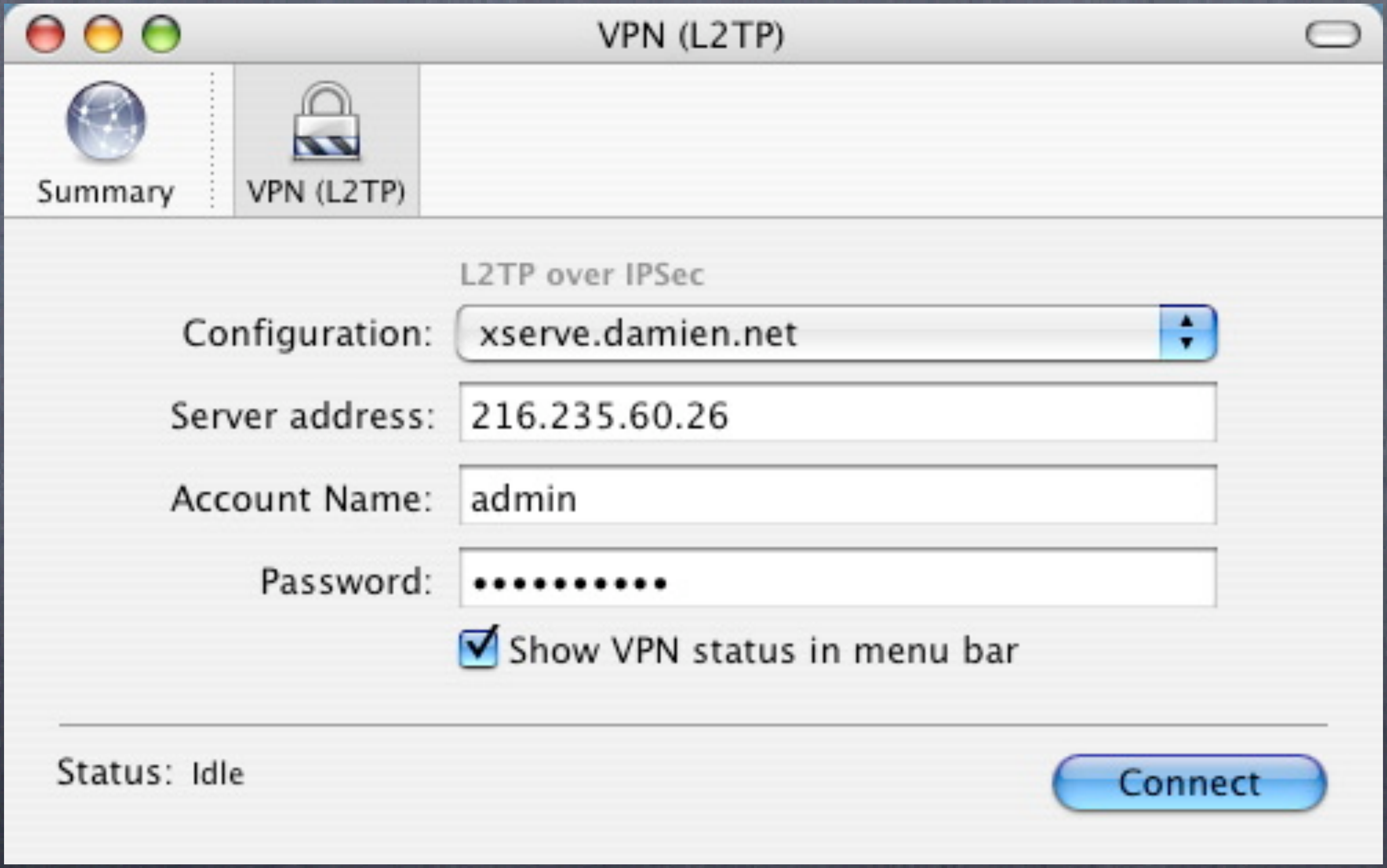
This config can be saved, stored on a web server as a .dmg file

# VPN connection menu



If only one config setup, no names will appear, just "connect"

# VPN: Internet Connect



Configuration: xserve.damien.net

Server address: 216.235.60.26

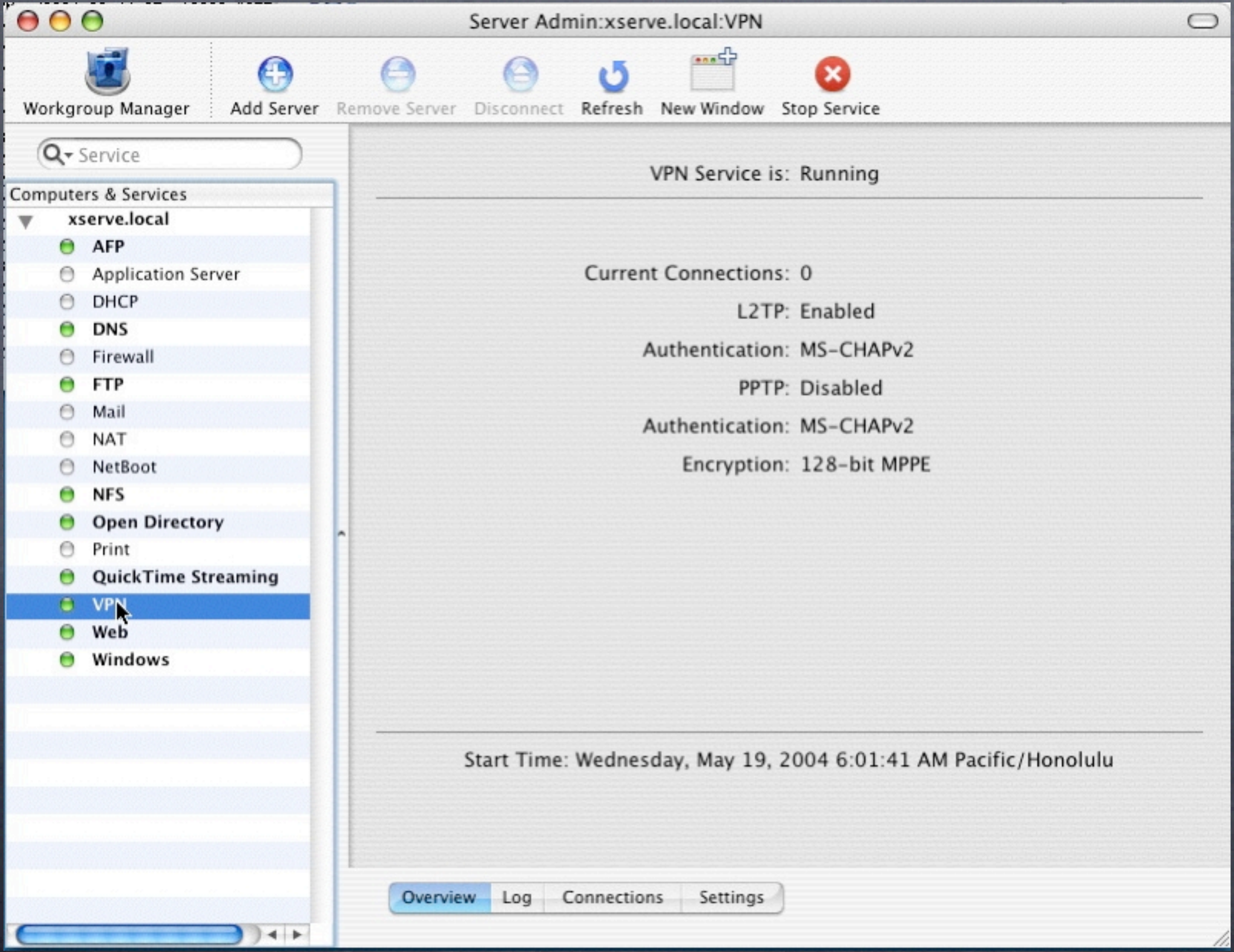
Account Name: admin

Password: •••••••••••

☑ Show VPN status in menu bar

Status: Idle

# VPN: Panther/Tiger/Leopard server



VPN Service is: Running

Current Connections: 0

L2TP: Enabled

Authentication: MS-CHAPv2

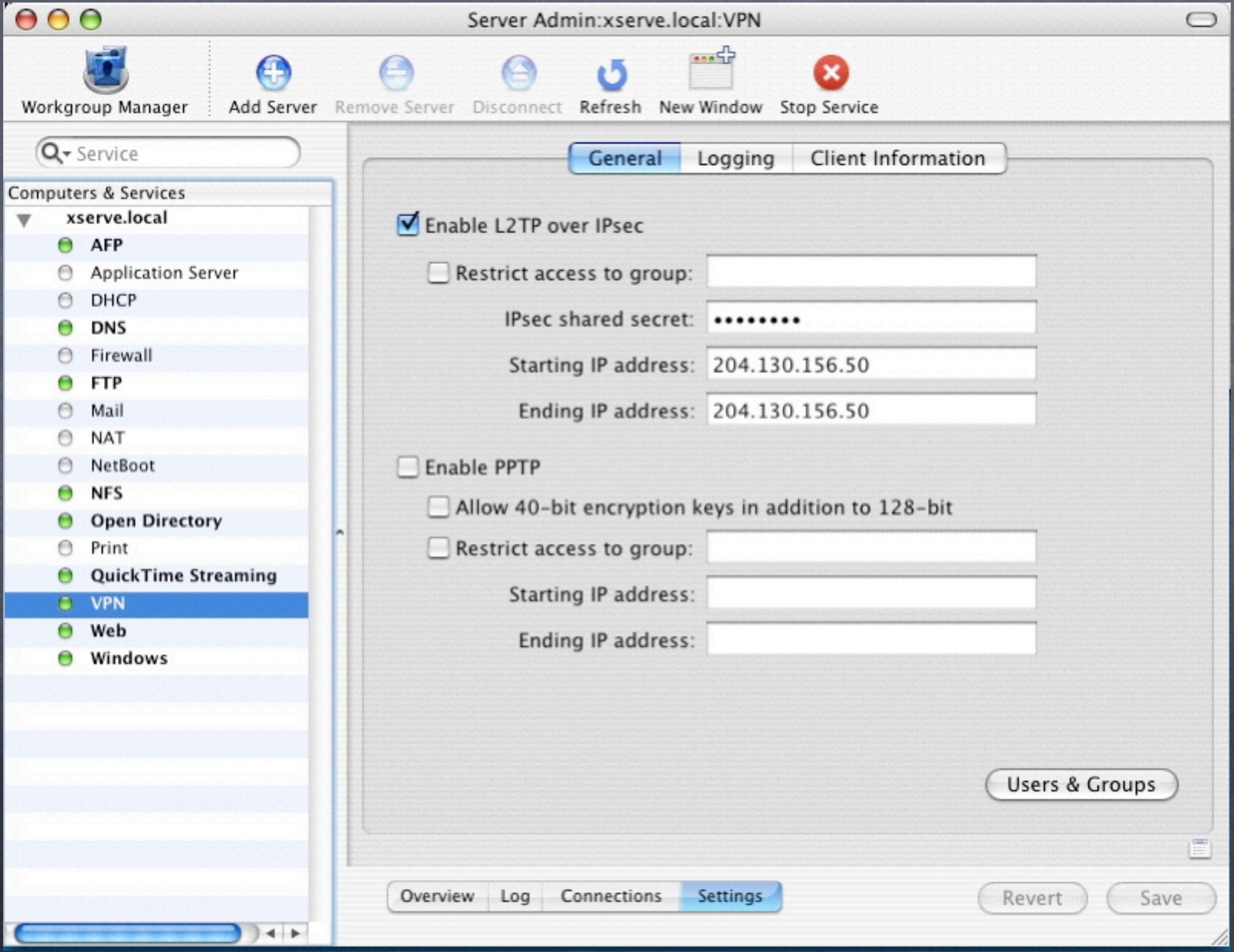
PPTP: Disabled

Authentication: MS-CHAPv2

Encryption: 128-bit MPPE

Start Time: Wednesday, May 19, 2004 6:01:41 AM Pacific/Honolulu

# VPN: Panther/Tiger/Leopard Server



☑ Enable L2TP over IPsec

☐ Restrict access to group:

IPsec shared secret: •••••••••

Starting IP address: 204.130.156.50

Ending IP address: 204.130.156.50

☐ Enable PPTP

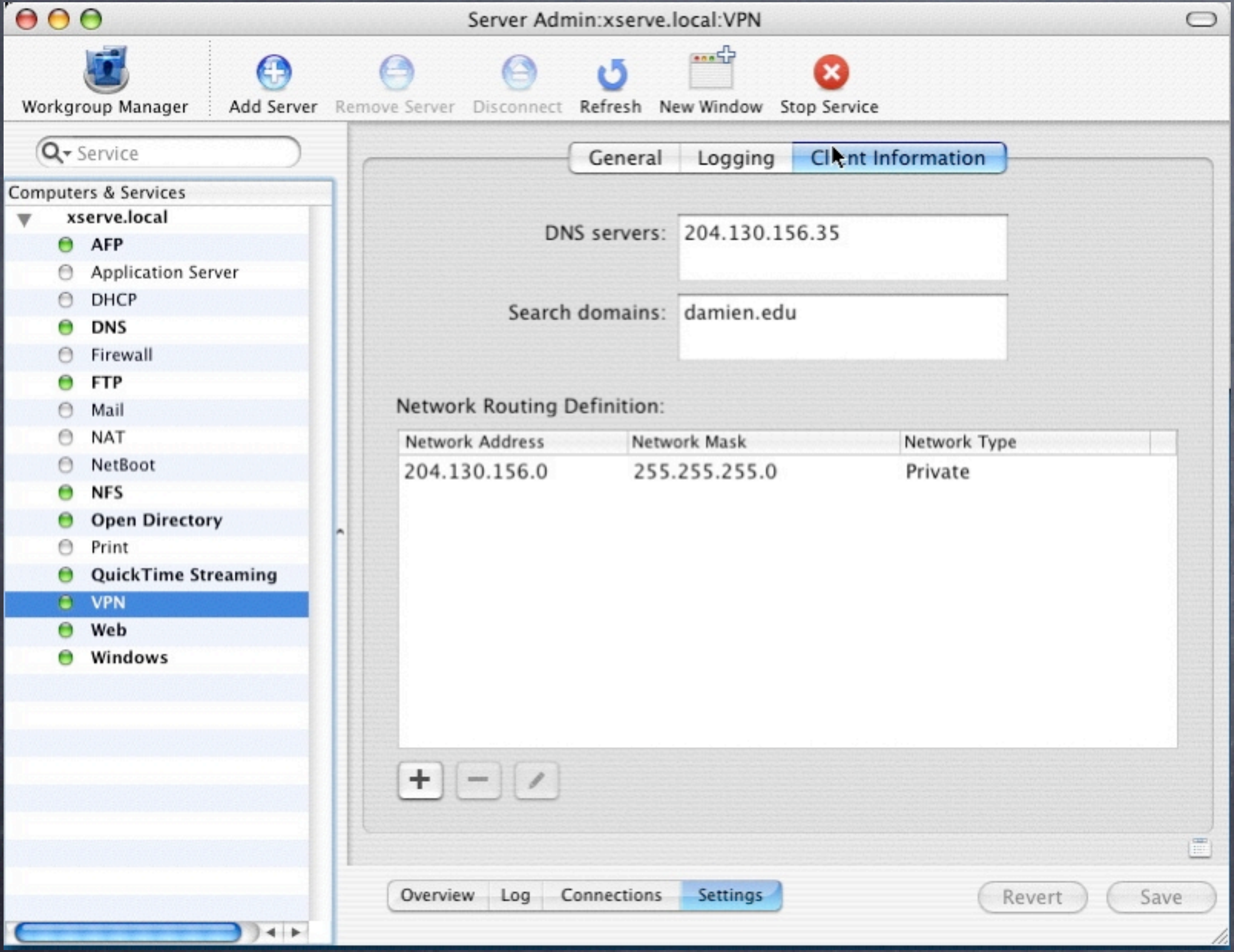
☐ Allow 40-bit encryption keys in addition to 128-bit

☐ Restrict access to group:

Starting IP address:

Ending IP address:

# VPN routes table



DNS servers: 204.130.156.35

Search domains: damien.edu

Network Routing Definition:

| Network Address | Network Mask | Network Type |
|---|---|---|
| 204.130.156.0 | 255.255.255.0 | Private |

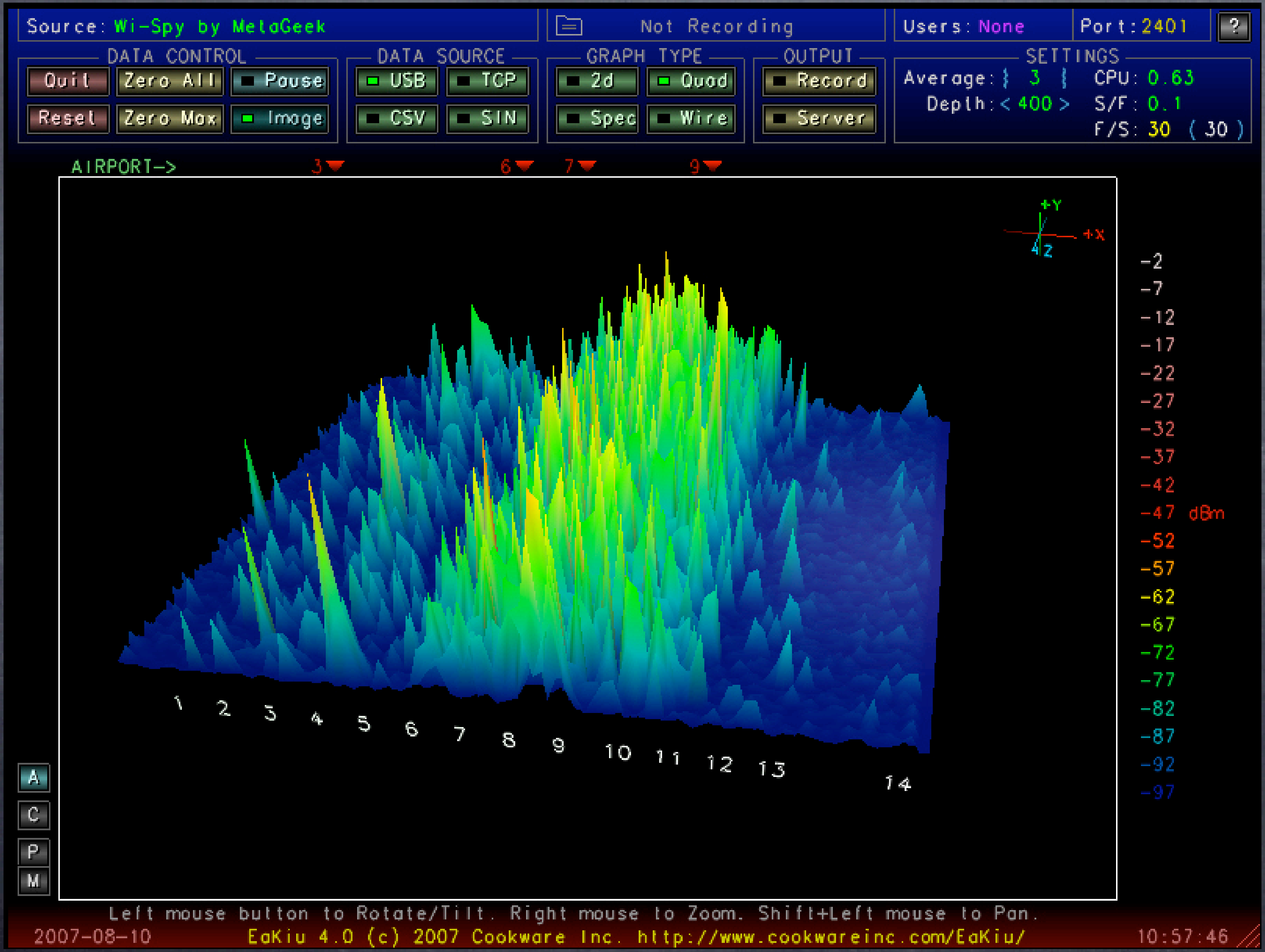
Note private and public network types

# Hands-on: Packet Sniffing

- Using your laptop, connect to the network named alpha
- Install Interarchy http://nolobe.com/interarchy/
- Open File->net->traffic
- Check your own webmail, and watch for your password
- Login to the VPN provided, and retest, looking for browser traffic from others
- If interested, you can do this as well with IP Net monitor http://www.sustworks.com/
- Share your results

# Section 3

# Infrastructure: yours, theirs



Source: Wi-Spy by MetaGeek

Not Recording

Users: None

Port:2401

Average: { 3 }

Depth: < 400 >

CPU: 0.63

S/F: 0.1

F/S: 30 ( 30 )

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

# Wired networks

- Secure(depends on physical access)
- Full duplex
- Max range 300 ft, more in segments w/ switches
- One protocol (802.3 vs. 802.2, SNAP, Ethernet II)
- Planned and installed
- 10/100/1000 mb/s
- Collision Detection (CSMA-CD)
- Switch manages traffic
- OK with 802.1x and VPN
- One "band"
- Packet Sniffer on LAN hard w/ switch
- HW address authentication possible (RADIUS)

# Wireless networks

- Different from Ethernet, though similarly standardized (802.11 vs. 802.2 etc.)
- Uses radio waves instead of wires
- Channelized
- Shares frequency with Bluetooth, cordless phones, microwave ovens, Police RADAR, others
- Limited range with OEM equipment
- Speed and reliability depend on signal
- Signal depends on both ends: Access Point and client (laptop or iPhone)
- Possible to augment signals with antennas and amplifiers

# Wireless networks

- Often insecure (physical access less restricted)
- Half duplex (802.11a,b,g)
- Max range 150 ft. w/ OEM, 42 miles in other cases
- Several protocols: 802.11a, b, g, n
- Flexible, expandable, portable
- 11/54 mb/s (802.11b,g)
- Collision avoidance (CSMA-CA) also used in AppleTalk
- Hidden node problem
- Channelized
- Packet Sniffers very easy and hard to detect
- HW address authentication possible (RADIUS)

# 802.11 standards decoder ring

802.11 wireless IEEE standards evolution:

- 802.11: 900 mhz (0.9 ghz), 2 mb/s, ca. 1998
- 802.11b: 2.4 ghz, 11 mb/s, ca. 2000
- 802.11a: 5.8 ghz, 54 mb/s, ca.2000, uses OFDM data encryption
- 802.11g: 2.4 ghz, 54 mb/s, 802.11b with OFDM for 54 mb/s
- 802.11n: 2.4 and 5.8 ghz, 600 mb/s MIMO, 802.1x security, dual band
- 802.11i: a security protocol standard including 802.1x authentication

# Wireless tips

- Range is usually limited to several hundred feet
- Rain, water, wet leaves, people-anything with water tend to stop the signal
- Hidden nasties: chicken wire, wire mesh, re-bar, security glass, window tint, lots of paper, sharp metallic objects
- “Plant your antennas in the spring”
- Others: energy saving bulbs, microwave ovens (physical interference)
- Most wireless networks have “invisible company” (logical interference) such as tunnels, closed networks, video leapfrogs

# Wireless terms

- LAN: local area network
- wLAN: Wireless local area network
- AP: Access point
- Client: the user (usually a laptop)
- WEP: Wired Equivalent Privacy (passwords)
- WPA: better than WEP, changing passwords(TKIP)
- Radio: the part of the computer/AP that handles the wireless system
- Backhaul: a link back to the servers or LAN

# User issues: good stuff

- Flexibility in location (couch, etc.)
- Flexibility in numbers of users (conferences, classrooms need not be wired for each user)
- Can be deployed for temporary setups
- Allows users to access resources when buildings (e.g. libraries) are closed
- Lower TCO (total cost of ownership) in many cases
- Roaming possible in many cases
- Multimedia? 802.11n

# User issues: bad stuff

- Less predictable than wired (weather, traffic, etc.)
- Less secure (in most deployments)
- Can be poached, intercepted, etc. exposing LAN assets
- Very difficult to locate users for service/diagnostics
- Half-Duplex vs. Full-Duplex
- Can be a challenge for novice users: switching from wired to wireless client and back, poor setups

# Wireless planning

- Site Survey
- Expansion needs
- User survey
- Walk-around: foliage, power, obstructions, interference

# Site survey

- Virtual cloud needed?
- Bridging to wired LAN needed?
- Remote buildings?
- Neighbors?
- Other interference?

# Wireless Survey: Software tools

- iStumbler
- MacStumbler
- KisMAC
- IP Net Monitor
- WiSpy (Eakiu)

# Wireless Survey:
# Hardware tools

- Rayming TN-200/BU-353 GPS receiver
- Zyxel AG-225H USB scanner/receiver
- Netgear MA-111 USB wireless adapter
- QuickerTek amps/antennas

# Wireless History, via Access Points:

Precambrian Era: 802.11 (no letters), "wavelan" 1-2 mb/s, 900 mHz ISM band

3.x--Airport I ("graphite"): 802.11b, 2.4 gHz, 11 mb/s, WEP only, easy to hack into for amps, antennas etc.

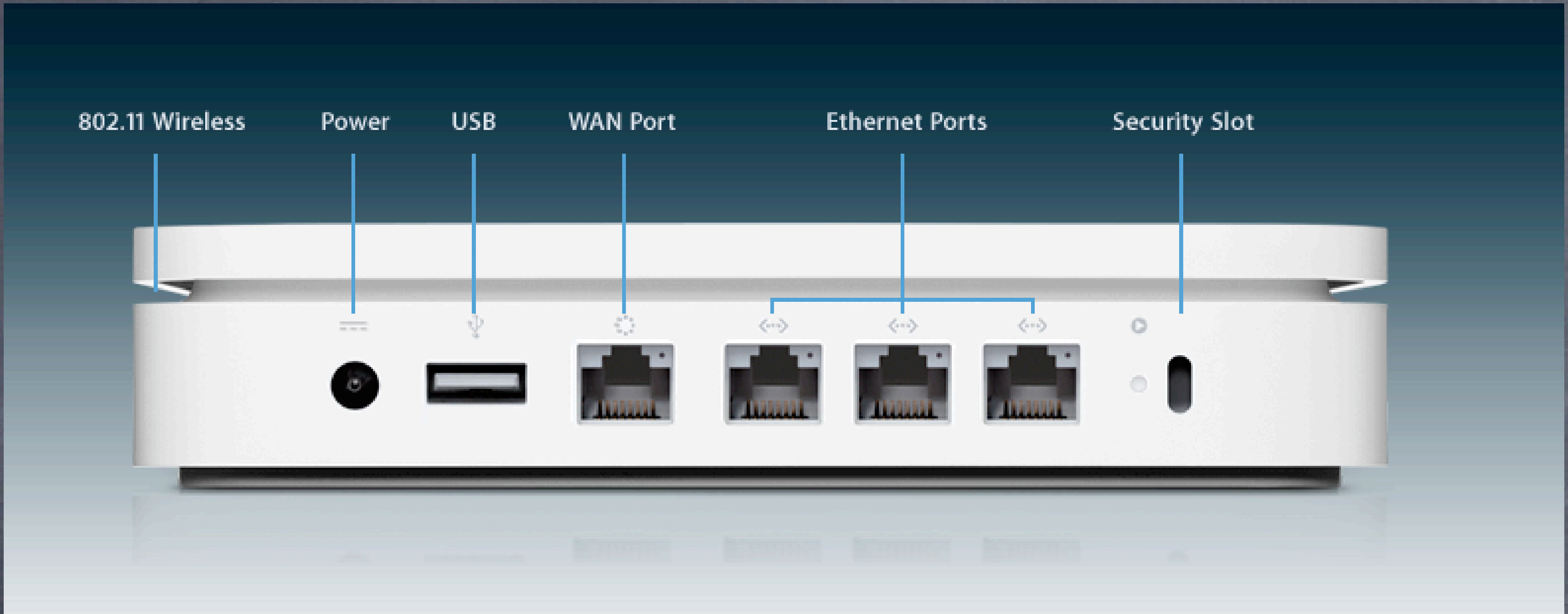
4.x--Airport II ("snow"): 802.11b, 2.4 gHz, 11 mb/s, added PPP server, non-lucent proprietary card (harder to hack into)

5.x--Airport III ("extreme"): 802.11b/g, 2.4 gHz, 11/54 mb/s, added WPA, WPA2, 802.1X, USB printing, SNMP, telnet, and WDS. External antenna connector, and power adjust via software.

6.x--Airport Express: 802.11b/g, 2.4 gHz, 11/54 mb/s, integral power supply, USB printing, audio output, WDS base/client

7.x--Airport Extreme ("X2"): 802.11b/g/n, 2.4 and 5.8 gHz, 11/54/600 mb/s, soon to be in iPods/iTV?

# Airport Extreme Base Station v.7: MIMO, 802.11n



- Latest Airport Extreme
- 600 mb/s throughput
- Uses MIMO (multiple in, multiple out) with many antennas
- Greater range, esp. to smart 802.11n clients
- Range can be extended using QuickerTek antennas (3)
- USB printer sharing, as well as disk sharing
- Supports latest version of WPA2 802.1x security

# Lab: Airport Setup

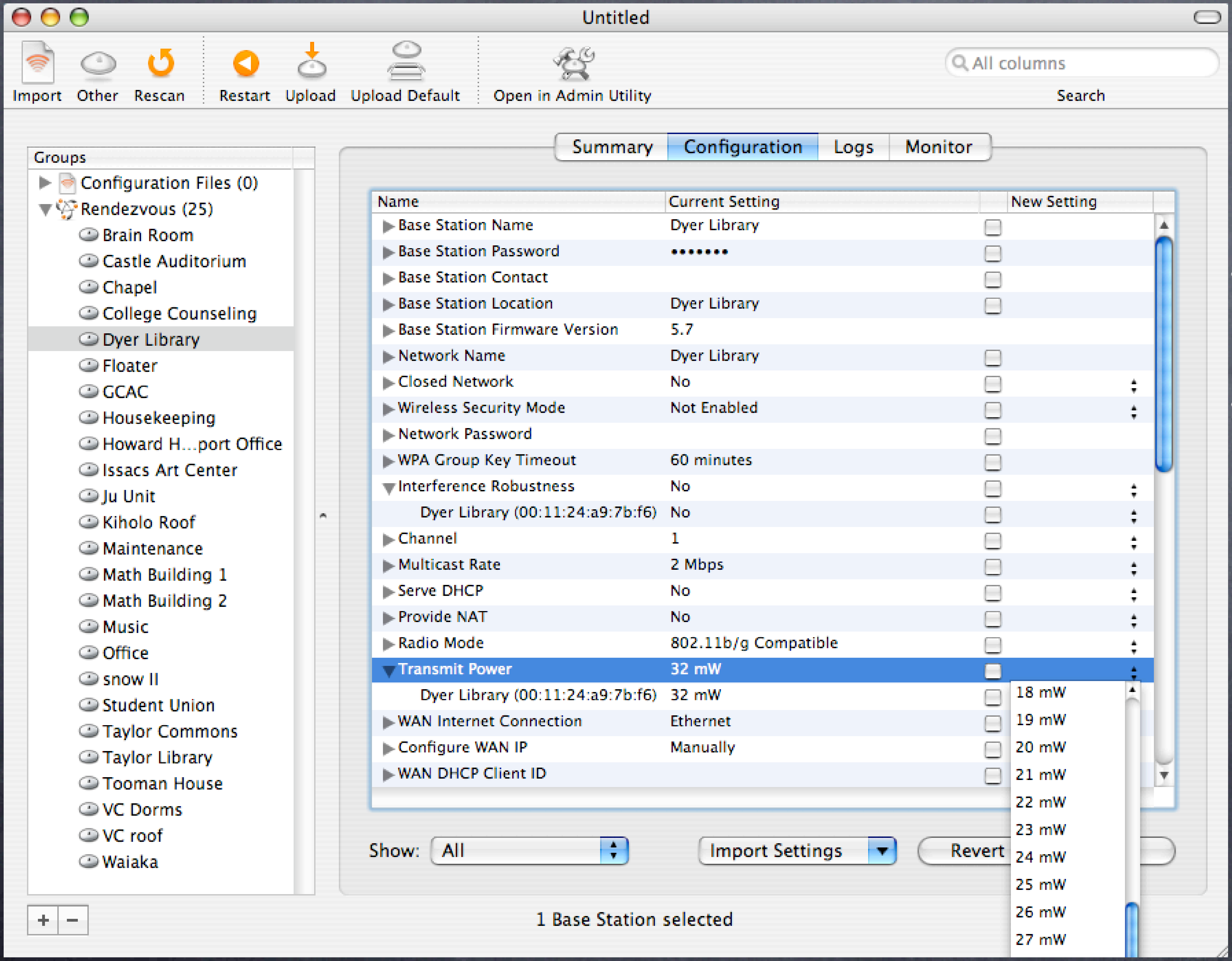
1. Setup airport with no security, test SNR using client apps
2. Repeat using Airport Management Utility to test SNR
3. Fire up the video unit and watch what happens to the SNR on each channel
4. Activate WEP on the AP, test access from a client
5. Activate WPA2 on the AP, test access from a client
6. Activate SNMP, watch traffic using Cybergauge
7. Activate syslog to server, watch log entries
8. Try telnet access
9. Setup PPP server
10. Monitor SNR for various clients using Airport Management Utility (AMU)

(n.b. See appendix for Airport setup pages)

# Airport Extreme:
# When things go wrong

- If you cannot connect to the Airport, try connecting to the LAN port instead of the WAN port
- If the LAN port is unreachable, make sure you are using a hub or direct cable (crossover or straight) instead of a switch between the computer and the base station
- The IP address configuration of the control computer must be on the same subnet as the base station. You can setup a temporary location to handle this (169.x.x.x address)
- If you are still having difficulty, connect wirelessly, and set your computer to DHCP, with only the airport connection active
- To reset the base station, insert a paperclip or pen into the small hole on the front. This works much better if you unplug the wired network cables
- Be very careful with DHCP: enabling it on your LAN can knock out the existing DHCP server on that LAN (another reason never to use the LAN port as an uplink port)

# Airport Management Utility (a.k.a. wireless Plutonium)



Groups

- Configuration Files (0)
- Rendezvous (25)
  - Brain Room
  - Castle Auditorium
  - Chapel
  - College Counseling
  - Dyer Library
  - Floater
  - GCAC
  - Housekeeping
  - Howard H...port Office
  - Issacs Art Center
  - Ju Unit
  - Kiholo Roof
  - Maintenance
  - Math Building 1
  - Math Building 2
  - Music
  - Office
  - snow II
  - Student Union
  - Taylor Commons
  - Taylor Library
  - Tooman House
  - VC Dorms
  - VC roof
  - Waiaka

| Name | Current Setting | | New Setting |
|---|---|---|---|
| ▶ Base Station Name | Dyer Library | ☐ | |
| ▶ Base Station Password | ••••••• | ☐ | |
| ▶ Base Station Contact | | ☐ | |
| ▶ Base Station Location | Dyer Library | ☐ | |
| ▶ Base Station Firmware Version | 5.7 | | |
| ▶ Network Name | Dyer Library | ☐ | |
| ▶ Closed Network | No | ☐ | |
| ▶ Wireless Security Mode | Not Enabled | ☐ | |
| ▶ Network Password | | ☐ | |
| ▶ WPA Group Key Timeout | 60 minutes | ☐ | |
| ▼ Interference Robustness | No | ☐ | |
| Dyer Library (00:11:24:a9:7b:f6) | No | ☐ | |
| ▶ Channel | 1 | ☐ | |
| ▶ Multicast Rate | 2 Mbps | ☐ | |
| ▶ Serve DHCP | No | ☐ | |
| ▶ Provide NAT | No | ☐ | |
| ▶ Radio Mode | 802.11b/g Compatible | ☐ | |
| ▼ Transmit Power | 32 mW | ☐ | |
| Dyer Library (00:11:24:a9:7b:f6) | 32 mW | ☐ | |
| ▶ WAN Internet Connection | Ethernet | ☐ | |
| ▶ Configure WAN IP | Manually | ☐ | |
| ▶ WAN DHCP Client ID | | ☐ | |

Show: All

Import Settings

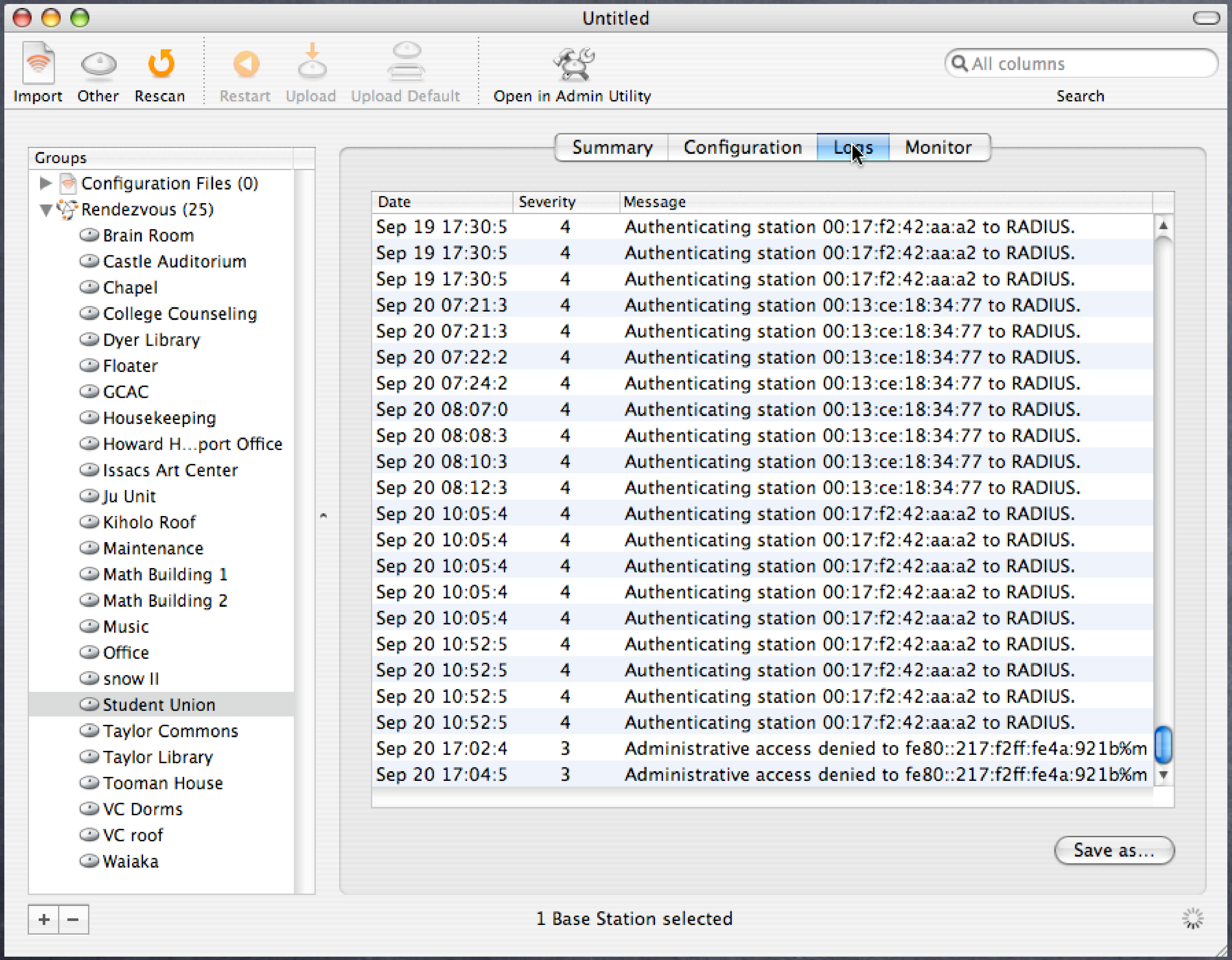
Revert

1 Base Station selected

Airport Management Utility

- Changes are in XML format, as in Property List Editor (plist editor)
- Control over many functions not possible in other utilities (see power here, listed as numbers rather than lower/higher)

# Airport Management Utility (a.k.a. wireless Plutonium)

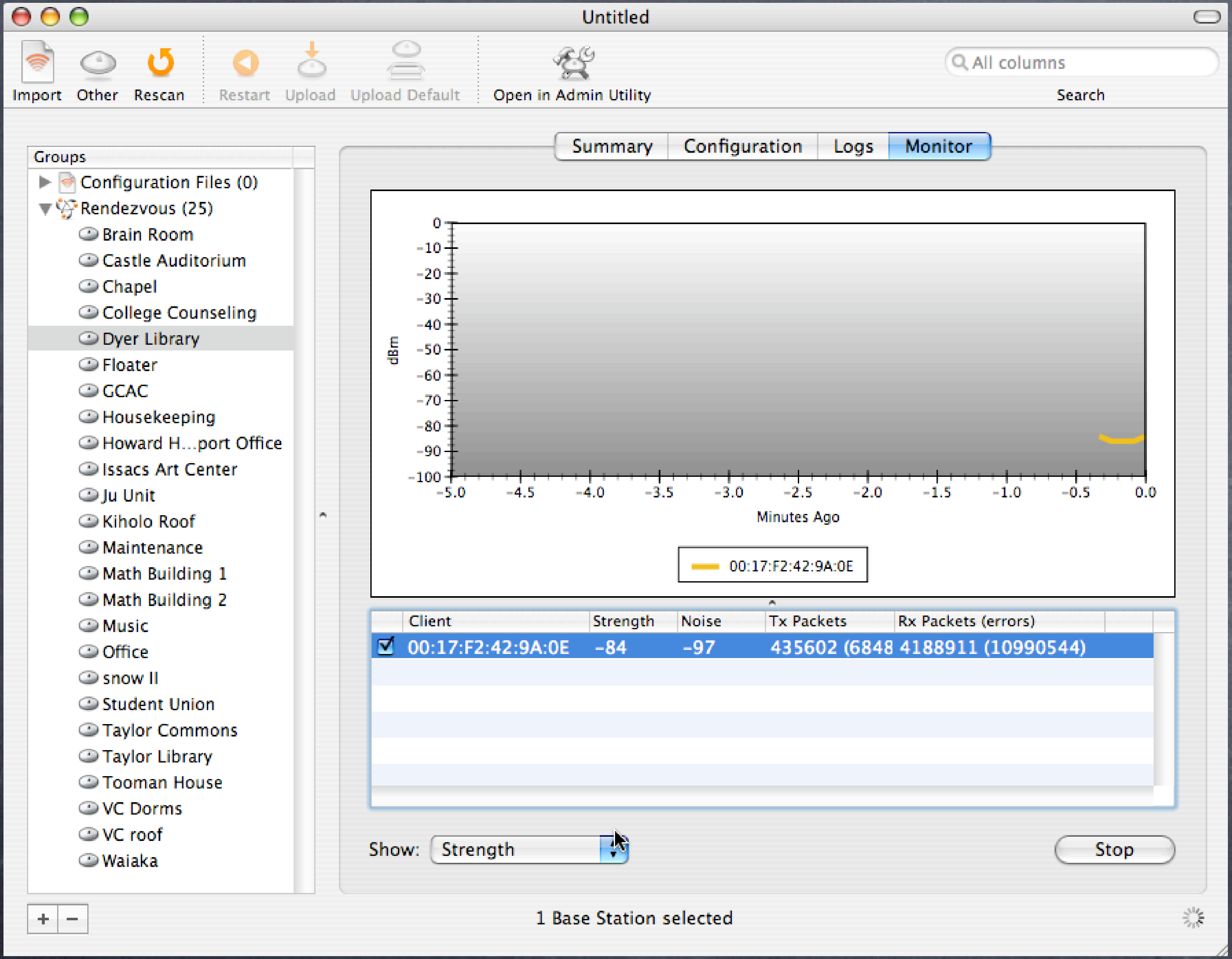


```
Date           Severity  Message
Sep 19 17:30:5    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 19 17:30:5    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 19 17:30:5    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 20 07:21:3    4      Authenticating station 00:13:ce:18:34:77 to RADIUS.
Sep 20 07:21:3    4      Authenticating station 00:13:ce:18:34:77 to RADIUS.
Sep 20 07:22:2    4      Authenticating station 00:13:ce:18:34:77 to RADIUS.
Sep 20 07:24:2    4      Authenticating station 00:13:ce:18:34:77 to RADIUS.
Sep 20 08:07:0    4      Authenticating station 00:13:ce:18:34:77 to RADIUS.
Sep 20 08:08:3    4      Authenticating station 00:13:ce:18:34:77 to RADIUS.
Sep 20 08:10:3    4      Authenticating station 00:13:ce:18:34:77 to RADIUS.
Sep 20 08:12:3    4      Authenticating station 00:13:ce:18:34:77 to RADIUS.
Sep 20 10:05:4    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 20 10:05:4    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 20 10:05:4    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 20 10:05:4    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 20 10:05:4    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 20 10:52:5    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 20 10:52:5    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 20 10:52:5    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 20 10:52:5    4      Authenticating station 00:17:f2:42:aa:a2 to RADIUS.
Sep 20 17:02:4    3      Administrative access denied to fe80::217:f2ff:fe4a:921b%m
Sep 20 17:04:5    3      Administrative access denied to fe80::217:f2ff:fe4a:921b%m
```

Airport Management Utility

- Log screen shows access and denial (good for security and troubleshooting user issues)

# Airport Management Utility (a.k.a. wireless Plutonium)



Groups

- Configuration Files (0)
- Rendezvous (25)
  - Brain Room
  - Castle Auditorium
  - Chapel
  - College Counseling
  - Dyer Library
  - Floater
  - GCAC
  - Housekeeping
  - Howard H...port Office
  - Issacs Art Center
  - Ju Unit
  - Kiholo Roof
  - Maintenance
  - Math Building 1
  - Math Building 2
  - Music
  - Office
  - snow II
  - Student Union
  - Taylor Commons
  - Taylor Library
  - Tooman House
  - VC Dorms
  - VC roof
  - Waiaka

| | Client | Strength | Noise | Tx Packets | Rx Packets (errors) |
|---|---|---|---|---|---|
| ☑ | 00:17:F2:42:9A:0E | -84 | -97 | 435602 (6848 | 4188911 (10990544) |

Show: Strength

1 Base Station selected

Airport Management Utility

- Strength or noise graphs, multiple clients on same screen for site survey work

# Airport Management Utility (a.k.a. wireless Plutonium)

Notes:

- Caution Caution Caution
- Very powerful
- Will not warn you if you try to do something wrong
- Uses Rendezvous, much faster, less configuration of the manager machine
- Can save config files for multiple deployment (as in Admin Utility)
- Works best with Airport Extreme, not so well on the new MIMO access points

## Access Point Security Basics (in order of severity):

1. Change the admin password and login
2. DHCP off
3. WEP
4. Closed network (no SSID)
5. Admin access on wired LAN only
6. Remote admin to non-standard port
7. Hardware ACL lists
8. VPN
9. WPA2

10 802.1X

# Summary

Day one take-aways:

- Case studies show similar issues, solutions
- Access methods may vary
- Security is a major issue for mobile users
- Timbuktu and ARD can extend your reach
- VPN is a good security solution: easy and safe
- Wireless setups require a survey of what's up already
- Simple steps can secure your mobile access
- Mobile users must appreciate their impact on the wired/home network

# Section 4: Security: as guest and as host

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

- Solutions
  - VPN for secure tunnel (see section 2)
  - 802.1x/WPA2 for encrypted authentication

# Access Control Basics

Access Control History:

- No Access Control
- WEP (passwords, easily broken)
- MAC authentication-based on wireless hardware address
- WPA/WPA2-based on the 802.1x standard
  - TKIP (temporal Key integrity protocol-password changes frequently)
  - TTLS-EAP (tunneled authentication protocols, processes)
  - CCMP and MIC (data integrity checks)
  - can be personal (negotiation with AP) or Enterprise (RADIUS server)

# Authentication: why is it so important?

- Open access points are similar to leaving an ethernet cable in your parking lot: they expose everything on your network to interlopers
- If you deal with any health records, HIPAA outlines fines for allowing access to these records
- As a wireless client, anyone authenticated has more access to your data (see interarchy demo)
- Note that VPN mitigates this vulnerability
- Man-in-the-middle attacks involve an attacker masquerading as an AP to get your login info/sensitive data (coffee shop example-Kismac)
- Solution: 802.1x and the EAPS (Extensible Authentication Protocols)

# 802.1x

- WEP: AP and client agree on a password, this is used to control access
- Problem: the key is used repeatedly, so can be cracked (see Kismac)
- Solution: Make the keys change (TKIP)

- Problem: how to agree on the first key in the open?
- Solution: 802.1x authentication to the host

- Host: Access point-can negotiate this authentication solo (WPA2 personal mode) or pass on the requests to a central server (RADIUS)
- Problems: some legacy and PC users may not be able to play, so the security falls to the lowest common denominator (fence analogy)

# Authentication options

## MAC address authentication:

- Add users (mac or pc) to Access Point Access Control List (ACL)
- Good practice: export ACL as text/excel file and upload to other APs
- Good points: no user intervention required

## WPA2 personal authentication:

- Add user accounts to access point
- Setup 802.1x on client machines, using login and password from AP
- Good points: stronger than MAC ACL

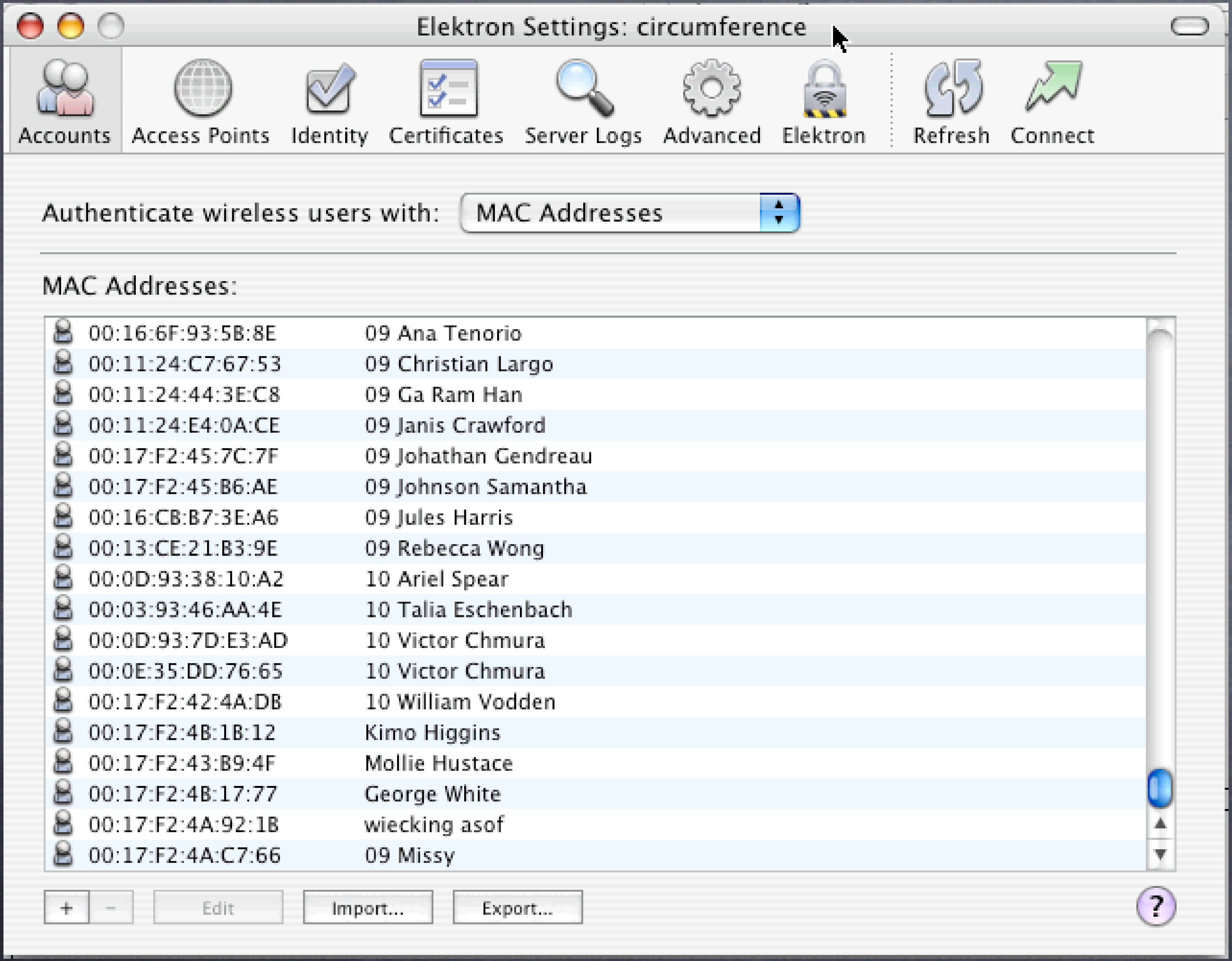
## WPA2 enterprise authentication:

- Add user accounts to RADIUS server
- Setup 802.1x on client machines, using login and password from AP
- Good points: central administration

# Elektron: what is it?

- **Basic**: HW address management: Hands-off, centrally located, no restart needed on Access Points, can be an import/export from other apps (xls, billing?)
- **Advanced**: 802.1X authentication: time sensitive passwords, public key encryption, various types of authentication, can be used as one stop shop: access points and managed switches can use the same 802.1X server

# Elektron RADIUS/WPA2 server



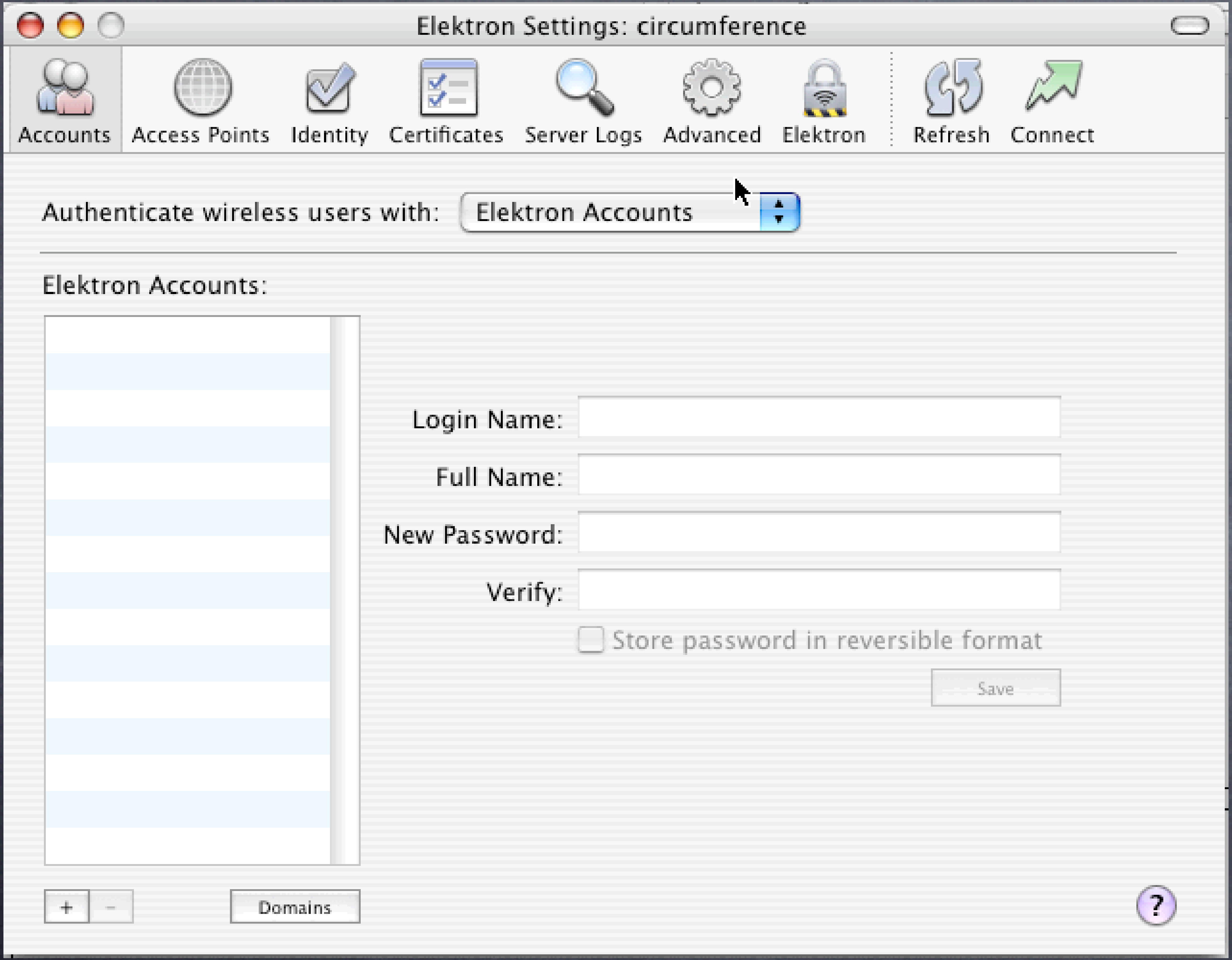
Authenticate wireless users with: MAC Addresses

MAC Addresses:

| | |
|---|---|
| 00:16:6F:93:5B:8E | 09 Ana Tenorio |
| 00:11:24:C7:67:53 | 09 Christian Largo |
| 00:11:24:44:3E:C8 | 09 Ga Ram Han |
| 00:11:24:E4:0A:CE | 09 Janis Crawford |
| 00:17:F2:45:7C:7F | 09 Johathan Gendreau |
| 00:17:F2:45:B6:AE | 09 Johnson Samantha |
| 00:16:CB:B7:3E:A6 | 09 Jules Harris |
| 00:13:CE:21:B3:9E | 09 Rebecca Wong |
| 00:0D:93:38:10:A2 | 10 Ariel Spear |
| 00:03:93:46:AA:4E | 10 Talia Eschenbach |
| 00:0D:93:7D:E3:AD | 10 Victor Chmura |
| 00:0E:35:DD:76:65 | 10 Victor Chmura |
| 00:17:F2:42:4A:DB | 10 William Vodden |
| 00:17:F2:4B:1B:12 | Kimo Higgins |
| 00:17:F2:43:B9:4F | Mollie Hustace |
| 00:17:F2:4B:17:77 | George White |
| 00:17:F2:4A:92:1B | wiecking asof |
| 00:17:F2:4A:C7:66 | 09 Missy |

- Can be used as pure MAC based or as WPA2 server

# Elektron RADIUS/WPA2 server



Authenticate wireless users with: Elektron Accounts

Elektron Accounts:

Login Name:

Full Name:

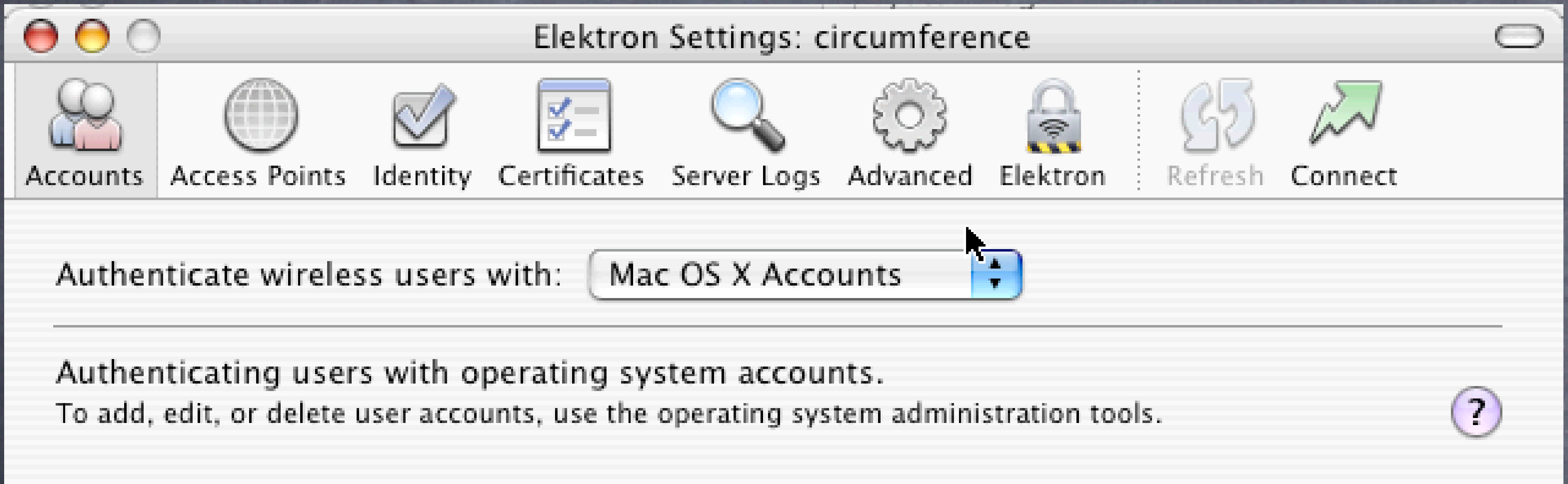
New Password:

Verify:

□ Store password in reversible format

- Accounts can be Elektron or OSX users

# Elektron RADIUS/WPA2 server

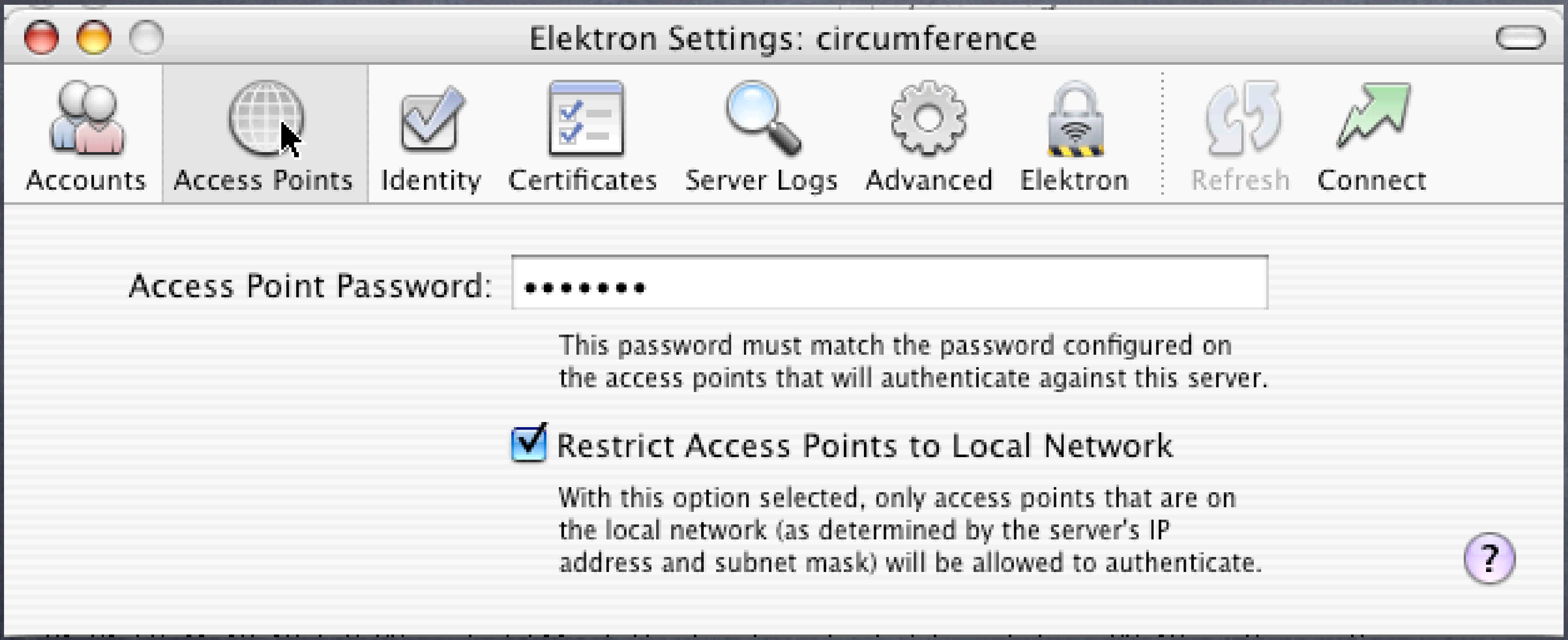


Authenticate wireless users with: Mac OS X Accounts

Authenticating users with operating system accounts.
To add, edit, or delete user accounts, use the operating system administration tools.

- OSX user accounts

# Elektron RADIUS/WPA2 server



Access Point Password: ••••••••

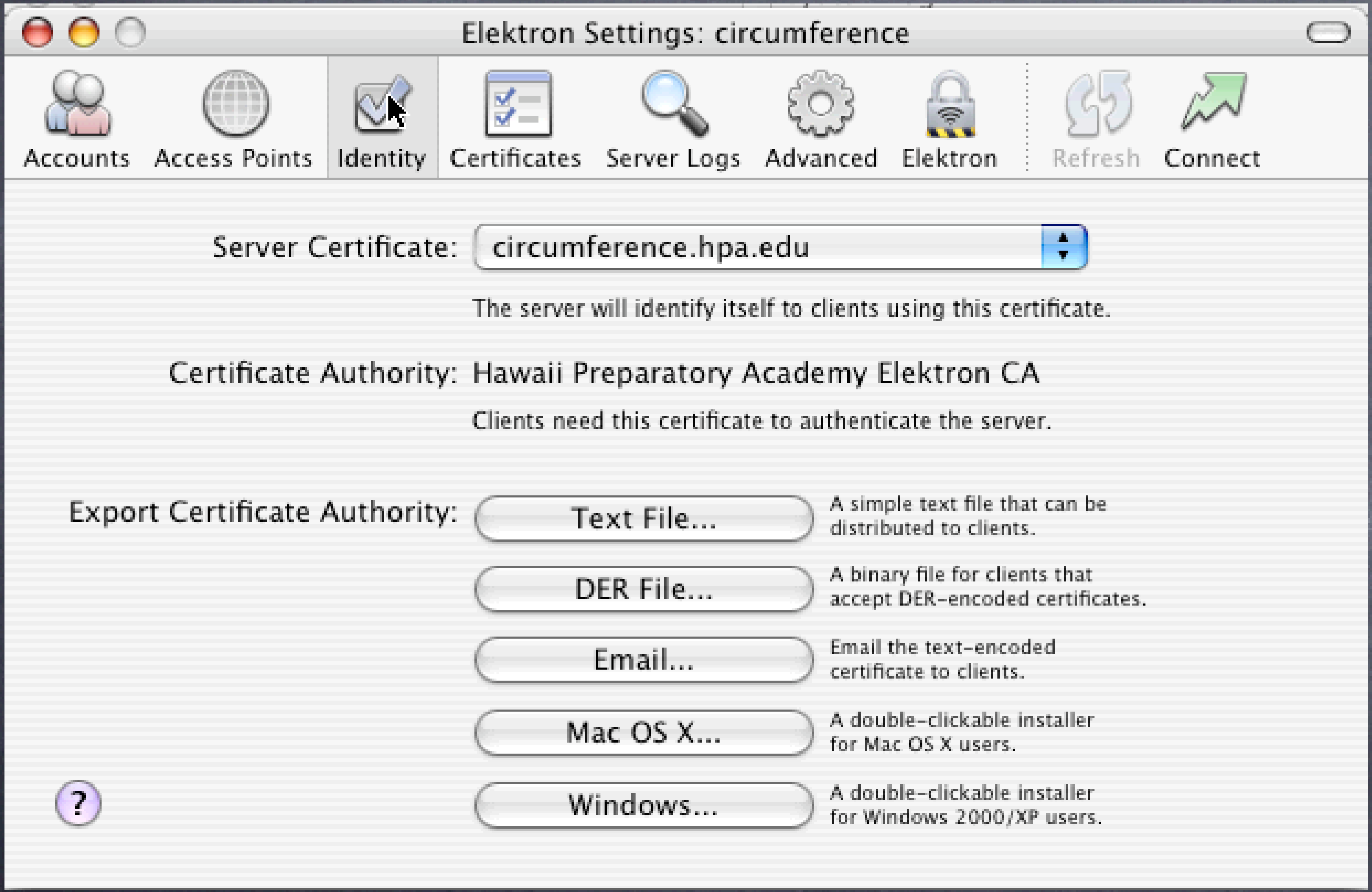
This password must match the password configured on the access points that will authenticate against this server.

☑ Restrict Access Points to Local Network

With this option selected, only access points that are on the local network (as determined by the server's IP address and subnet mask) will be allowed to authenticate.

- When configuring Access Points, passwords must agree

# Elektron RADIUS/WPA2 server



Server Certificate: circumference.hpa.edu

The server will identify itself to clients using this certificate.

Certificate Authority: Hawaii Preparatory Academy Elektron CA

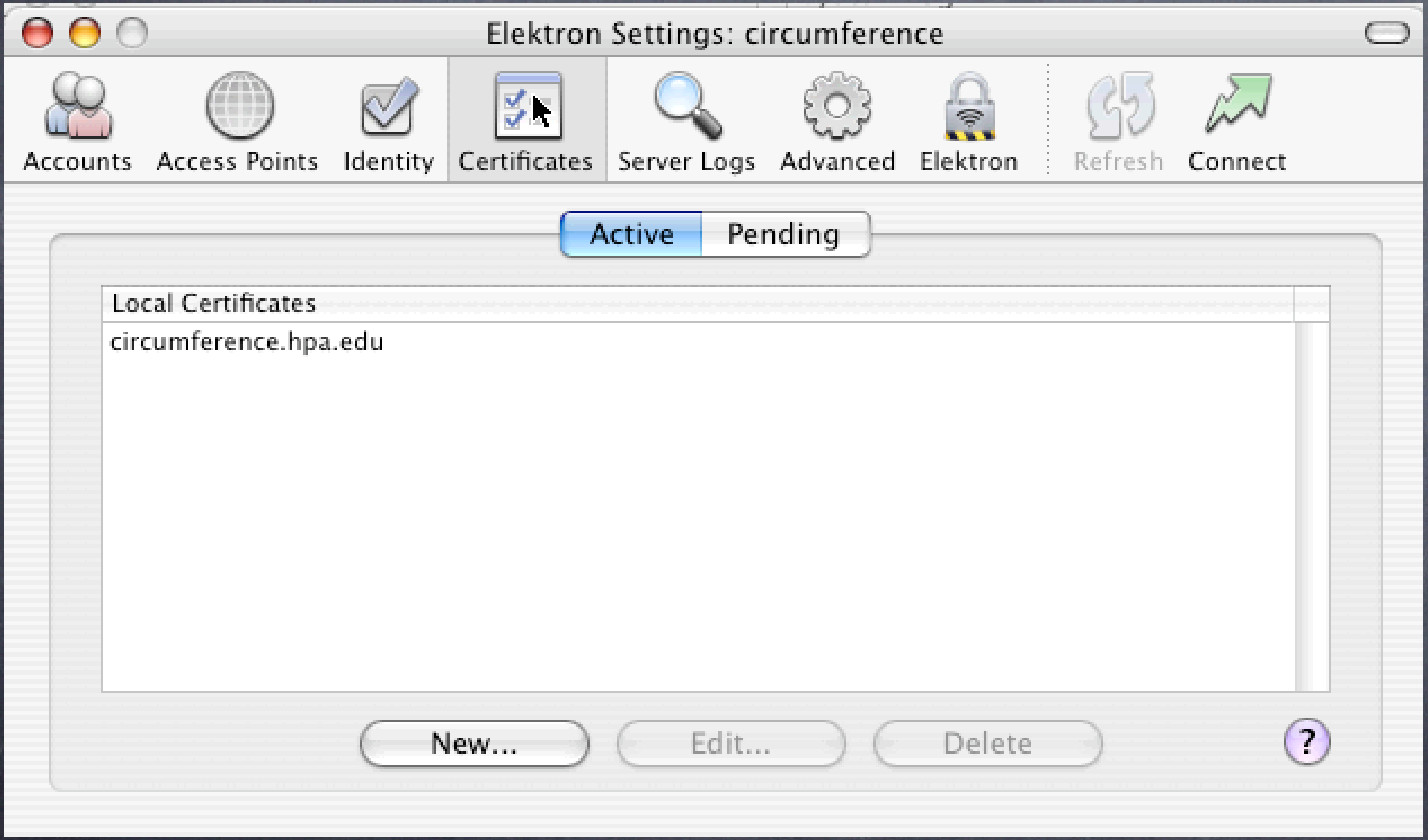
Clients need this certificate to authenticate the server.

Export Certificate Authority:

- Text File... A simple text file that can be distributed to clients.
- DER File... A binary file for clients that accept DER-encoded certificates.
- Email... Email the text-encoded certificate to clients.
- Mac OS X... A double-clickable installer for Mac OS X users.
- Windows... A double-clickable installer for Windows 2000/XP users.

- Certificates can be Verisign, Thawte or self-signed
- Generates Windows exe file for installation

# Elektron RADIUS/WPA2 server

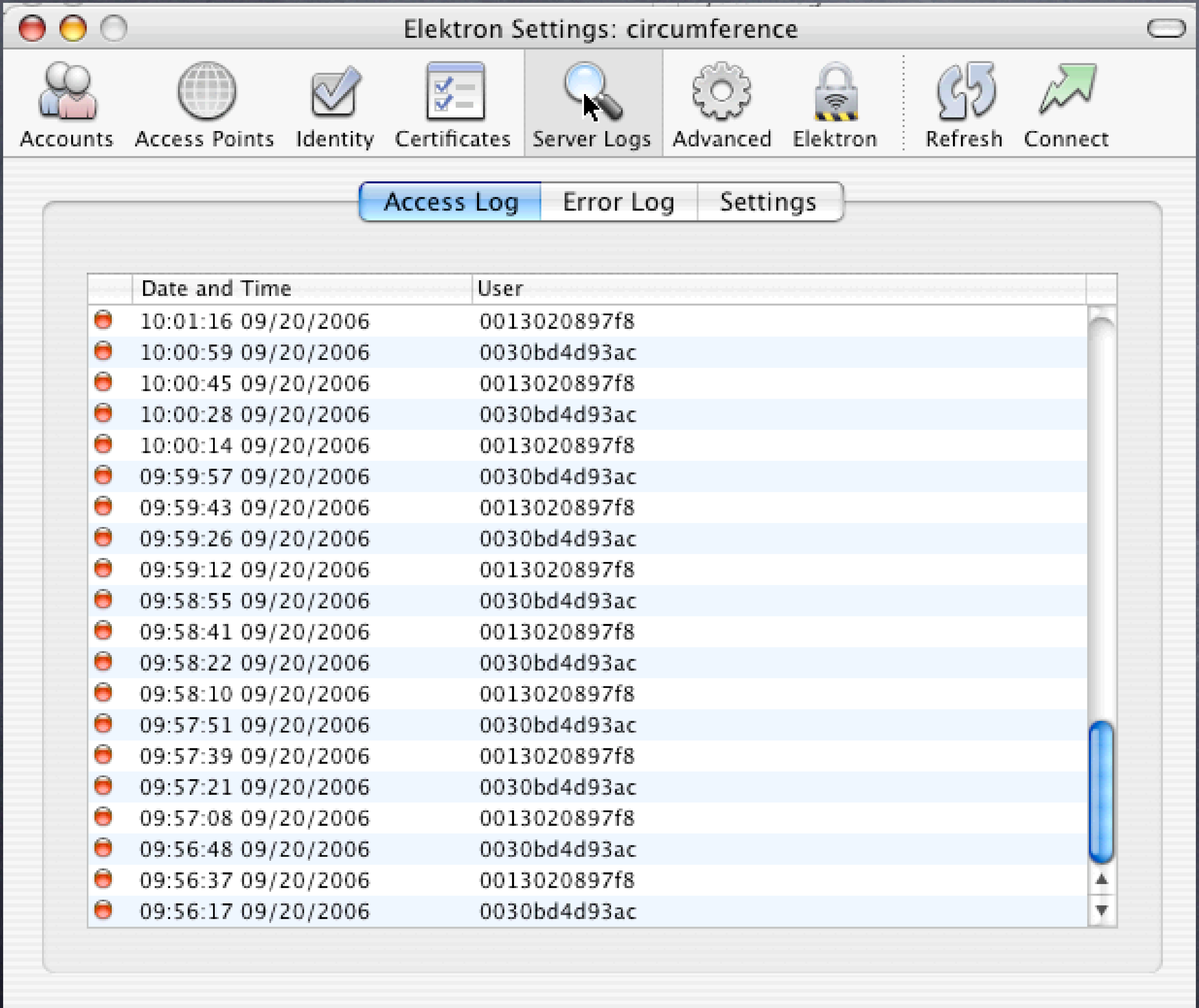


Local Certificates

circumference.hpa.edu

- Certificate window

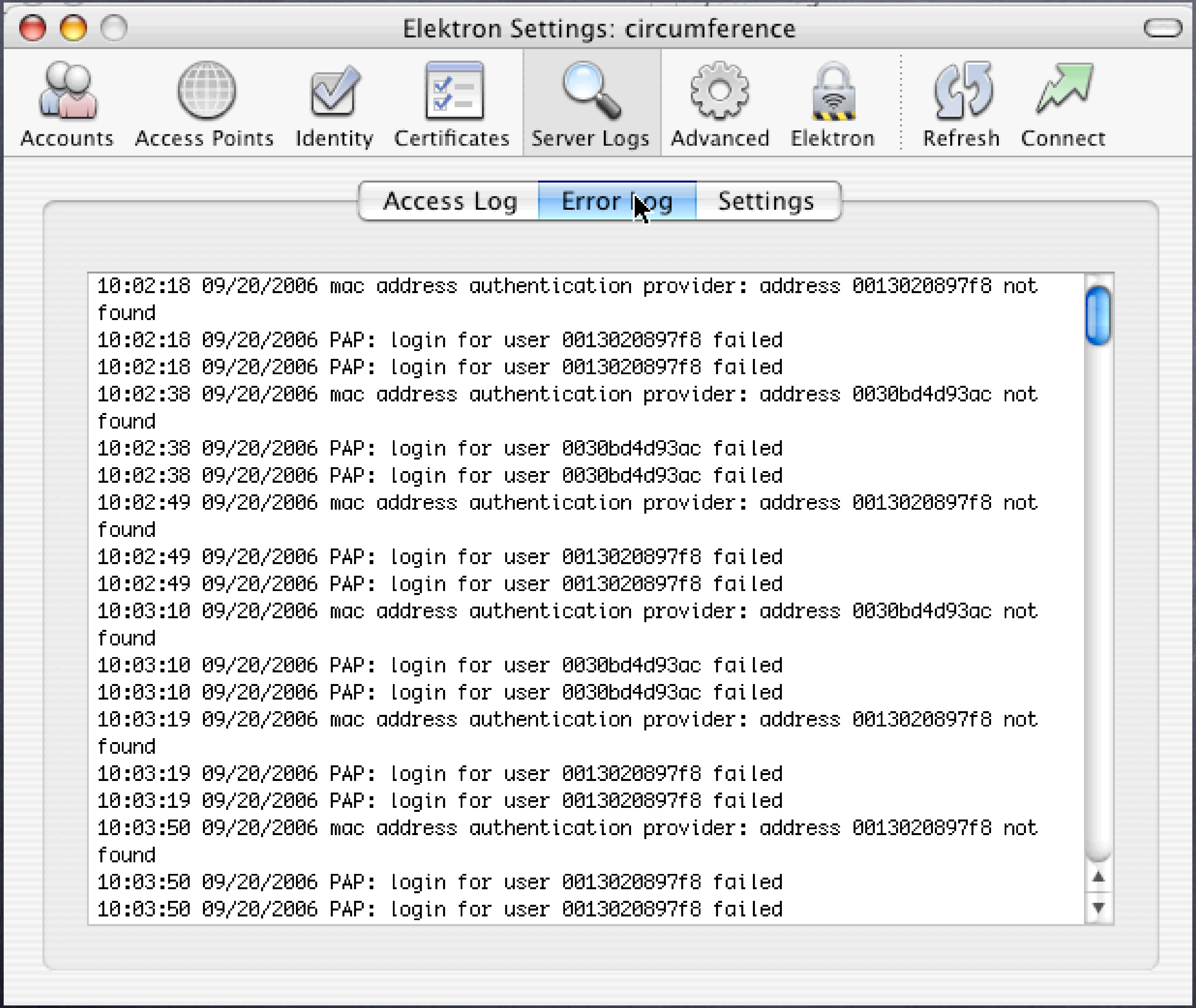
# Elektron RADIUS/WPA2 server



| | Date and Time | User |
|---|---|---|
| ● | 10:01:16 09/20/2006 | 0013020897f8 |
| ● | 10:00:59 09/20/2006 | 0030bd4d93ac |
| ● | 10:00:45 09/20/2006 | 0013020897f8 |
| ● | 10:00:28 09/20/2006 | 0030bd4d93ac |
| ● | 10:00:14 09/20/2006 | 0013020897f8 |
| ● | 09:59:57 09/20/2006 | 0030bd4d93ac |
| ● | 09:59:43 09/20/2006 | 0013020897f8 |
| ● | 09:59:26 09/20/2006 | 0030bd4d93ac |
| ● | 09:59:12 09/20/2006 | 0013020897f8 |
| ● | 09:58:55 09/20/2006 | 0030bd4d93ac |
| ● | 09:58:41 09/20/2006 | 0013020897f8 |
| ● | 09:58:22 09/20/2006 | 0030bd4d93ac |
| ● | 09:58:10 09/20/2006 | 0013020897f8 |
| ● | 09:57:51 09/20/2006 | 0030bd4d93ac |
| ● | 09:57:39 09/20/2006 | 0013020897f8 |
| ● | 09:57:21 09/20/2006 | 0030bd4d93ac |
| ● | 09:57:08 09/20/2006 | 0013020897f8 |
| ● | 09:56:48 09/20/2006 | 0030bd4d93ac |
| ● | 09:56:37 09/20/2006 | 0013020897f8 |
| ● | 09:56:17 09/20/2006 | 0030bd4d93ac |

- In hardware access mode, logs users and time authenticated

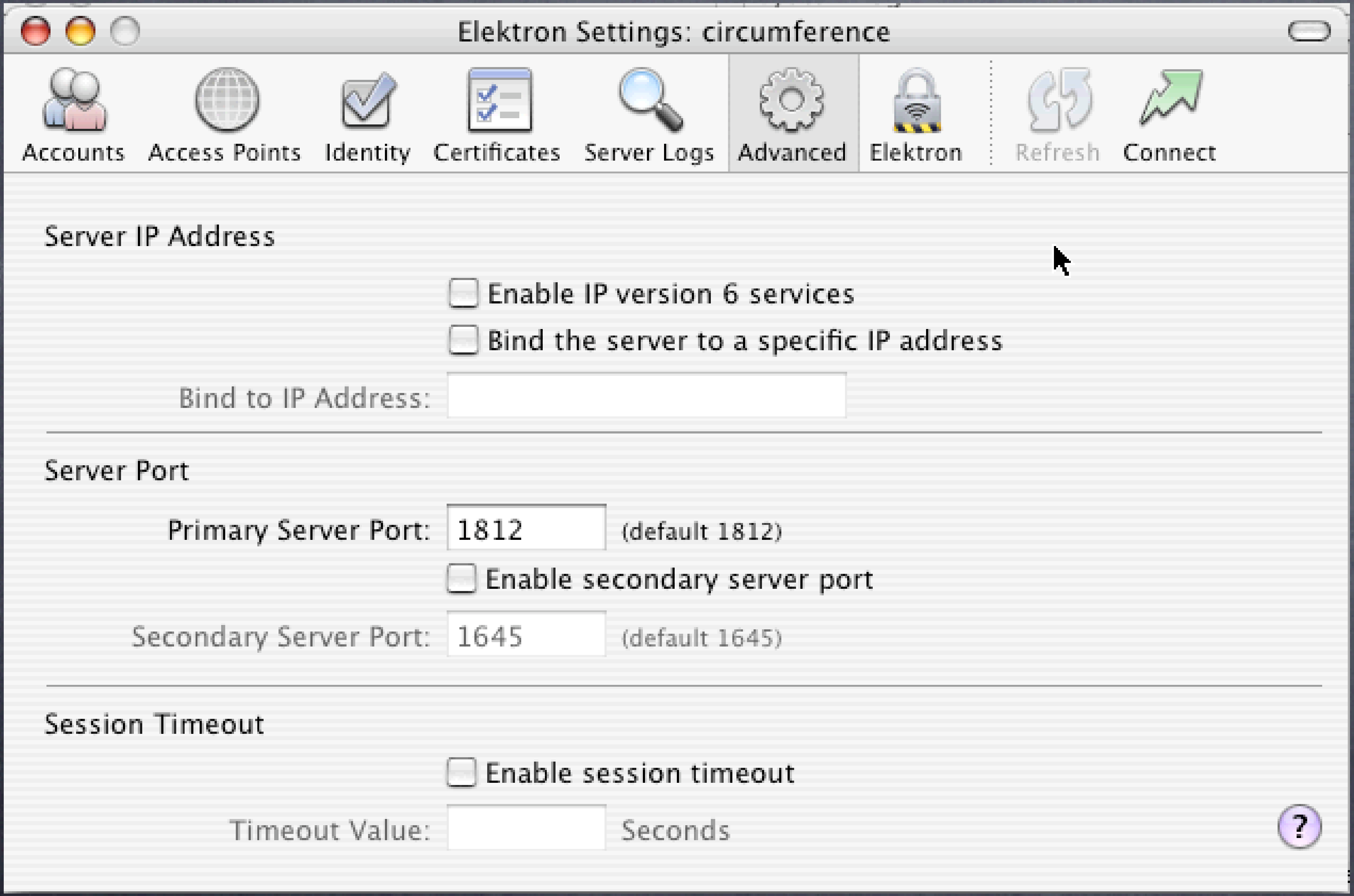
# Elektron RADIUS/WPA2 server



```
10:02:18 09/20/2006 mac address authentication provider: address 0013020897f8 not
found
10:02:18 09/20/2006 PAP: login for user 0013020897f8 failed
10:02:18 09/20/2006 PAP: login for user 0013020897f8 failed
10:02:38 09/20/2006 mac address authentication provider: address 0030bd4d93ac not
found
10:02:38 09/20/2006 PAP: login for user 0030bd4d93ac failed
10:02:38 09/20/2006 PAP: login for user 0030bd4d93ac failed
10:02:49 09/20/2006 mac address authentication provider: address 0013020897f8 not
found
10:02:49 09/20/2006 PAP: login for user 0013020897f8 failed
10:02:49 09/20/2006 PAP: login for user 0013020897f8 failed
10:03:10 09/20/2006 mac address authentication provider: address 0030bd4d93ac not
found
10:03:10 09/20/2006 PAP: login for user 0030bd4d93ac failed
10:03:10 09/20/2006 PAP: login for user 0030bd4d93ac failed
10:03:19 09/20/2006 mac address authentication provider: address 0013020897f8 not
found
10:03:19 09/20/2006 PAP: login for user 0013020897f8 failed
10:03:19 09/20/2006 PAP: login for user 0013020897f8 failed
10:03:50 09/20/2006 mac address authentication provider: address 0013020897f8 not
found
10:03:50 09/20/2006 PAP: login for user 0013020897f8 failed
10:03:50 09/20/2006 PAP: login for user 0013020897f8 failed
```

- Error log also logs unauthorized attempts (good for security as well as troubleshooting valid users)

# Elektron RADIUS/WPA2 server



Server IP Address

□ Enable IP version 6 services

□ Bind the server to a specific IP address

Bind to IP Address:

Server Port

Primary Server Port: 1812 (default 1812)

□ Enable secondary server port

Secondary Server Port: 1645 (default 1645)

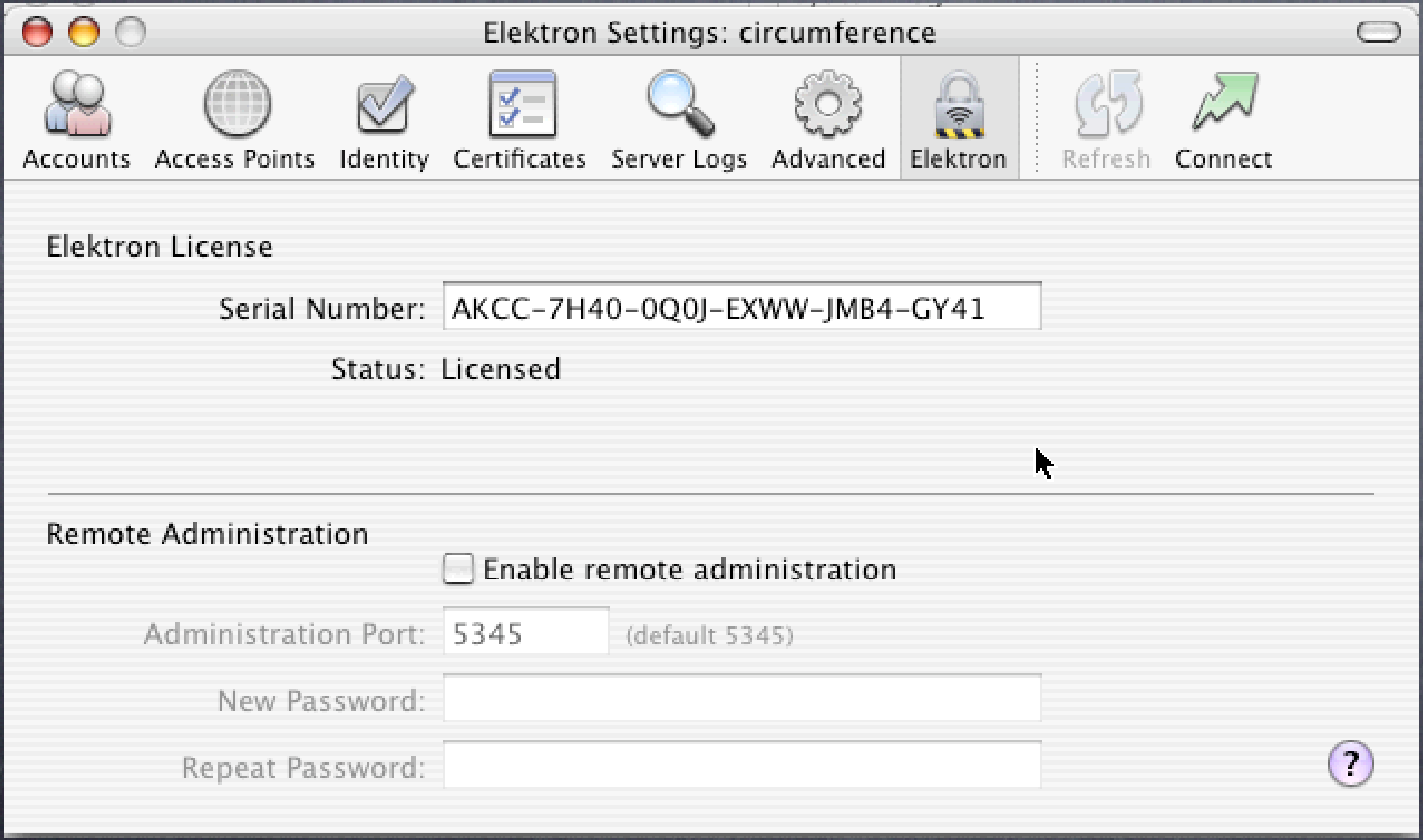
Session Timeout

□ Enable session timeout

Timeout Value: Seconds

- See default and secondary ports on Airport Extreme setup screens as well

# Elektron RADIUS/WPA2 server



Elektron License

Serial Number: AKCC-7H40-0Q0J-EXWW-JMB4-GY41

Status: Licensed

Remote Administration

□ Enable remote administration

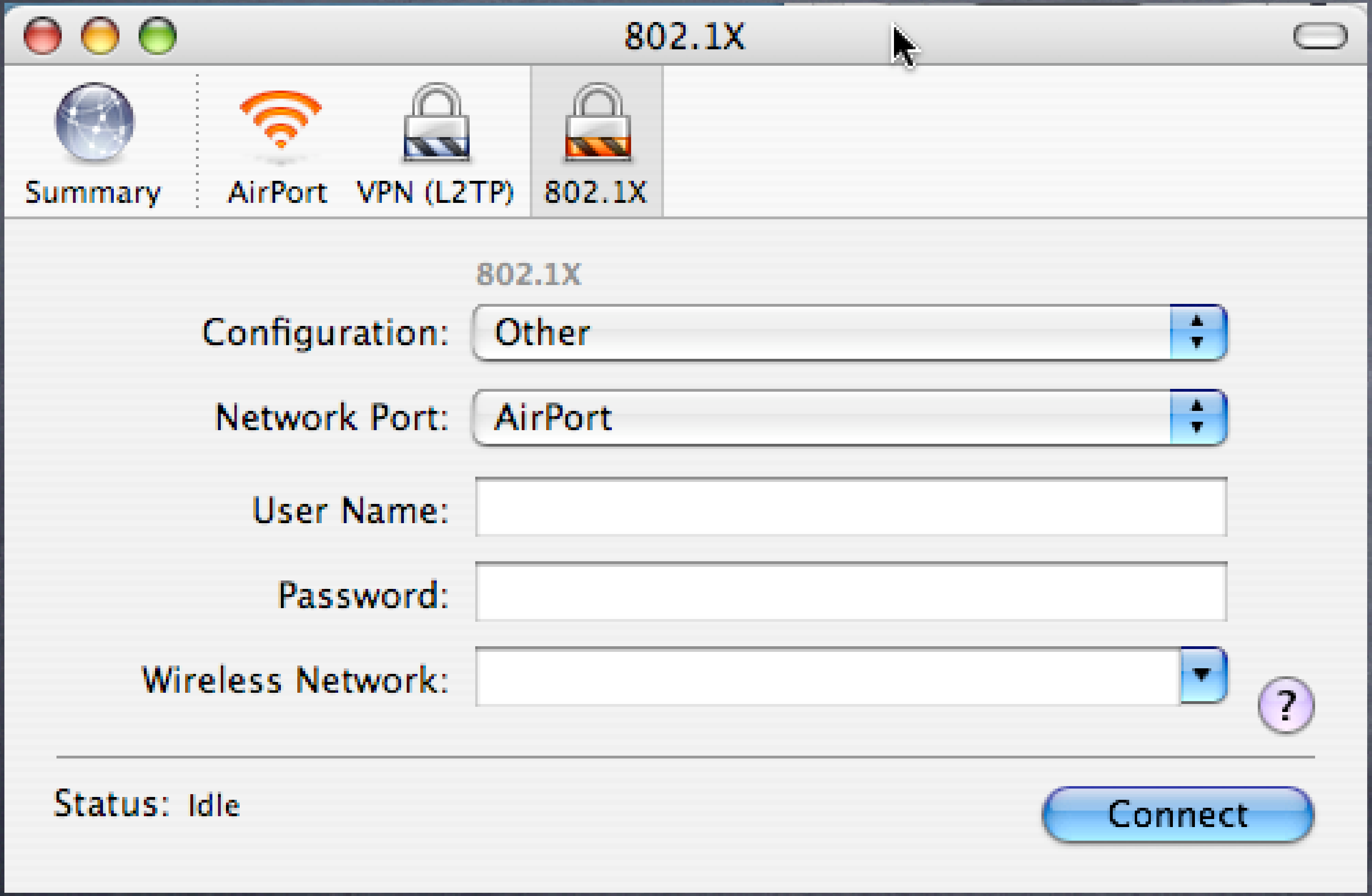
Administration Port: 5345 (default 5345)

New Password:

Repeat Password:

- License control screen
- Remote admin screen

# Elektron RADIUS/WPA2 server



802.1X

Configuration: Other

Network Port: AirPort

User Name:

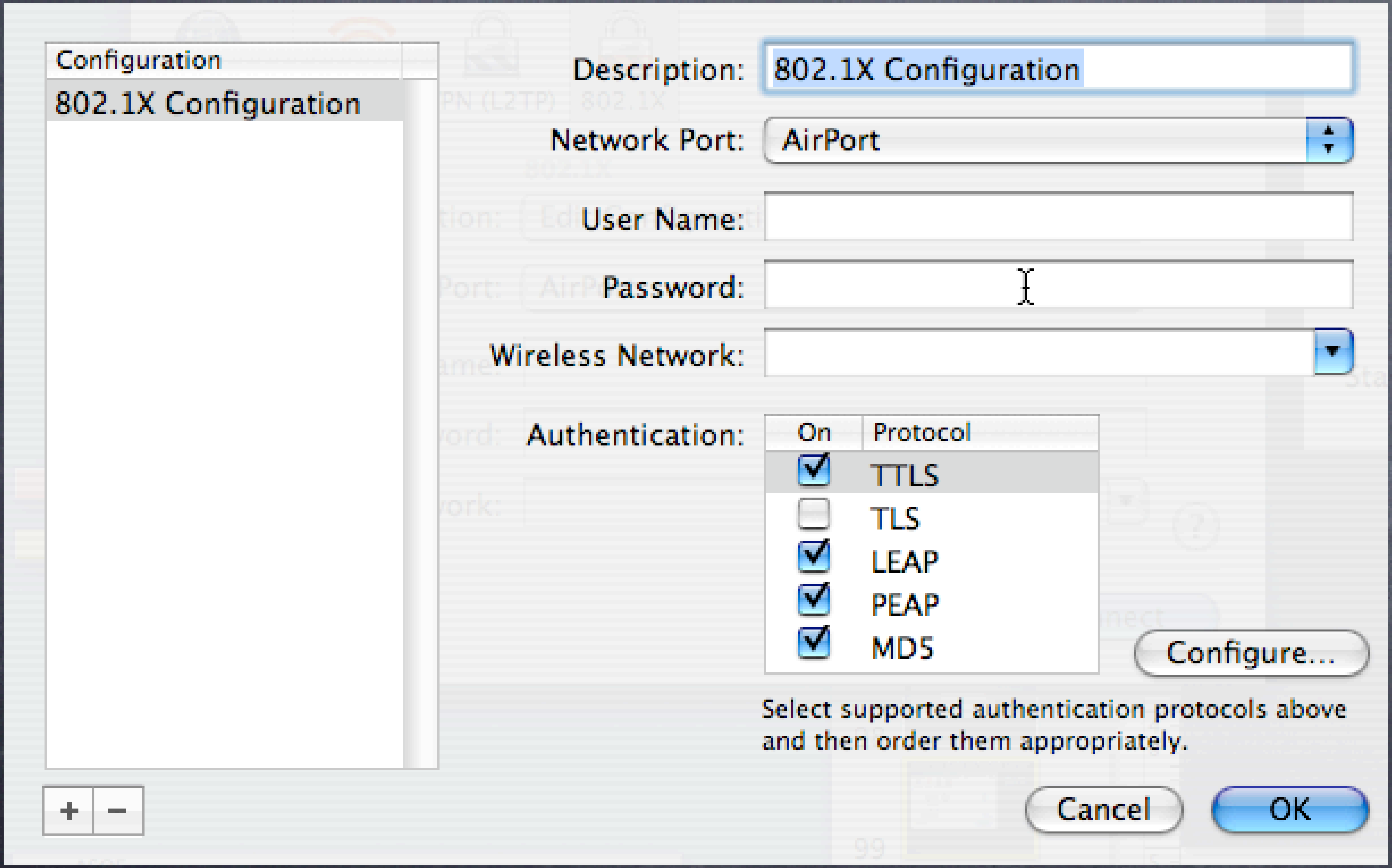
Password:

Wireless Network:

Status: Idle

- 802.1x setup screen on Tiger client

# Elektron RADIUS/WPA2 server



Configuration

802.1X Configuration

Description: 802.1X Configuration

Network Port: AirPort

User Name:

Password:

Wireless Network:

Authentication:

| On | Protocol |
|---|---|
| ☑ | TTLS |
| □ | TLS |
| ☑ | LEAP |
| ☑ | PEAP |
| ☑ | MD5 |

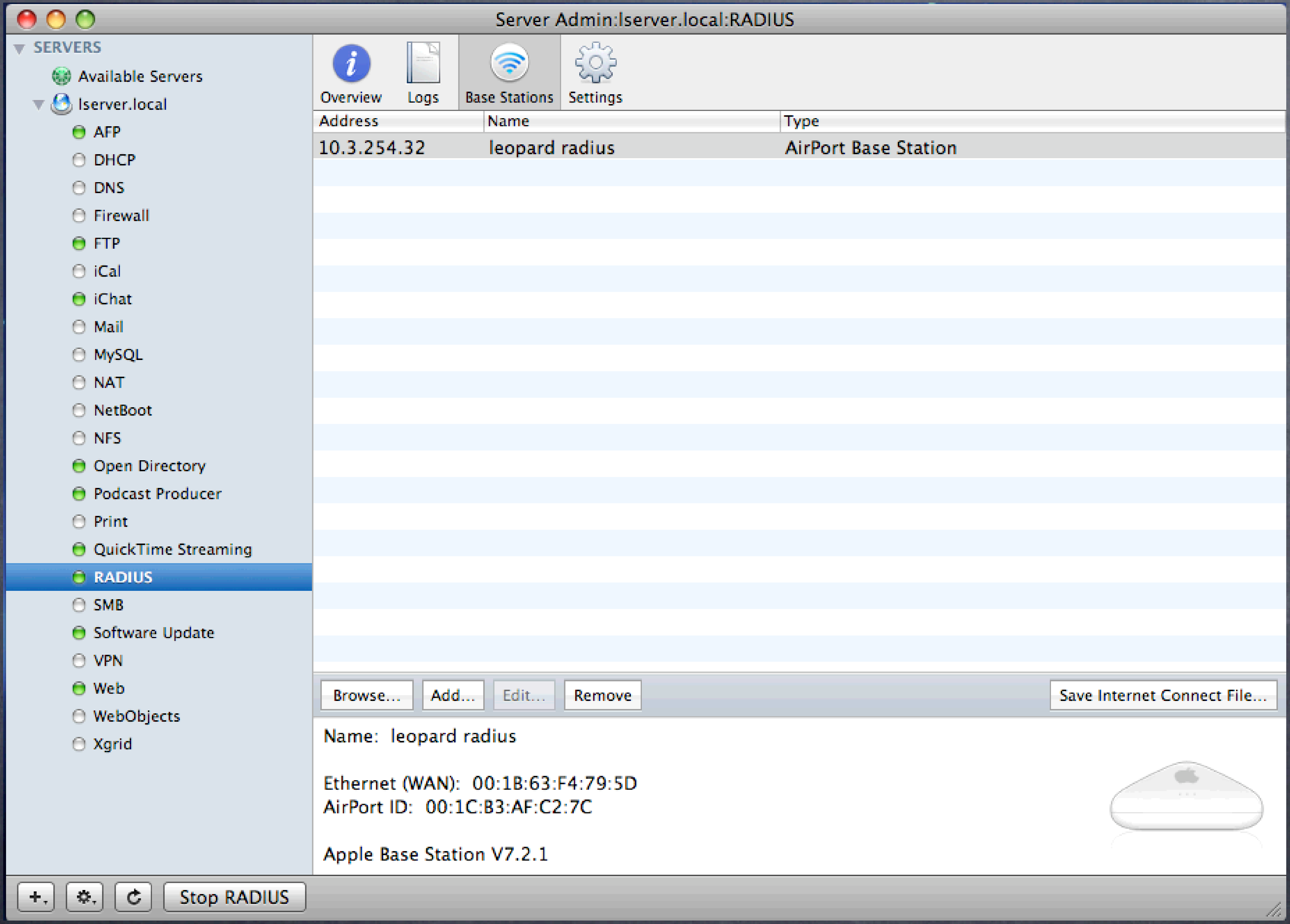
Select supported authentication protocols above and then order them appropriately.

- Note Protocols below, can be wireless or wired (managed switches)

# Lab: Elektron Server

1. Install/control RADIUS and 802.1X server, create certificates for 802.1X
2. Setup basic HW ACL access using Elektron server
3. Setup WPA2 using Elektron Server
4. Setup 802.1X using Elektron Server

# Leopard Server: RADIUS



Server Admin:lserver.local:RADIUS

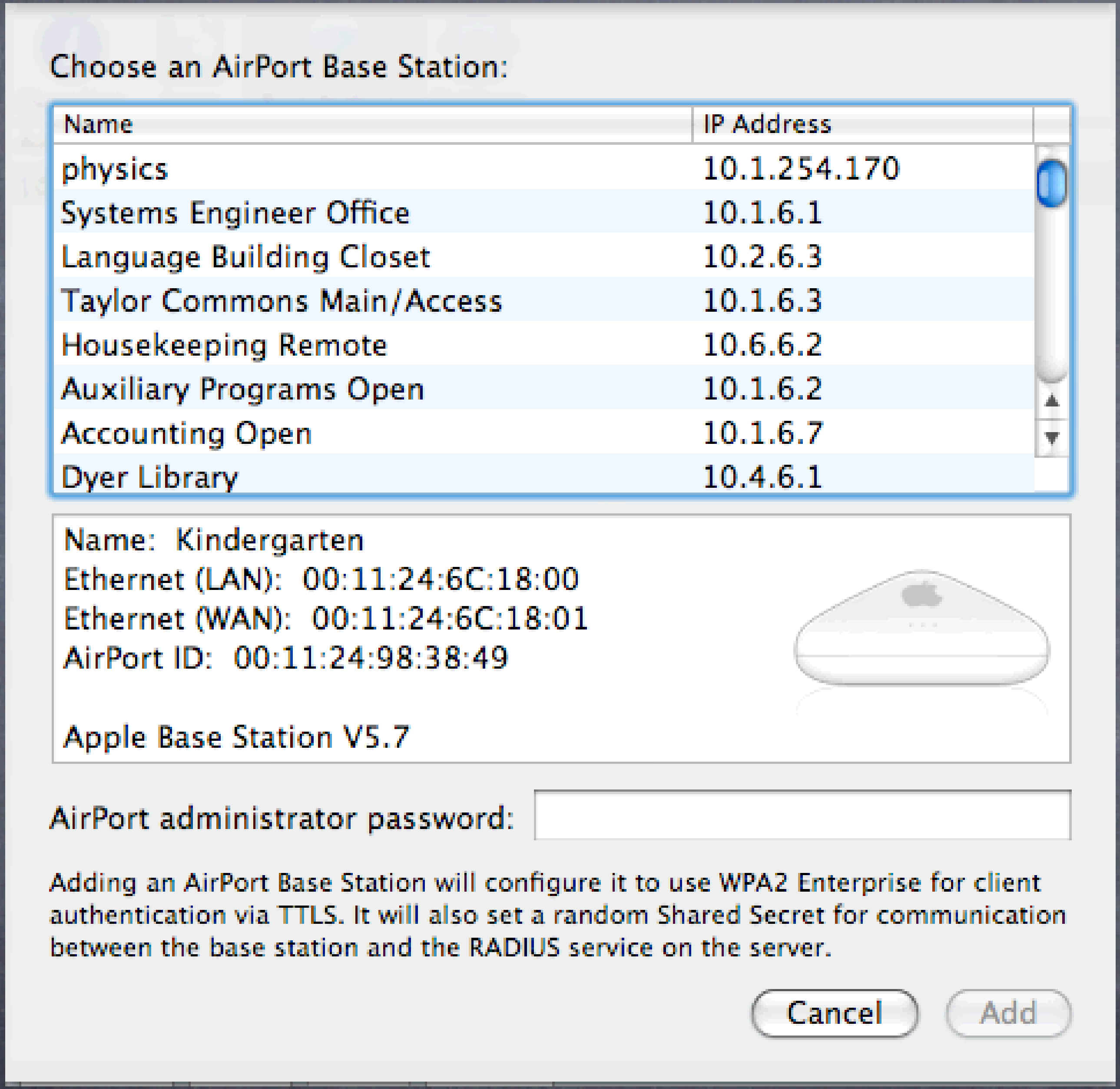
| Address | Name | Type |
|---|---|---|
| 10.3.254.32 | leopard radius | AirPort Base Station |

Name: leopard radius

Ethernet (WAN): 00:1B:63:F4:79:5D
AirPort ID: 00:1C:B3:AF:C2:7C

Apple Base Station V7.2.1

# Leopard Server: RADIUS



Choose an AirPort Base Station:

| Name | IP Address |
|---|---|
| physics | 10.1.254.170 |
| Systems Engineer Office | 10.1.6.1 |
| Language Building Closet | 10.2.6.3 |
| Taylor Commons Main/Access | 10.1.6.3 |
| Housekeeping Remote | 10.6.6.2 |
| Auxiliary Programs Open | 10.1.6.2 |
| Accounting Open | 10.1.6.7 |
| Dyer Library | 10.4.6.1 |

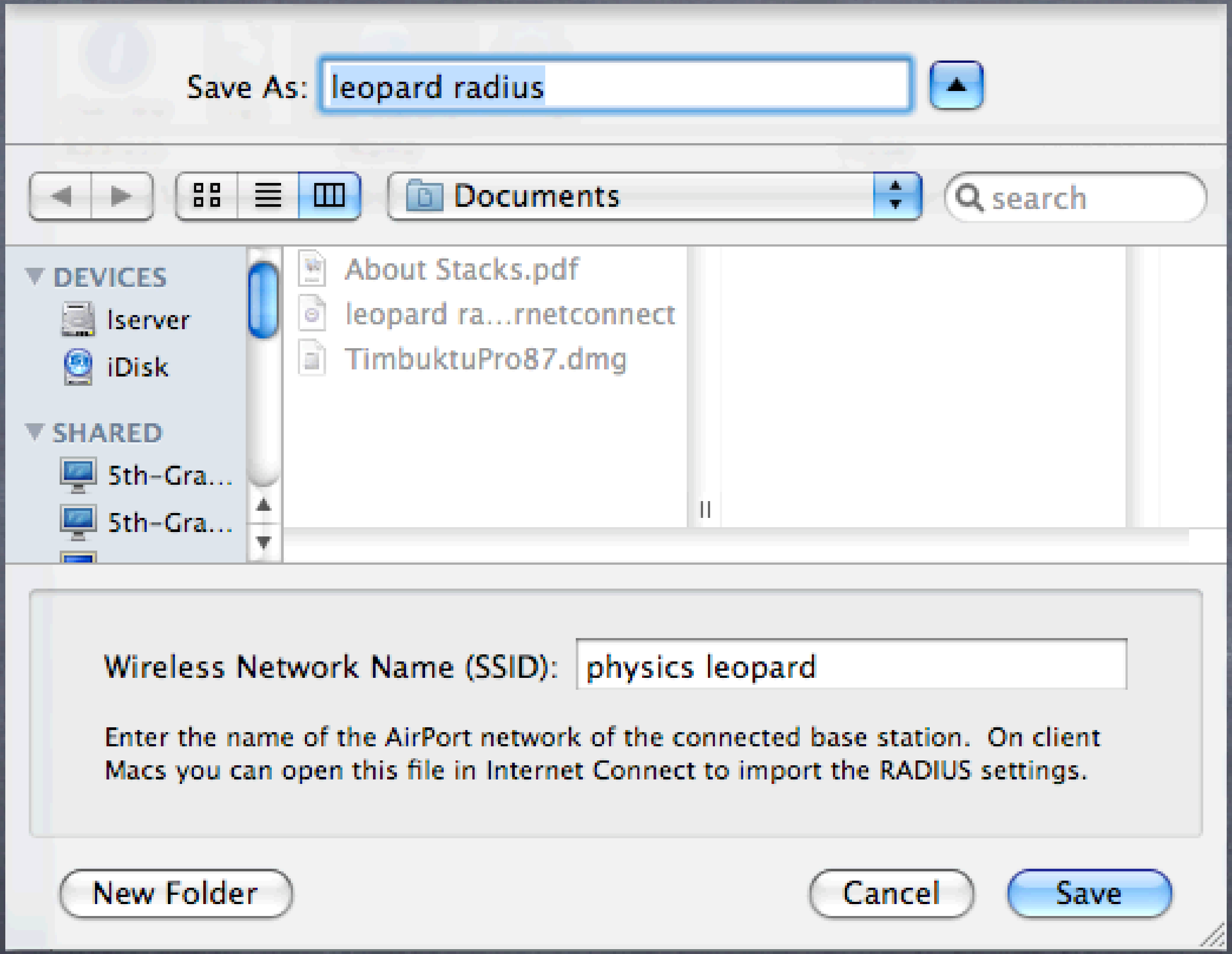
Name: Kindergarten
Ethernet (LAN): 00:11:24:6C:18:00
Ethernet (WAN): 00:11:24:6C:18:01
AirPort ID: 00:11:24:98:38:49

Apple Base Station V5.7

AirPort administrator password:

Adding an AirPort Base Station will configure it to use WPA2 Enterprise for client authentication via TTLS. It will also set a random Shared Secret for communication between the base station and the RADIUS service on the server.

# Leopard Server: RADIUS

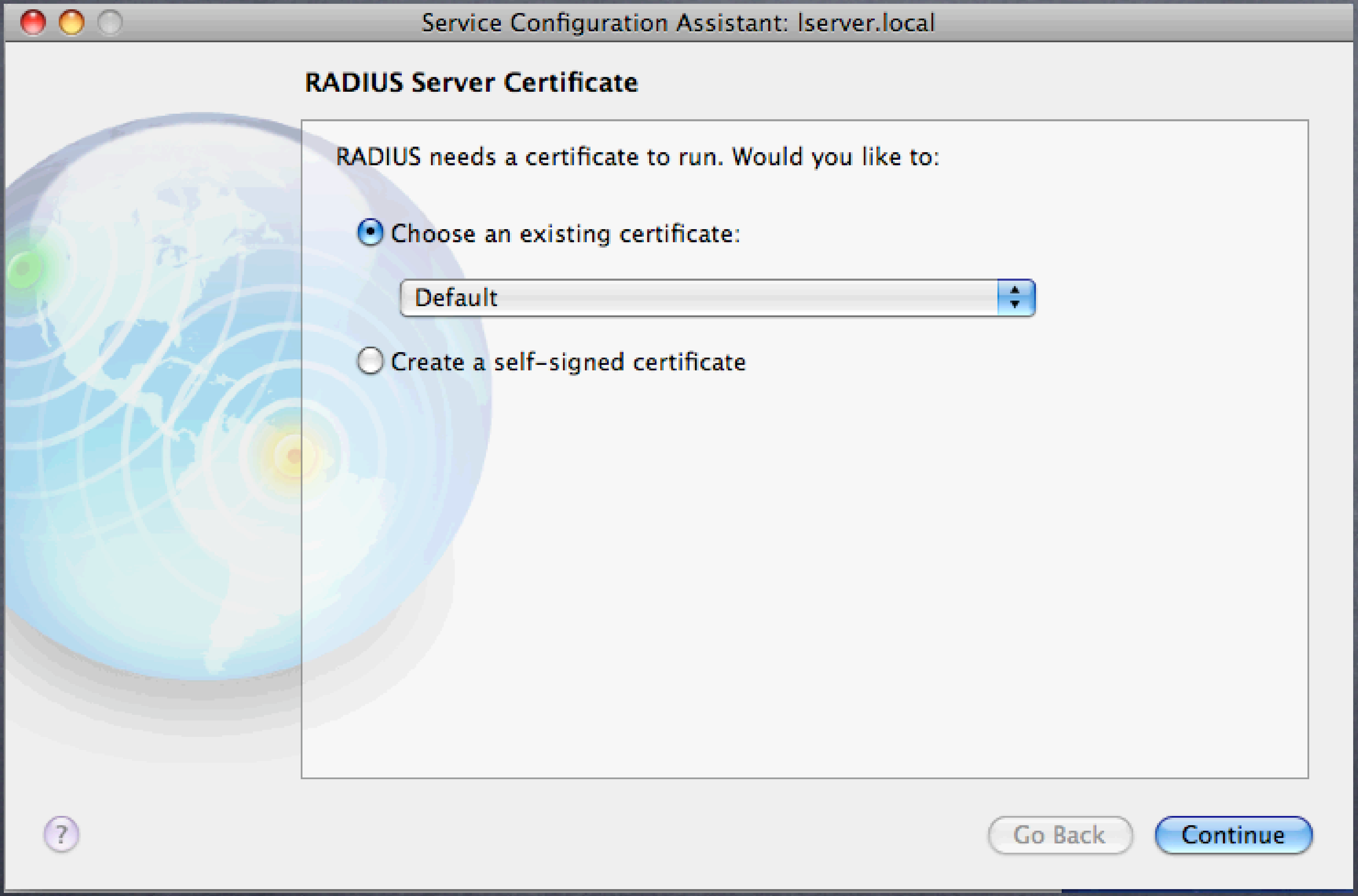


Save As: leopard radius

Wireless Network Name (SSID): physics leopard

Enter the name of the AirPort network of the connected base station. On client Macs you can open this file in Internet Connect to import the RADIUS settings.

# Leopard Server: RADIUS



Service Configuration Assistant: lserver.local

**RADIUS Server Certificate**

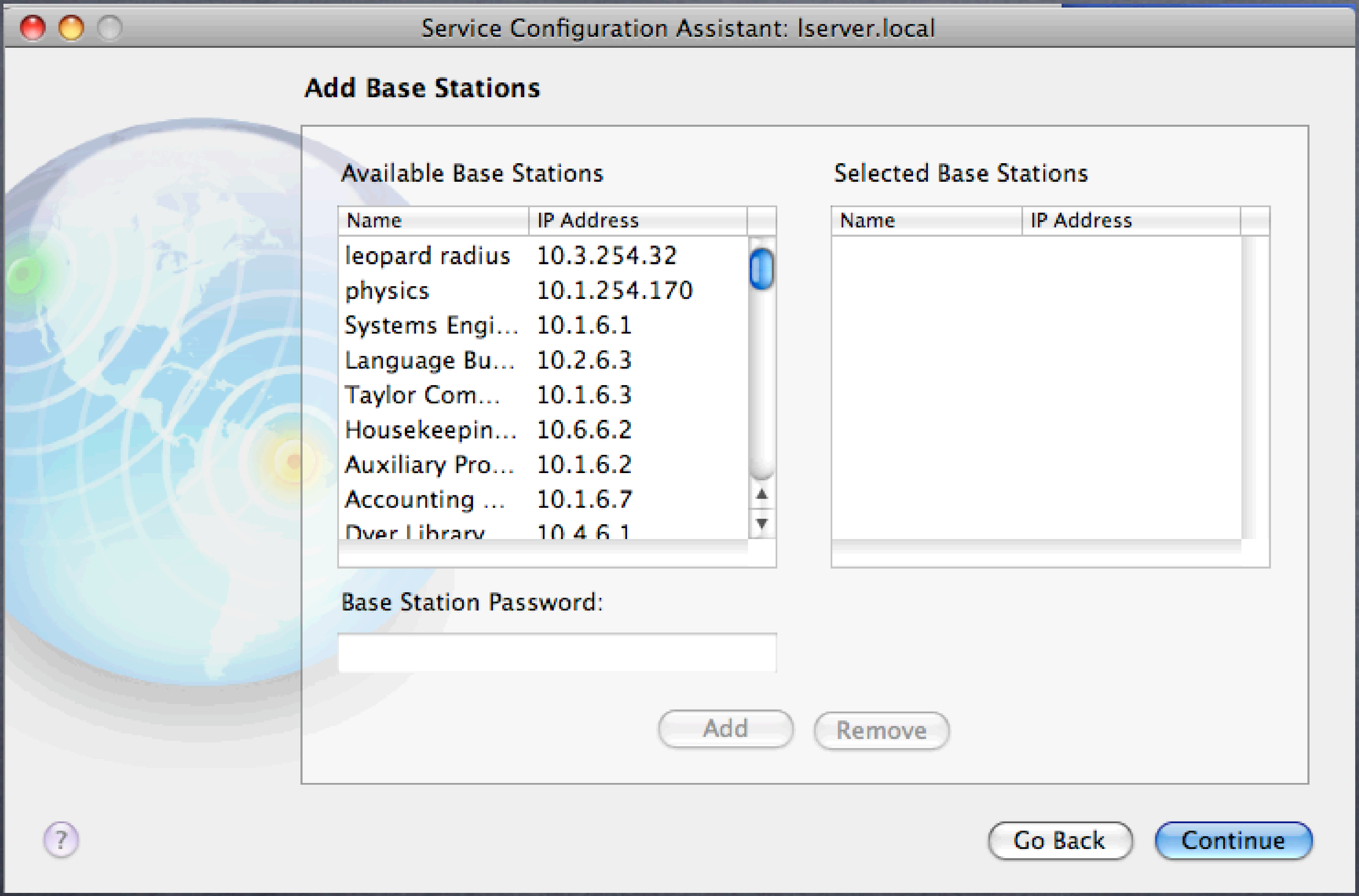
RADIUS needs a certificate to run. Would you like to:

● Choose an existing certificate:

Default

○ Create a self-signed certificate

# Leopard Server: RADIUS



Service Configuration Assistant: lserver.local

**Add Base Stations**

Available Base Stations

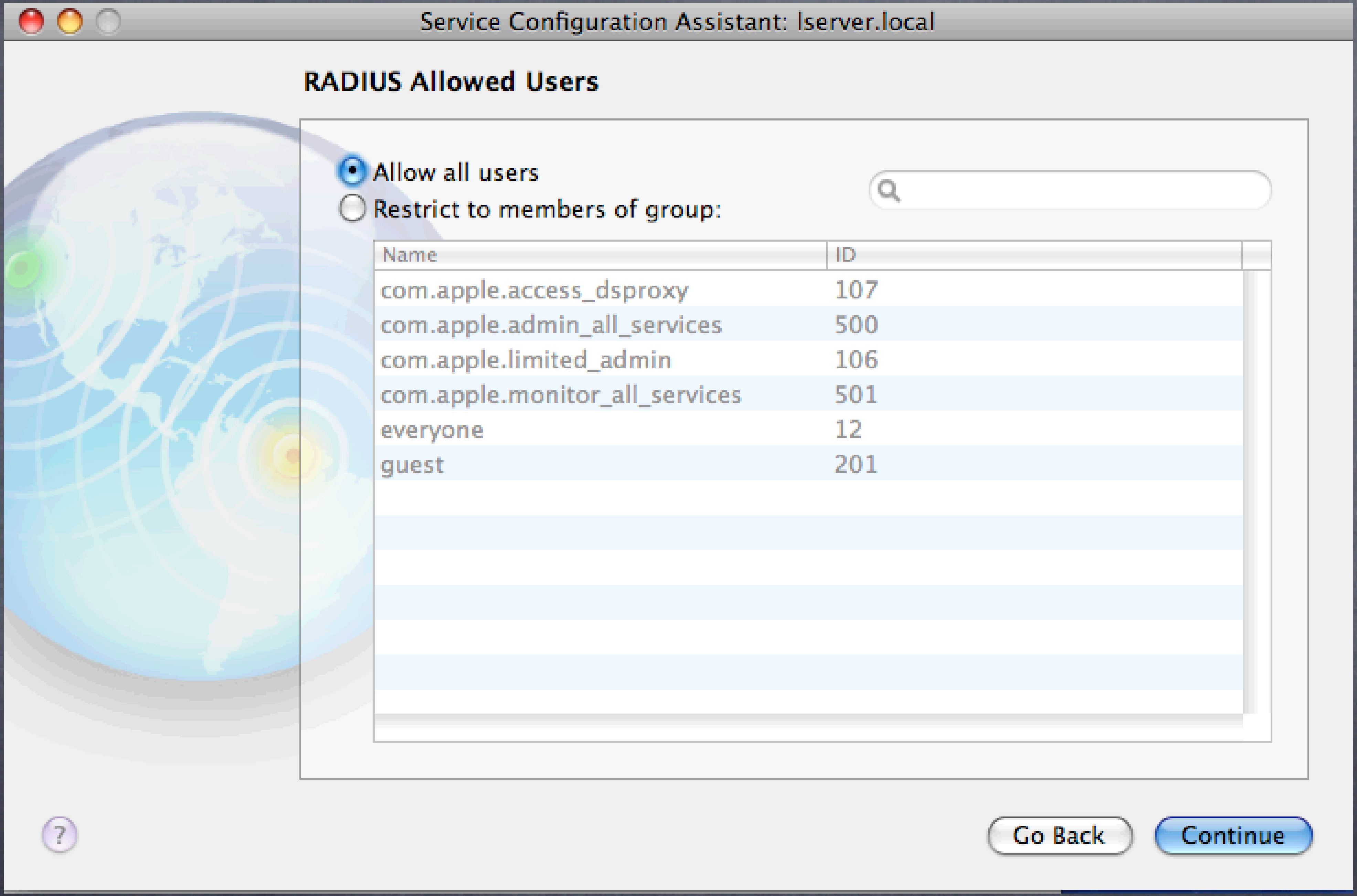
| Name | IP Address |
|---|---|
| leopard radius | 10.3.254.32 |
| physics | 10.1.254.170 |
| Systems Engi... | 10.1.6.1 |
| Language Bu... | 10.2.6.3 |
| Taylor Com... | 10.1.6.3 |
| Housekeepin... | 10.6.6.2 |
| Auxiliary Pro... | 10.1.6.2 |
| Accounting ... | 10.1.6.7 |
| Dyer Library | 10.4.6.1 |

Selected Base Stations

| Name | IP Address |
|---|---|

Base Station Password:

# Leopard Server: RADIUS



Service Configuration Assistant: lserver.local

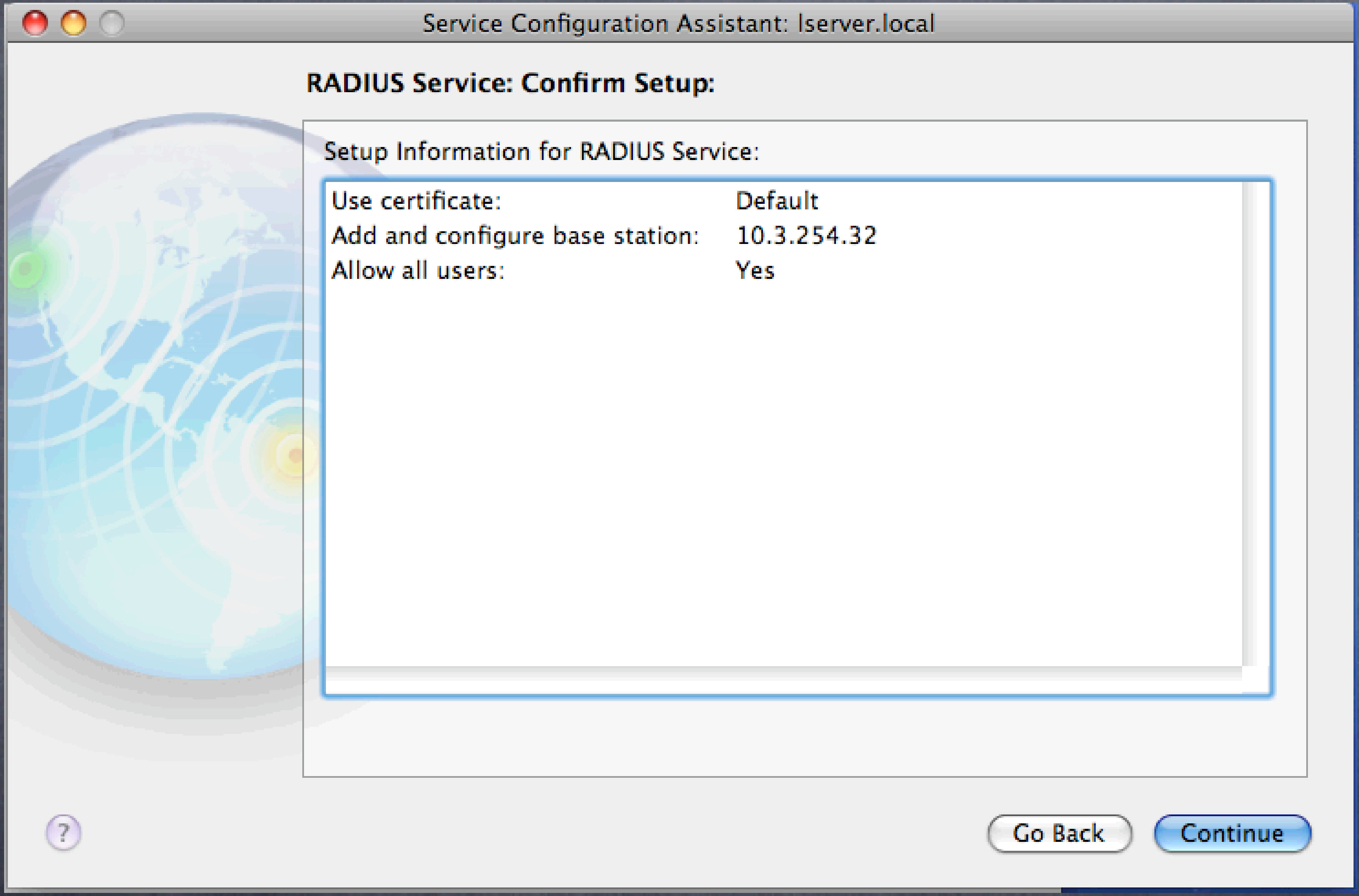
## RADIUS Allowed Users

● Allow all users

○ Restrict to members of group:

| Name | ID |
|---|---|
| com.apple.access_dsproxy | 107 |
| com.apple.admin_all_services | 500 |
| com.apple.limited_admin | 106 |
| com.apple.monitor_all_services | 501 |
| everyone | 12 |
| guest | 201 |

# Leopard Server: RADIUS

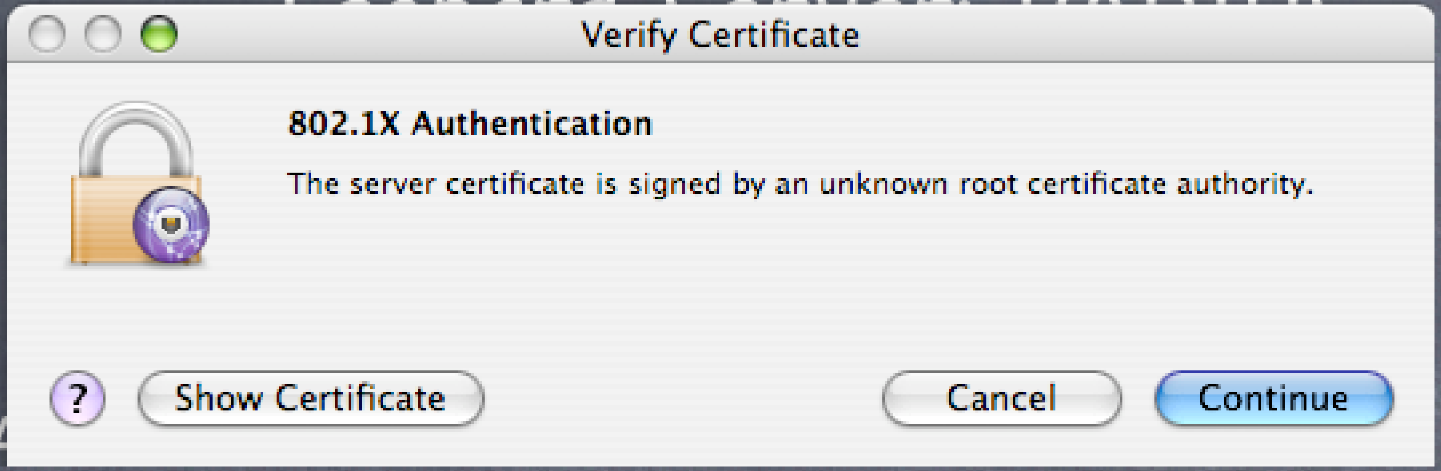


RADIUS Service: Confirm Setup:

Setup Information for RADIUS Service:

| | |
|---|---|
| Use certificate: | Default |
| Add and configure base station: | 10.3.254.32 |
| Allow all users: | Yes |

# 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

# Leopard Server RADIUS

Strong Points:

- Point and click addition of Access Points
- Must also add IP and shared secret of server to Access Point
- Shared secret must be 8 characters or more
- 802.1x security with relatively little hassle
- Integrates with user list on server
- Many users centrally administered, easier than WPA2 personal

Weak points:

- Forces you to use the 802.1x protocol, instead of MAC ACL
- All users must be added to the server (tough if you have limited client versions of the server)
- Must purchase server license and a dedicated machine

# Authentication: Elektron vs. Leopard Server

## Elektron:

- Cheaper
- Runs on client, not server
- More flexible (MAC ACL 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

# Authentication: Summary

- RADIUS/802.1x authentication is the way to go
- Best practices for your wireless and wired network
- Goes beyond the basic wireless safety steps
- Can track malicious attempts
- You may never know when or how you've been compromised without authentication control
- Latest wireless gear (e.g. Airport Extreme X2) force this option
- Sysadmins: you can use 802.1x on your managed switches as well

# Summary: Wireless concerns

- Users must be warned that any Hotmail type web mail account is sending passwords in the clear, as well as other user data
- Insecure: Web Mail, FTP (password and data), Web data, IM, Kazaa/Limewire, Retrospect (with encryption off), Mail message text (never include passwords in any email message)
- Secure: SSL (https://), SSH, VPN, Timbuktu Passwords, APOP, AppleShare passwords, PGP, Retrospect with encryption on, Kerberos, SSL mail
- If your network is bridged to the wired LAN, this is also true of all wired users on the LAN
- Etherpeek and Netminder can be used to illustrate this (demo)

# Advanced Security notes

- Rogue Access points: passive scanners can be used to monitor these (KisMAC in particular)
- Man in the middle attacks: acts like the AP, user authenticates, MIM vanishes, kicks off user, then logs in as user (802.1x blocks this)
- Password cracking can gain access to networks, but KisMAC can be used to sniff all traffic for later decoding/search (e.g. look for the word PASS)
- Even HW address security can be spoofed, WEP is worse
- 802.1X can be used as comprehensive solution on wired and wireless parts of your network

# Section 5: Integration

## iPhone integration

- Address book
- iCal
- iPod/iPhone as presentation device/backup drive
- Mail integration
- Security tips

## Mobility survival tools:

- Bootable jump/flash drives: USB and Firewire
- Portable drives, Leopard and Time Machine
- Presentation tools/tips
- Power solutions
- Repairs on the road: CD, DVD, Jump drive, portable drive
- Dotmac as presentation rescue

## Access on the road:

- Wireless antennas, amplifiers and warwalking tools
- ISP options/tests/security
- Hotel/Airport scenarios and solutions

# iPhone integration

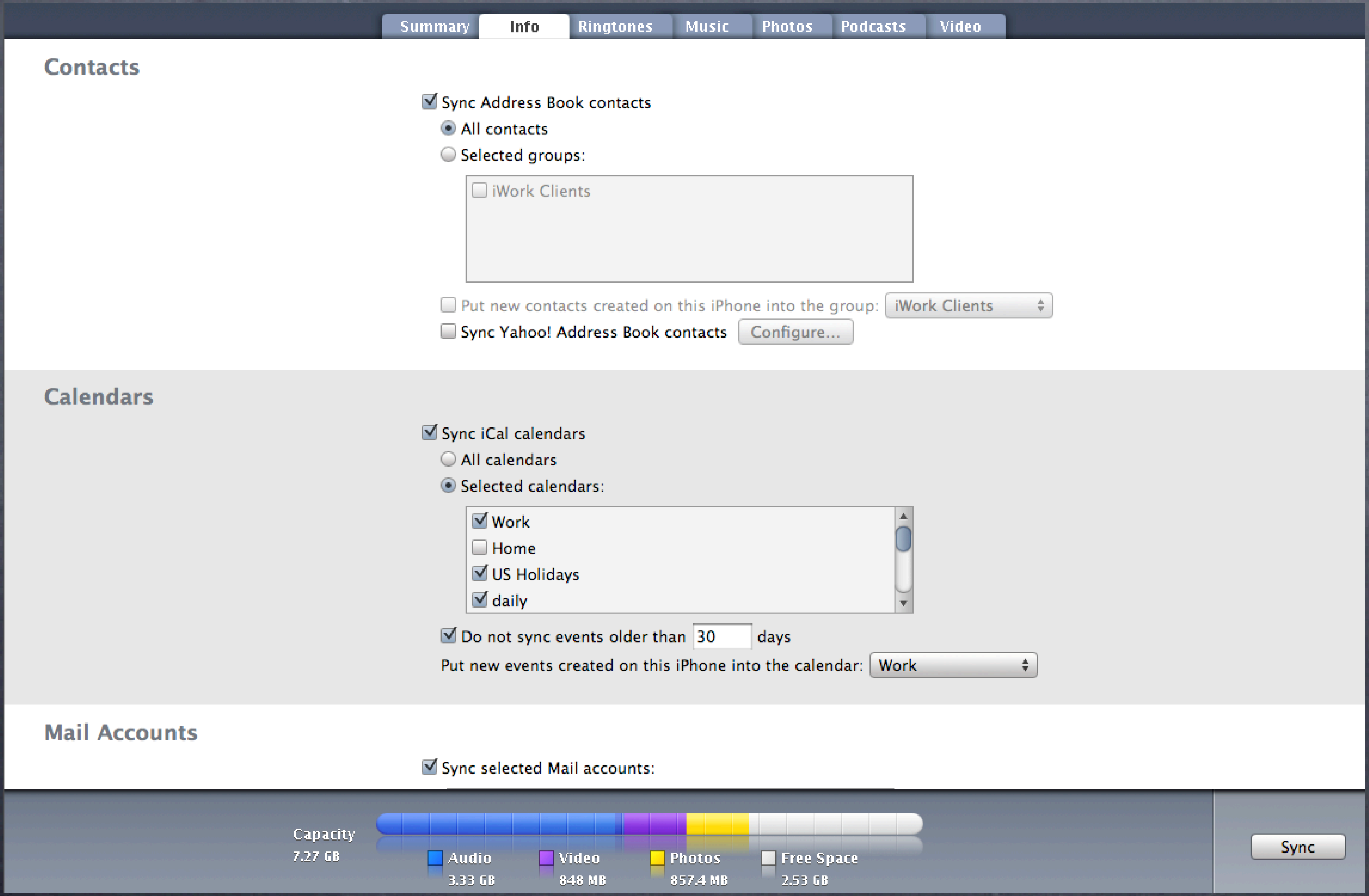
iPhone integration

- Address book
- iCal
- iPod/iPhone as presentation device/backup drive
- Mail integration
- Security tips

# iPhone integration

## iPhone integration: Address Book and iCal

- Access iPhone from iTunes (iPhoto sees it as well, but can be turned off)
- Address book can be synched at will, note field entered data is preserved and sorted on the laptop
- iCal calendars can by subscribed, but will only update when the phone is connected to the laptop



**Contacts**

☑ Sync Address Book contacts

● All contacts

○ Selected groups:

□ iWork Clients

□ Put new contacts created on this iPhone into the group: iWork Clients

□ Sync Yahoo! Address Book contacts

**Calendars**

☑ Sync iCal calendars

○ All calendars

● Selected calendars:

☑ Work
□ Home
☑ US Holidays
☑ daily

☑ Do not sync events older than 30 days

Put new events created on this iPhone into the calendar: Work

**Mail Accounts**

☑ Sync selected Mail accounts:

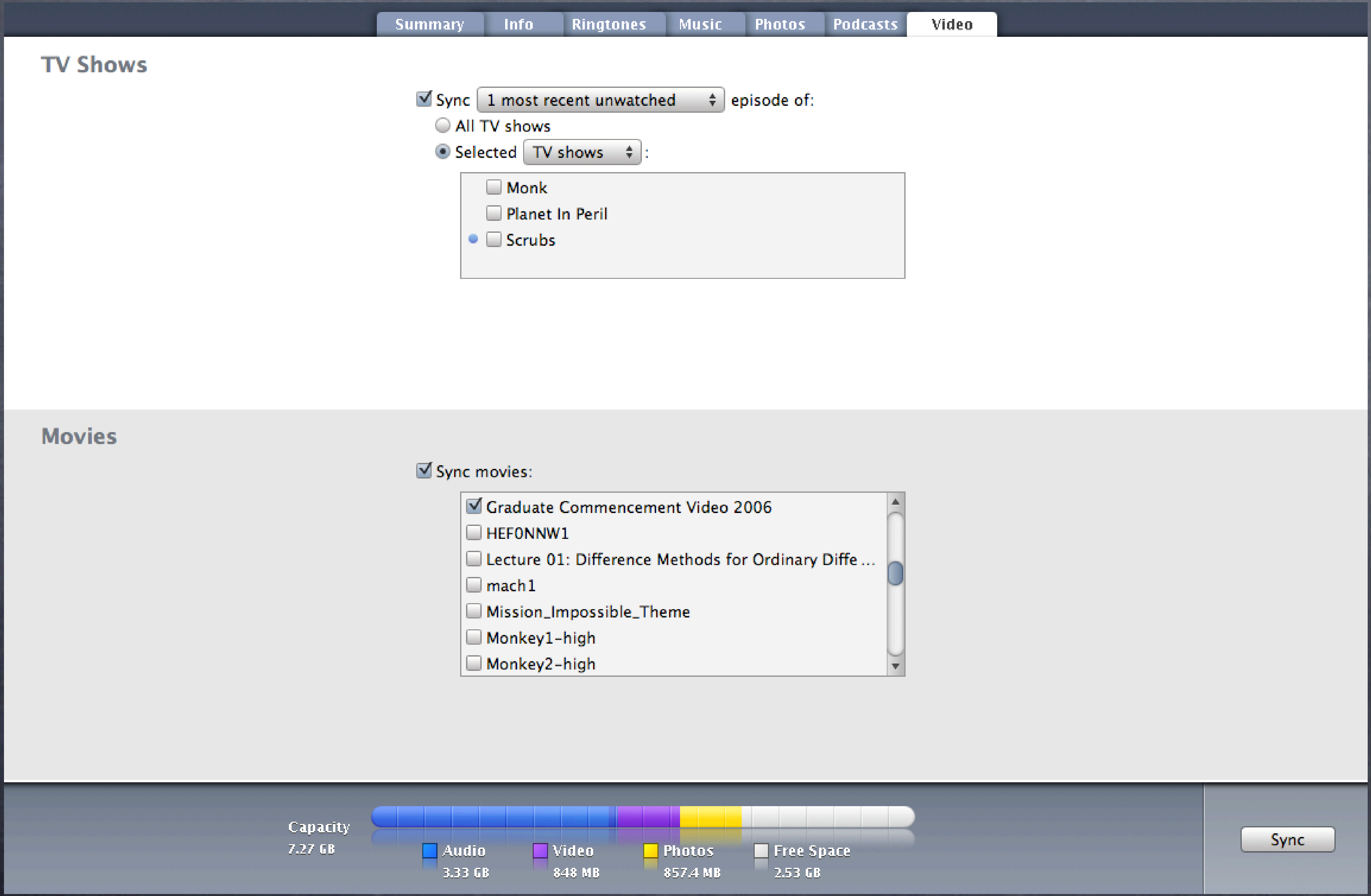
Capacity 7.27 GB

🟦 Audio 3.33 GB
🟪 Video 848 MB
🟨 Photos 857.4 MB
□ Free Space 2.53 GB

# iPhone integration

## iPhone integration: presentation device

- Any video uploaded to the iPhone can be presented via the HDMI converter cable through the headphone port
- This also works in composite mode from normal iPods (great use for the video iPod you have)
- Excellent when teamed with the data backup function for your presentations, and bootable partitions



TV Shows

☑ Sync 1 most recent unwatched episode of:

○ All TV shows

● Selected TV shows :

□ Monk
□ Planet In Peril
□ Scrubs

Movies

☑ Sync movies:

☑ Graduate Commencement Video 2006
□ HEFONNW1
□ Lecture 01: Difference Methods for Ordinary Diffe ...
□ mach1
□ Mission_Impossible_Theme
□ Monkey1-high
□ Monkey2-high

Capacity 7.27 GB

Audio 3.33 GB
Video 848 MB
Photos 857.4 MB
Free Space 2.53 GB

# iPhone integration

## iPhone integration: Mail integration

- Can be a dotmac account, or any POP or IMAP account
- Some issues with Gmail accounts (see their help pages on this)
- If you have a separate account for critical mail, set the iPhone to buzz when this gets an incoming message-just like Vmail/SMS/pager but you don’t have to listen to it, and it’s available to anyone with email access (some folks prefer email to SMS)
- Message sorting on dotmac accounts done on the phone are reflected on the main IMAP account
- Caution: don’t lend out your phone, and if it is lost, change your email password immediately, as well as any iTunes purchase info you may have
- If you are trying to send email to your server and use authentication for sending, try using the VPN as well/instead: much easier, and always works
- SMS messages can be archived using Syphone (see micromat.com)

# iPhone integration

## iPhone integration: Security Tips

- Use VPN whenever possible
- If you run the VPN server, you can make certain realms encrypted or all traffic encrypted. For large organizations, having an iPhone VPN server that encrypts everything is a good idea
- EDGE is slow, and should be safe, but there are exploits in the works, so keep an ear out for threats in 2008
- Web purchases on the iPhone are cool, but when done in the open may not be as secure as you think: try monitoring an iPhone web session using interarchy, Kismac or IP net monitor, you'll be stunned at what you can see.
- Use only certified webapps (ones that show up on the Apple site). This is not a problem yet, but again has been one area of hacker interest
- Use the VPN for mail and for any web traffic you don't want intercepted
- Excellent idea to backup the phone, address book and all music downloaded often.

# Mobility survival tools

Mobility survival tools:

- Bootable jump/flash drives: USB and Firewire
- Portable drives, Leopard and Time Machine
- Presentation tools/tips
- Power solutions
- Repairs on the road: CD, DVD, Jump drive, portable drive
- Dotmac as presentation rescue

# Mobility survival tools

Bootable jump/flash drives: USB and Firewire:

- Any USB jump drive can be used to boot intel macs
- Portable Firewire jump drives can be used to boot PPC or intel macs (see TechTool Pro site)
- USB options: CF or SD card readers are great, if fast
- Cardbus 34 card readers are the fastest, and can be loaded with the TechToolPro boot software
- Also have a look at DasBoot and Boot CD
- What to put on the bootable partition:
  - DiskWarrior
  - TechTool Pro
  - Disk Utility

# Mobility survival tools

**Portable drives, Leopard and Time Machine:**

- Two options: bus powered (smaller, portable) and external power (faster, larger, more robust)
- Bus powered: LaCie makes a nice orange drive with several interfaces, good speed, and can be partitioned into data and bootable partitions
- Unfortunately, if you need to boot PPC and intel macs, you'll need two drives
- External powered drives: G-tech makes a nice drive, sleeps when not in use, quiet, highly rated
- Either drive becomes a Time Machine backup disk on command with Leopard

# Mobility survival tools

- Presentation tools/tips:
  - Keyspan laser pointer/controllers have the usb dongle built-in
  - Try backing up your presentation (ppt, pdf, quicktime movie) on an iPod, iPhone, video iPod, jump drive, DVD/CD, dot mac account, email it to yourself, or put it onto your digital camera-just do it
  - Bring your own power strip, wireless mouse, ethernet cable and Airport Express: you may be providing the only good wireless access in the place
  - Bring a set of smaller USB/jump drives to pass out your presentation to guests: cheaper and lighter than CDs, and you can update at the last minute
  - If your computer is pre-iSight, bring one along, it makes a great ELMO
  - Portable speakers are nice, a noise cancelling USB headset is better for VTC
  - You may be in a location where cel phones don't work, you may find that iChat/Skype/Vonage softphone does.

# Mobility survival tools

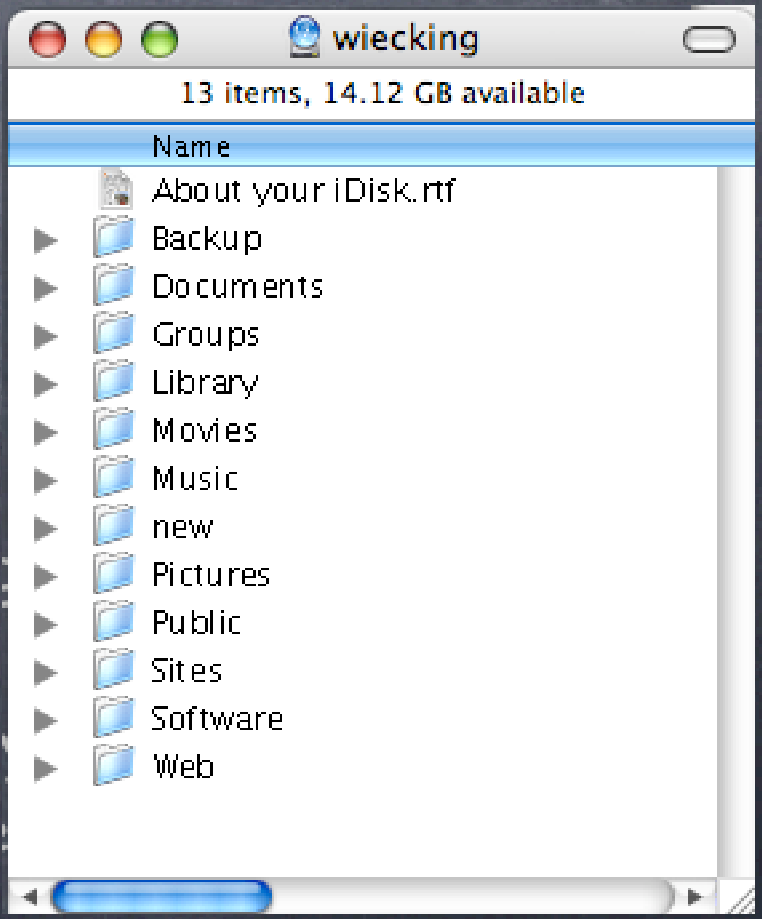
- Power solutions:
  - Bring along a separate battery, at least ONE. Batteries fail, and have done so during presentations. Don't be one of the unlucky ones
  - Airplane adapters have limited penetration on aircraft, but there are online sources for checking this
  - Car inverters are nice, and can charge your laptop if on a conference call or if you lose your charger
  - NewerTech batteries have much greater life, particularly on long plane trips
  - External battery packs work on Video iPod, and should on the iPhone, though I'm reluctant to try it on mine...
  - TSA is very suspicious of most external battery packs, best to leave them in the outer pocket of your roll-away
  - TSA is also suspicious of GPS, wireless and other non-traditional gear. If you must carry on, keep them in separate bags, as they insist on checking these separately
  - A USB powered wireless adapter and panel antenna can reach over a mile to an open access point-good for sharing (yours, theirs)

# Mobility survival tools

- **Repairs on the road: CD, DVD, Jump drive, portable drive**
  - DiskWarrior is the best, fast repair mode: finds even zombied drives
  - Best on an external drive, slow on jump drives, faster on bus drives, fastest on external powered 7200 rpm drives
  - Good idea to do repairs before traveling, and after a full backup
  - Unless you like living dangerously, don't do any repairs the night before your talk, trust me.
  - Where to have backups: home before you leave, online (data only), and on your portable drive. Worst case: your office/home/family can email you the files you need
  - Good also to carry along a system installer disk (Puma, Cheetah, Jaguar, Panther, Tiger, Leopard, tabby-cat)
  - Bring along a firewire cable to rescue/share data quickly. You may be the hero on site
  - If you ARE the hero on site, and you travel with other comrades, bring along a disk image of one of your machines (clean)

# Mobility survival tools

- **Dotmac as presentation rescue:**
  - Suppose you lose your presentation (TSA, Gremlins, repairing your computer the night before...)
  - Get on another computer, download your presentation from your dotmac account to your jump drive, then load onto another computer for your presentation
  - You can also save your presentation online with dotmac for distribution to your participants
  - Advice: password protect your files online (either as secure pdf or the folder on the site)



wiecking

13 items, 14.12 GB available

Name

About your iDisk.rtf
Backup
Documents
Groups
Library
Movies
Music
new
Pictures
Public
Sites
Software
Web

# Access on the road

Access on the road:

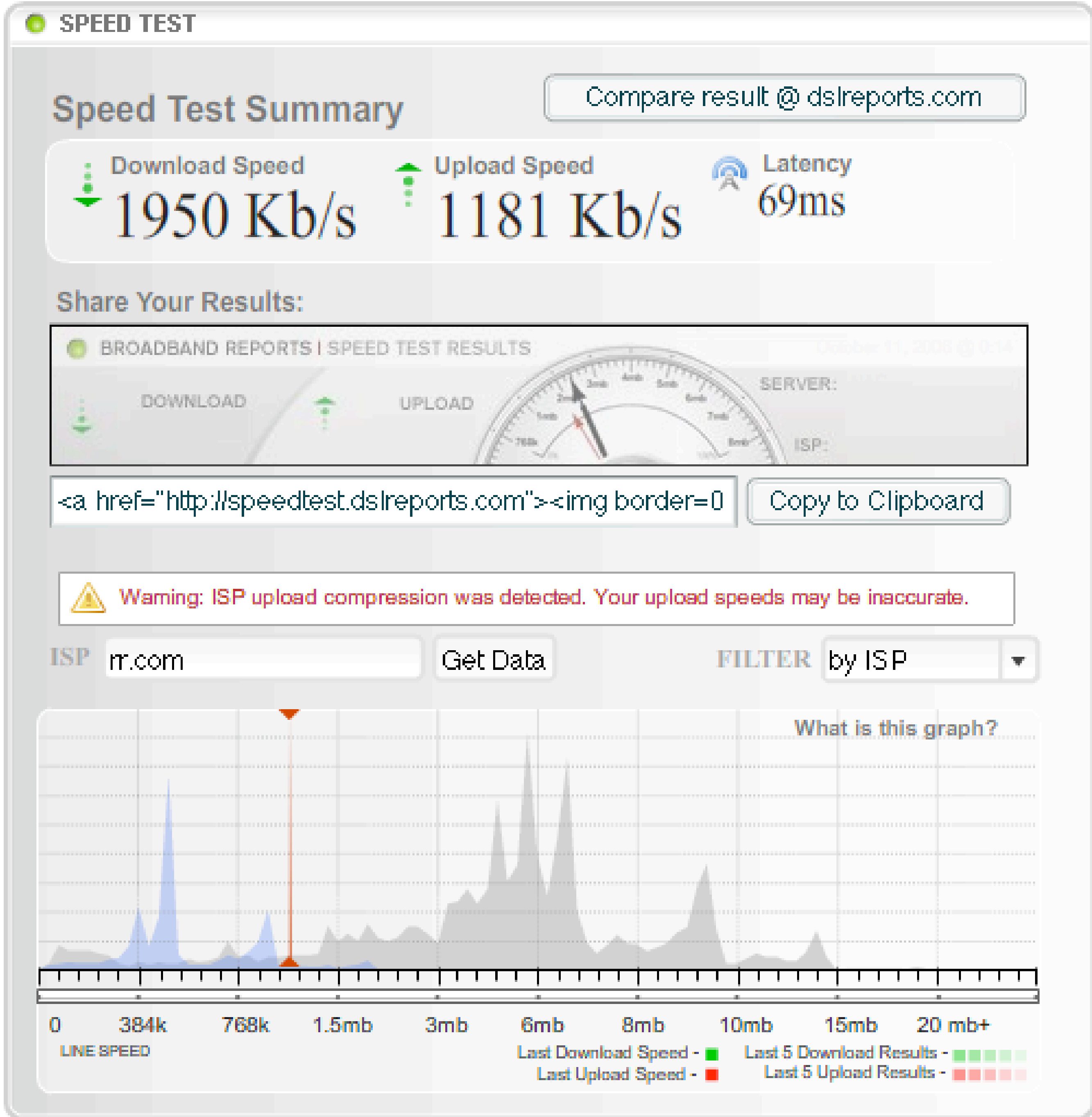
- Wireless antennas, amplifiers and warwalking tools
- ISP options/tests/security
- Hotel/Airport scenarios and solutions

# Access on the road

- Wireless antennas, amplifiers and warwalking tools
  - Portable USB is the easiest, though limited for scanning purposes
  - Mobile wireless in your car can let you wardrive up to 12 miles from any Access point, 46 miles from one with a directed antenna
  - Warchalking: Mother Theresa version of Wardriving
  - For more on wardriving, see appendix

# Access on the road

- ISP options/tests/security
  - Test your access speed at speedstest.dslreports.com
  - DSL and Cable Modems differ greatly in speed with region
  - Both can be used to host services if you check the DHCP status often



SPEED TEST

Speed Test Summary

Compare result @ dslreports.com

Download Speed 1950 Kb/s

Upload Speed 1181 Kb/s

Latency 69ms

Share Your Results:

BROADBAND REPORTS | SPEED TEST RESULTS

DOWNLOAD

UPLOAD

SERVER:

ISP:

<a href="http://speedtest.dslreports.com"><img border=0

Copy to Clipboard

Warning: ISP upload compression was detected. Your upload speeds may be inaccurate.

ISP rr.com

Get Data

FILTER by ISP

# Access on the road

- Hotel/Airport scenarios and solutions
  - Many hotels offer wired access to rooms. Bring along an airport express to allow mobility/sharing of the wired connection
  - Most use a captive portal system, authenticating you on your MAC address. If you login with a different computer, you are charged twice. Bring along your own AP, or share from one computer to another
  - Old Days: I used to carry one g4 iBook with an amplifier and panel antenna to capture open APs, then shared it via ethernet and an airport express. These days, I just use the airport express
  - Whenever on a hotel network, use VPN, many of these networks are shared, meaning you can intercept traffic from other hotel guests, and so can they...

# Section 6: Collaboration

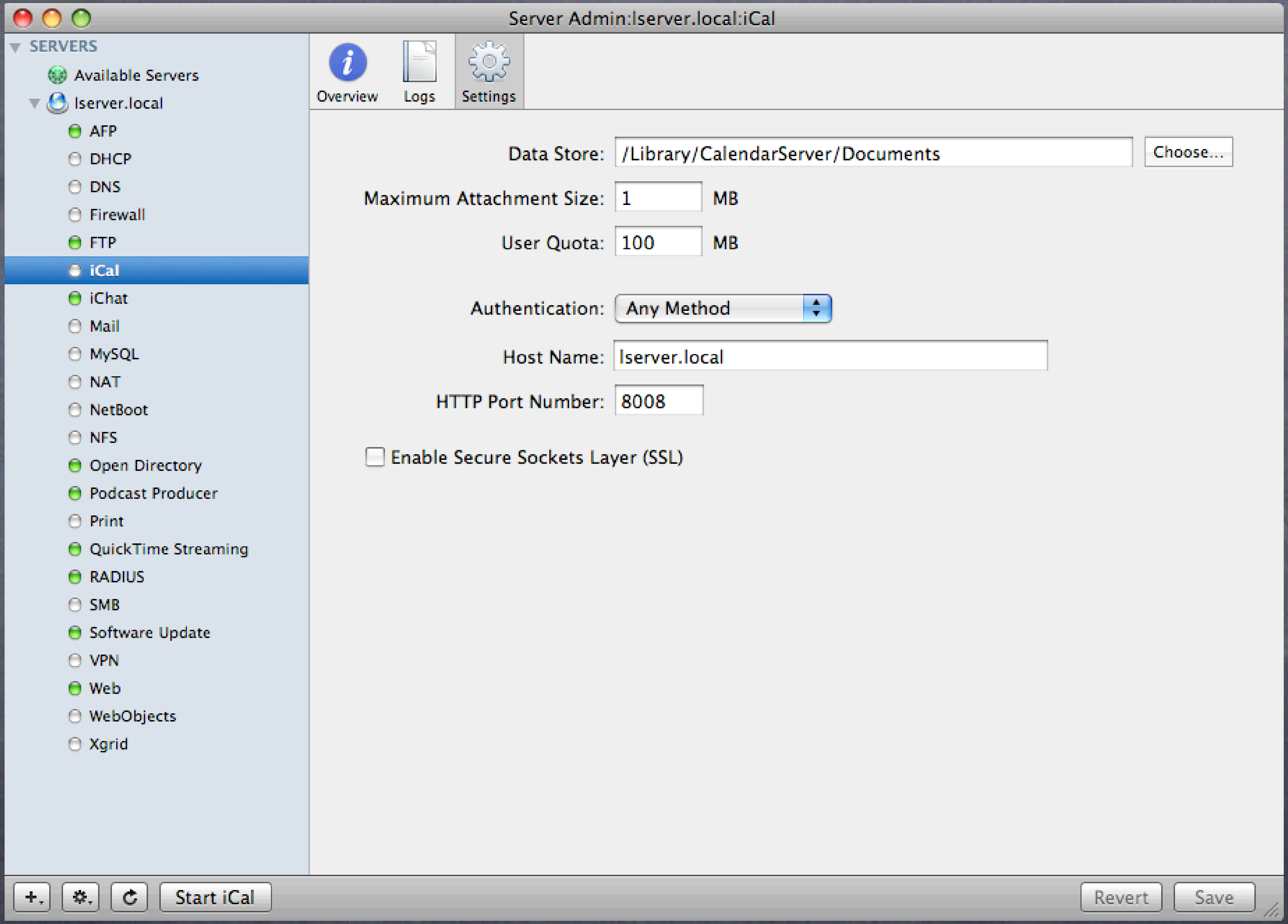
## Collaboration tools: Leopard Server era

- iCal webcal server
- Video Teleconferencing (VTC): iSight/iChatAV/Skype/Jabber server
- VoIP: Skype, Skype-out, Vonage soft phones
- Webmail server
- Weblogs
- LPR printing to home office
- File sharing with sFTP and AFP

# Section 6: Collaboration

## iCal Webcal server

- works with any webdav calendaring system
- Format: webcal://ical.mac.com/hawaiiprep/daily.ics
- If no Leopard server, this can be done on any webDAV server (see Tenon documents)



Data Store: /Library/CalendarServer/Documents

Maximum Attachment Size: 1 MB

User Quota: 100 MB

Authentication: Any Method

Host Name: lserver.local

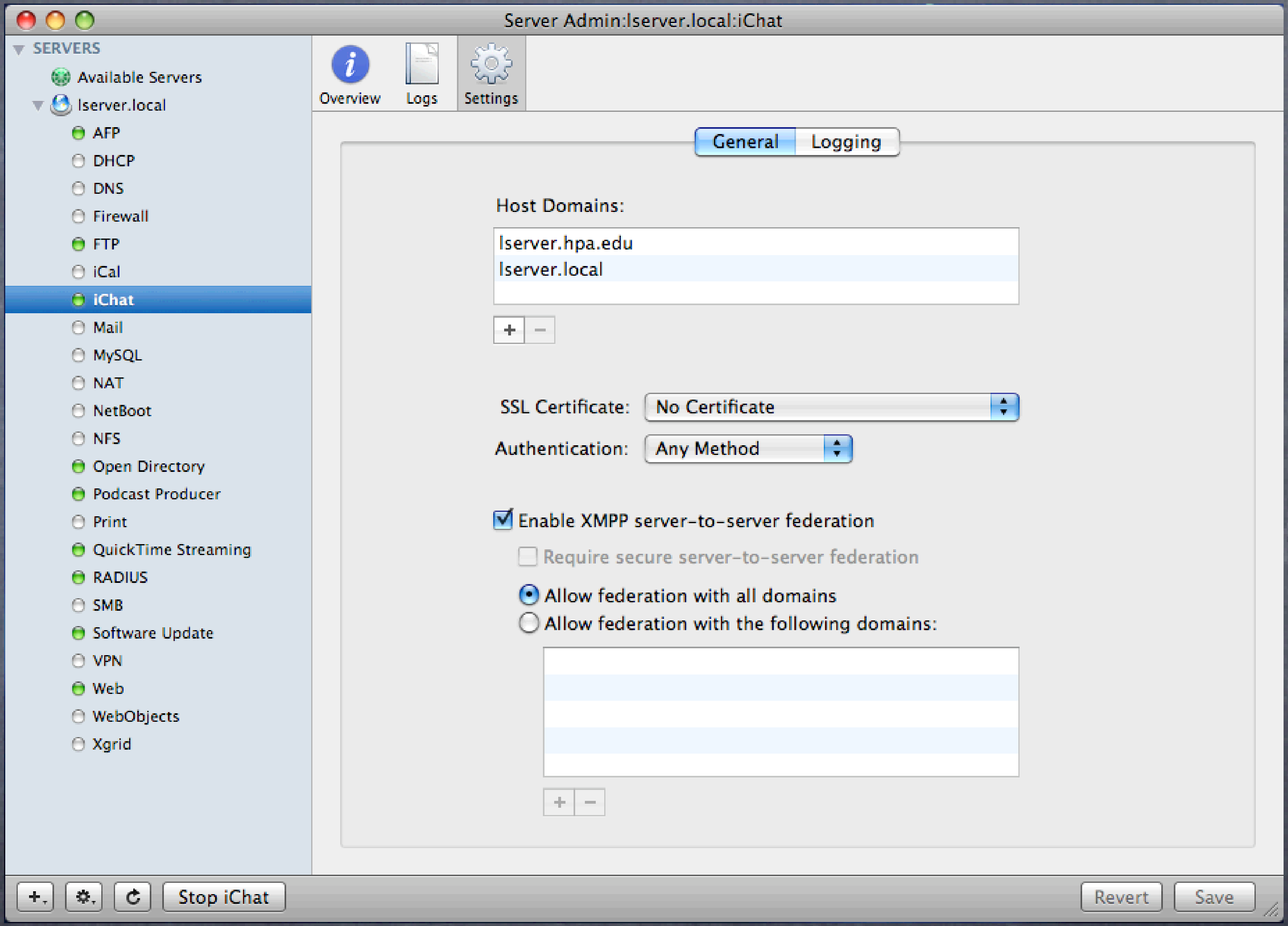
HTTP Port Number: 8008

☐ Enable Secure Sockets Layer (SSL)

# Section 6: Collaboration

## iChatAV jabber server

- Hosts jabber users internal and external
- Use VPN for outside clients to share
- Logging utilities can log chats, conferences for future archives



Host Domains:

lserver.hpa.edu
lserver.local

SSL Certificate: No Certificate

Authentication: Any Method

☑ Enable XMPP server-to-server federation

□ Require secure server-to-server federation

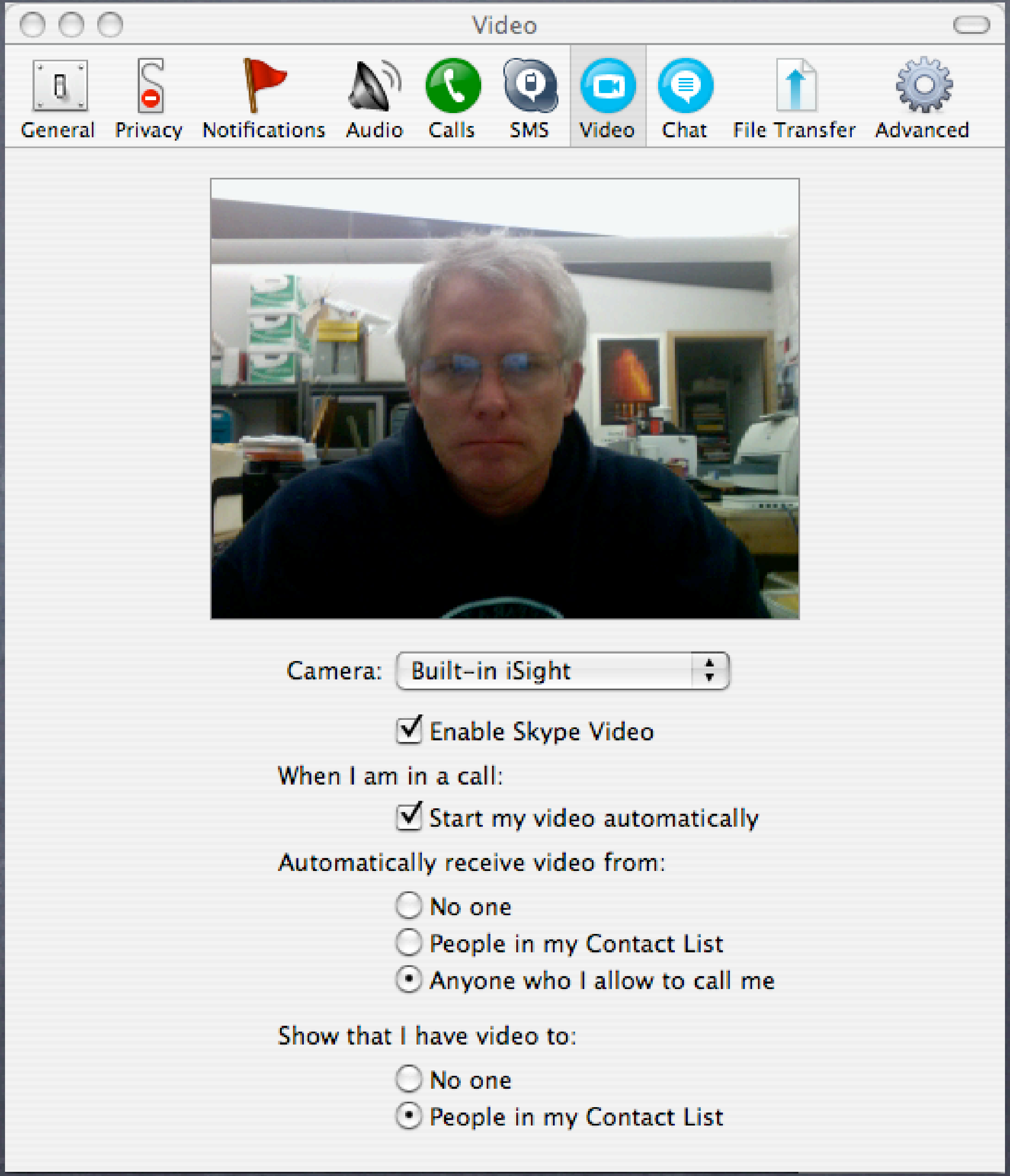
● Allow federation with all domains

○ Allow federation with the following domains:

# Section 6: Collaboration

## Skype

- Easy, cross platform, free client
- Very good video/ audio quality
- Offers many features iChatAV will soon have



Camera: Built-in iSight

☑ Enable Skype Video

When I am in a call:

☑ Start my video automatically

Automatically receive video from:

○ No one
○ People in my Contact List
● Anyone who I allow to call me

Show that I have video to:

○ No one
● People in my Contact List

# Section 6: Collaboration

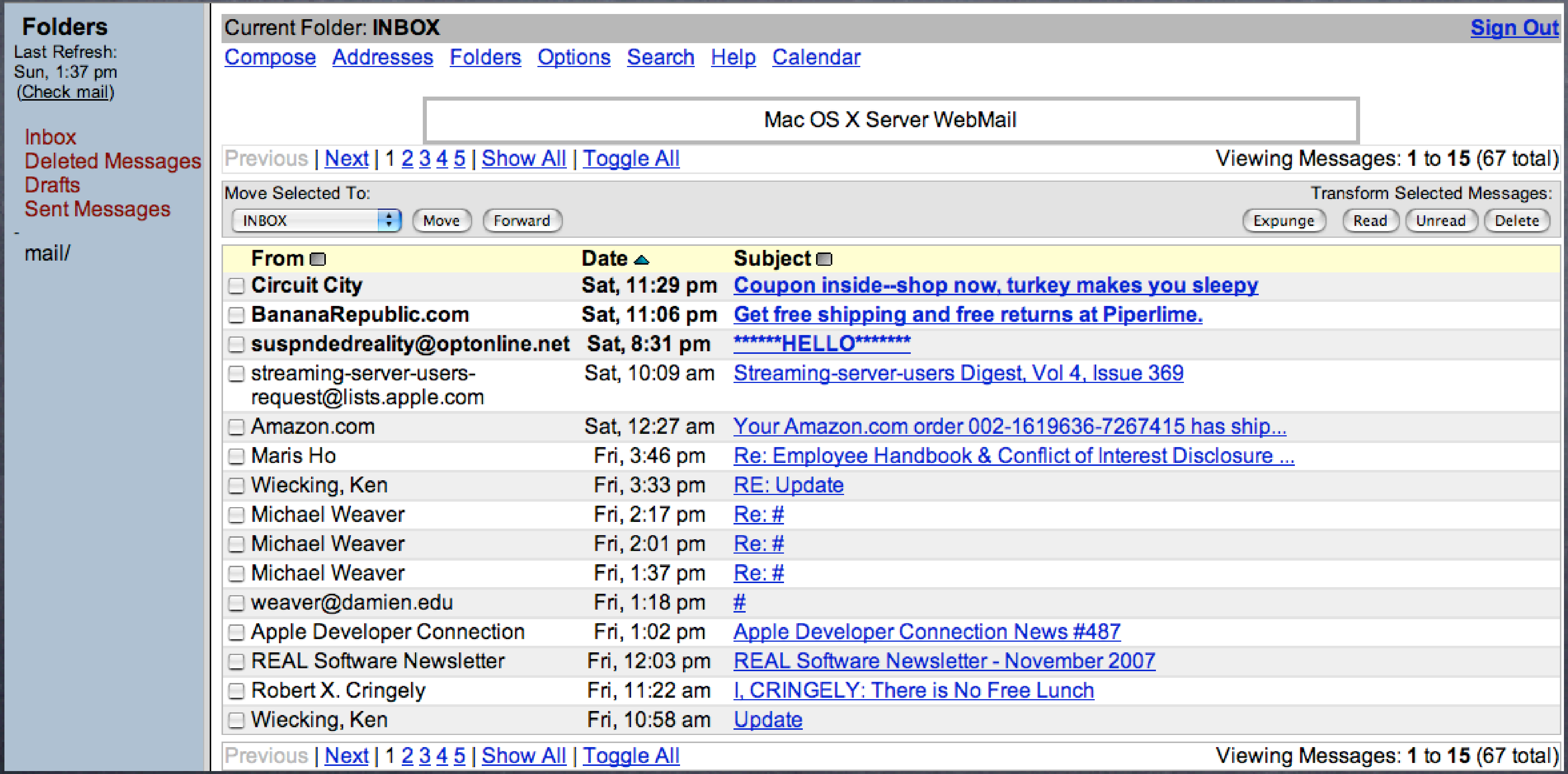
## VoIP

- Voice over IP: free phone calls to other VoIP users
- Skype-out allows skype users to call POTS (plain old telephone service) users
- Vonage Softphone allows computer users to make cheap/free calls worldwide to POTS users
- Tips: make sure you have a good, fast connection
- Wireless latency is usually acceptable, but in long shots (e.g. satellite) the latency may be too great to be comfortable

# Section 6: Collaboration

## Webmail: Tiger and Leopard Server

- Needed some config under Tiger (see Schoun Regan's excellent book on this: Mac OSX Server Essentials)
- Config is simple under Leopard server
- Many plugins/addons are available



**Folders**
Last Refresh:
Sun, 1:37 pm
(Check mail)

Inbox
Deleted Messages
Drafts
Sent Messages
-
mail/

Current Folder: **INBOX** **Sign Out**

Compose Addresses Folders Options Search Help Calendar

Mac OS X Server WebMail

Previous | Next | 1 2 3 4 5 | Show All | Toggle All Viewing Messages: **1** to **15** (67 total)

Move Selected To: INBOX Move Forward

Transform Selected Messages: Expunge Read Unread Delete

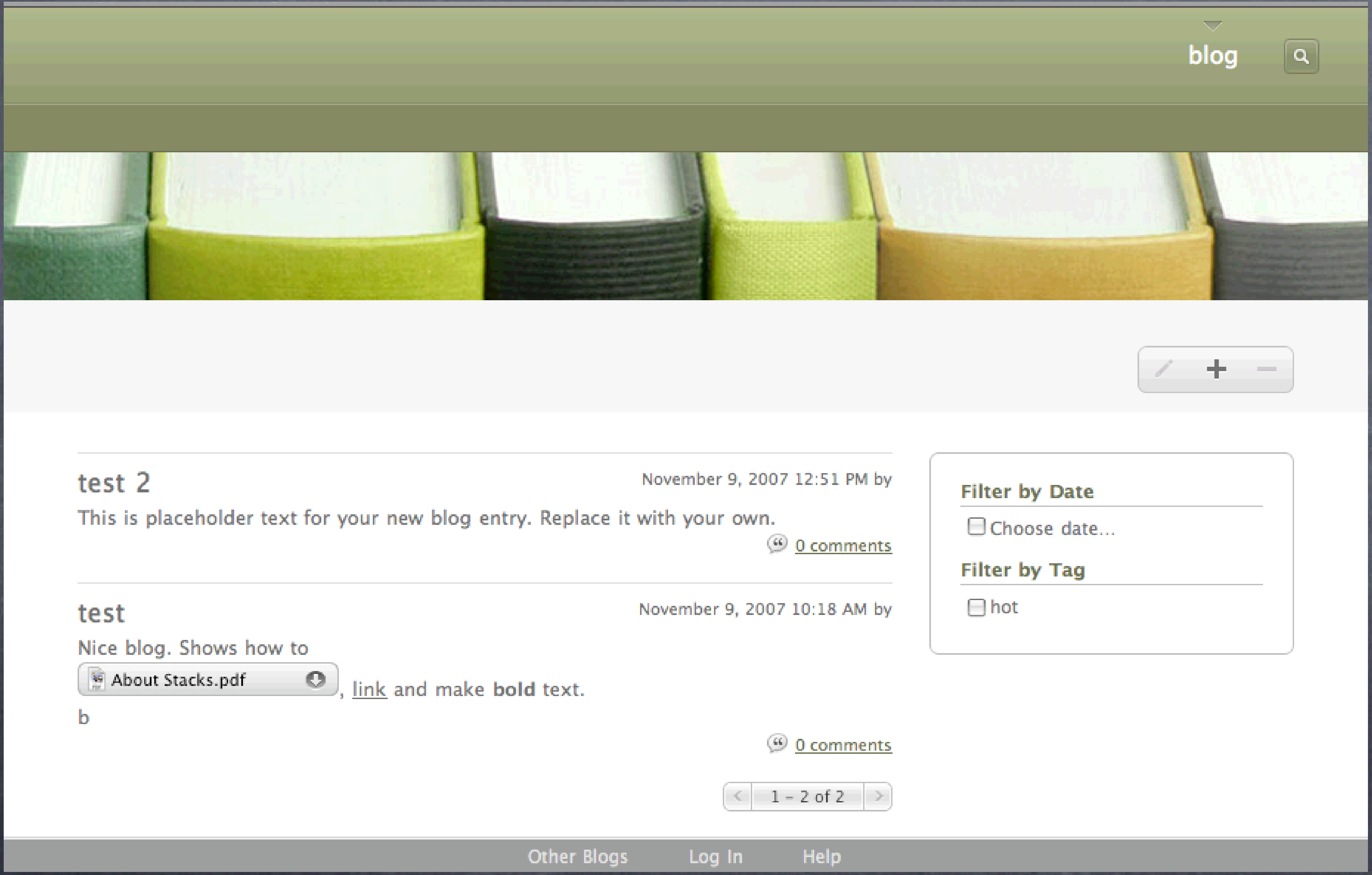
| | From | Date ▲ | Subject |
|---|---|---|---|
| ☐ | **Circuit City** | **Sat, 11:29 pm** | **Coupon inside--shop now, turkey makes you sleepy** |
| ☐ | **BananaRepublic.com** | **Sat, 11:06 pm** | **Get free shipping and free returns at Piperlime.** |
| ☐ | **suspndedreality@optonline.net** | **Sat, 8:31 pm** | ********HELLO********* |
| ☐ | streaming-server-users-request@lists.apple.com | Sat, 10:09 am | Streaming-server-users Digest, Vol 4, Issue 369 |
| ☐ | Amazon.com | Sat, 12:27 am | Your Amazon.com order 002-1619636-7267415 has ship... |
| ☐ | Maris Ho | Fri, 3:46 pm | Re: Employee Handbook & Conflict of Interest Disclosure ... |
| ☐ | Wiecking, Ken | Fri, 3:33 pm | RE: Update |
| ☐ | Michael Weaver | Fri, 2:17 pm | Re: # |
| ☐ | Michael Weaver | Fri, 2:01 pm | Re: # |
| ☐ | Michael Weaver | Fri, 1:37 pm | Re: # |
| ☐ | weaver@damien.edu | Fri, 1:18 pm | # |
| ☐ | Apple Developer Connection | Fri, 1:02 pm | Apple Developer Connection News #487 |
| ☐ | REAL Software Newsletter | Fri, 12:03 pm | REAL Software Newsletter - November 2007 |
| ☐ | Robert X. Cringely | Fri, 11:22 am | I, CRINGELY: There is No Free Lunch |
| ☐ | Wiecking, Ken | Fri, 10:58 am | Update |

Previous | Next | 1 2 3 4 5 | Show All | Toggle All Viewing Messages: **1** to **15** (67 total)

# Section 6: Collaboration

## Weblogs: Leopard Server

- Extension of the Blojsom open source weblog system



test 2 November 9, 2007 12:51 PM by

This is placeholder text for your new blog entry. Replace it with your own.

0 comments

test November 9, 2007 10:18 AM by

Nice blog. Shows how to

About Stacks.pdf, link and make **bold** text.

b

0 comments

Filter by Date

□ Choose date…

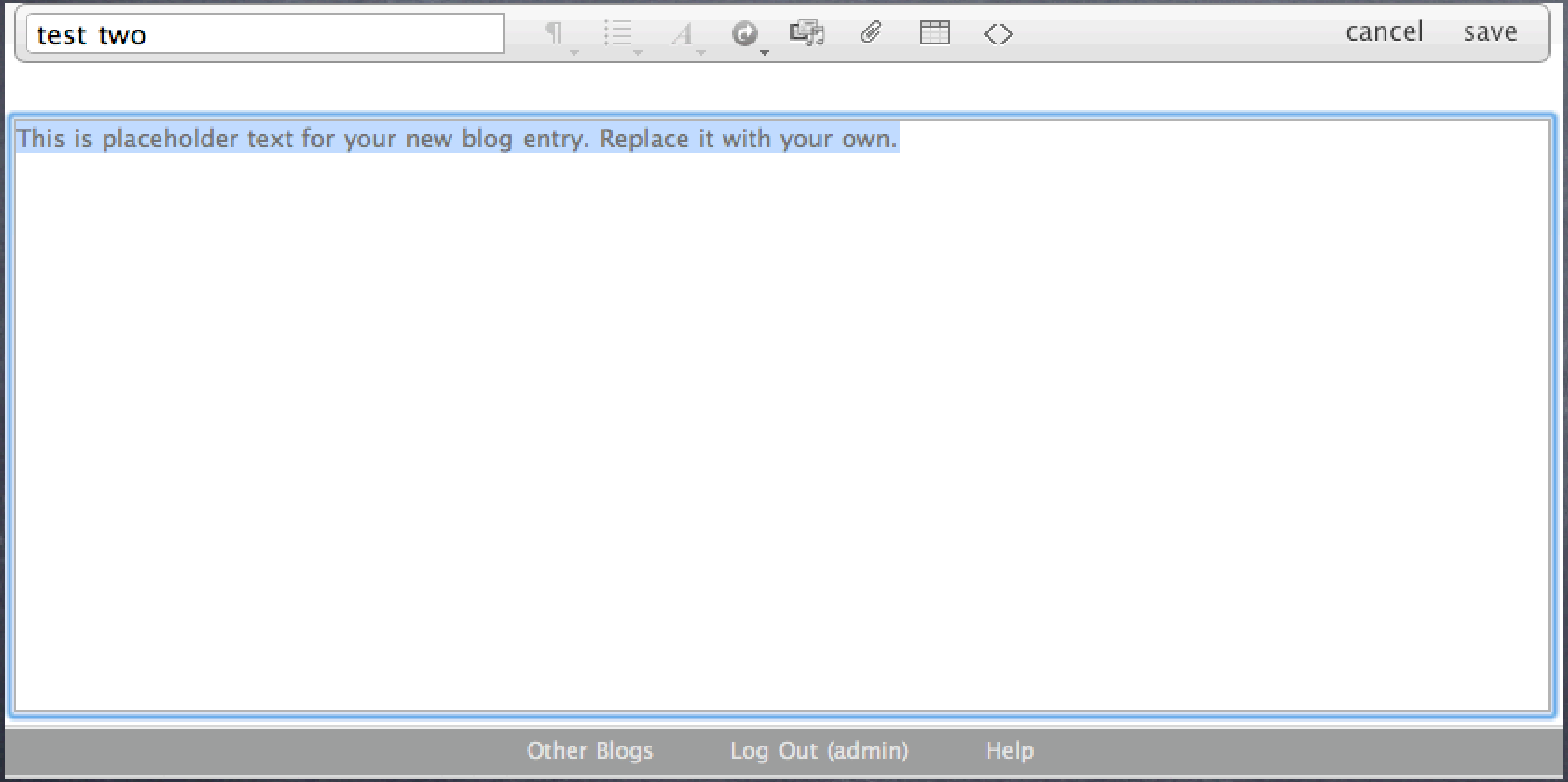
Filter by Tag

□ hot

# Section 6: Collaboration

## Weblogs: Leopard Server

- Many more options under Leopard: attachments, fonts, media, urls, html view, tables, bullets, outlines.



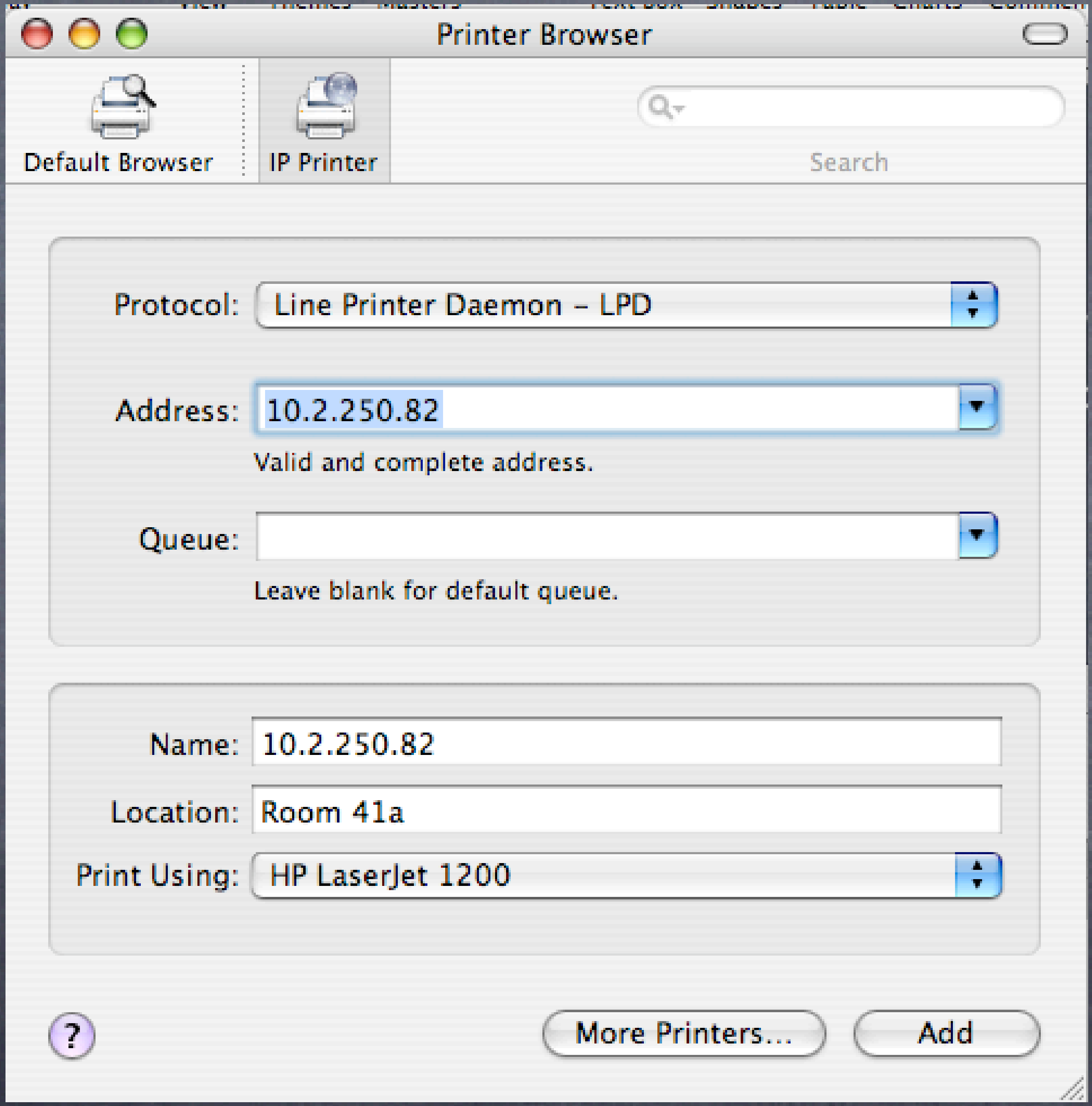
test two

This is placeholder text for your new blog entry. Replace it with your own.

# Section 6: Collaboration

## LPR printing from anywhere

- Enables you to print from anywhere to an LPR enabled printer or your server (many queues possible)



Protocol: Line Printer Daemon – LPD

Address: 10.2.250.82

Valid and complete address.

Queue:

Leave blank for default queue.

Name: 10.2.250.82

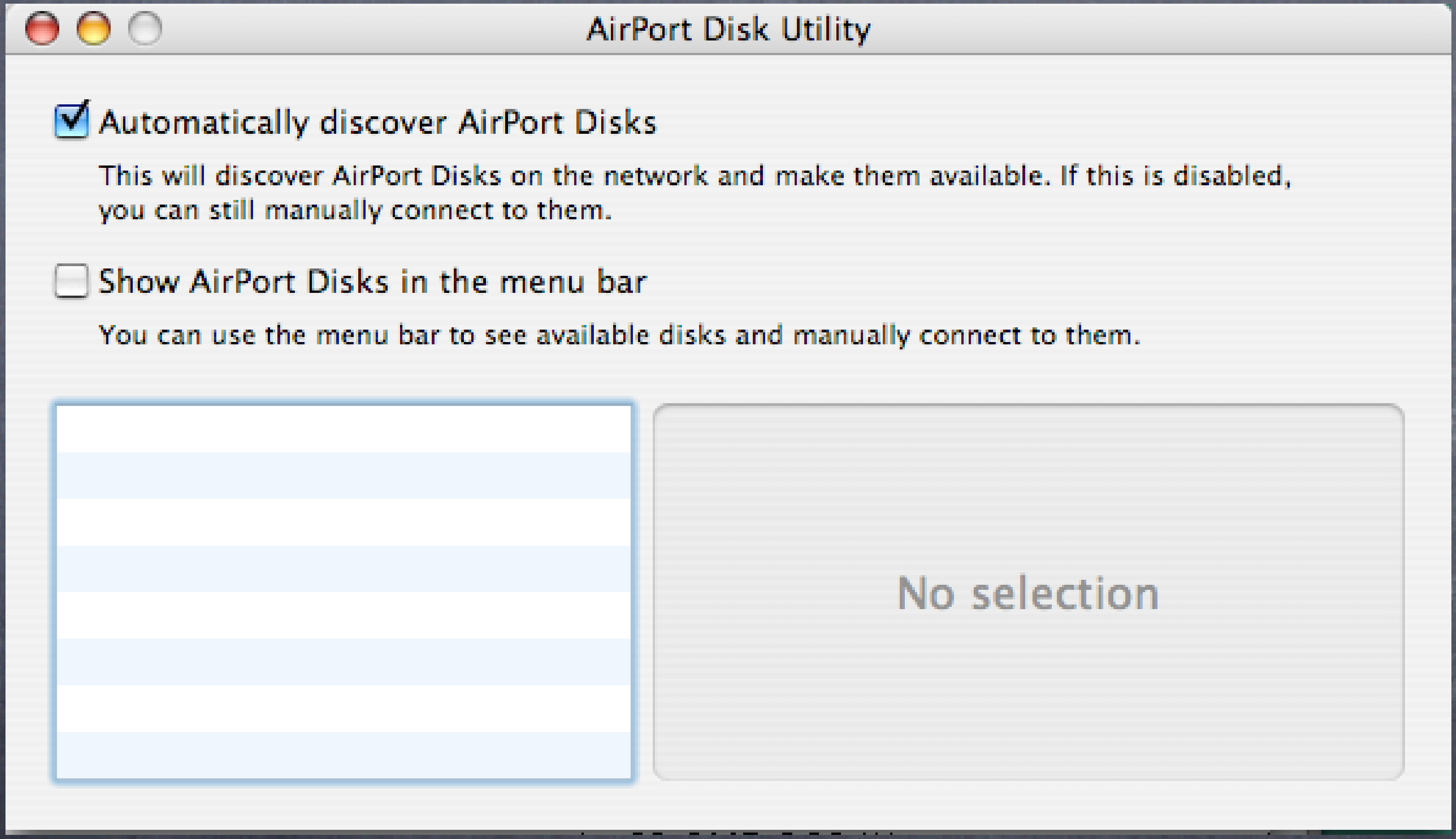
Location: Room 41a

Print Using: HP LaserJet 1200

# Section 6: Collaboration

## File Sharing: sFTP and AFP

- Access to shared files locally or on the internet.
- Options: Leopard OSX server, local file sharing with incoming Network Address Translation (NAT), using Airport disk utility, can share an attached drive to an Airport Extreme X2
- sFTP is secure (encrypted) File transfer protocol, and is not looked on affectionately among the sysadmin community. How to make it better? Use a VPN whenever possible



☑ Automatically discover AirPort Disks

This will discover AirPort Disks on the network and make them available. If this is disabled, you can still manually connect to them.

□ Show AirPort Disks in the menu bar

You can use the menu bar to see available disks and manually connect to them.

No selection

FIN

# Summary

Day two take-aways:

- Access control skills: access and authentication issues
- Elektron and Leopard server as RADIUS servers
- Wired vs. Wireless practices
- Integration: how to make the best of mobility
- Collaboration: work better from a distance