

Wired and Wireless Security with RADIUS Servers

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

Wireless Security Issues

- 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

Access Control Basics

Access Control History:

- ① No Access Control
- ① WEP (passwords, easily broken)
- ① MAC authentication-based on wireless hardware address
- ① WPA/WPA2-based on the 802.1x standard
 - ① TKIP (temporal Key integrity protocol—password changes frequently)
 - ① TTLS-EAP (tunneled authentication protocols, processes)
 - ① CCMP and MIC (data integrity checks)
 - ① 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 (WPA2 Enterprise, with RADIUS server)
- 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, can be added on the fly
- Bad point: can be spoofed using Kismac and unix tools

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
- Bad point: need to manage separate access points (this may be a good thing)

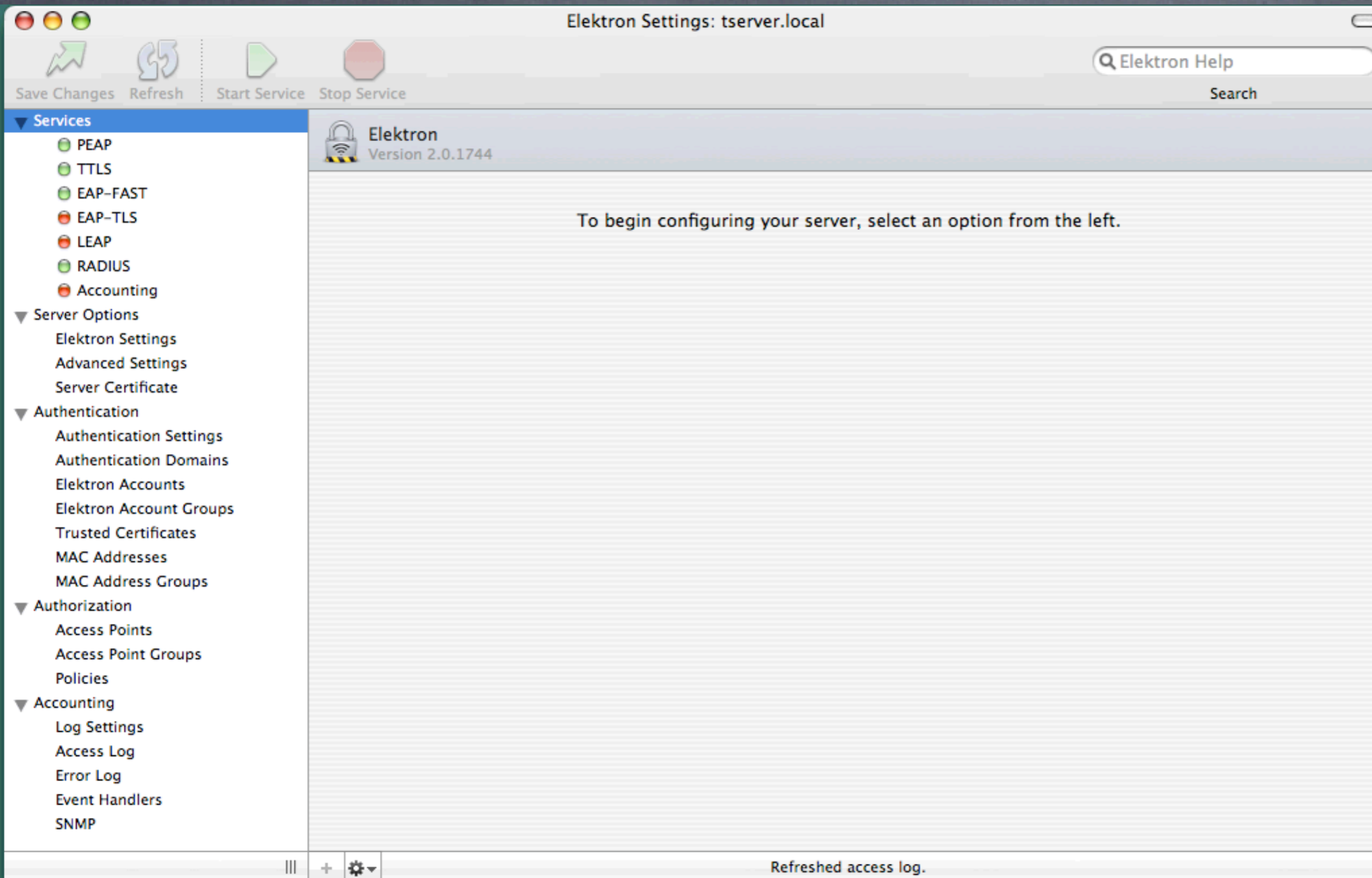
WPA2 enterprise authentication:

- Add user accounts to RADIUS server
- Setup 802.1x on client machines, using login and password from AP
- Good points: central administration, no restart of AP needed to add users
- Much easier logging and detection of attacks

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



- ▶ Can be used as pure MAC based or as WPA2 server
- ▶ Note services on left

Elektron RADIUS/WPA2 server

The screenshot shows the Elektron Settings application for tserver.local. The interface includes a top toolbar with 'Save Changes', 'Refresh', 'Start Service', and 'Stop Service' buttons. A left sidebar contains a tree view of settings categories: Services, Server Options, Authentication, Authorization, and Accounting. The 'Access Points' option under 'Authorization' is selected. The main content area displays the 'Access Points' configuration page, which includes a sub-header 'Configure devices using Elektron for user authentication' and a table with columns 'Access Point' and 'Friendly Name'. The table lists three entries: '0.0.0.0/0' with friendly name 'Created by the Elektron Setup Assistant', '192.168.3.121' with friendly name 'zebra', and '192.168.3.122' with friendly name 'zebra2'. At the bottom right, a status bar indicates 'Refreshed access log.'

Access Point	Friendly Name
0.0.0.0/0	Created by the Elektron Setup Assistant
192.168.3.121	zebra
192.168.3.122	zebra2

► Access point capture

Elektron RADIUS/WPA2 server

Elektron Settings: tserver.local

Save Changes Refresh Start Service Stop Service

Services

- PEAP
- TTLS
- EAP-FAST
- EAP-TLS
- LEAP
- RADIUS
- Accounting

Server Options

- Elektron Settings
- Advanced Settings**
- Server Certificate

Authentication

- Authentication Settings
- Authentication Domains
- Elektron Accounts
- Elektron Account Groups
- Trusted Certificates
- MAC Addresses
- MAC Address Groups

Authorization

- Access Points
- Access Point Groups
- Policies

Accounting

- Log Settings
- Access Log
- Error Log
- Event Handlers
- SNMP

Advanced Settings
Configure advanced Elektron server settings

Primary Server Port

Enable Primary Server Port

Server Port: (default 1812)

Secondary Server Port

Enable Secondary Server Port

Secondary Port: (default 1645)

Server Address

Bind Elektron To a Specific IP Address

IP Address:

Session Timeout

Enable Session Timeout

Session Lifetime: Seconds

Privilege Separation

Run With Least Privilege (change requires server restart)

Refreshed access log.

► See default and secondary ports on Access Point setup screens as well

Elektron RADIUS/WPA2 server

The screenshot shows the Elektron Settings application for tserver.local. The interface includes a top toolbar with 'Save Changes', 'Refresh', 'Start Service', and 'Stop Service' buttons. A left sidebar contains a tree view of settings categories: Services, Server Options, Authentication, Authorization, and Accounting. The 'Authentication' category is expanded, and 'MAC Addresses' is selected. The main pane displays a table of MAC addresses used for authentication, with columns for 'MAC Address' and 'Friendly Name'. The table lists 18 entries, including devices like 'tserver', 'minitel', 'olpc laptop', and various 'tsunami intel' and 'john ray' devices. The status bar at the bottom right indicates 'Refreshed access log.'

MAC Address	Friendly Name
00:0A:95:F4:95:3A	tserver
00:14:51:EF:32:D5	minitel
00:17:C4:0D:48:55	olpc laptop
00:17:F2:47:A2:B2	iboat mbook
00:17:F2:E9:7C:FC	claudius saalfeld
00:19:7D:30:FF:8A	tsunami intel asof
00:19:E3:07:9C:FC	jambake macbook
00:19:E3:D4:82:42	iboat macbook black
00:19:E3:D5:FA:B5	kkd laptop
00:1C:B3:6B:5B:D4	iphone bill
00:1C:B3:6F:B7:AF	john ray iphone
00:1C:B3:B0:40:67	intel mini 2.0
00:1C:B3:B0:42:F2	mini
00:1C:B3:B3:9F:0C	tsunami intel d
00:1C:B3:BF:D7:E1	tsunami intel green
00:1C:B3:C1:14:0D	john ray mbook bro
00:30:65:00:5B:63	pbook g4
00:30:65:0A:28:D8	pbook g4 tserver
00:30:65:1A:D1:09	pilot g3 ibook
00:30:65:1B:C4:37	cube

- ▶ MAC Address list
- ▶ Groups listed below

Elektron RADIUS/WPA2 server

Elektron Settings: tserver.local

Save Changes Refresh Start Service Stop Service

Services

- PEAP
- TTLS
- EAP-FAST
- EAP-TLS
- LEAP
- RADIUS
- Accounting

Server Options

- Elektron Settings
- Advanced Settings
- Server Certificate

Authentication

- Authentication Settings
- Authentication Domains
- Elektron Accounts
- Elektron Account Groups
- Trusted Certificates
- MAC Addresses
- MAC Address Groups

Authorization

- Access Points
- Access Point Groups
- Policies

Accounting

- Log Settings
- Access Log
- Error Log
- Event Handlers
- SNMP

Access Log

Recent Access Log Entries

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

Refreshed

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

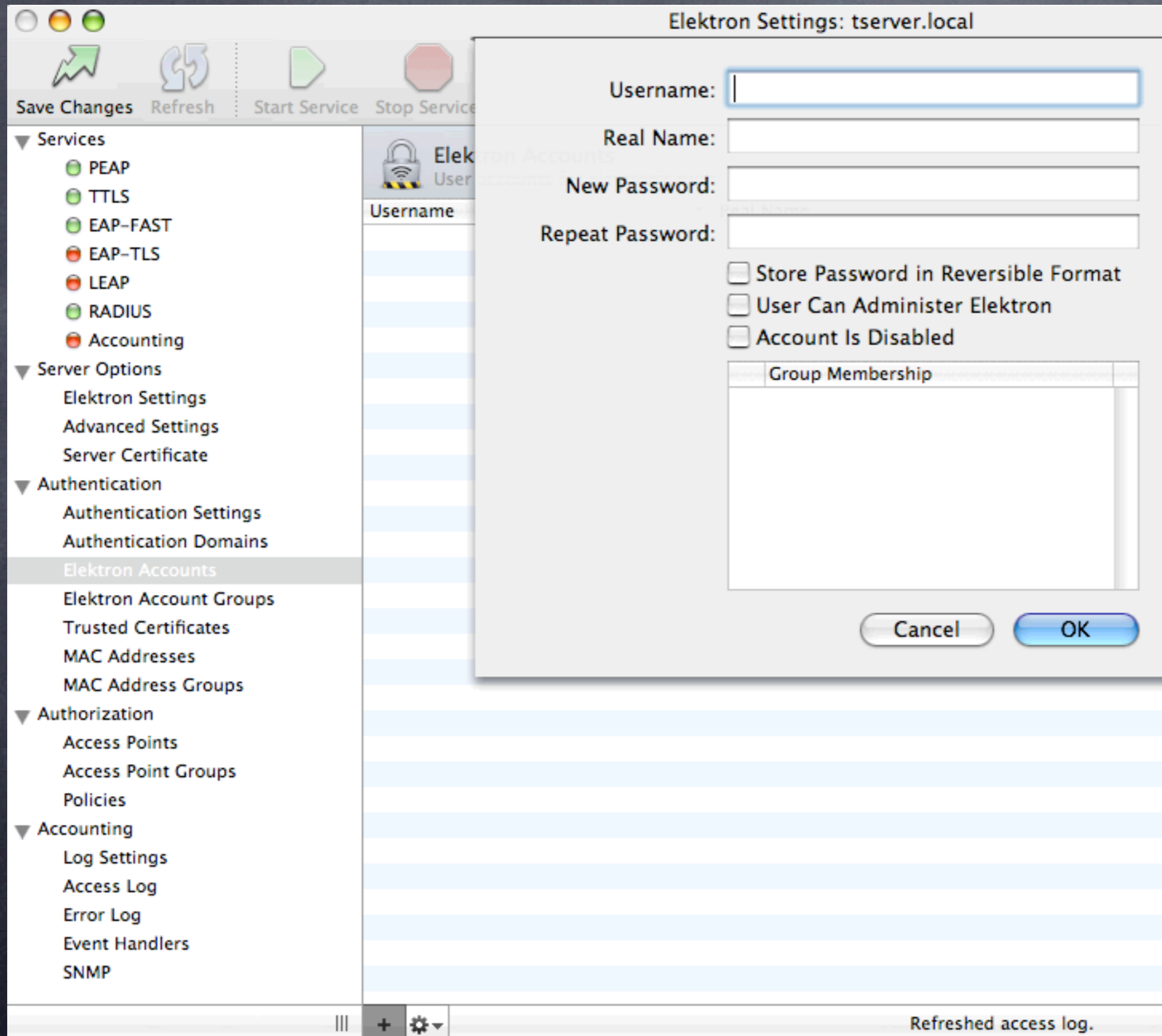
Elektron RADIUS/WPA2 server

The screenshot shows the Elektron Settings application window for 'tserver.local'. The interface includes a top toolbar with 'Save Changes', 'Refresh', 'Start Service', and 'Stop Service' buttons. A left sidebar contains a tree view of settings categories: Services, Server Options, Authentication, Authorization, and Accounting. The 'Server Certificate' option is selected and highlighted in blue. The main content area is titled 'Server Certificate' and contains the following configuration options:

- Server Certificate:** A dropdown menu showing 'tserver' with 'View...' and 'Delete' buttons. Below it, a note states: 'The server will identify itself to clients using this certificate.'
- Certificate Authority:** A section titled 'Certificate Authority: local Elektron CA' with a note: 'Clients need this certificate to authenticate the server.'
- Export Certificate:** Four buttons with descriptions:
 - 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.
 - Installers...**: Double-clickable installers for Mac OS X and Windows.

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

Elektron RADIUS/WPA2 server



► Adding users for WPA2 authentication

Elektron RADIUS/WPA2 server

The screenshot shows the Elektron Settings application for tserver.local. The interface includes a top bar with window controls and action buttons: Save Changes, Refresh, Start Service, and Stop Service. A left sidebar lists various configuration categories: Services, Server Options, Authentication, Authorization, and Accounting. The main content area is titled 'SNMP' and 'Simple Network Management Protocol configuration'. Under 'SNMP Settings', the following options are visible:

- Enable SNMP on Port: 5398 (Default 5398)
- Enable SNMPv1
- Enable SNMPv2c
- Community: [] (Default "public")

- ▶ SNMP access
- ▶ Good idea for monitoring with Intermapper/Cybergauge

Elektron Server RADIUS

Strong Points:

- ① Cheaper than Leopard Server
- ① Runs on client (Mac OS 10.3, 10.4, 10.5) not server
- ① More flexible (MAC ACL and/or WPA2)
- ① 802.1x security with relatively little hassle
- ① Integrates with Open Directory
- ① Can also run an independent access list (good with limited server versions)
- ① Many users centrally administered, easier than WPA2 personal
- ① Can export certificates for mac, pc users

Weak points:

- ① Extra cost if you already own Leopard Server

Client configurations: Tiger and Leopard

Tiger client WPA2 setup

802.1X

Summary AirPort VPN (L2TP) 802.1X

802.1X

Configuration: Other

Network Port: AirPort

User Name:

Password:

Wireless Network:

Status: Idle

Connect

▶ 802.1x setup screen on Tiger client

Tiger Client WPA2 config

Configuration

802.1X Configuration

Description: 802.1X Configuration

Network Port: AirPort

User Name:

Password:

Wireless Network:

Authentication:

On	Protocol
<input checked="" type="checkbox"/>	TTLS
<input type="checkbox"/>	TLS
<input checked="" type="checkbox"/>	LEAP
<input checked="" type="checkbox"/>	PEAP
<input checked="" type="checkbox"/>	MDS

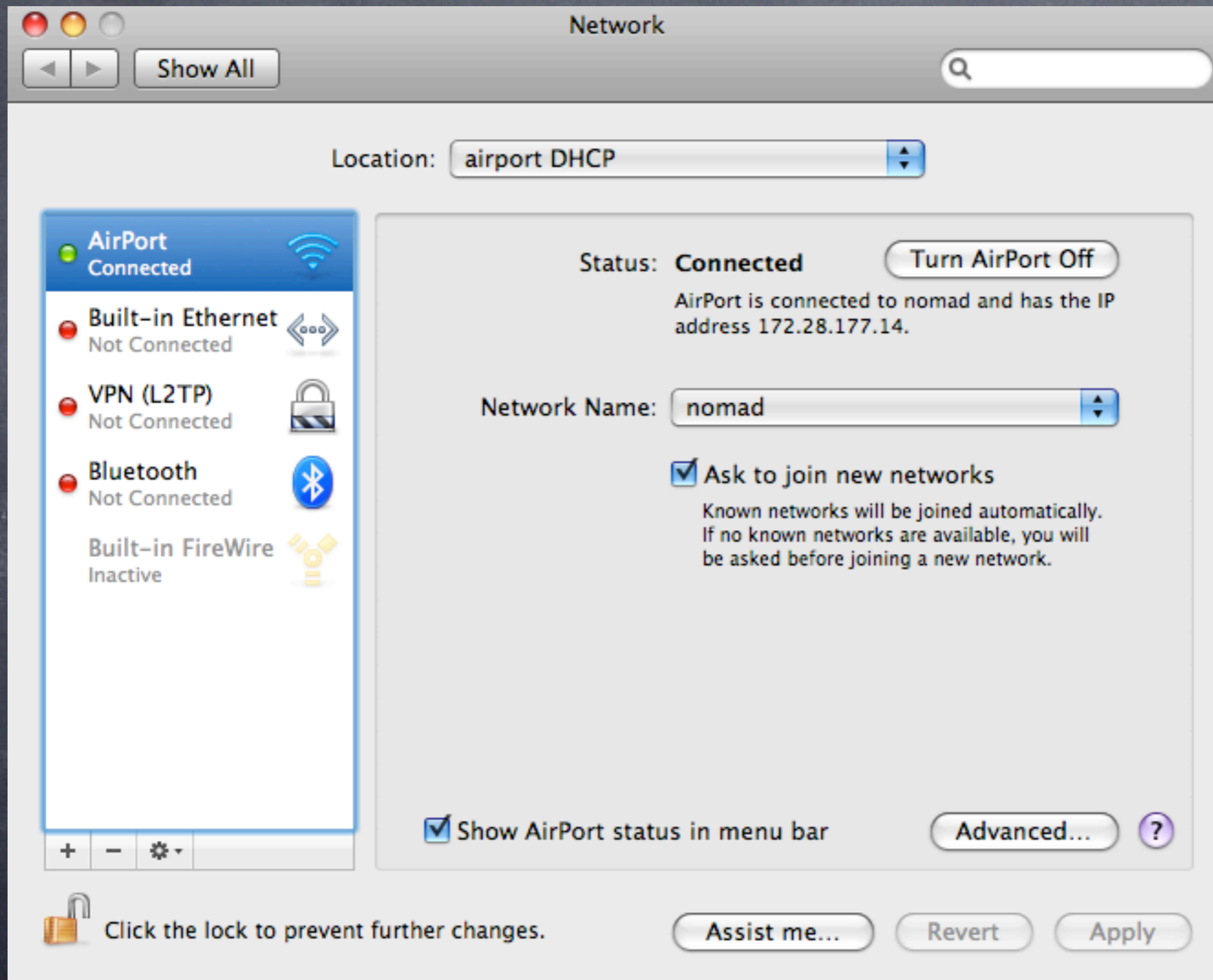
Configure...

Select supported authentication protocols above and then order them appropriately.

Cancel OK

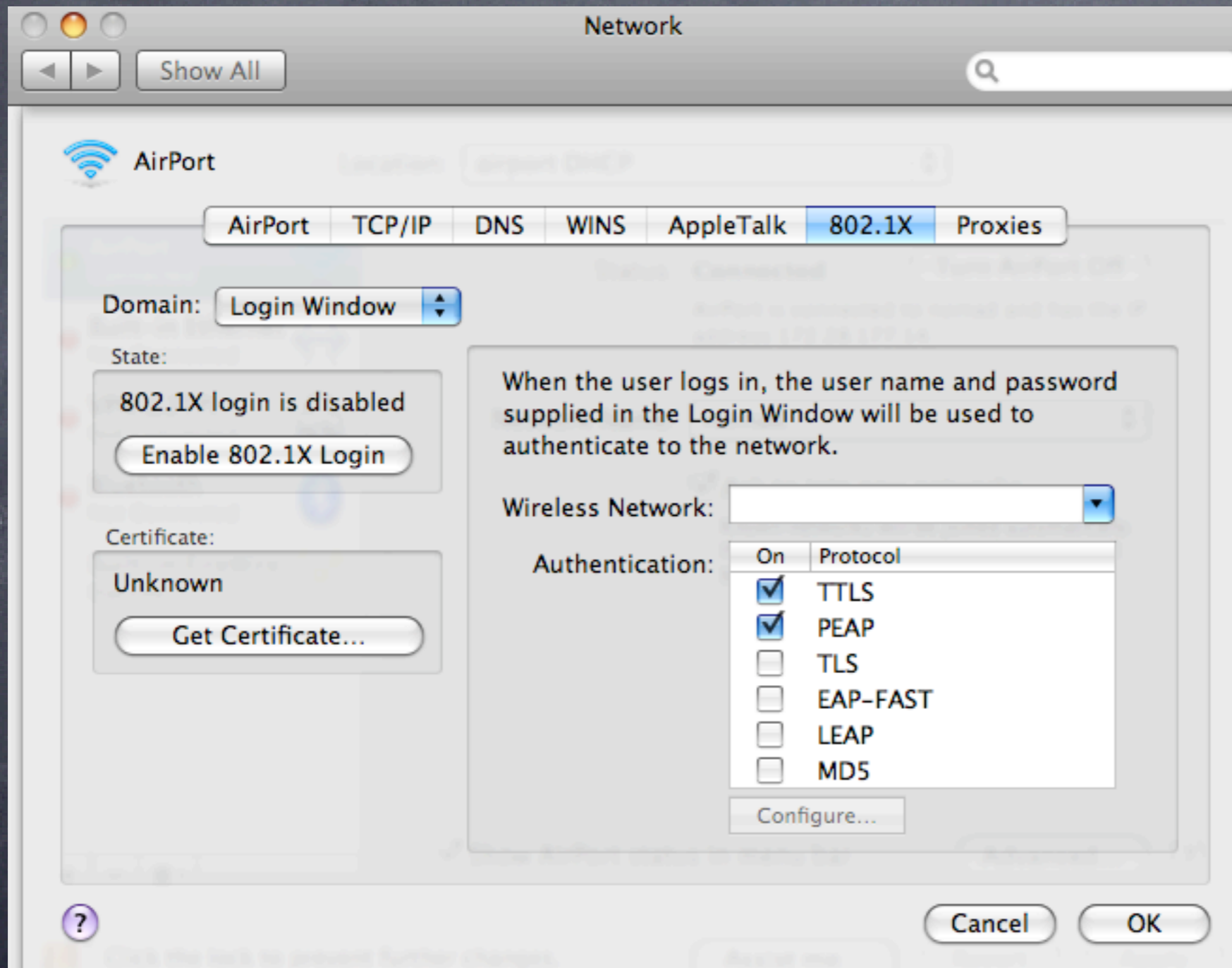
► Note Protocols below, can be wireless or wired (managed switches)

Leopard Client WPA2 config



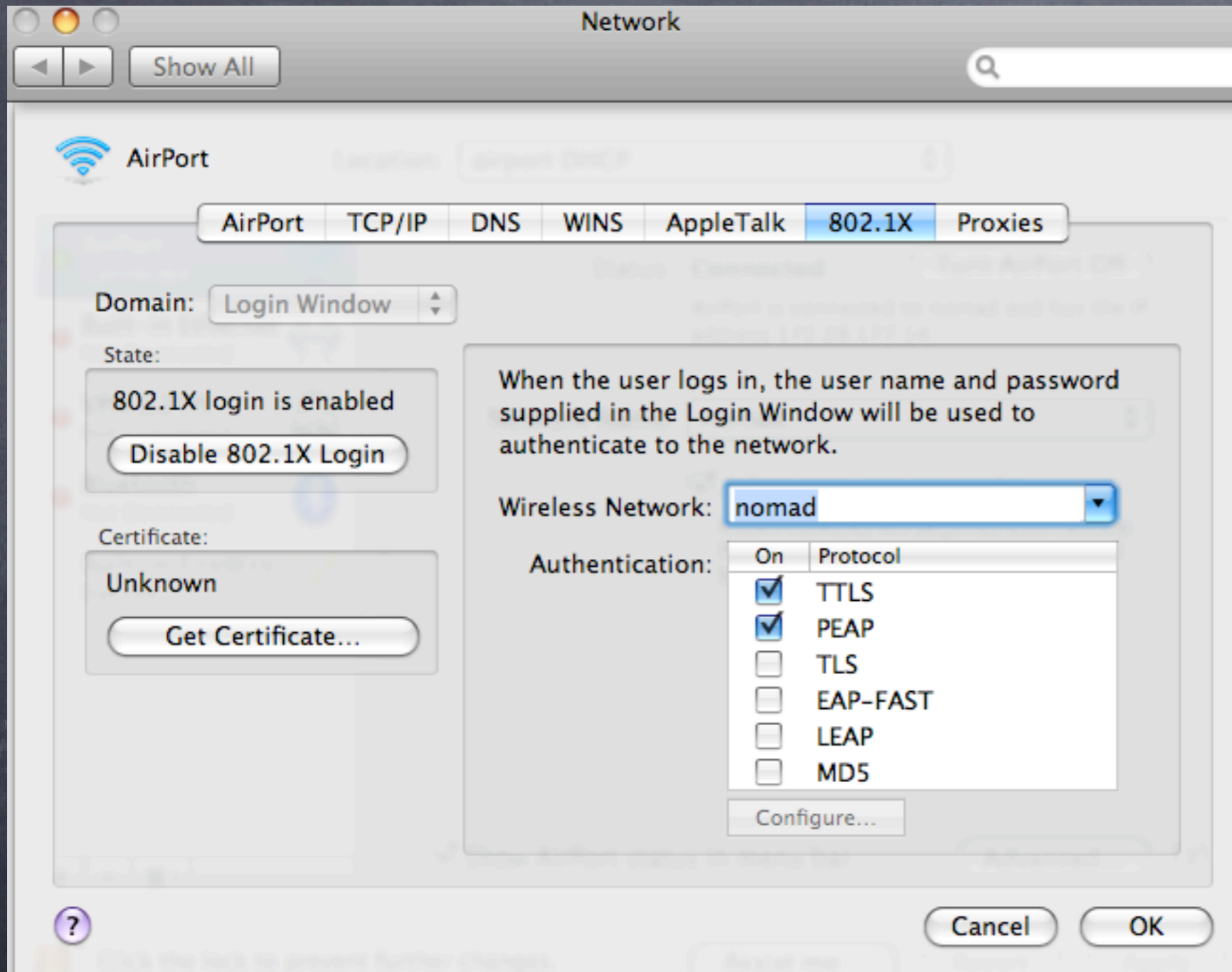
► Network settings control panel

Leopard Client WPA2 config



▶ 802.1x control panel

Leopard Client WPA2 config



► Note network selection option

Mac OS X Leopard Server:
WPA2 RADIUS server

Leopard Server: RADIUS

The screenshot shows the Server Admin application window titled "Server Admin:lserver.local:RADIUS". The interface is divided into several sections:

- Left Sidebar (SERVERS):** A list of services with radio buttons. "RADIUS" is selected and highlighted in blue. Other services include Available Servers, Iserver.local, AFP, DHCP, DNS, Firewall, FTP, iCal, iChat, Mail, MySQL, NAT, NetBoot, NFS, Open Directory, Podcast Producer, Print, QuickTime Streaming, SMB, Software Update, VPN, Web, WebObjects, and Xgrid.
- Top Navigation:** Four icons for "Overview" (info), "Logs", "Base Stations" (Wi-Fi), and "Settings" (gear).
- Table:** A table with columns "Address", "Name", and "Type". It contains one entry: "10.3.254.32", "leopard radius", and "AirPort Base Station".
- Buttons:** "Browse...", "Add...", "Edit...", "Remove", and "Save Internet Connect File..."
- Configuration Details:** "Name: leopard radius", "Ethernet (WAN): 00:1B:63:F4:79:5D", "AirPort ID: 00:1C:B3:AF:C2:7C", and "Apple Base Station V7.2.1".
- Right Image:** A small image of an Apple Base Station device.
- Bottom Bar:** A "Stop RADIUS" button with a plus icon, a gear icon, and a refresh icon.

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

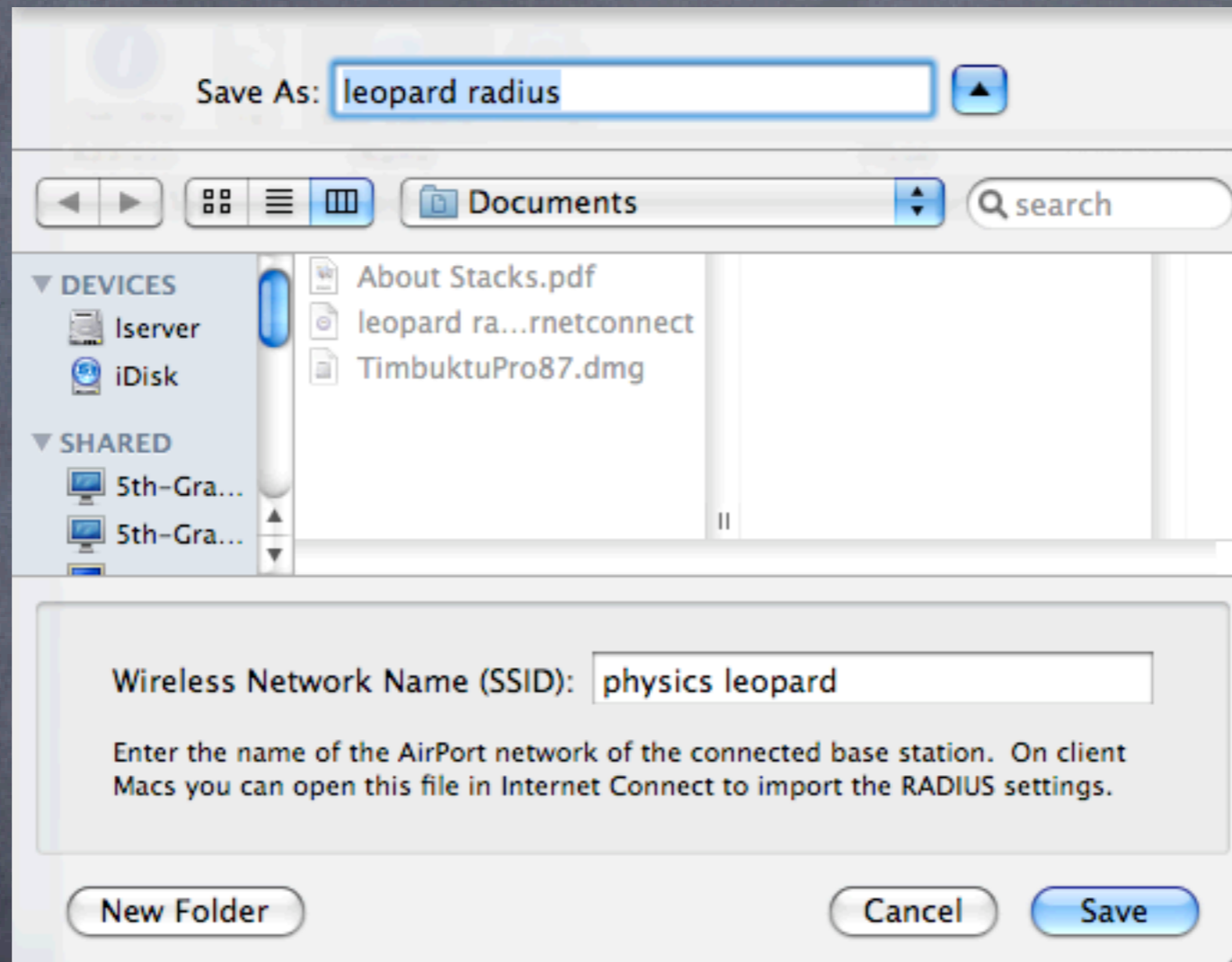
AirPort administrator password:

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.

Cancel

Add

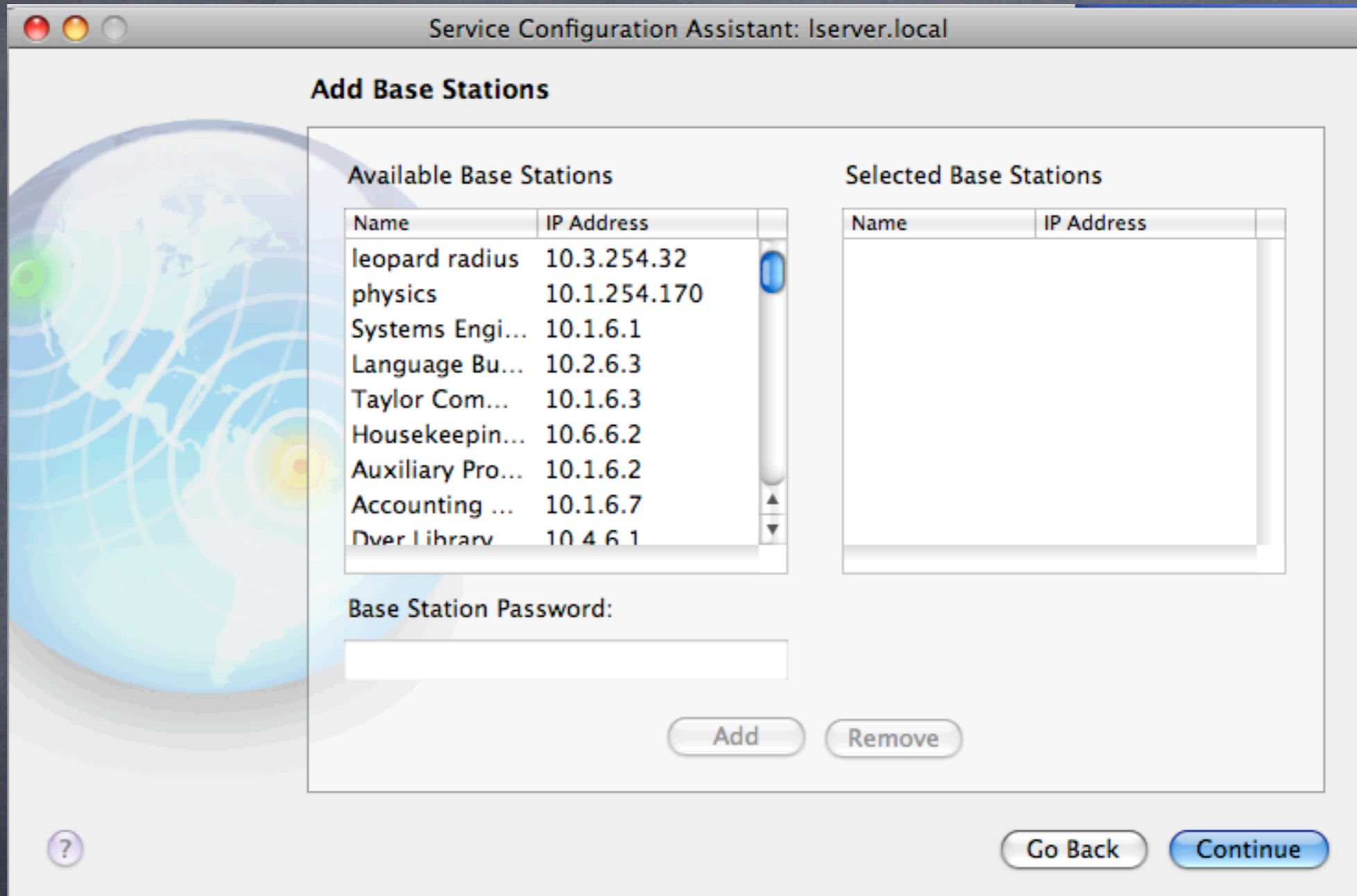
Leopard Server: RADIUS



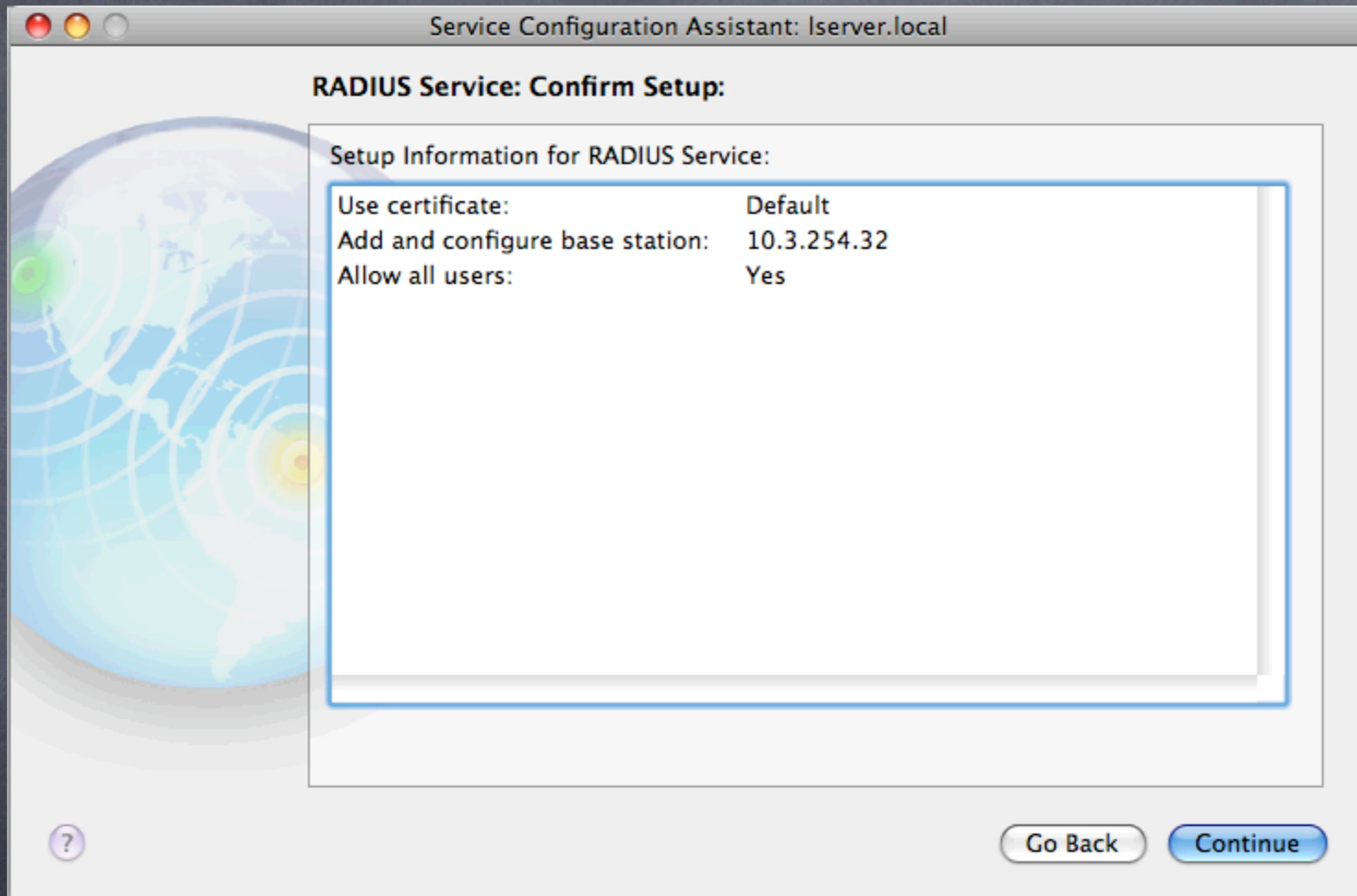
Leopard Server: RADIUS



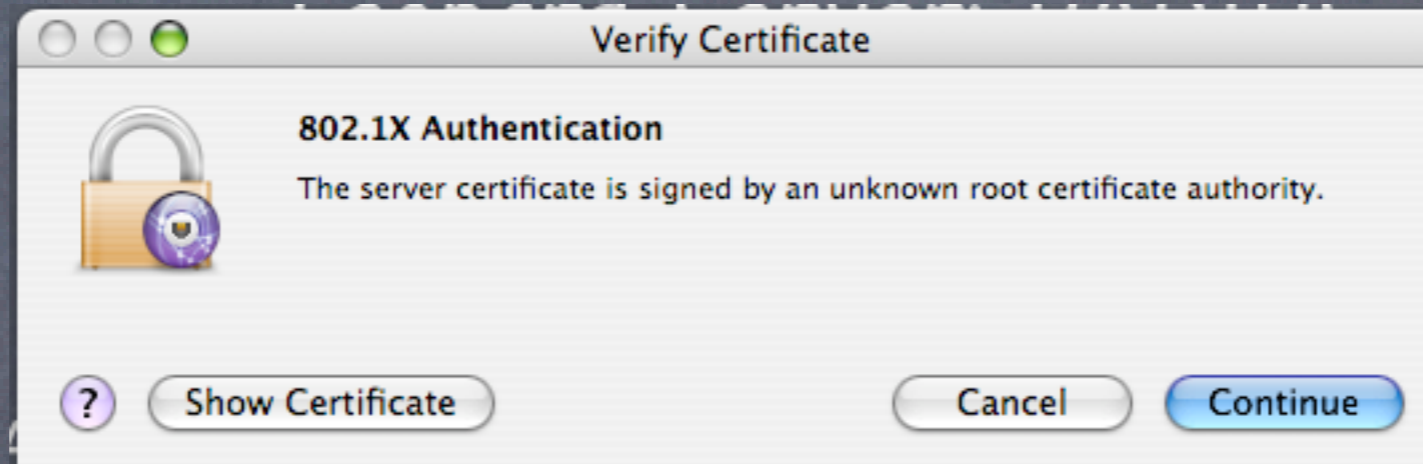
Leopard Server: RADIUS



Leopard Server: RADIUS



Leopard Server: RADIUS Exported Internet Connect file



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
- May not work and play well with older PC versions

Authentication: Elektron vs. Leopard Server

Elektron:

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

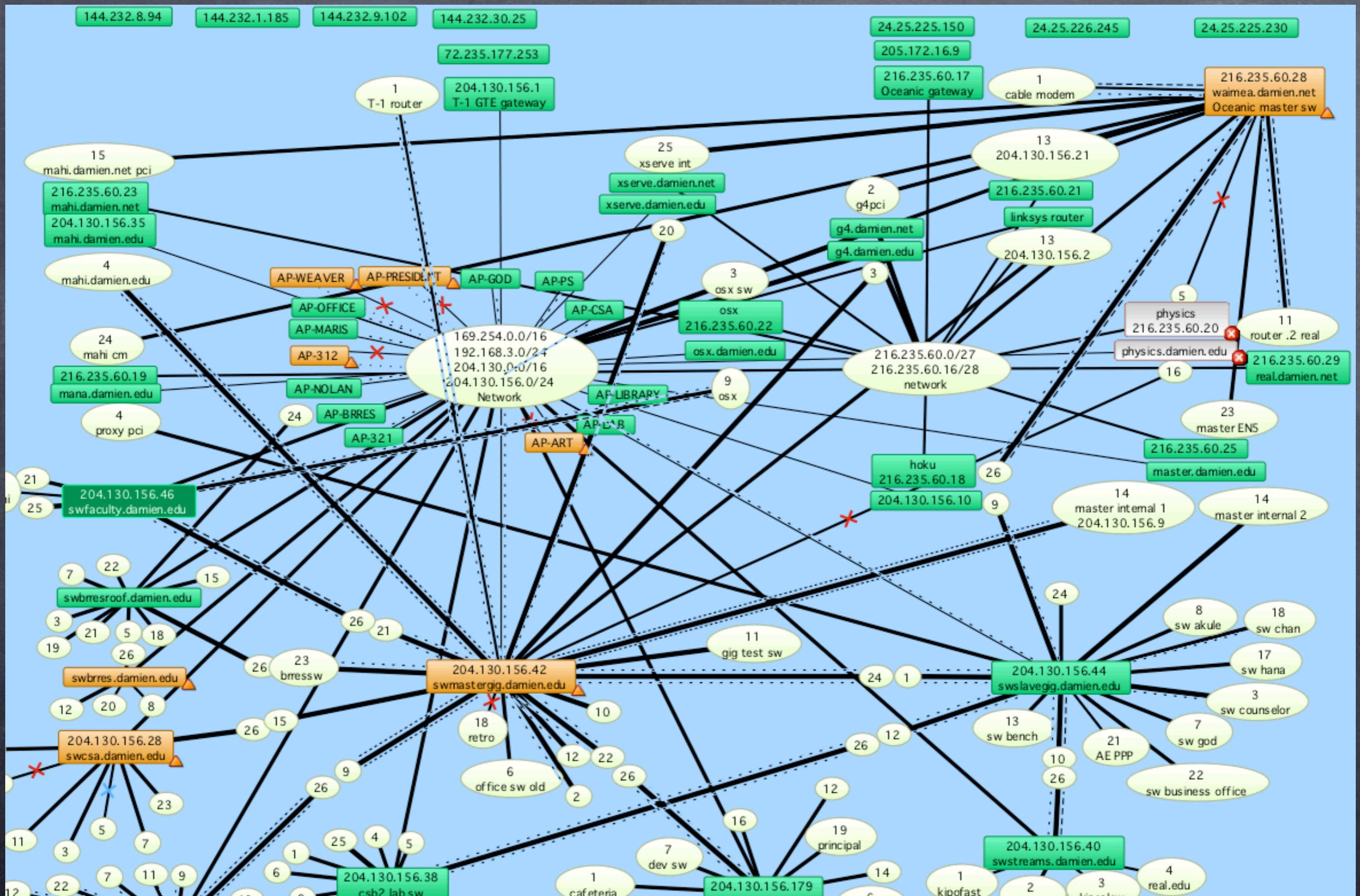
Leopard Server:

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

Authentication: Summary

- RADIUS/802.1x authentication is the way to go: personal for one AP, enterprise/RADIUS for multiple APs
- Best practices for your wireless and wired network
- Goes beyond the basic wireless safety steps
- Can track and log malicious attempts
- You may never know when or how you've been compromised without authentication control AND log analysis
- Latest wireless gear (e.g. Airport Extreme X2) encourage this option (MAC address control is still an option on the X2 under "Timed Access")
- Sysadmins: you can use 802.1x on your managed switches as well for a comprehensive security solution (see next slides)

Managed Switches



Managed Switches: MAC address access control



NETGEAR® FSM726 Managed Switch

Support



Navigation

- System
- [-] Status
- [-] Set-up
- [-] Tools
- [-] Security
 - [-] Advanced
 - Disable Advanced Alert
 - Port Mirroring
 - Port Trunking
 - Virtual Cable Tester
 - [-] Advanced Security
 - System Authentication**
 - Port-Based Authentication
 - Trusted MAC Address
 - MAC Address Lock
 - [-] Advanced Tools
 - [-] Traffic Management
 - [-] VLANs
 - [-] Spanning Tree
 - [-] MAC

Advanced > Advanced Security > System Authentication

User Authentication Mode:

Basic Password Only

RADIUS Server IP Address:

0.0.0.0

RADIUS Shared Secret:

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

IP Filtering is:

Disabled

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

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

Managed Switches: 802.1x access control



NETGEAR® FSM726 Managed Switch

Support



Navigation

- System
- [-] Status
- [-] Set-up
- [-] Tools
- [-] Security
- [-] Advanced
 - Disable Advanced Alert
 - Port Mirroring
 - Port Trunking
 - Virtual Cable Tester
 - [-] Advanced Security
 - System Authentica
 - Port-Based Authen**
 - Trusted MAC Addre
 - MAC Address Lock
 - [-] Advanced Tools
 - [-] Traffic Management
 - [-] VLANs
 - [-] Spanning Tree
 - [-] MAC

Advanced > Advanced Security > Port-Based Authentication

RADIUS Server IP Address:

RADIUS Shared Secret:

802.1x Port-Based Authentication Setting:

The Port-Based Authentication setting enables you to authenticate each port before making available any services offered by the switch. After authentication is successful, normal traffic can pass through the port. The default setting is Force **Authorized** (disabled 802.1x function). The user can also choose Force **Unauthorized** (deny client to access network) or **Auto Detected**. The **Reauthentication Timer** allows the user to specify the time interval between the authentication server's checks of users connected to the network. The default time interval is 3600 seconds. This field will take effect when the Authentication mode is Auto.

Note: The RADIUS server IP address and Shared Secret must be configured first before enabling 802.1x. The 802.1x RADIUS server's connected port must be configured as "**Authorized**" only. Otherwise 802.1x won't take effect.

Re-authentication Timer: (1 - 65535 seconds)

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

Try this yourself


- Go to <http://www.periodiklabs.com> and download a trial version of Elektron
- Setup with an Access point with MAC and 802.1x options
- Test access to wireless network with permitted and blocked clients

Next steps:

- SNMP monitoring using Intermapper and/or Cybergauge will help with your log analysis and system integrity
- Integrate with Snort/HenWen NIDS system for best results
- Other products to check out: IPNetRouter (<http://www.sustworks.com>) and Door Stop Security Suite (<http://www.opendoor.com>)


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)

- Read Me First 2
- Introduction 5
- Wi-Fi Security Quick Start 7
- Determine Your Security Risk 9
- Prevent Access to Your Wireless Network 23
- Secure Your Data in Transit 35
- Protect Your Systems 56
- Secure Small Office Wi-Fi 65
- Perform a Security Audit 79
- Appendix A: Use WPA Enterprise 92
- Appendix B: Password Advice 101
- Glossary 104
- About This Ebook 111

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

\$10

ISBN 0-9759503-9-8
TidBITS Electronic Publishing