Wireless Campus: issues and solutions

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

Wireless campus outline

1. Background: what is a wireless campus, who uses it, and how?
2. Concerns: access and security
3. Case Studies
4. Wireless campus in the age of Leopard
5. Where do we go from here?

Campus Networks: a brief history

- Sneaker net: carry the floppy from one machine to another
- LANs:
  - 10base2 (coax cable)
  - AppleTalk (phone line)
  - 10baseT (Cat 5 cable)
- Wireless LANs
  - 802.11b (11 mb/s)
  - 802.11g (54 mb/s)
  - 802.11n (600 mb/s)
- Hybrid networks: roaming users, ethernet and wireless

Campus Devices

- Terminals (the old days)
- Desktop computers
- laptop computers
- iPhones, hybrid devices

How is the campus network used?

- Admin users:
  - Student Information System (SIS)
  - Business office system
  - Development resources
- School presence:
  - Web pages
  - Online grades
  - SIS portal
  - Student portfolios
  - email in and out

How is the campus network used?

- Faculty users:
  - Online grades
  - Weblogs
  - Online resources/textbooks/course materials
  - Laptop classrooms
- Student users:
  - Student Web pages/portfolios
  - webmail in and out
  - research use, online courses
  - Instant Messaging (where permitted)
  - Data collection (e.g. vernier science probes)

Issues:

- Physical network access
- Network authentication
- User mangement
- Home access to resources
- Content/application filtering
- Legal issues: logging, backups of email, liability

Physical Access: Network Implementation

- Legacy gear
  - Ethernet, usually 10/100 mb/s
  - Some wireless networks, usually bridged (yikes!)
- Newer gear:
  - wired and wireless security and authentication control
  - central authentication servers
  - wireless clouds, allowing roaming
- Issues: coverage and physical access (e.g. can I get a signal?)

Security Issues

packet sniffing example

Capture 1

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

Stop Capture

Packets | Nodes | Protocols | Conversations | Size | Summary | History | Log | Filters

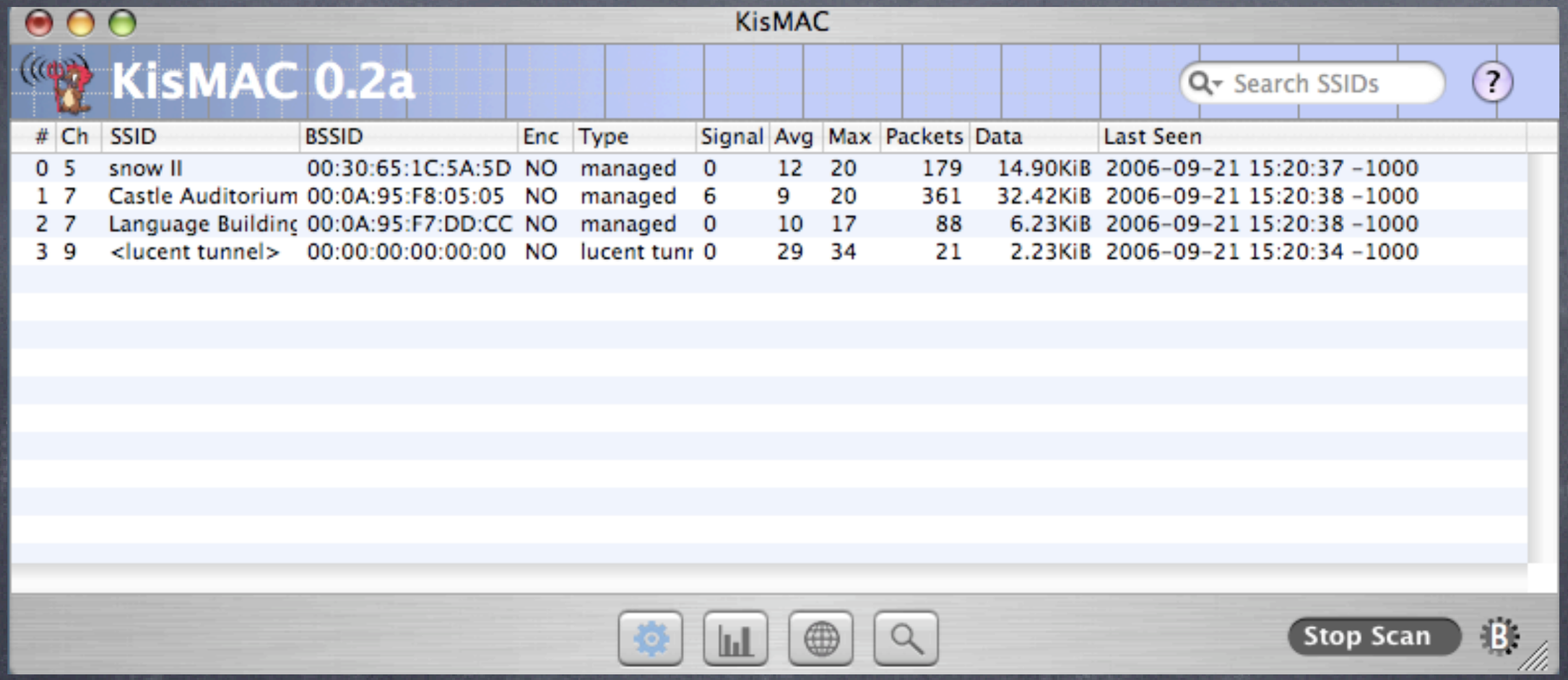
Packet	Source	Destination	Size	Time-Stamp	Protocol	Plug-in Info
415	IP-10.0.1.13	IP-65.167.181.2	81	10:47...99627	TCP POP3	USER nick
416	IP-209.223.121.30	IP-239.255.255.253	95	10:47...40024	IP UDP	
417	IP-209.208.202.130	IP-10.0.1.12	153	10:47...62435	TCP POP3	+OK fmaonline.com runnin...4119676@fmaonline.com>
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...09448	TCP POP3	+OK logged in
424	IP-10.0.1.12	IP-209.208.202.130	64	10:47...12308	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

Kismac wireless scanner

- Able to invisibly scan even closed and protected networks
- Able to crack locked networks
- Able to capture data for later analysis

- Lesson: all traffic on wireless networks is vulnerable
- Solutions:
  - Safer data methods (APOP and SSL)
  - System monitoring
  - Education of users and possible interlopers

KisMAC in passive mode:



#	Ch	SSID	BSSID	Enc	Type	Signal	Avg	Max	Packets	Data	Last Seen
0	5	snow II	00:30:65:1C:5A:5D	NO	managed	0	12	20	179	14.90KiB	2006-09-21 15:20:37 -1000
1	7	Castle Auditorium	00:0A:95:F8:05:05	NO	managed	6	9	20	361	32.42KiB	2006-09-21 15:20:38 -1000
2	7	Language Building	00:0A:95:F7:DD:CC	NO	managed	0	10	17	88	6.23KiB	2006-09-21 15:20:38 -1000
3	9	<lucent tunnel>	00:00:00:00:00:00	NO	lucent tunr	0	29	34	21	2.23KiB	2006-09-21 15:20:34 -1000

note lucent tunnel

KisMAC decode window, with packet and HW info

KisMAC

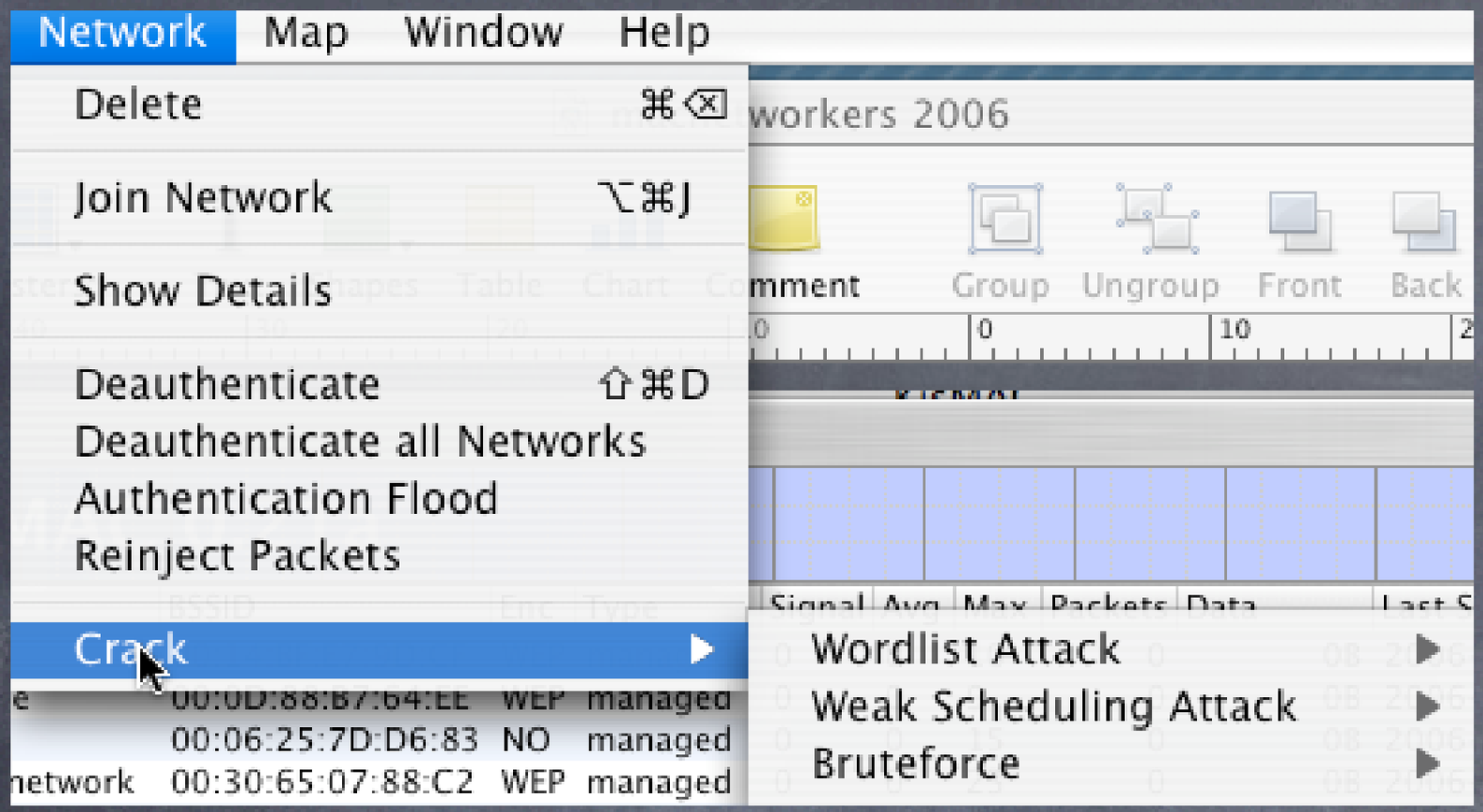
KisMAC 0.2a

Property	Setting
SSID	snow II
BSSID	00:30:65:1C:5A:5D
Vendor	Apple
First Seen	2006-09-21 15:20:17 -1000
Last Seen	2006-09-21 15:20:42 -1000
Channel	4
Main Channel	4
Signal	14
MaxSignal	21
AvgSignal	4

Comment:

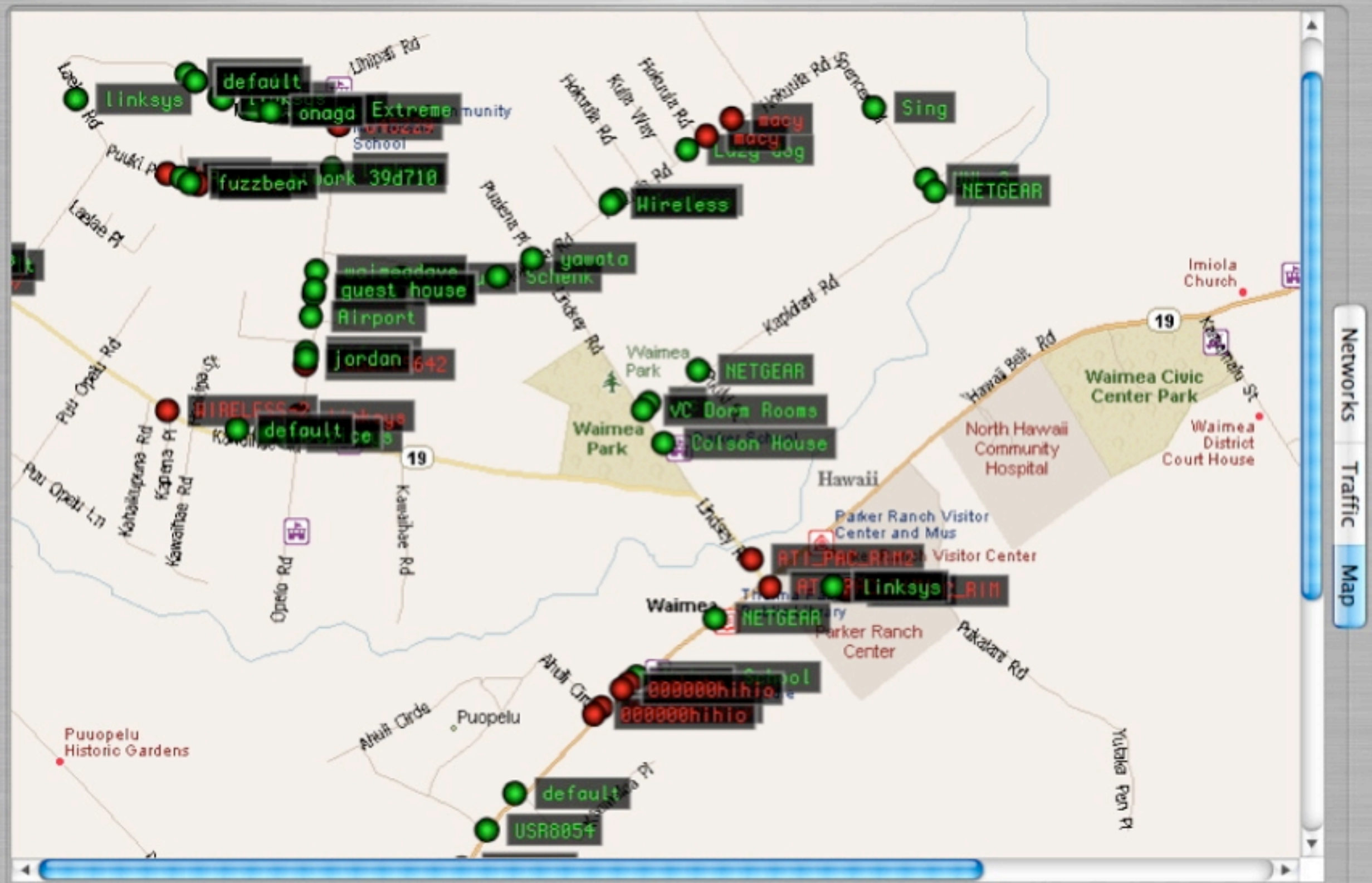
Client	Vendor	Signal	sent Bytes	recv. Bytes	Last Seen
FF:FF:FF:FF:FF:FF	Broadcast	0	0B	16.13KiB	
00:0A:95:7B:F9:F	Apple	8	10.74KiB	0B	2006-09-21 15:2(
00:30:65:1C:5A:!	Apple	14	2.72KiB	0B	2006-09-21 15:2(
00:0A:95:E1:27:E	Apple	17	460B	0B	2006-09-21 15:2(
00:50:E4:10:4C:3	Apple	8	161B	0B	2006-09-21 15:2(
00:14:51:0B:04:5	unknown	3	165B	0B	2006-09-21 15:2(
09:00:07:FF:FF:FI	EtherTalk-	0	0B	59B	
00:17:F2:3F:82:C	unknown	3	59B	0B	2006-09-21 15:2(
01:80:C2:00:00:(	BPDU-mult	0	0B	124B	
00:D0:58:69:86:(	unknown	11	124B	0B	2006-09-21 15:2(
01:00:5E:00:00:F	multicast	0	0B	1.36KiB	
00:0D:93:9B:BA:(	Apple Com	8	621B	0B	2006-09-21 15:2(
00:30:65:37:1A:(	Apple	12	78B	0B	2006-09-21 15:2(
00:0D:93:7D:F4:I	Apple Com	19	0.85KiB	0B	2006-09-21 15:2(
01:00:5E:7F:FF:FI	multicast	0	0B	109B	

Start Scan



<--The truly scary stuff

KisMAC - 0.10a



Last Position 20.028984N, 155.697693W, Elevation: 798.900024m @ 2004-04-26 17:44:03 -1000

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:

- 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 (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

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)

Wireless campus case studies

- Small campus
- Medium campus
- Large campus
- District

Wireless campus case studies

- Small campus
  - usually little or no IT staff
  - still need access to email, web, some faculty services
  - security awareness is often low
  - good points:
    - small number of users, often well known
    - smaller campus, easier to control
- Solutions:
  - Webmail offsite, Powerschool type SIS, vendor email

Wireless campus case studies

- Medium campus
  - IT staff has limited budget, training, access to shared resources
  - access to email, web, some faculty services expected by faculty and parents
  - security awareness is still often low, though they often have first hand experience of compromised integrity
  - good points:
    - limited number of users, often well known
    - smaller campus, easier to control
    - often skilled faculty can help with education/shared mentoring
- Solutions:
  - local servers, local admin and monitoring
  - comprehensive user authentication/access control

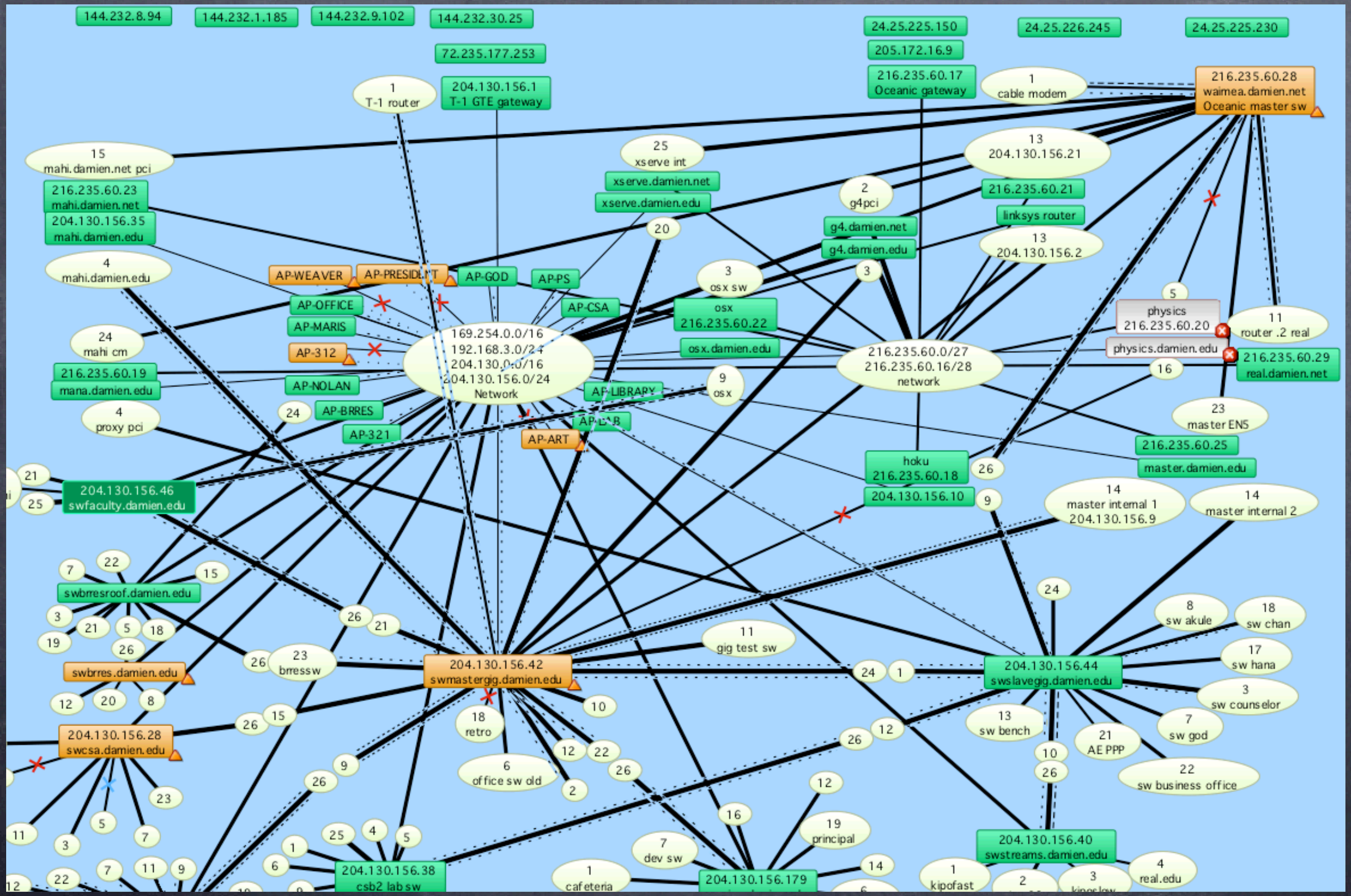
Wireless campus case studies

- Large campus
  - IT staff has larger budget, training, access to shared resources
  - access to email, web, some faculty services expected by faculty and parents, along with SIS online
  - security awareness is still limited, may be cultural or unique to the school population
  - good points:
    - better trained, dedicated IT staff
    - greater resources for monitoring, not just keeping things running with minimal resources
    - often skilled faculty can help with education/shared mentoring
    - often attend conferences to learn how to do better (;-)
- Solutions:
  - multiple servers for redundancy
  - Open Directory for portable folders/server access
  - Some home access to resources via web servers, VPN for faculty/staff

Wireless campus case studies

- Districts
  - IT staff has larger budget, training, access to shared resources, often aggregate servers, resources
  - access to email, web, some faculty services expected by faculty and parents, along with SIS online
  - security awareness is still limited, may be cultural or unique to the school population
  - good points:
    - better trained, dedicated IT staff
    - greater resources for monitoring, not just keeping things running with minimal resources
    - resources may be off-site which cuts both ways
    - often skilled faculty can help with education/shared mentoring
    - often attend conferences to learn how to do better (;-)
- Solutions:
  - Enterprise level management and monitoring, server farms, ISP like services for parents, students, faculty and staff

Wireless campus: network monitoring



Wireless campus: Network Monitoring

- Need not be a large school to use essential tools
- SNMP management is critical at even the smallest contact with the public or even more critical: devious, smart students with resources, time, and great collaborative skills
- Access control is just a start: logging and tracking are critical pieces of the solution
- Disaster recovery is better thought out before it is needed
- This subject is critical and often poorly understood or appreciated: we take safe highways for granted and expect the same sort of safety (and adherence to the rules of the road) on our networks, but this is seldom the case.

Wireless campus: The Leopard Era

- Clients:
  - screen sharing allows classroom use, admin use
  - time machine backups can recover lost data
  - Open Directory with portable logins means students always see the same desktop from any machine on campus
  - Great wireless security with 802.1x and WPA2 built in

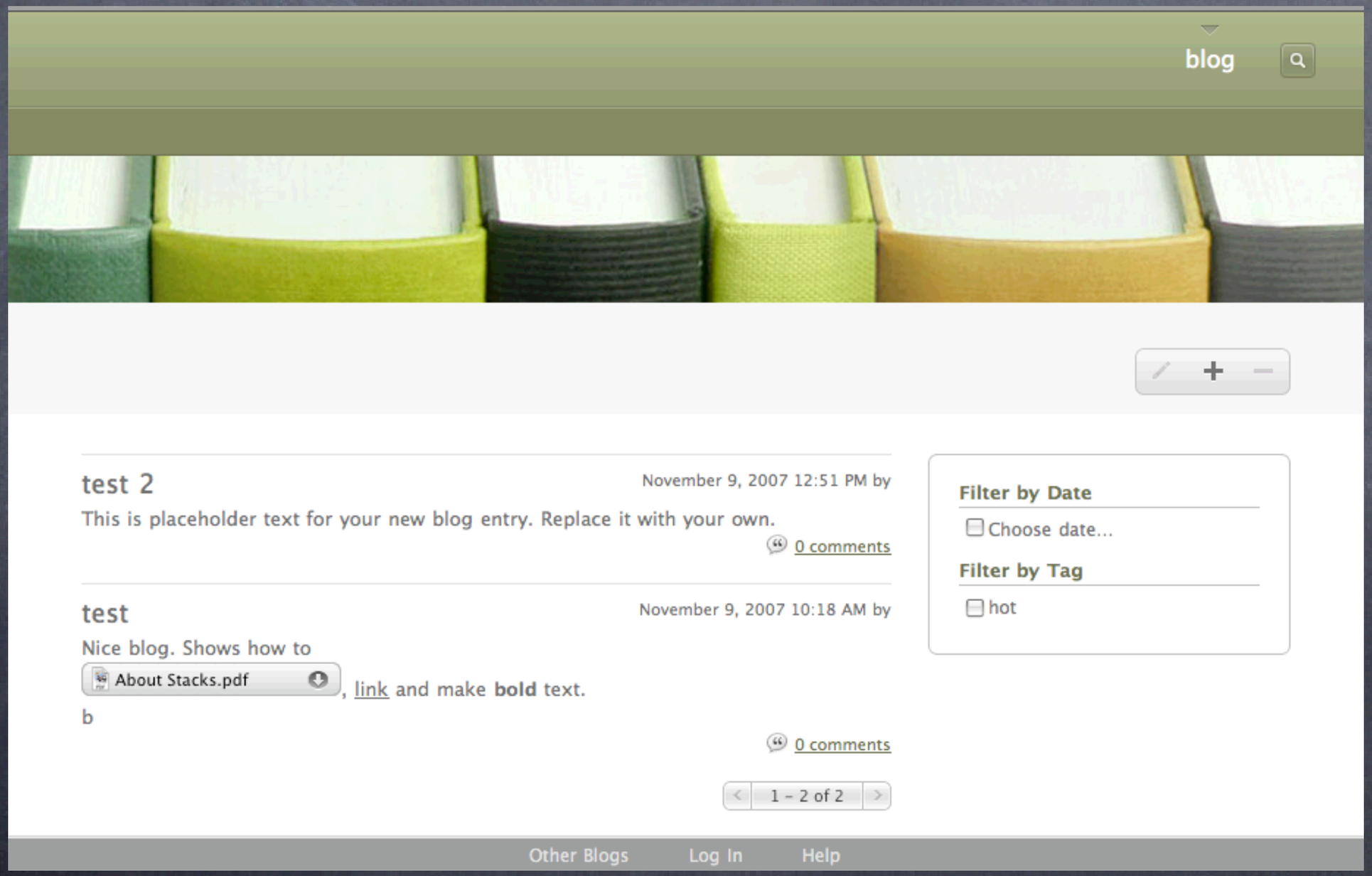
Wireless campus: The Leopard Era

- Server:
  - Weblogs and Wikis now truly professional looking
  - iChat Server allows for Video Teleconferencing intramural and extramural (mura means wall in latin)
  - iCal server: school schedule on laptops, iPhones, any webDAV calendaring device
  - Home page streaming: allows streaming of lectures, projects, interviews
  - Podcast Producer: allows for real time production of lecture archives from any ichat camera (e.g. laptop)
  - Webmail: great access, built-in spam and virus filters
  - Software update server: update all local machines from one server
  - Web server: supports Ruby and other new protocols
  - VPN server: allows safe connection from home/wireless access
  - about 20 other cool things you can use to improve how we educate our students

weblogs

Weblogs: Leopard Server

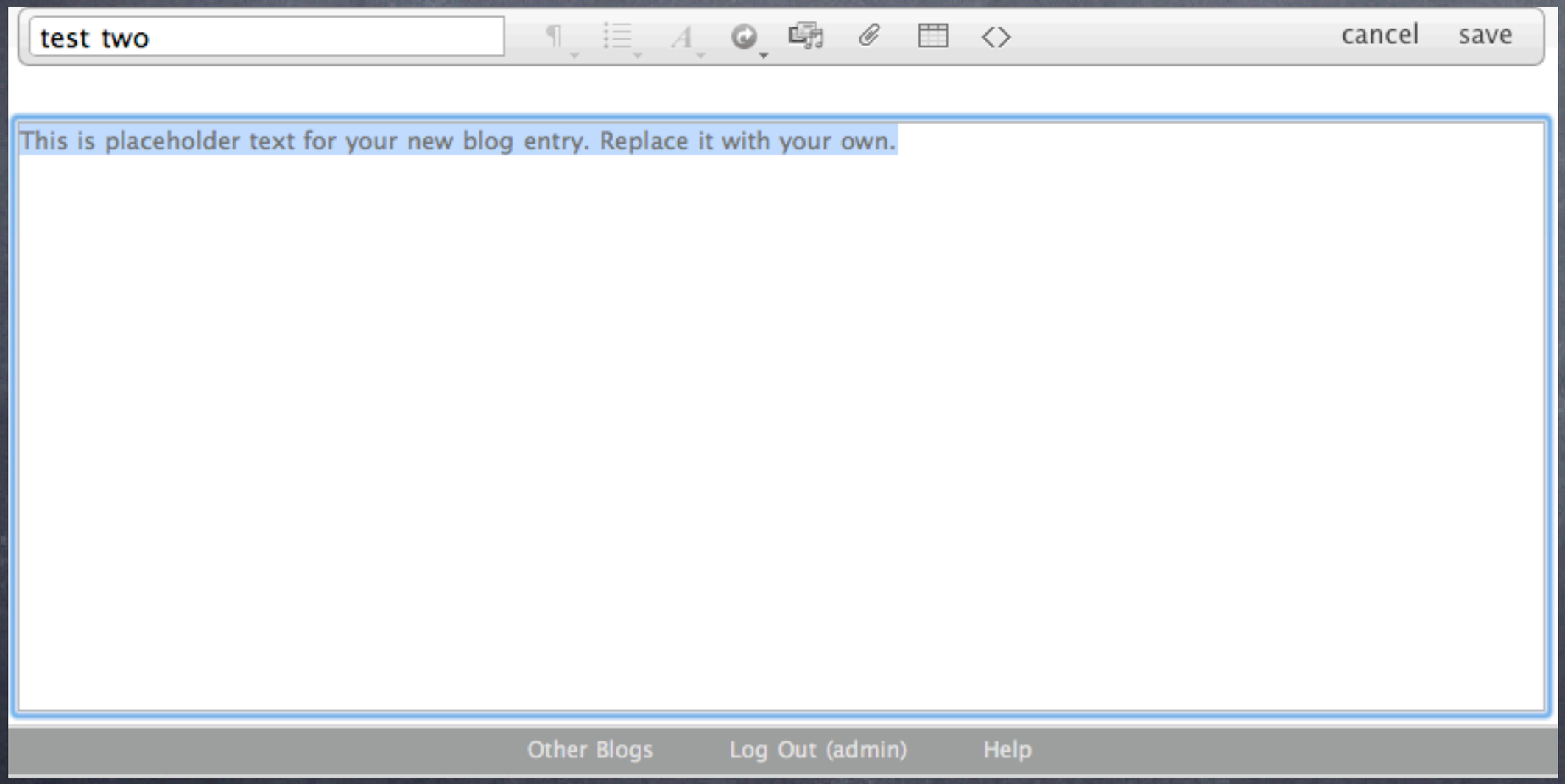
- Extension of the Blojsom open source weblog system



weblogs

Weblogs: Leopard Server

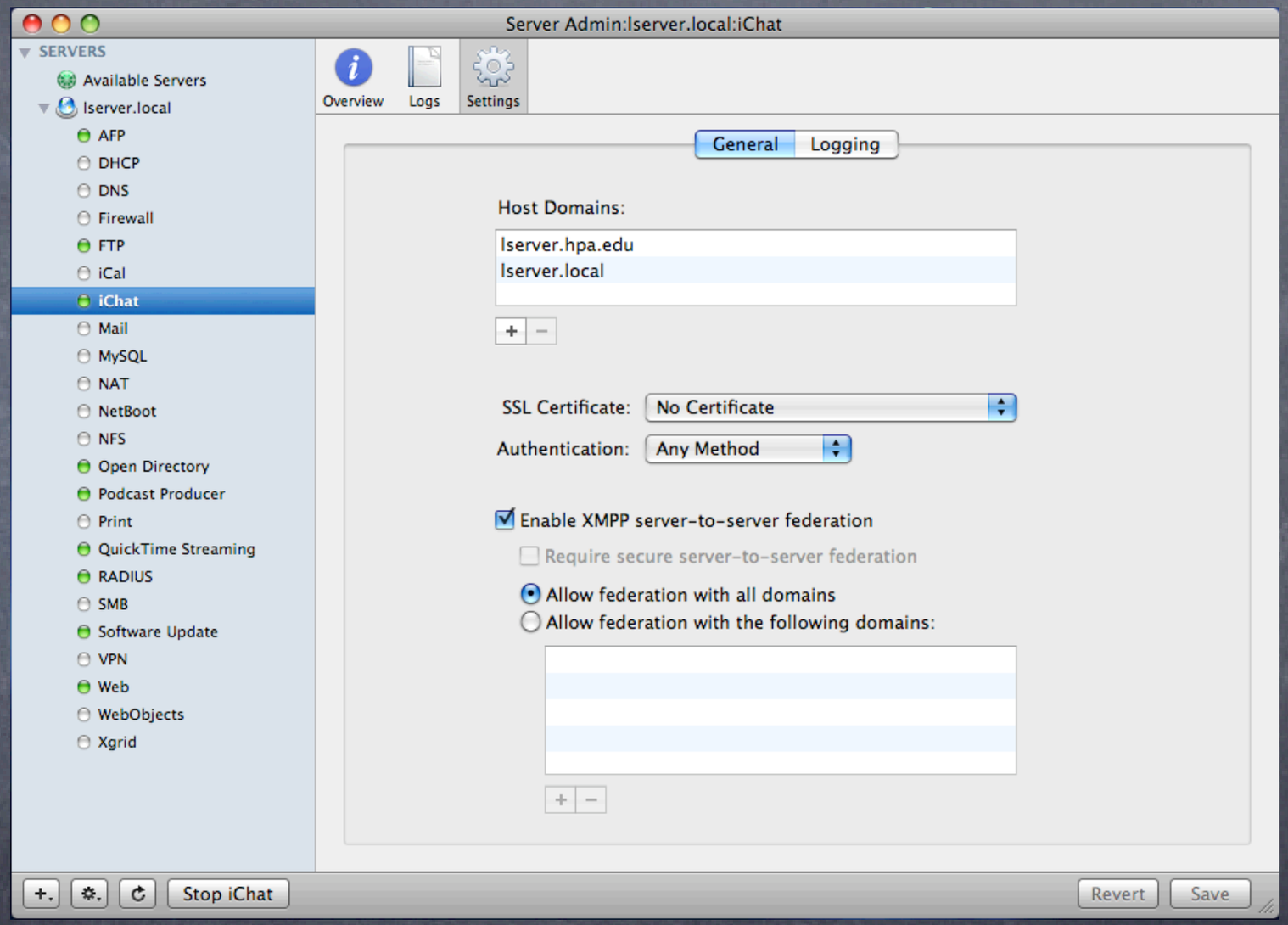
- Many more options under Leopard: attachments, fonts, media, urls, html view, tables, bullets, outlines.



iChatAV server

iChatAV jabber server

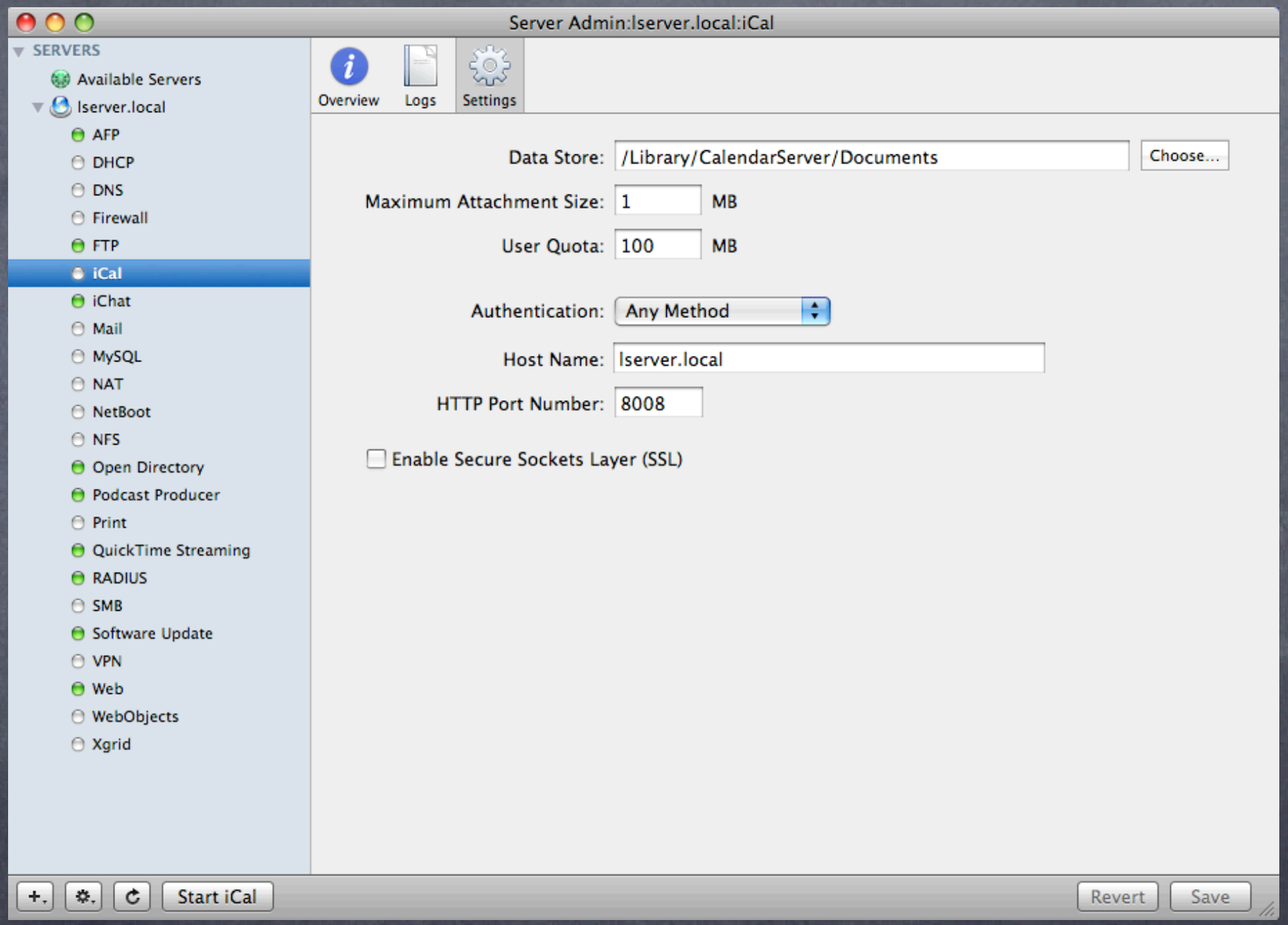
- Hosts jabber users internal and external
- Use VPN for outside clients to share
- Logging utilities can log chats, conferences for future archives



iCal server

iCal Webcal server

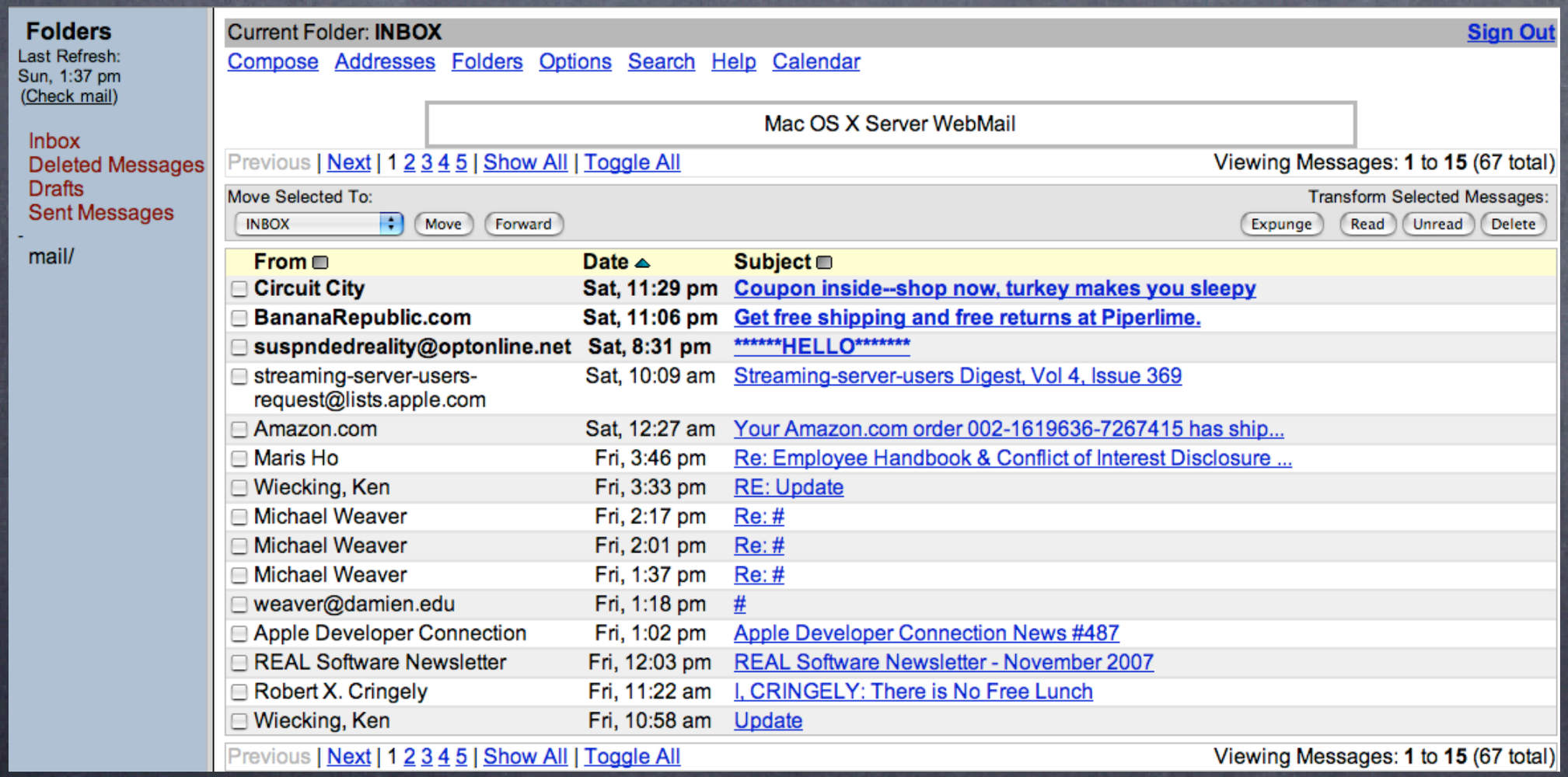
- works with any webdav calendaring system
- Format: webcal://ical.mac.com/hawaiiprep/daily.ics
- If no Leopard server, this can be done on any webDAV server (see Tenon documents)



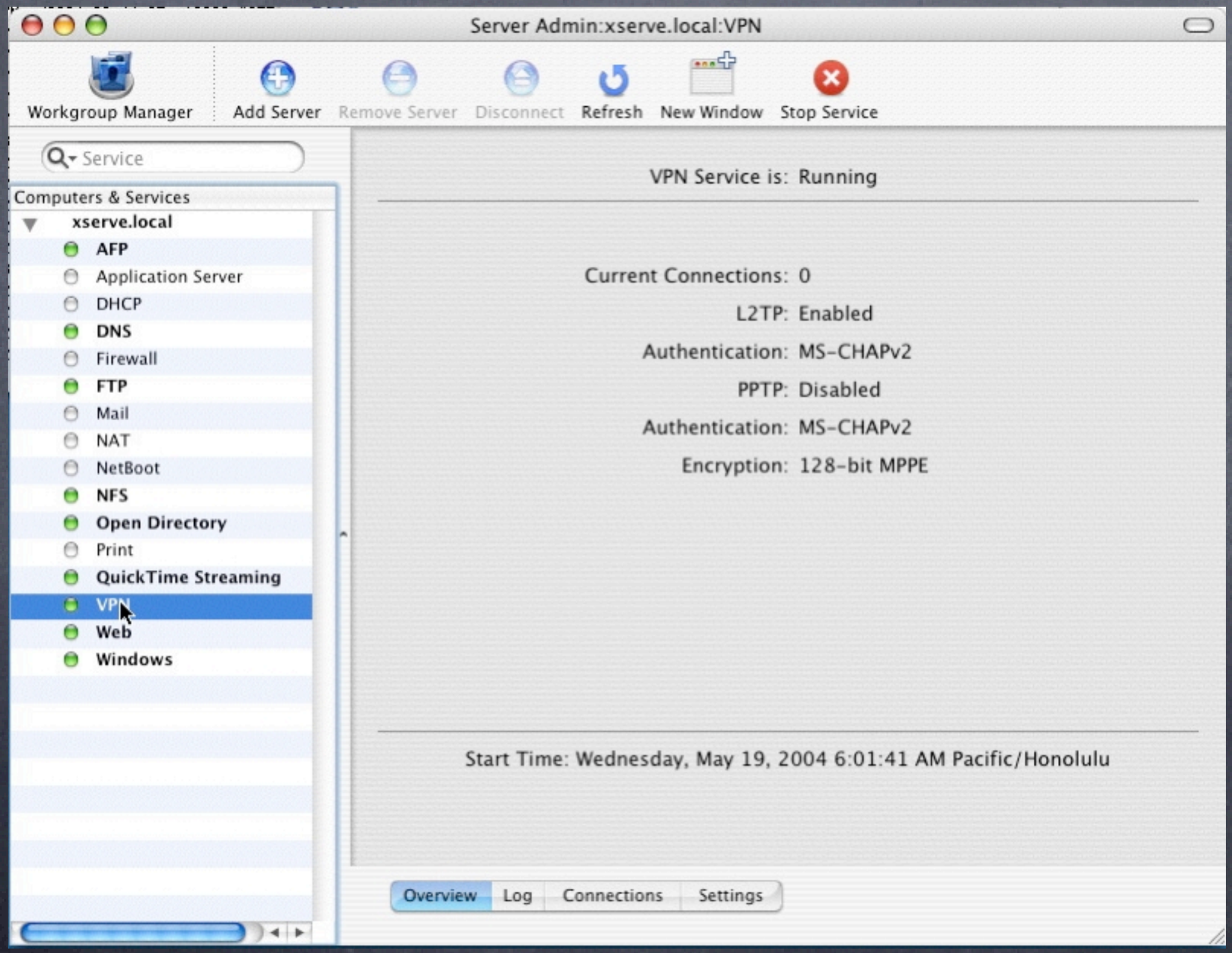
Webmail

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



VPN: Part of Panther/Tiger/Leopard server



Wireless campus: Where do we go from here?

- SIS online (e.g. PowerSchool)
- Laptop classrooms (carts, personal laptops)
- Online courses (see http://www.kineticbooks.com)
- iPhone integration: calendar, lectures (see iTunesU)
- Greater, more professional interaction between colleagues and students
- Professional development: online screen sharing/help, recorded solutions
- Podcasts of lectures (see also CSUMB intellectual property tussle)