Mac OS X Server

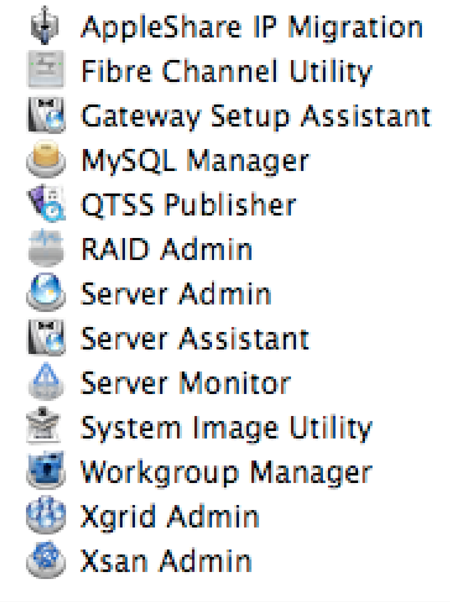
LayerOne

PRESENTED BY:Charles Edge

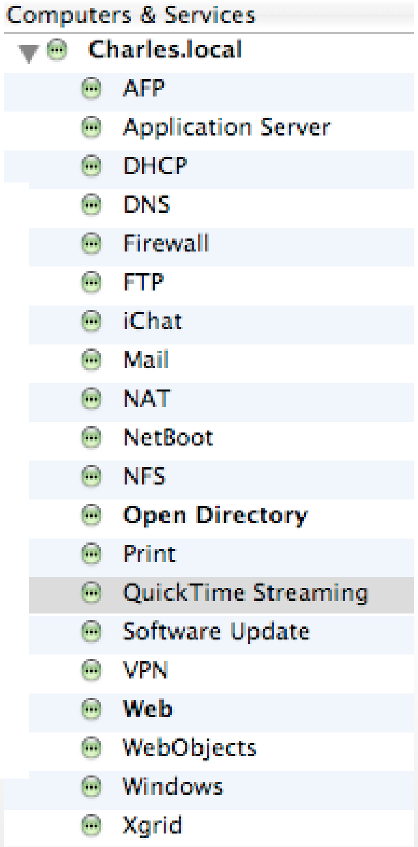
Mac OS X Server

Open Source Made Easy

- The Mac is now a typical *nix distro
- Users that require an easy solution often do not have the skills to secure their solution
- End users resistant to basic security concepts



AppleShare IP Migration
Fibre Channel Utility
Gateway Setup Assistant
MySQL Manager
QTSS Publisher
RAID Admin
Server Admin
Server Assistant
Server Monitor
System Image Utility
Workgroup Manager
Xgrid Admin
Xsan Admin



Computers & Services

- Charles.local
  - AFP
  - Application Server
  - DHCP
  - DNS
  - Firewall
  - FTP
  - iChat
  - Mail
  - NAT
  - NetBoot
  - NFS
  - Open Directory
  - Print
  - QuickTime Streaming
  - Software Update
  - VPN
  - Web
  - WebObjects
  - Windows
  - Xgrid

Mac Specifics

Well, mostly Open Source...

- Many conf files are replaced with plists
- NetInfo
- File System is usually Mac OS Extended, but NTFS and UFS are also supported
- All of the files and apps are in the wrong place
- Servermgr
- GUI tools for everything – www.versiontracker.com

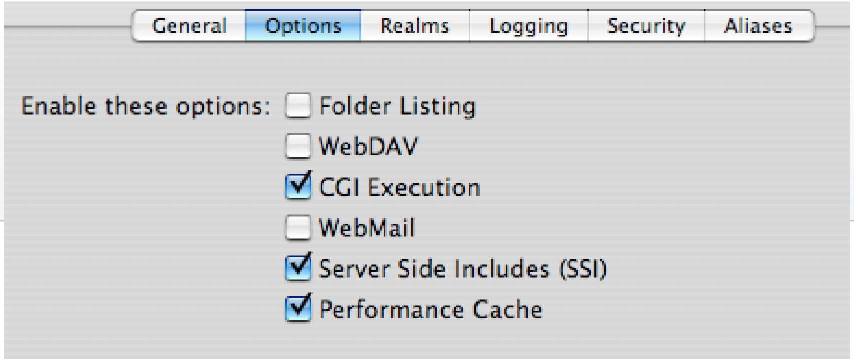
AFP

Apple Filing Protocol

- AppleTalk is a thing of the past
- AFP runs over port 548 and is an easy way to find Mac servers
- AFP had a known vulnerability for 10.3 that gave root and is included in Metasploit
- AFP still has similar vulnerabilities
- AFP can work over SSH for maximum security

Apache

Mods R Us



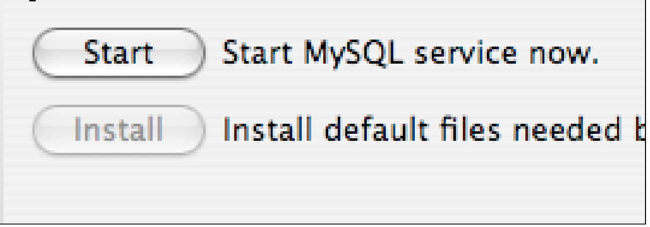
Enable these options:
- □ Folder Listing
- □ WebDAV
- ☑ CGI Execution
- □ WebMail
- ☑ Server Side Includes (SSI)
- ☑ Performance Cache

- Apache 1.3.33
- SSI, PHP, Perl, Tomcat, Ruby can be enabled by clicking a checkbox
- And users do check those boxes, which is dangerous if they have no idea what they’re doing
- I have picked up about 30 new clients from servers turned into phishing boxes
- Many users enable the proxy with no auth on wide open boxes

MySQL

MAMP?

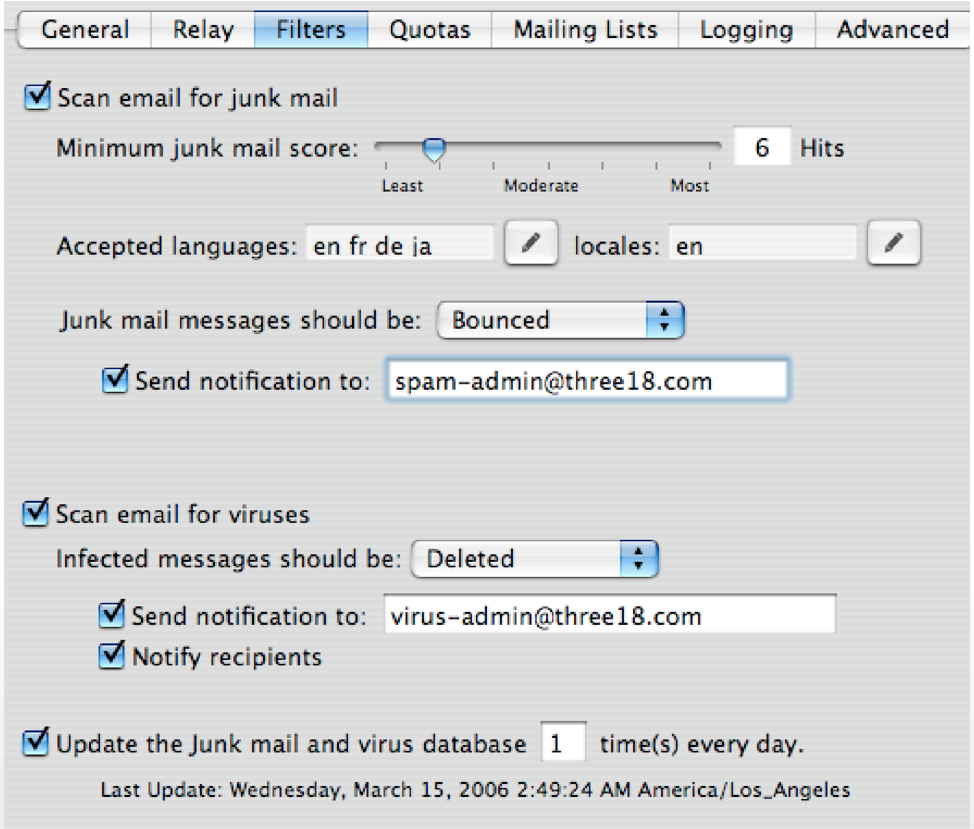
- Distrib 4.1.13a
- Every client I’ve worked on so far that uses MySQL on Mac servers also uses phpMyAdmin
- Only one out of maybe 50 bothered to require auth to access phpMyAdmin
- Every client allowed network connections to MySQL when only maybe 2 actually needed to
- One client used root as the root password for MySQL



Mail Services

Postfix never looked so easy

- Integrated with SASL
- SpamAssassin and ClamAV are built in
- MailMan services available with a click
- Automatically update virus and spam databases



☑ Scan email for junk mail

Minimum junk mail score: 6 Hits

Accepted languages: en fr de ja   locales: en

Junk mail messages should be: Bounced

☑ Send notification to: spam-admin@three18.com

☑ Scan email for viruses

Infected messages should be: Deleted

☑ Send notification to: virus-admin@three18.com

☑ Notify recipients

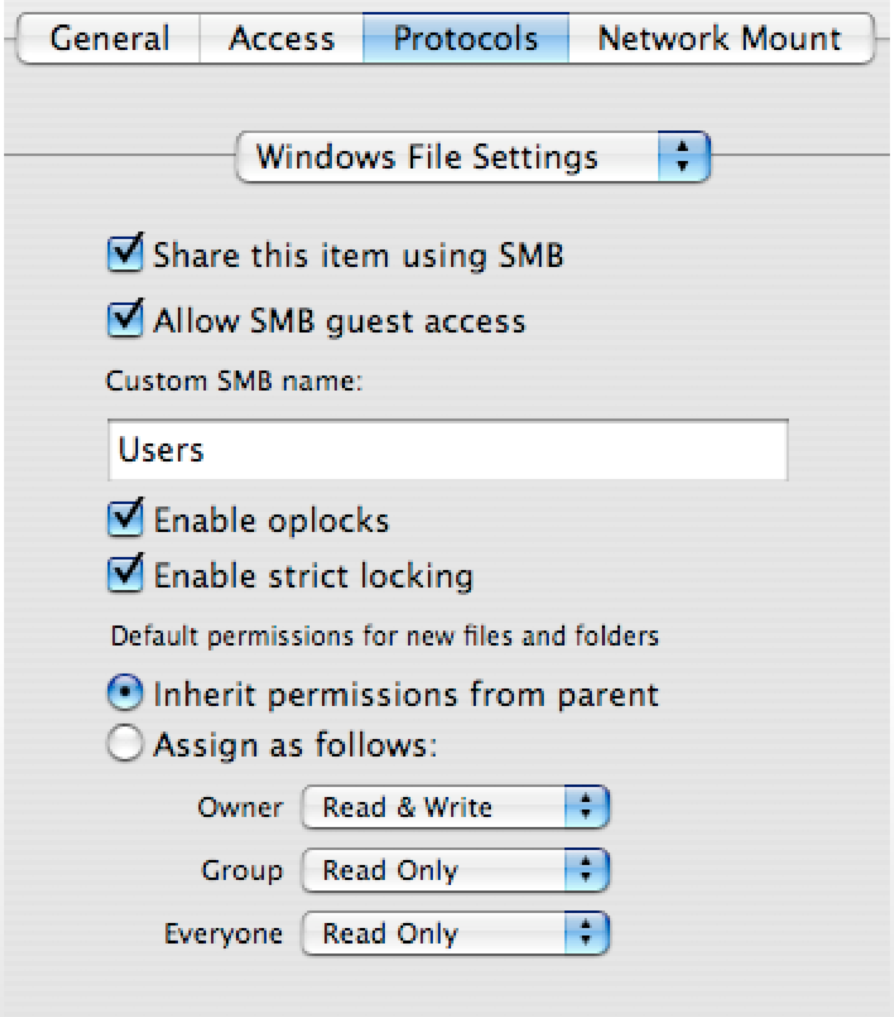
☑ Update the Junk mail and virus database 1 time(s) every day.

Last Update: Wednesday, March 15, 2006 2:49:24 AM America/Los_Angeles

Samba

SMB/CIFS Sharing

- Version 3.0.10
- SMB Signing not supported
- Allow SMB Guest, FTP Guest and AFP Guest access enabled by default for each sharepoint and rarely changed



☑ Share this item using SMB

☑ Allow SMB guest access

Custom SMB name:

Users

☑ Enable oplocks

☑ Enable strict locking

Default permissions for new files and folders

● Inherit permissions from parent

○ Assign as follows:

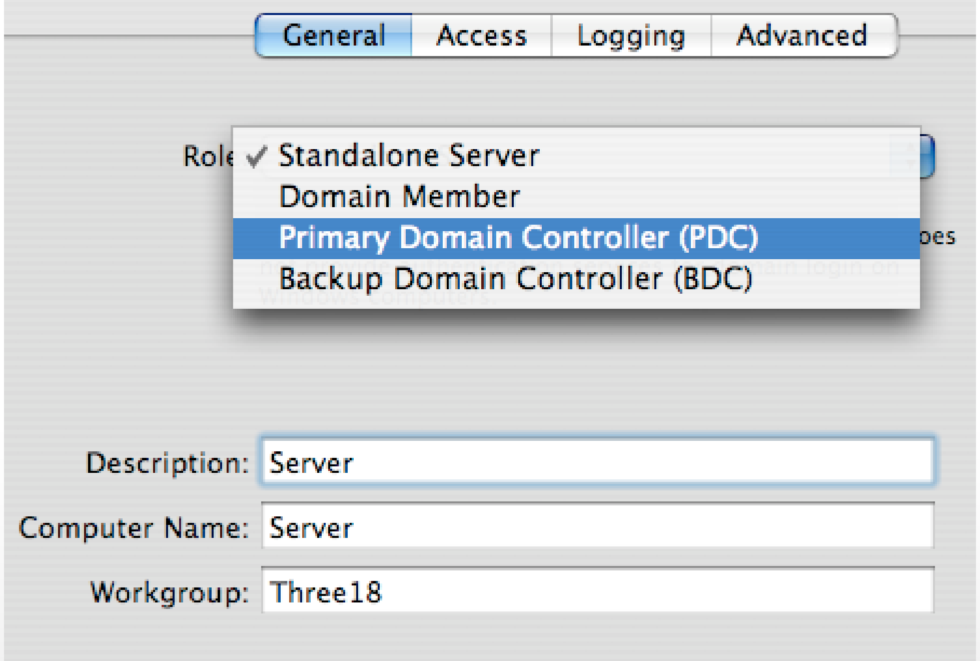
Owner	Read & Write
Group	Read Only
Everyone	Read Only

318.COM

Samba

Authentication Methods

- NTLMv2, NTLM, LAN Manager enabled by defualt
- Low logging by default
- Virtual Shares enabled by default
- Workgroup Master Browser enabled by default



Description: Server

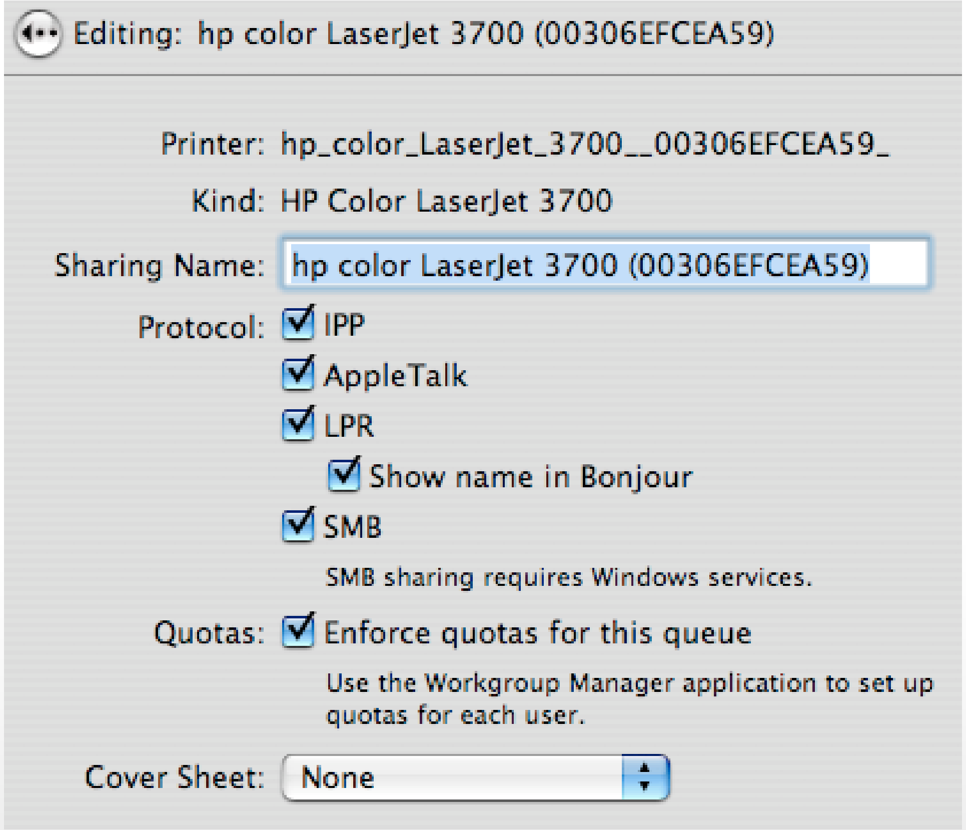
Computer Name: Server

Workgroup: Three18

Print Server

cupsd

- Cups version 1.47.2.1
- By default cupsd listens on all adapters
- Printers can be shared over any protocol



Editing: hp color LaserJet 3700 (00306EFCEA59)

Printer: hp_color_LaserJet_3700__00306EFCEA59_

Kind: HP Color LaserJet 3700

Sharing Name: hp color LaserJet 3700 (00306EFCEA59)

Protocol: ☑ IPP

☑ AppleTalk

☑ LPR

☑ Show name in Bonjour

☑ SMB

SMB sharing requires Windows services.

Quotas: ☑ Enforce quotas for this queue

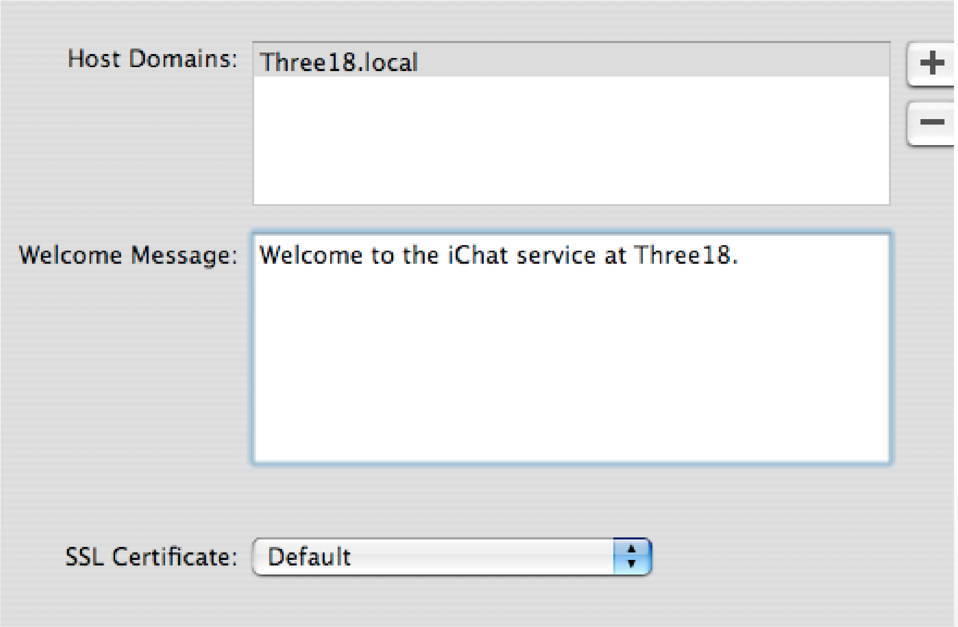
Use the Workgroup Manager application to set up quotas for each user.

Cover Sheet: None

iChat Server

Jabberd

- Jabberd Version 1.4.3.1
- Integrated with SSL
- Known connection handling vulnerability
- No encryption support unless using Fire as Jabber client



Host Domains: Three18.local

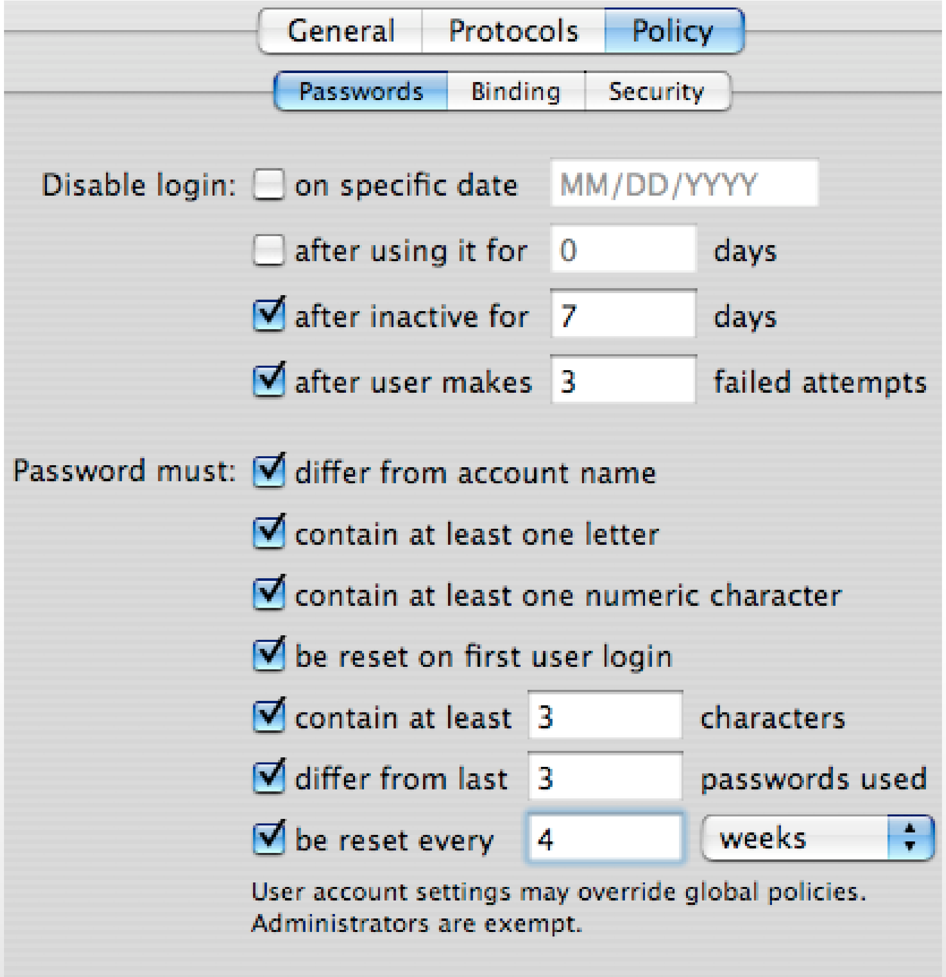
Welcome Message: Welcome to the iChat service at Three18.

SSL Certificate: Default

Open Directory

LDAP and then some

- OpenLDAP 2.2.19, SASL2, Kerberos and other Directory Service Standards incorporated as Open Directory
- All usernames and password in netinfo
- All policies disabled by default



Disable login: ☐ on specific date MM/DD/YYYY

☐ after using it for 0 days

☑ after inactive for 7 days

☑ after user makes 3 failed attempts

Password must: ☑ differ from account name

☑ contain at least one letter

☑ contain at least one numeric character

☑ be reset on first user login

☑ contain at least 3 characters

☑ differ from last 3 passwords used

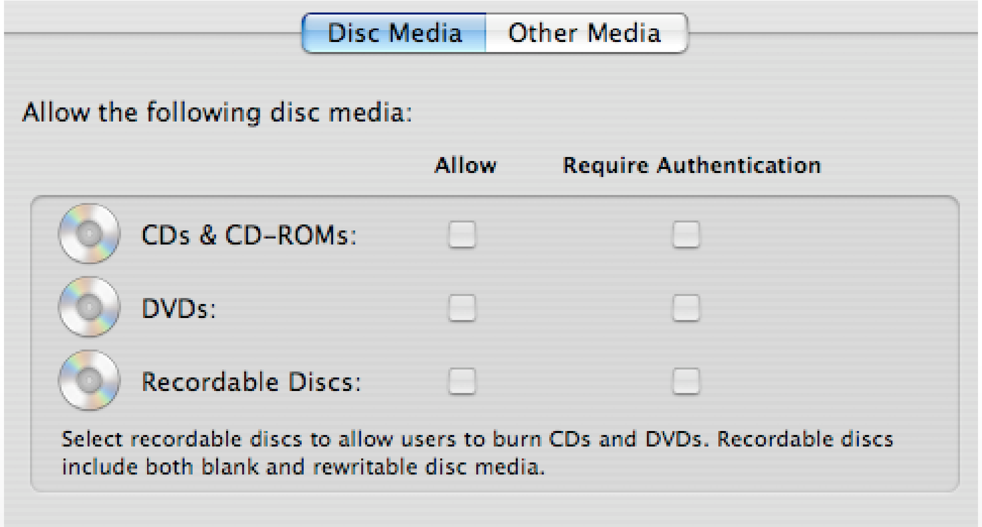
☑ be reset every 4 weeks

User account settings may override global policies.
Administrators are exempt.

Client Management

Centralized Lock Down – Mac Clients Only

- Open Directory can control local access for Mac clients
- This includes disks, applications, prefs, printers, software updates and appearances
- Settings can be assigned to groups, computers and users



Allow the following disc media:

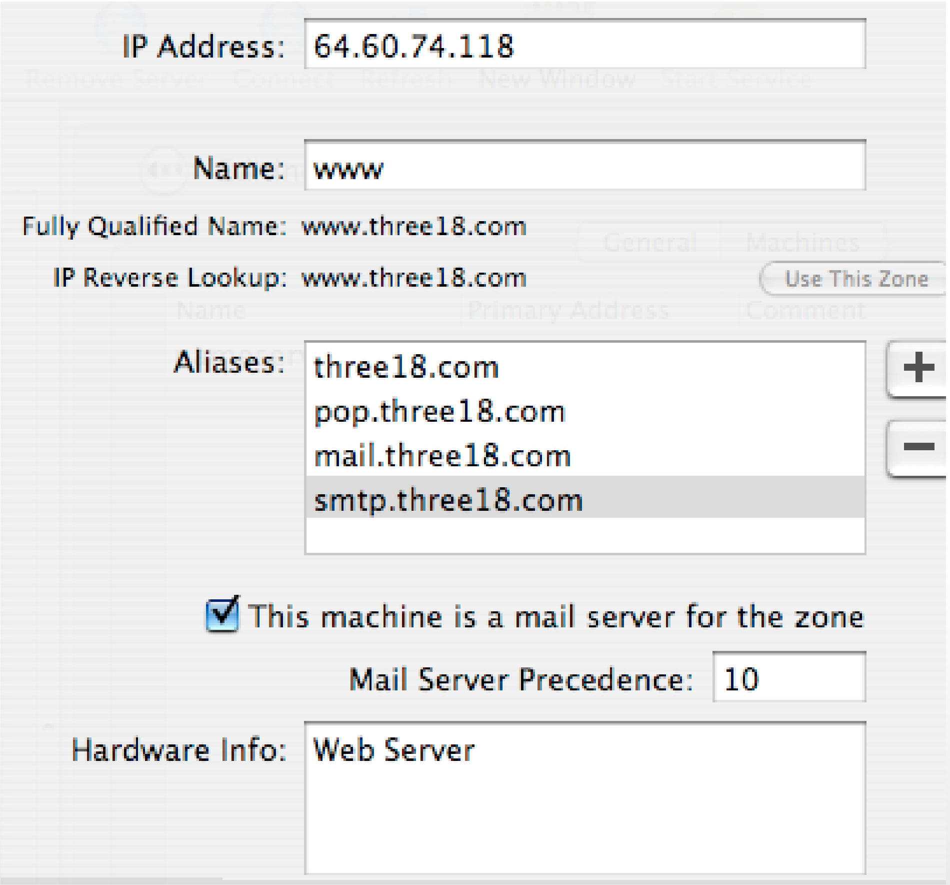
	Allow	Require Authentication
CDs & CD-ROMs:	□	□
DVDs:	□	□
Recordable Discs:	□	□

Select recordable discs to allow users to burn CDs and DVDs. Recordable discs include both blank and rewritable disc media.

DNS

Looking at DNS from the perspective of the IP

- BIND 9.2.2
- Tiger Server represents a change in the way that Apple views DNS – IPs get names, names don't get IPs
- Known DoS exploit



IP Address: 64.60.74.118

Name: www

Fully Qualified Name: www.three18.com

IP Reverse Lookup: www.three18.com

Aliases: three18.com
pop.three18.com
mail.three18.com
smtp.three18.com

☑ This machine is a mail server for the zone

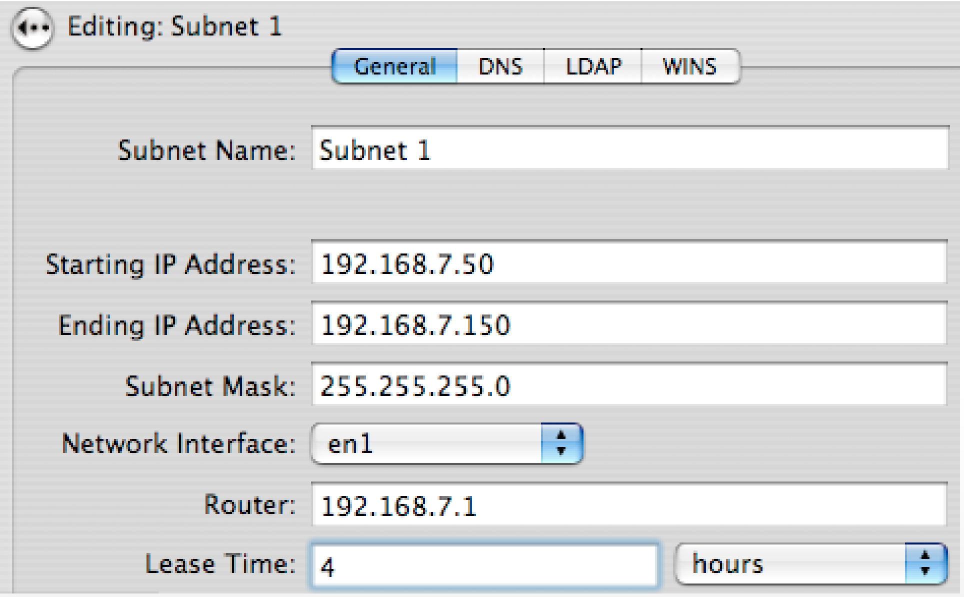
Mail Server Precedence: 10

Hardware Info: Web Server

DHCP

DHCP made easy

- LDAP settings can be deployed dynamically, giving a map of the network
- Clients can be bound to LDAP dynamically
- Dynamic LDAP updates can use SSL



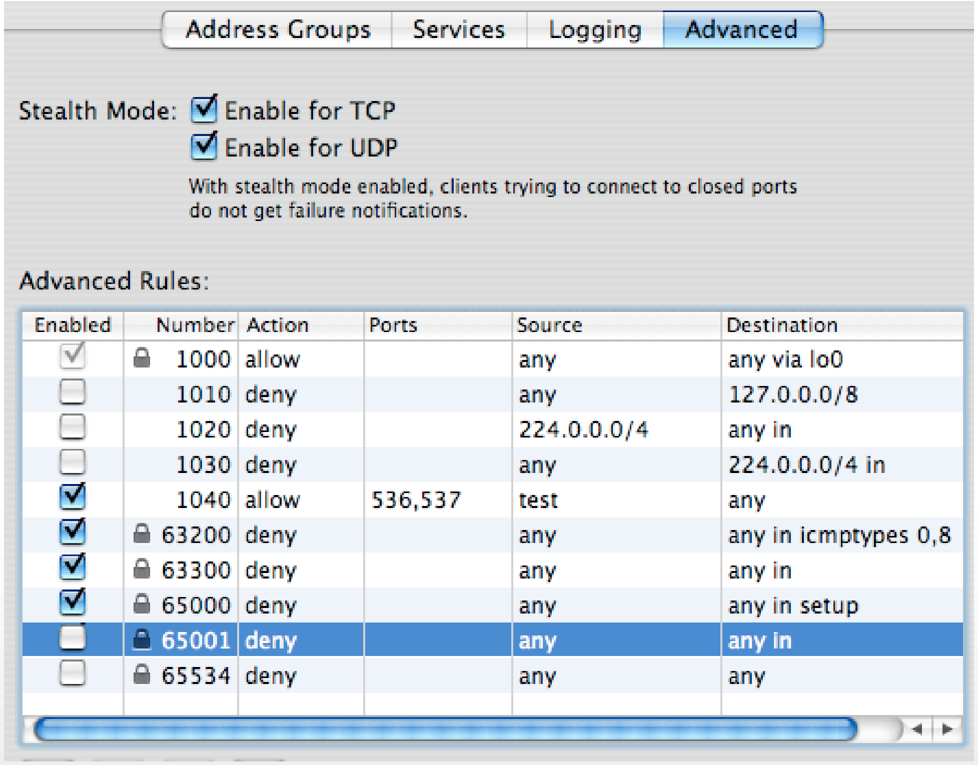
Editing: Subnet 1

Subnet Name:	Subnet 1
Starting IP Address:	192.168.7.50
Ending IP Address:	192.168.7.150
Subnet Mask:	255.255.255.0
Network Interface:	en1
Router:	192.168.7.1
Lease Time:	4 hours

Firewall and NAT

We don’t need no stinkin’ ipchains – or do we?

- IPFW instead of ipchains
- Dummynet can be used to shape traffic
- s2svpnadmin can be used to built site-to-site VPNs but it’s new and pretty much sucks
- natd-Darwin specific



Stealth Mode: ☑ Enable for TCP
☑ Enable for UDP

With stealth mode enabled, clients trying to connect to closed ports do not get failure notifications.

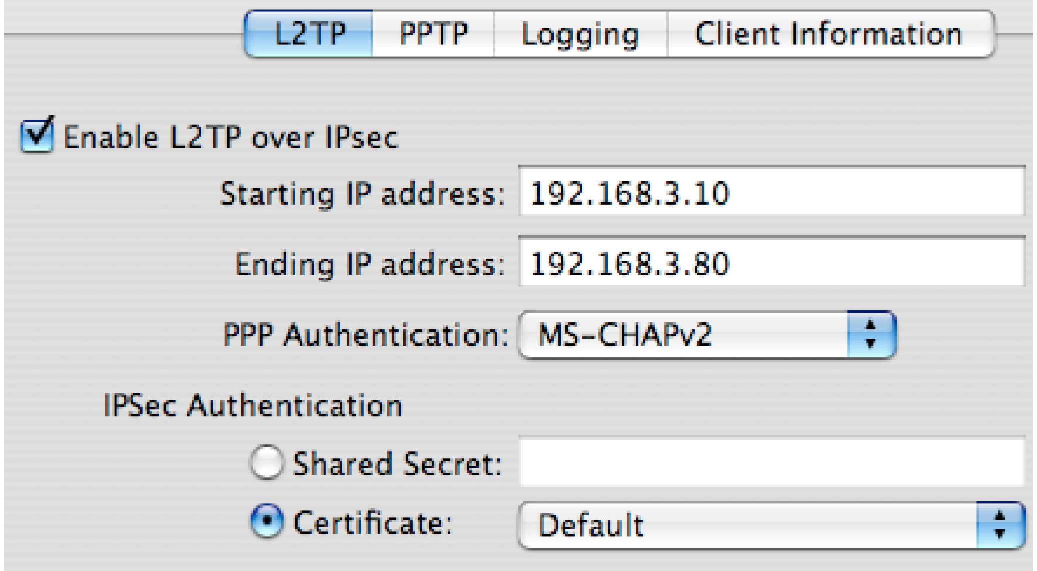
Advanced Rules:

Enabled	Number	Action	Ports	Source	Destination
☑	🔒 1000	allow		any	any via lo0
□	1010	deny		any	127.0.0.0/8
□	1020	deny		224.0.0.0/4	any in
□	1030	deny		any	224.0.0.0/4 in
☑	1040	allow	536,537	test	any
☑	🔒 63200	deny		any	any in icmptypes 0,8
☑	🔒 63300	deny		any	any in
☑	🔒 65000	deny		any	any in setup
□	🔒 65001	deny		any	any in
□	🔒 65534	deny		any	any

VPN

vpnd

- vpnd written by Apple for OS X
- openvpn available from darwinports
- s2svpn allows admins to configure site based VPNs using an interactive command mode



☑ Enable L2TP over IPsec

Starting IP address: 192.168.3.10

Ending IP address: 192.168.3.80

PPP Authentication: MS-CHAPv2

IPSec Authentication

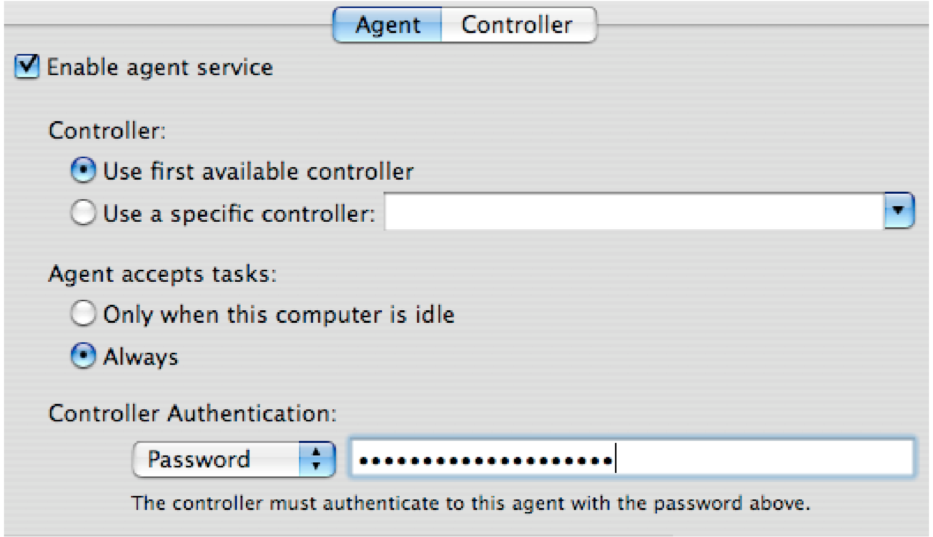
○ Shared Secret:

● Certificate: Default

FTP

TNFTP

- TNFTP is the ftp implementation within OS X Server 10.5
- TNFTP requires FTP users to have a shell and be listed in ftpusers
- Apple has integrated the ftpusers file into NetInfo



☑ Enable agent service

Controller:

● Use first available controller

○ Use a specific controller:

Agent accepts tasks:

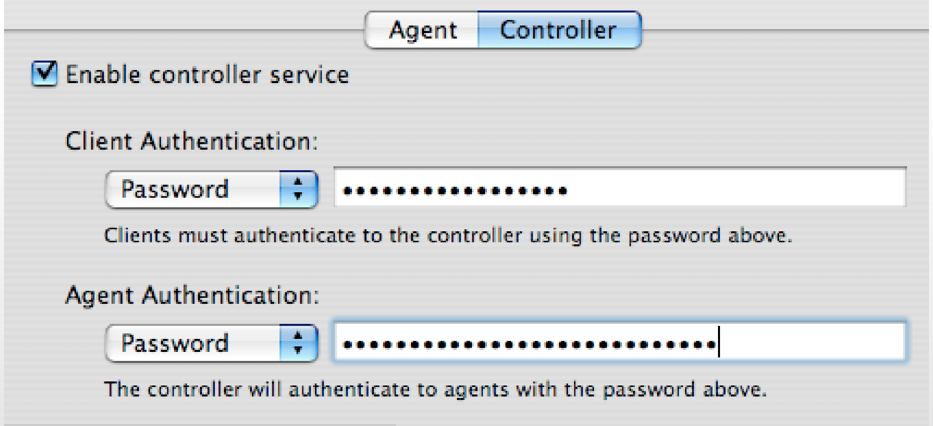
○ Only when this computer is idle

● Always

Controller Authentication:

Password ••••••••••••••••••••

The controller must authenticate to this agent with the password above.



☑ Enable controller service

Client Authentication:

Password •••••••••••••••••

Clients must authenticate to the controller using the password above.

Agent Authentication:

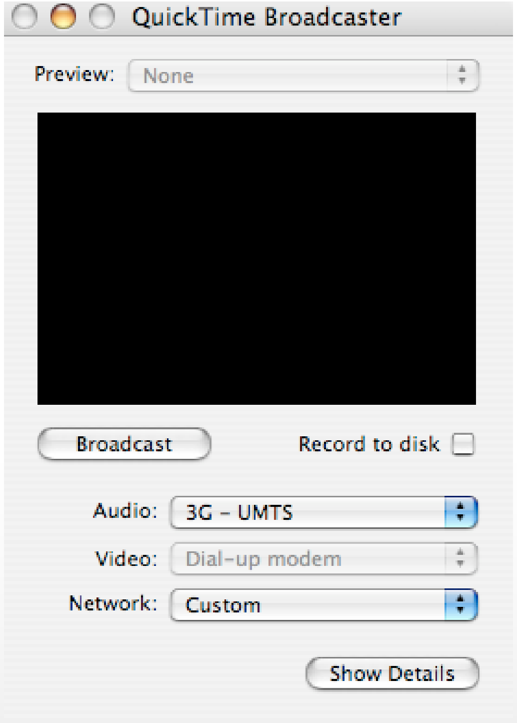
Password •••••••••••••••••••••••••••••

The controller will authenticate to agents with the password above.

QuickTime Streaming

Simple radio = simple snooping

- QuickTime Broadcaster and Streaming
- Heap overflow for rtsp could allow remote code execution
- Relay communications sent in clear text
- QTSS and QTSP need to be further investigated



QuickTime Broadcaster

Preview: None

Record to disk □

Audio: 3G - UMTS

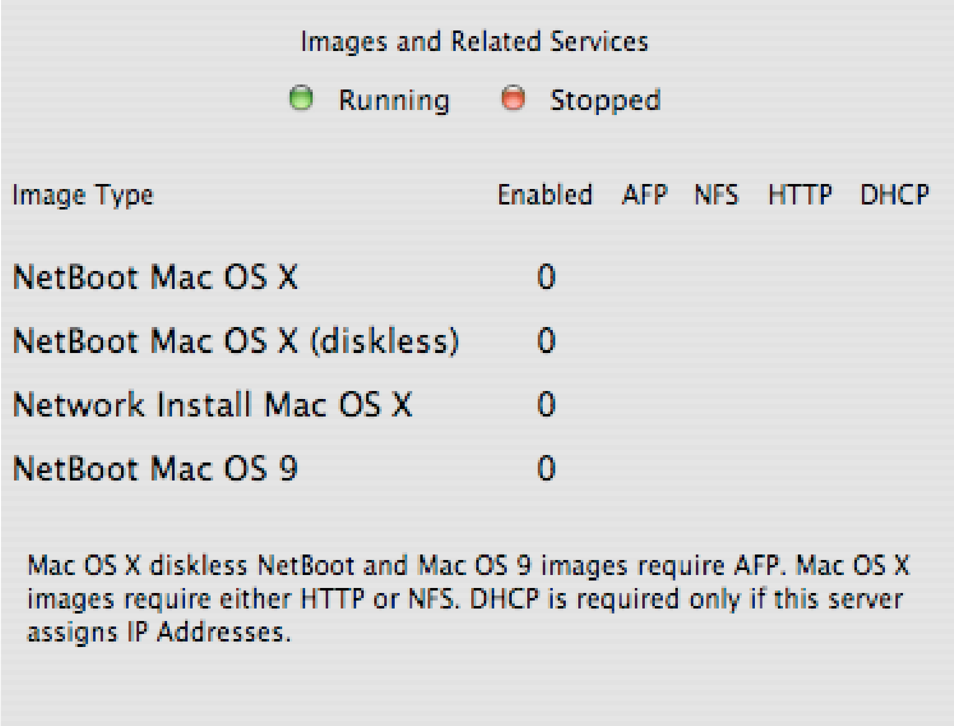
Video: Dial-up modem

Network: Custom

NetBoot

Images = known application settings

- Central image server
- Client systems boot to different images for different roles
- Clients home folders in Open Directory – can use FileVault
- Images must be stored on servers with no security



Images and Related Services

● Running ● Stopped

Image Type	Enabled	AFP	NFS	HTTP	DHCP
NetBoot Mac OS X	0				
NetBoot Mac OS X (diskless)	0				
Network Install Mac OS X	0				
NetBoot Mac OS 9	0				

Mac OS X diskless NetBoot and Mac OS 9 images require AFP. Mac OS X images require either HTTP or NFS. DHCP is required only if this server assigns IP Addresses.

Forensics

Mac Specifics

- Before you plug in a drive you will be doing forensics work on you should install a write-blocker or:
  - Rename /private/etc/mach_init.d/diskarbitrationd.plist to diskarbitrationd.plist.old
  - Kill the PID for diskarbitrationd
- Don’t forget to check AAC files and PICT files to see if they’re being used as secure channels (eg – Stego 1.0)

Security Tools

The Usual Suspects

- Snort using HenWen
- Tripwire using CheckMate
- Metasploit
- Nessus
- DarwinPorts
- By default all logs at low levels

Apple Utilities

More info

- Rendezvous Browser
- Secure Empty Trash
- FileVault
- FinkCommander
- SquidMan
- Concatenated RAID
- GPG for Mail.app
- Lingon – No more CRON

More Information

Links and stuff...

- www.afp548.com
- www.xsanity.com
- http://www.nsa.gov/snac/downloads_macX.cfm
- www.securemac.com
- www.macsecurity.org
- http://www.info.apple.com/usen/security
- www.macintoshsecurity.com
- www.sans.org

- Charles Edge, ACSA, MCSE, CCNA
- Partner :: Three18 :: www.318.com
- Author :: Mac Tiger Server Little Black Book
- Author Web Admin Scripting Little Black