



# Mac OS X

Playing nice in a heterogeneous world  
PRESENTED BY: Charles Edge



# Whoami

- Charles Edge, MCSE, CCNA, ACSA, Network+
- Partner, Three18 – Consulting firm in Santa Monica, California
- Author, Mac Tiger Server Little Black Book and Web Admin Scripting Black Book



# Mac and \*nix

## Crossing the bridge

- Xcode, AppleScript Studio and Web languages offers a development environment that is fairly easy to pick up and robust.
- OS X has X11, bash/tcsh/sh built in
- OS X has most of the same CLI stuff that most flavors of BSD and Linux. AIX/Solaris gurus might have more differences to learn
- Most CLI tools have GUI apps either available on the web or in the OS, such as Kerberos



# Mac and \*nix

## Differences

- Much of the OS is similar but there are some key differences:
  - rc.local and rc.common are not meant to be changed, launchd is meant to be used
  - Darwin is open source but Aqua (the GUI) is not – Apple is aggressive about this
  - Not all packages have been ported
  - Darwinports can be used to find lots of software that has already been ported



# Mac OS X Server

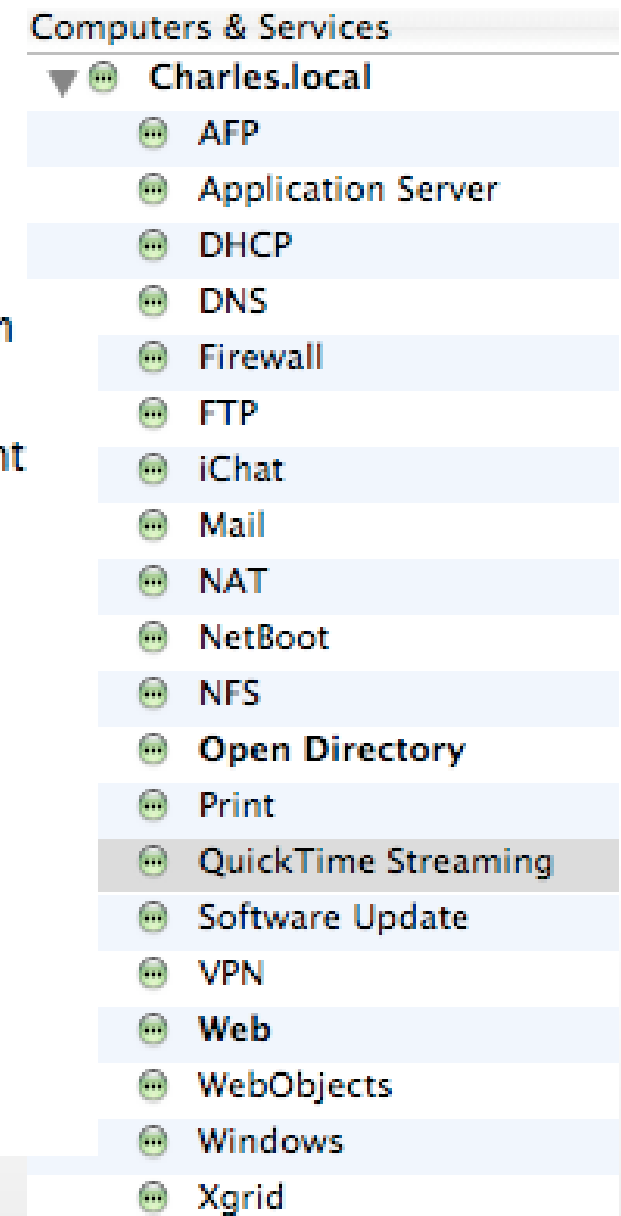
## Open Source Made Easy

- Essentially Mac OS X Server is a FreeBSD server with a NetInfo database that acts like a Windows Registry
- Very similar to Webmin but with a larger user base



A screenshot of the Mac OS X Server utilities window. It displays a list of various server management tools, each with a small icon to its left. The tools are arranged in a single column.

- 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

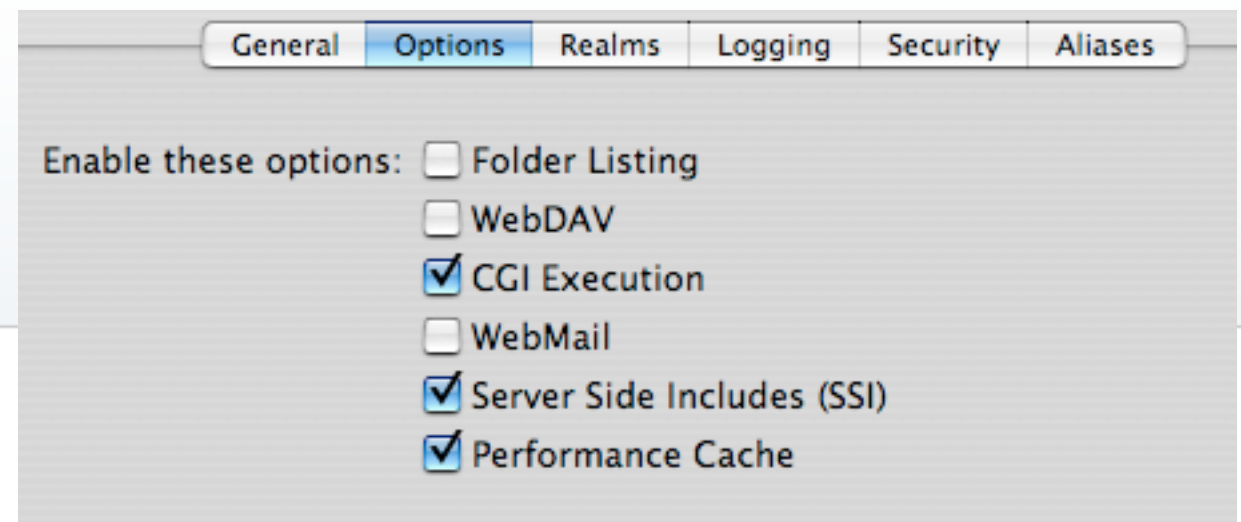


A screenshot of the 'Computers & Services' pane in the Mac OS X Server interface. It shows a list of services and their status for the local machine, 'Charles.local'. Each item has a small icon to its left, representing its status (e.g., a green dot for 'on' or a red dot for 'off').

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



- Apache 1.3.33
- SSI, PHP, Perl, Tomcat, Ruby can be enabled by clicking a checkbox
- Performance Cache, realms and virtual hosts are easily setup as well
- WebDAV can be used as a more secure alternative to providing FTP-style access to remote users

- Distrib 4.1.13a
- Every client I've worked on so far that uses MySQL on Mac servers also uses phpMyAdmin to administer the server
- MySQL can be turned on by simply assigning a root password and clicking on the Start button
- You can easily upgrade to the latest version of MySQL using DarwinPorts

Start MySQL service now.

Install default files needed by MySQL se

New MySQL root password:

••••••••

Verify:



# Mail Services

Postfix and so much more

- Easy GUI for Postfix
- Manage multiple domains from a GUI
- SpamAssassin and ClamAV are built in
- MailMan services available with a click
- Automatically update virus and spam databases

The screenshot shows the 'Filters' tab of the 318 Mail Services GUI. It contains settings for scanning email for junk mail and viruses. The 'Scan email for junk mail' section is checked, with a 'Minimum junk mail score' slider set to 6 (Hits) and 'Accepted languages' set to 'en fr de ja'. The 'Junk mail messages should be' dropdown is set to 'Bounced', and 'Send notification to' is 'spam-admin@three18.com'. The 'Scan email for viruses' section is also checked, with 'Infected messages should be' set to 'Deleted', 'Send notification to' is 'virus-admin@three18.com', and 'Notify recipients' is checked. At the bottom, 'Update the Junk mail and virus database' is checked, set to '1' time(s) every day, with a 'Last Update' timestamp of 'Wednesday, March 15, 2006 2:49:24 AM America/Los\_Angeles'.

General Relay **Filters** Quotas Mailing Lists Logging Advanced

☒ Scan email for junk mail

Minimum junk mail score:  Hits

Accepted languages:  locales:

Junk mail messages should be:

☒ Send notification to:

☒ Scan email for viruses

Infected messages should be:

☒ Send notification to:

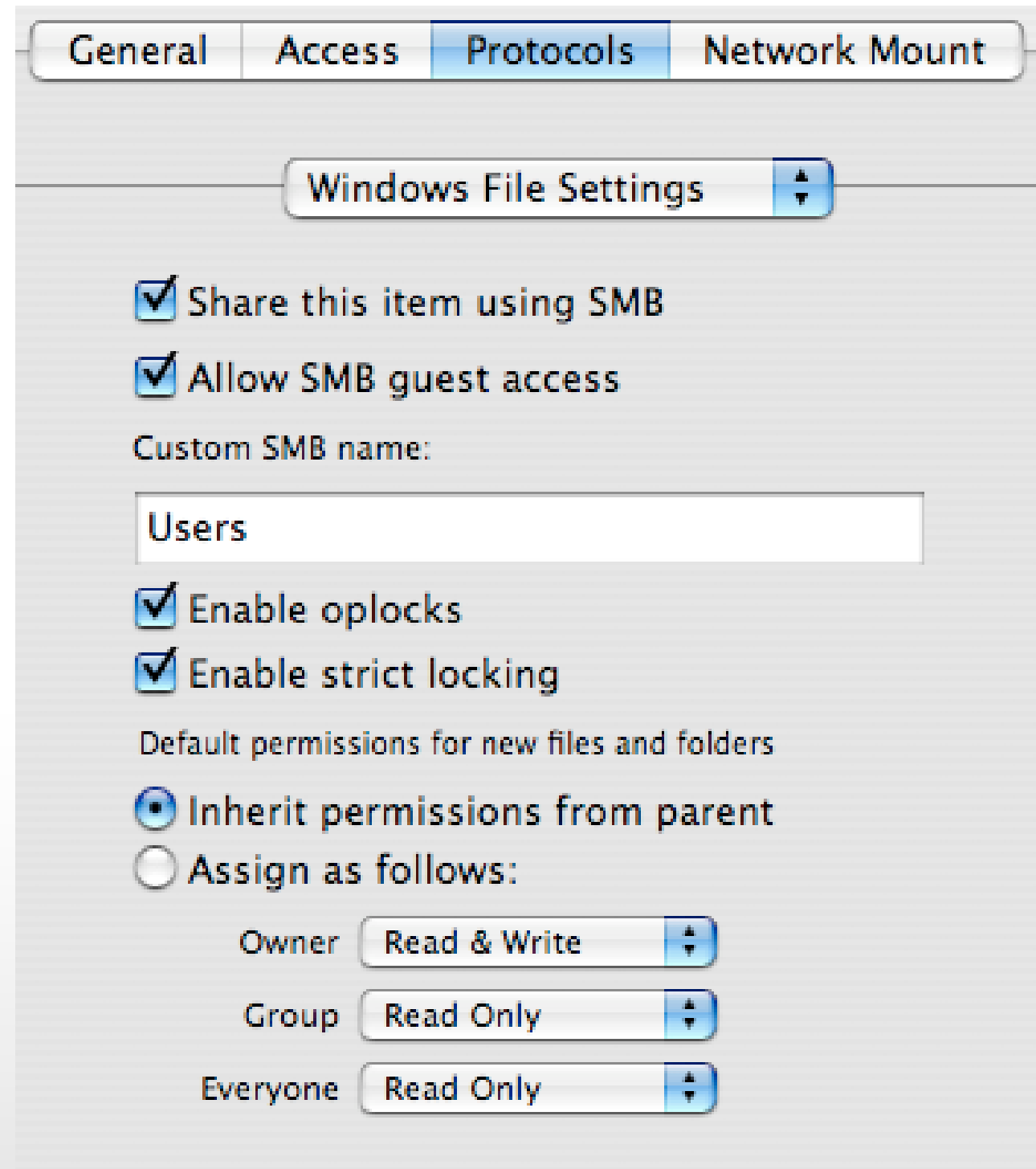
☒ Notify recipients

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

Last Update: Wednesday, March 15, 2006 2:49:24 AM America/Los\_Angeles



- Version 3.0.10 enabled just by clicking start
- Share files with Windows stations easily
- Rather than creating share points in a configuration file you can use a GUI



The screenshot shows the Samba GUI with the 'Protocols' tab selected. The 'Windows File Settings' dropdown is set to 'Windows File Settings'. The following options are checked:

- ☒ 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



# Samba

## Windows Directory Services

- NTLMv2, NTLM, LAN Manager enabled by default
- Enable PDC or BDC for NT 4.0 style domain services
- Works with Active Directory and has a migration wizard from NT 4.0 based domains

General Access Logging Advanced

Role: ☒ Standalone Server  
☐ Domain Member  
☒ Primary Domain Controller (PDC)  
☐ Backup Domain Controller (BDC)

Description:

Computer Name:

Workgroup:



# Print Server

- By default cupsd listens on all adapters
- Printers can be shared and reshared over any protocol – including LPR, SMB and IPP
- Printer quotas can be configured for users or groups

Editing: hp color LaserJet 3700 (00306EFCEA59)

Printer: hp\_color\_LaserJet\_3700\_\_00306EFCEA59\_  
Kind: HP Color LaserJet 3700

Sharing Name:

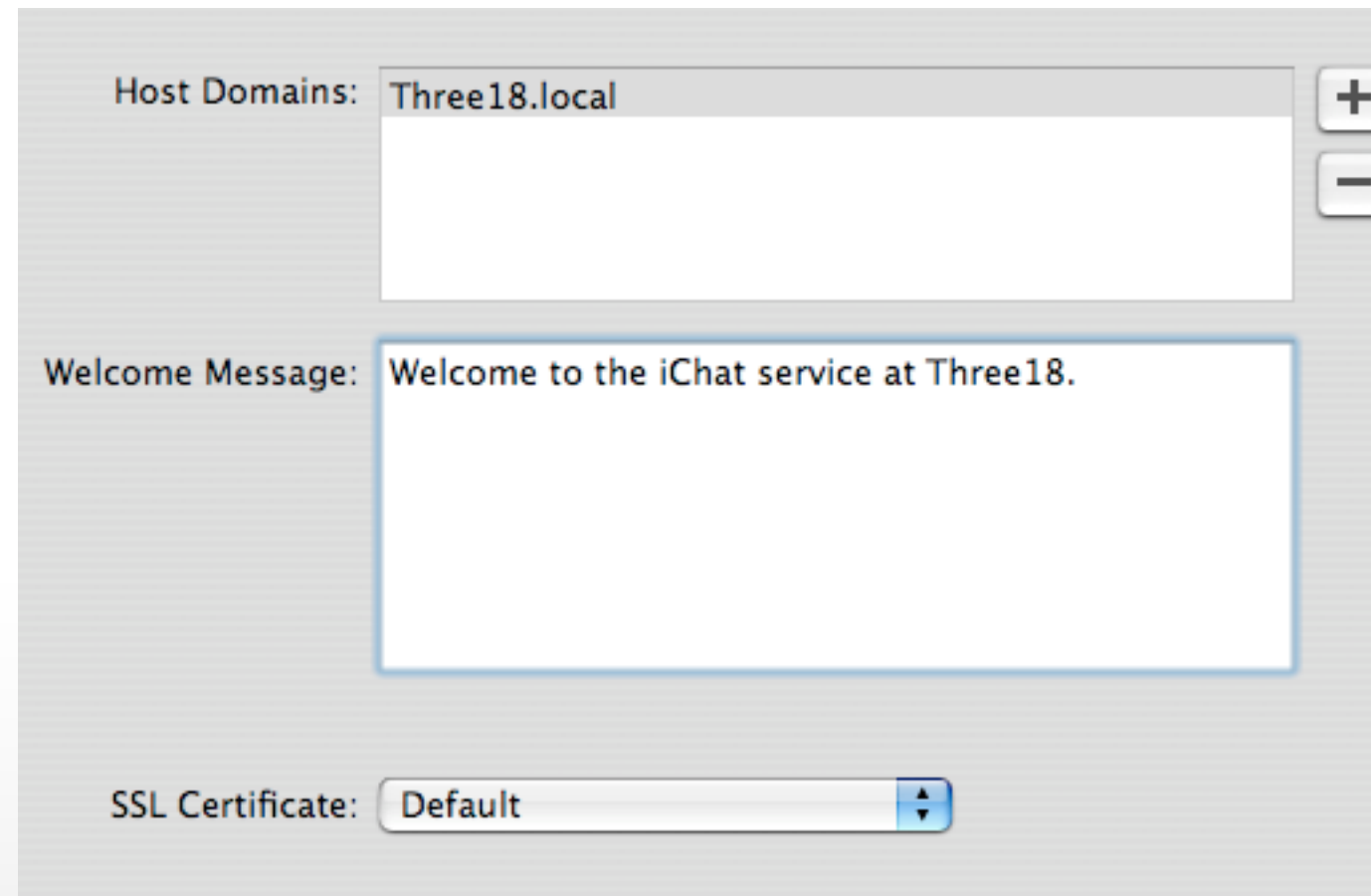
Protocol: ☒ IPP  
☒ AppleTalk  
☒ LPR  
☒ Show name in Bonjour  
☒ SMB  
SMB sharing requires Windows services.

Quotas: ☒ Enforce quotas for this queue  
Use the Workgroup Manager application to set up quotas for each user.

Cover Sheet:

# iChat Server

- iChat Server uses Jabber (1.x) to provide audio, video and text messaging
- SSL Certificates help keep things safe
- Jabber can run for multiple domains helping to separate departments



Host Domains: Three18.local

Welcome Message: Welcome to the iChat service at Three18.

SSL Certificate: Default

The image shows a screenshot of the iChat Server configuration window. It has a light gray background. At the top, there's a section for 'Host Domains' with a text field containing 'Three18.local' and a list box below it. To the right of the list box are '+' and '-' buttons. Below that is a 'Welcome Message' section with a text field containing 'Welcome to the iChat service at Three18.'. At the bottom is an 'SSL Certificate' section with a dropdown menu showing 'Default' and a small blue arrow button to its right.



# Directory Services

## Open Directory

- OpenLDAP, SASL, Kerberos and other Directory Service Standards incorporated as Open Directory
- Works with Active Directory
- Allows for shared username and password databases

The screenshot shows the 'Policy' tab of the Open Directory configuration window. It includes sub-tabs for 'General', 'Protocols', 'Policy', 'Passwords', 'Binding', and 'Security'. The 'Disable login' section has four options: 'on specific date' (disabled), 'after using it for' (0 days), 'after inactive for' (7 days, checked), and 'after user makes' (3 failed attempts, checked). The 'Password must' section has seven options, all checked: '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', and 'be reset every 4 weeks'. A note at the bottom states: 'User account settings may override global policies. Administrators are exempt.'

General Protocols Policy

Passwords Binding Security

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.



# Directory Services

## Integration

- Using the Active Directory Plug-in you can cross-realm with AD
- You can also cross-realm with Sun ONE and iPlanet
- In a cross-realmed environment one directory service is used for authenti

General Protocols Policy

Passwords Binding Security

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.



# DNS

Looking at DNS from the perspective of the IP

- DNS services are easy to configure
- You can still use the configuration files
- Tiger Server represents a change in the way that Apple views DNS – IPs get names, names don't get IPs

The screenshot shows a DNS configuration window for the IP address 64.60.74.118. The window has a title bar with buttons for 'Remove Server', 'Connect', 'Refresh', 'New Window', and 'Start Service'. The 'Name' field is set to 'www'. Below it, the 'Fully Qualified Name' is 'www.three18.com' and the 'IP Reverse Lookup' is 'www.three18.com'. There are tabs for 'General' and 'Machines'. A 'Use This Zone' button is visible. The 'Aliases' list contains 'three18.com', 'pop.three18.com', 'mail.three18.com', and 'smtp.three18.com'. A checkbox is checked, indicating 'This machine is a mail server for the zone'. The 'Mail Server Precedence' is set to 10. The 'Hardware Info' field is set to 'Web Server'.

IP Address: 64.60.74.118

Name: www

Fully Qualified Name: www.three18.com

IP Reverse Lookup: www.three18.com

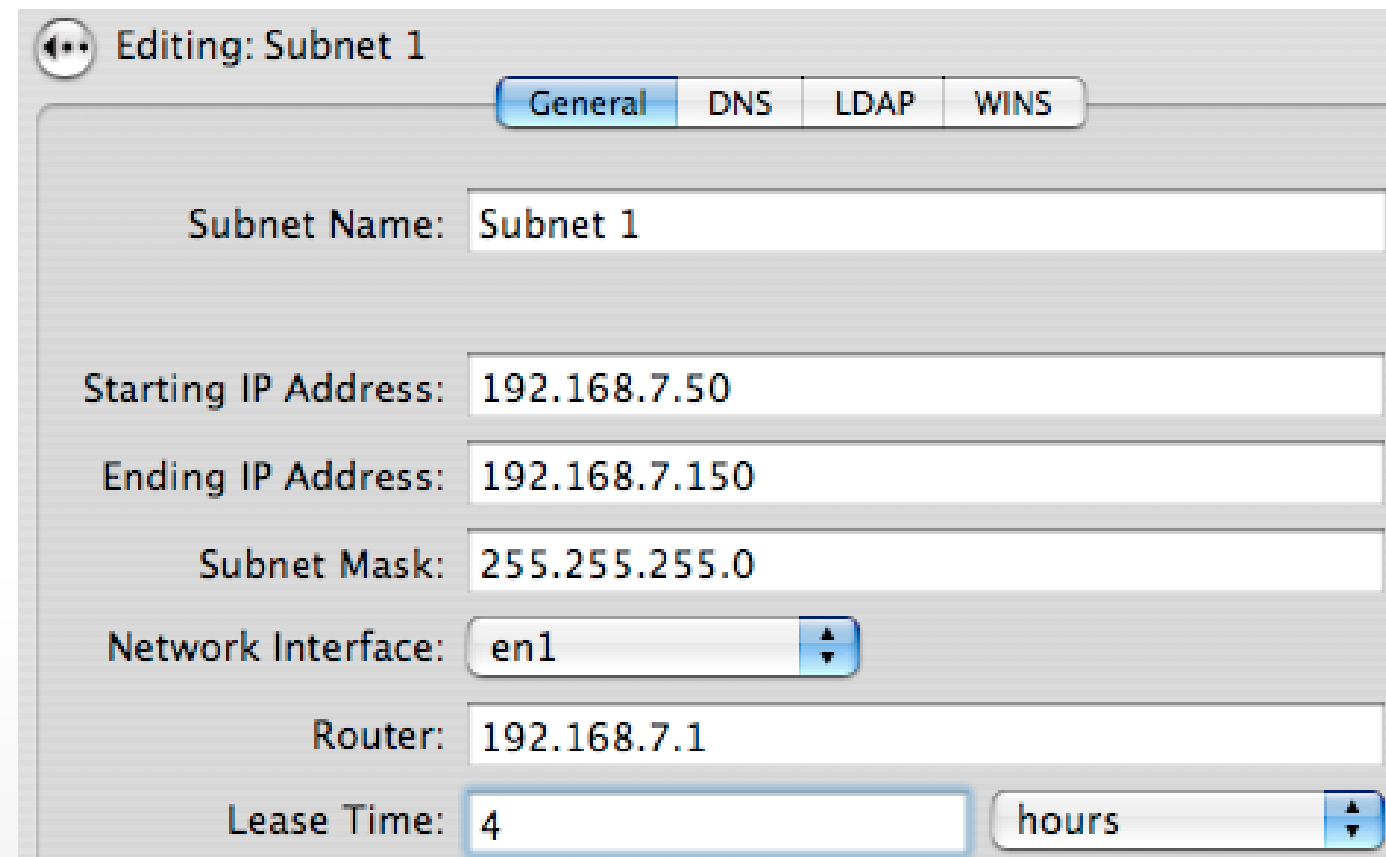
Aliases: three18.com, pop.three18.com, mail.three18.com, smtp.three18.com

☒ This machine is a mail server for the zone

Mail Server Precedence: 10

Hardware Info: Web Server

- DHCP is easy to setup and use
- LDAP settings can be deployed dynamically
- OS X Server can run Multiple subnets on one Network Interface



Editing: Subnet 1

General DNS LDAP WINS

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

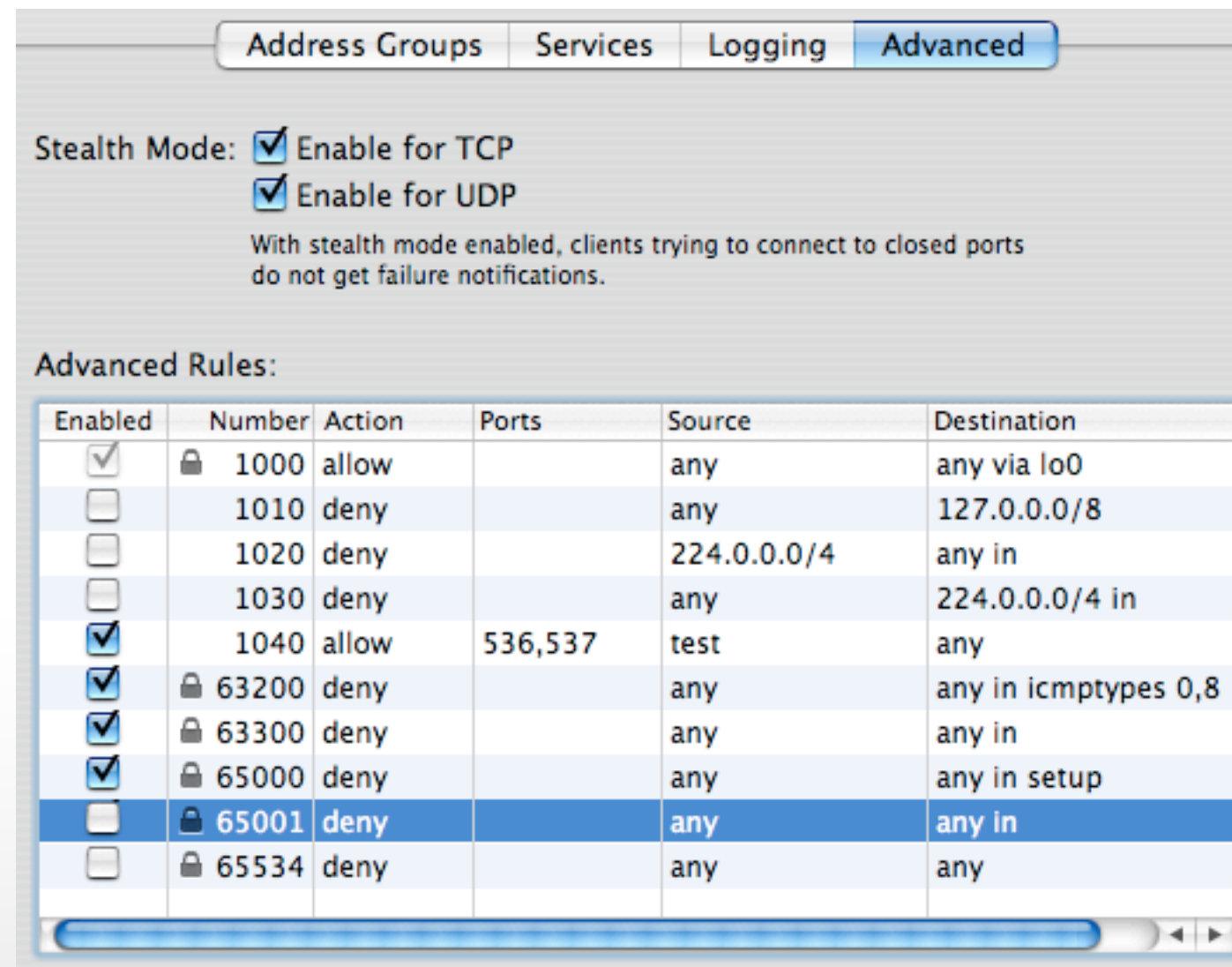




# Firewall and NAT

## with the Gateway Setup Assistant

- Apple provides the Gateway Setup Assistant to help setup NAT
- IPFW rules can easily be copied between systems and written using a GUI
- Dummynet can be used to shape traffic





# VPN

## PPTP and L2TP

- Open Source VPN Standards (openVPN) easily configured
- Supports PPTP and L2TP
- s2svpn allows admins to configure site based VPNs – not the greatest feature in the world...

The screenshot shows a configuration window with four tabs: L2TP, PPTP, Logging, and Client Information. The L2TP tab is selected. It contains the following settings:

- ☒ 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



- TNFTP is installed by default
- Apple has integrated the ftpusers file into NetInfo allowing you to use a GUI to restrict traffic for FTP users to specific folders

Agent Controller

☒ 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.

Agent Controller

☒ Enable controller service

Client Authentication:

Password

Clients must authenticate to the controller using the password above.

Agent Authentication:

Password

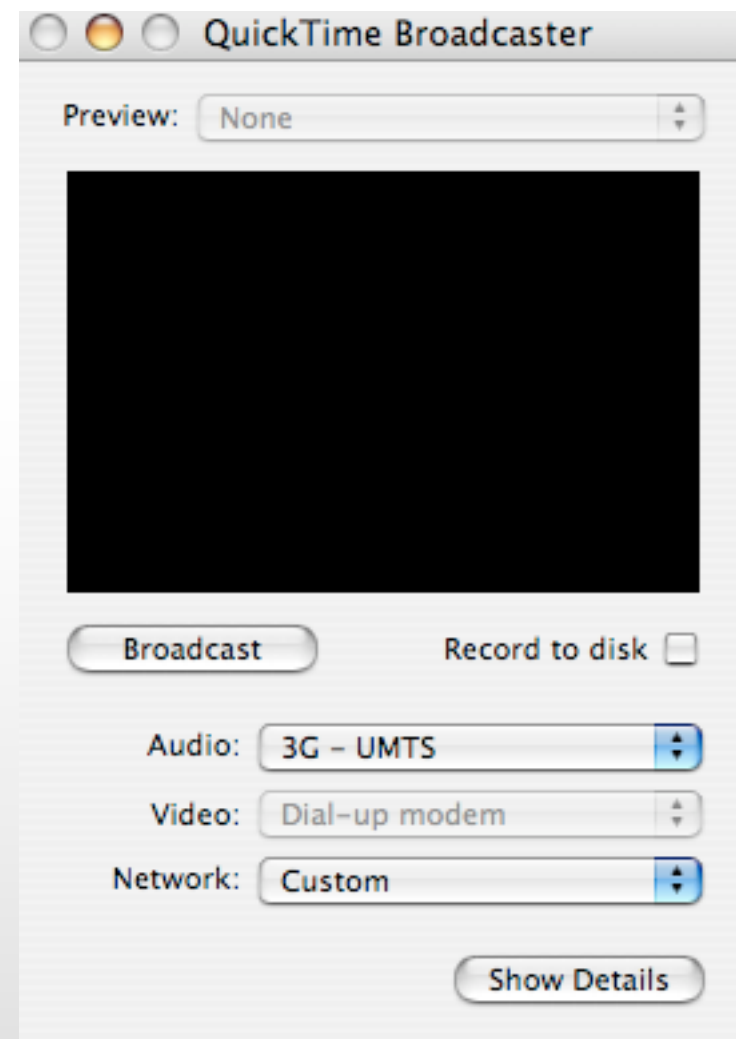
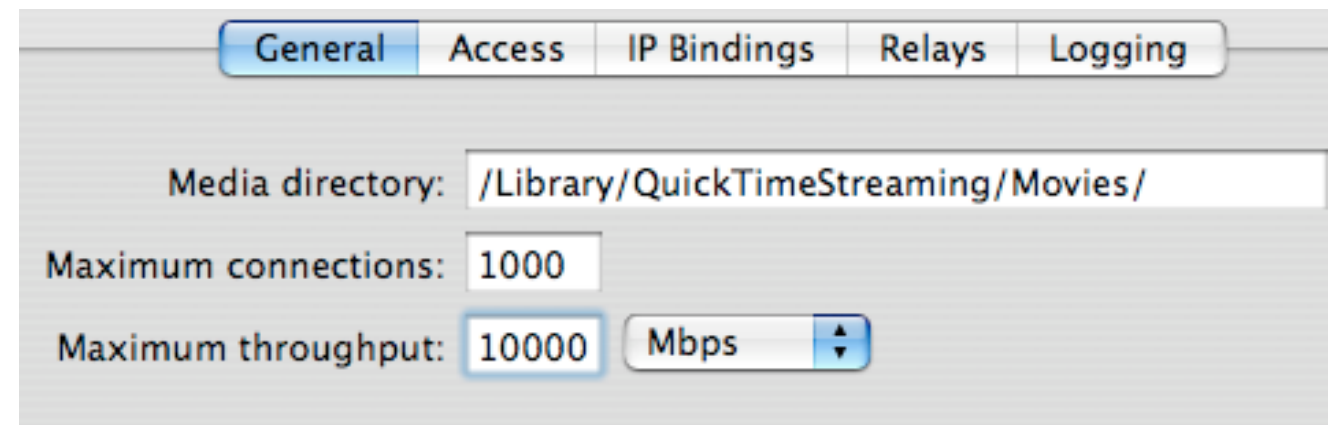
The controller will authenticate to agents with the password above.



# QuickTime Streaming

Simple radio

- QT Broadcaster has live broadcasts of video and audio, acting as a radio or television station
- QuickTime can also store audio and video for on demand
- Protect audio/video
- Linux compat.





# NetBoot

Manage the OS on Multiple Systems

- Use a centralized image store to run multiple systems
- Client systems boot to different images for different roles
- Clients home folders are stored in Open Directory

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.



Questions and Answers