Applied Network Management

Performance Tuning, VPN's and Secure Protocols

Joel Rennich

mactroll@afp548.com

Overview

- *DNS*
- *Routing/NAT*
- *VPN*
- *SSL*
- *Sniffing*

DNS

You need it!

BIND 9

- *www.isc.org*
- *2/3 of all DNS servers*
- *Open Source*
- *On both client and server*

Global Hierarchy

- *13 Root servers*
- *then TLD servers*
- *finally authoritative server*

Local Files

- */var/named*
- */etc/named.conf*

DNS Record Types

- *A*
- *CNAME*
- *NS*
- *MX*
- *PTR*
- *SRV*

A Record

- *name to IP address*

afp548.com.	*21104*	*IN*	A	*66.92.146.93*

CNAME Record

- *name to name*

www.apple.com. 1800 IN CNAME www.apple.com.akadns.net.

NS Record

- *the authoritative server for this domain*

afp548.com. *21104* *IN* *NS* *udns1.ultradns.net.*

MX Record

- *mail server for this domain*

afp548.com. *86400* *IN* *MX* *10 mrsgale.fates.org.*

PTR Record

- *IP address to name*
- *reverse record, only in a reverse zone*

91.0.254.17.in-addr.arpa. 65760 IN PTR www.apple.com.

SRV Record

- *lets clients know what server hosts a service*
- *primarily used with AD plugin*

_ldap._tcp.rennich.com. 600 IN SRV 0 100 389 joda2k3.rennich.com.

Testing DNS

- *dig*
- *host*
- *nslookup*
- *Network Utility*

/etc/named.conf

- *lists what zones you have active*
- *can be used to set up forwarding DNS*
- *all global server configuration goes here*

/var/named/db.*

- *where the actual records are kept*
- *enabled/disabled by /etc/named.conf*

OS X Server GUI

- *guided text editor*
- *best for basic edits*

Demo

DNS on OS X Server

When you need DNS

- *to surf the web*
- *to use Kerberos*
- *to do most anything*

Forwarding Only

- *does not have any local records*
- *does not lookup any answers*
- *only forwards DNS off to another system*

Demo

Forwarding DNS server

Split View

- *used primarily with NAT*
- *cover later when we go over NAT*

Best practices for server

- *you NEED DNS*
- *set up DNS before becoming an OD Master*
- *include reverse records too*

Troubleshooting

- *use CLI tools*
- *check for basic network connectivity*
  - *ping*
- *use another DNS server*

More Resources

- *O'Reilly's DNS and BIND book*
- *Apple Server Documentation*

Questions?

DNS

Routing/NAT

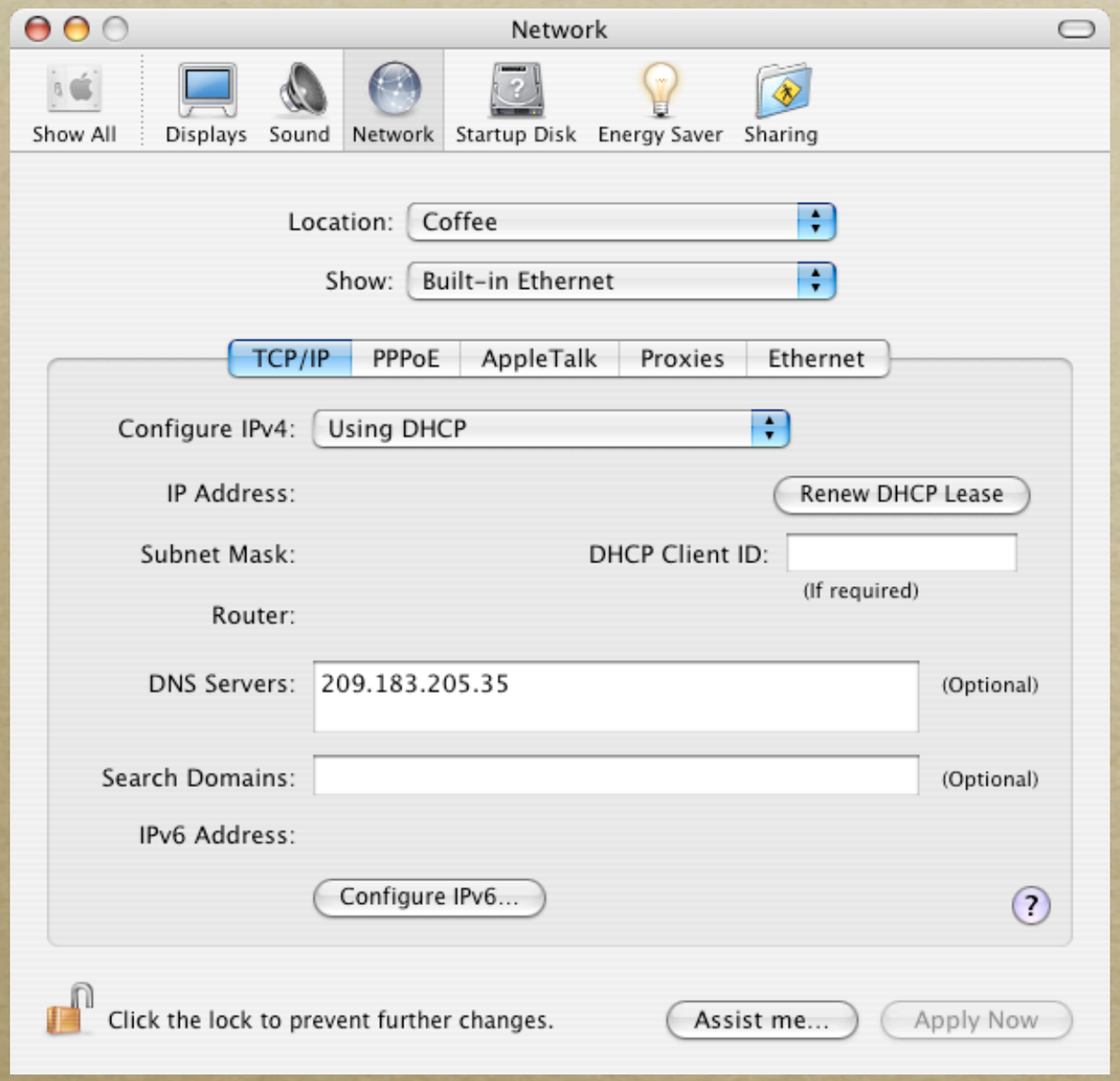
Network Topology

Making do with less IPs

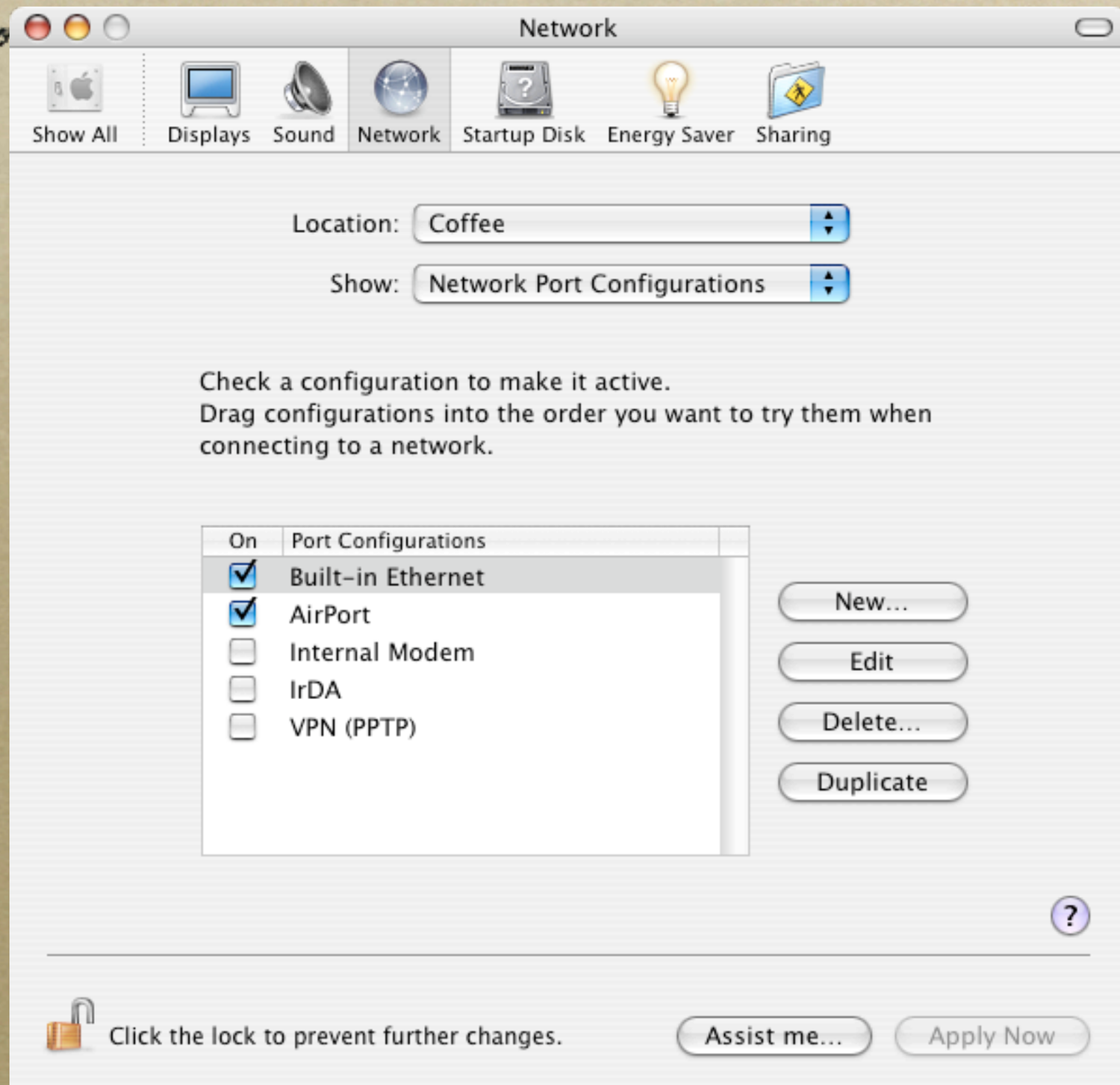
Routing

- *getting a packet to where it needs to go*
- *only one default route*
- *set in Network Preference Pane*

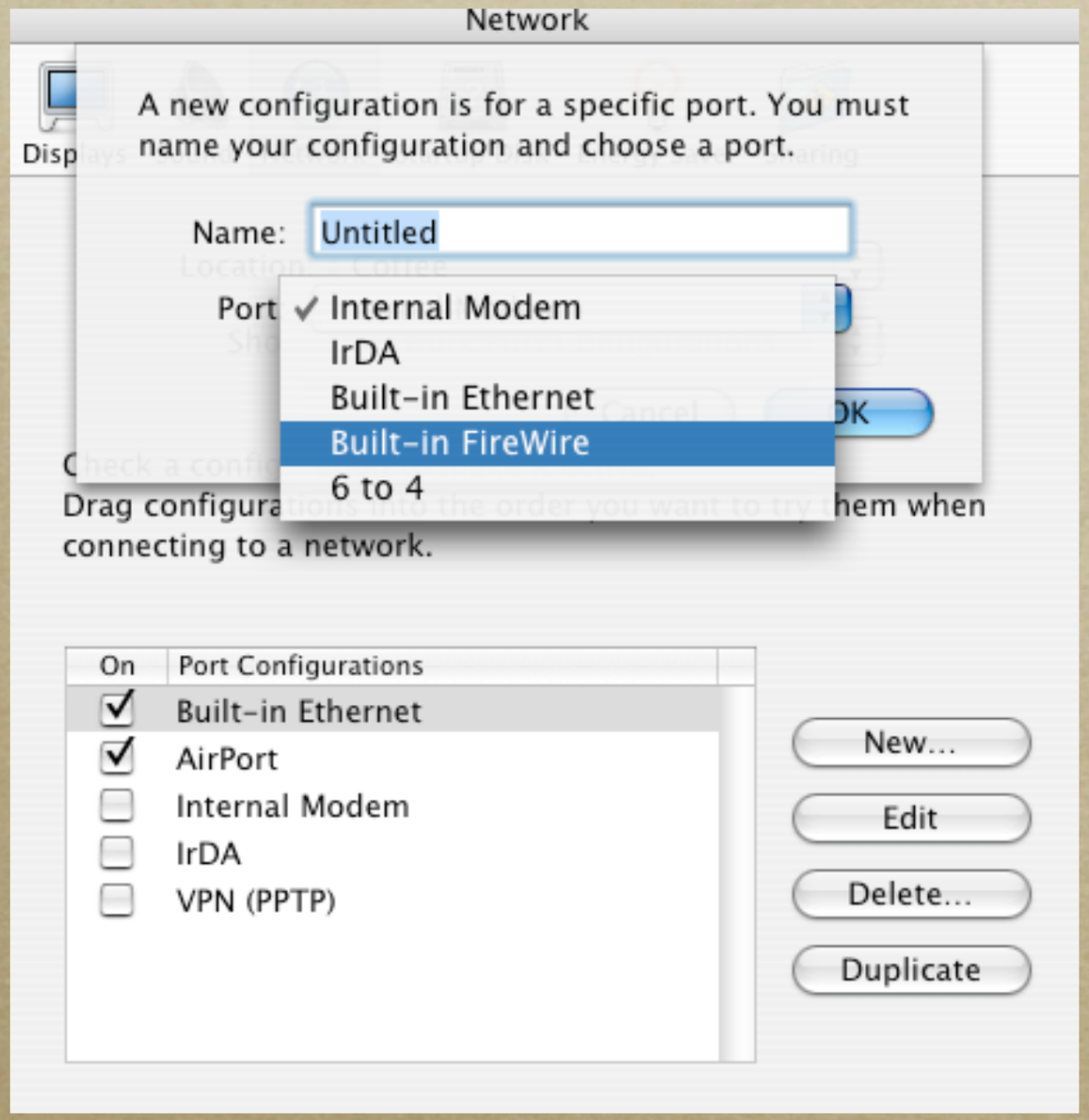
Network Pref Pane



Order Matters



Add new interfaces



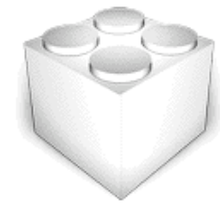
Multi-home

- *Duplicate the interface and add a new IP address to that interface*
- *Add a new physical interface*

configd

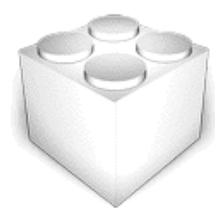
- *reads preferences file written by System Preferences*
- *notifies agents of configuration*
- *agents make change*
- *reads preferences file written by System Preferences*
- *notifies agents of configuration*
- *agents make change*

/Library/Preferences/
SystemConfiguration/preferences.plist



Kernel Event Monitor

Configuration Agents



IP Monitor

Route Table

Route Table

- *Determines what packets go where*
- *Auto-built by configd and friends but can be manually adjusted*
- *Reset at boot time*

Terminal — bash — 95x31

```
MacTrolls-Computer:~ mactroll$ netstat -rn
Routing tables

Internet:
Destination        Gateway            Flags    Refs      Use  Netif Expire
default            161.253.43.254     UGSc       86      462    en1
127                127.0.0.1          UCS         0        0    lo0
127.0.0.1          127.0.0.1          UH         30     7644    lo0
161.253.42/23      link#5             UCS         1        0    en1
161.253.43.187     127.0.0.1          UHS         0        0    lo0
161.253.43.254     0:60:9:b1:2b:0     UHLW        8        0    en1   1117
169.254            link#5             UCS         0        0    en1

Internet6:
Destination                       Gateway                       Flags      Netif Expire
::1                               ::1                           UH          lo0
fe80::1                           link#1                        UHL         lo0
fe80::/64                         link#5                        UC         en1
fe80::230:65ff:fe02:c463          0:30:65:2:c4:63               UHL         lo0
ff01::/32                         ::1                           U           lo0
ff02::/32                         ::1                           UC          lo0
ff02::/32                         link#5                        UC         en1
MacTrolls-Computer:~ mactroll$
```

Demo

adding routes by hand

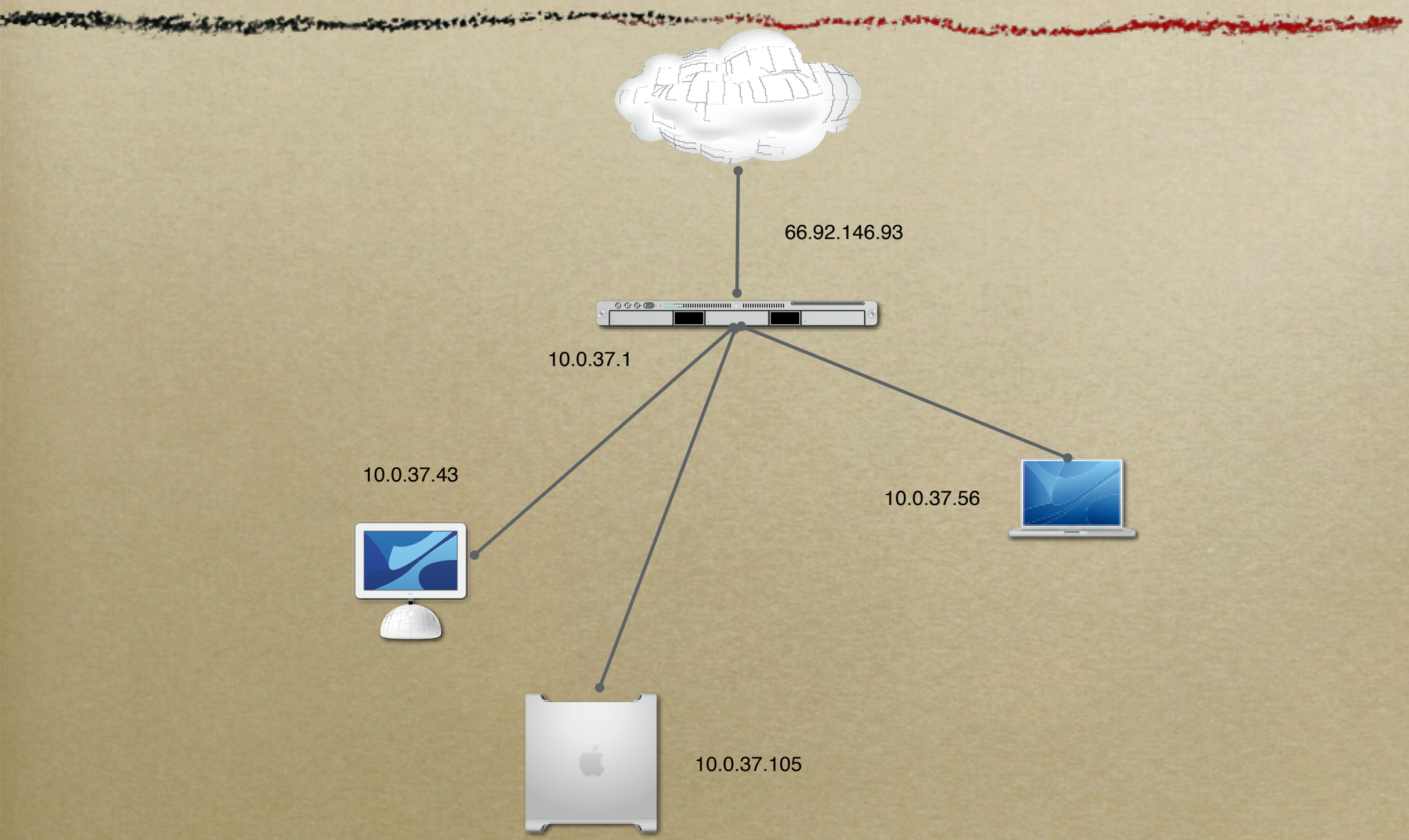
Troubleshooting

- *ping*
- *traceroute*
- *Network Utility*

NAT

- *turning one IP into many*
- *more and more common*
- *need to be aware of issues*

NAT topology



NAT on client

- *Network Preference Pane*
- *also turns on*
  - *DNS*
  - *DHCP*
- *can share one to many*

NAT on Server

- *setup through Server Admin*
- *need to launch the firewall also*

NAT processes

- *natd*
- *ipfw*

Demo

NAT on OS X Server

Questions?

Routing/NAT

VPN

SSH

PPTP

IPSec

L2TP/IPSec

Protections

- *SSH*
- *VPN*
- *SSL*
- *S/MIME*

SSH

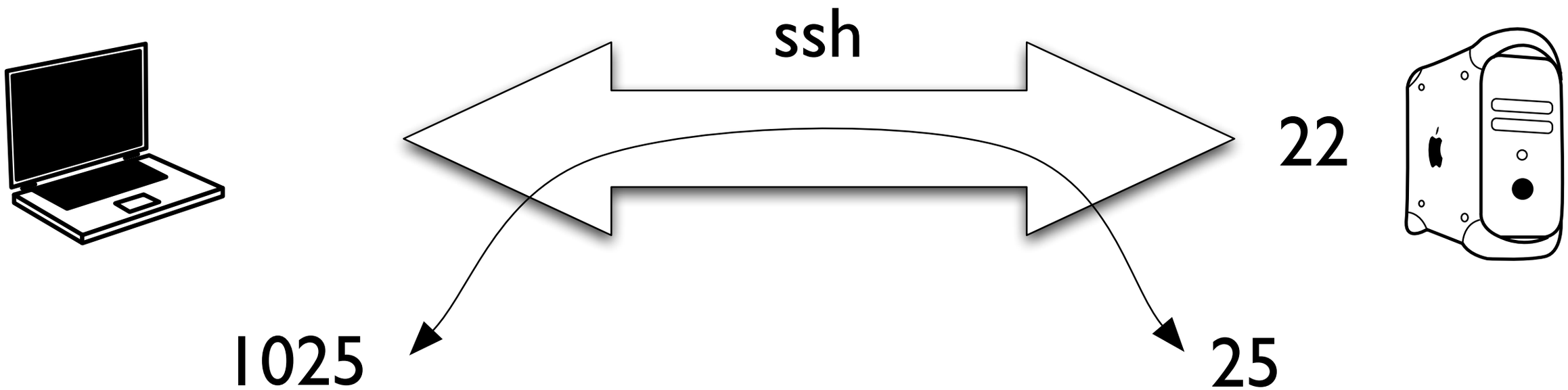
- *Simple CLI connection*
- *Tunnel*

Simple Connection

ssh mactroll@afp548.com

Tunnel

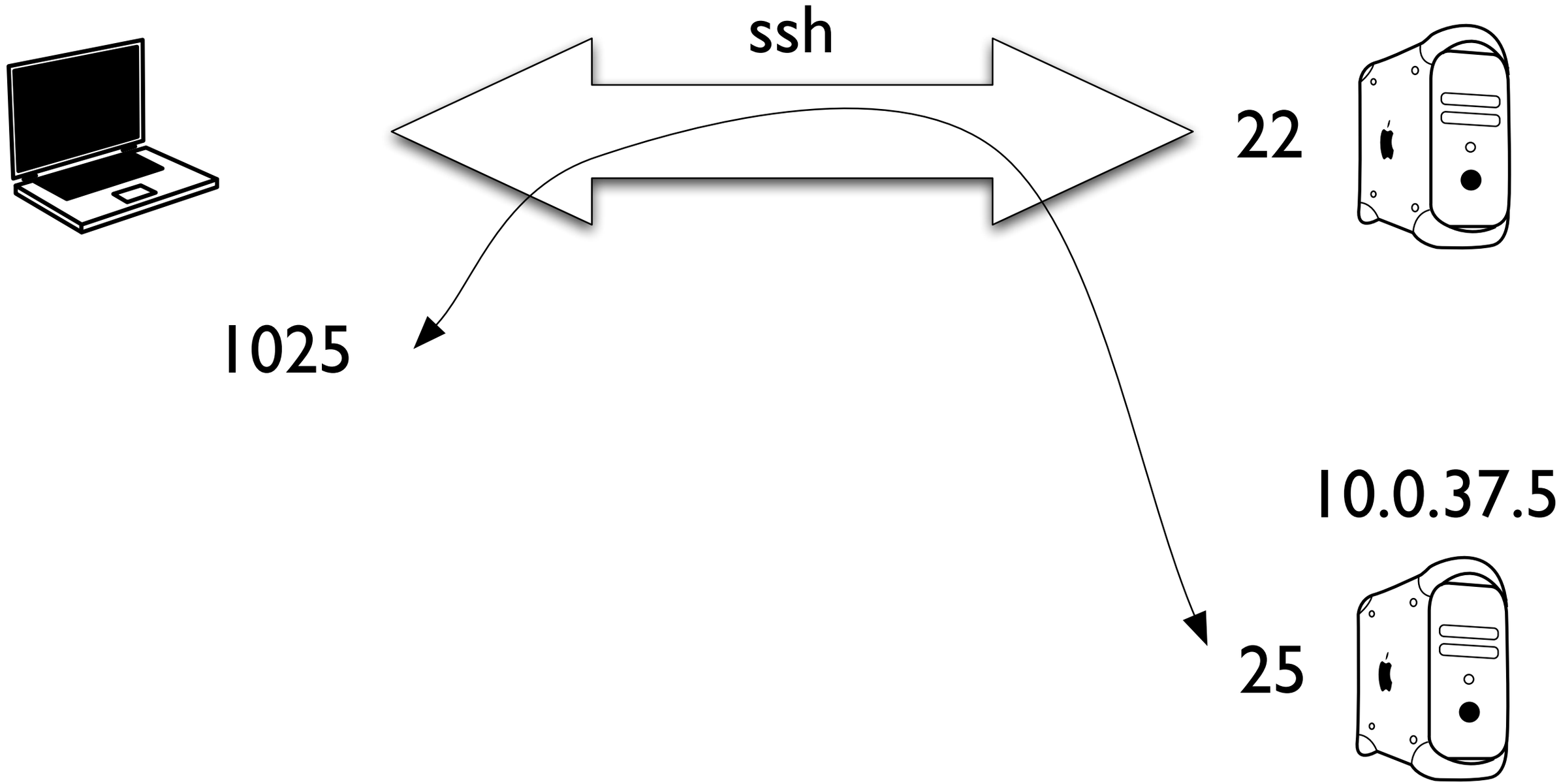
ssh mactroll@www.afp548.com -L 1025:localhost:25




```
ssh mactroll@www.afp548.com -L 1025:localhost:25
```

Tunnel to another host

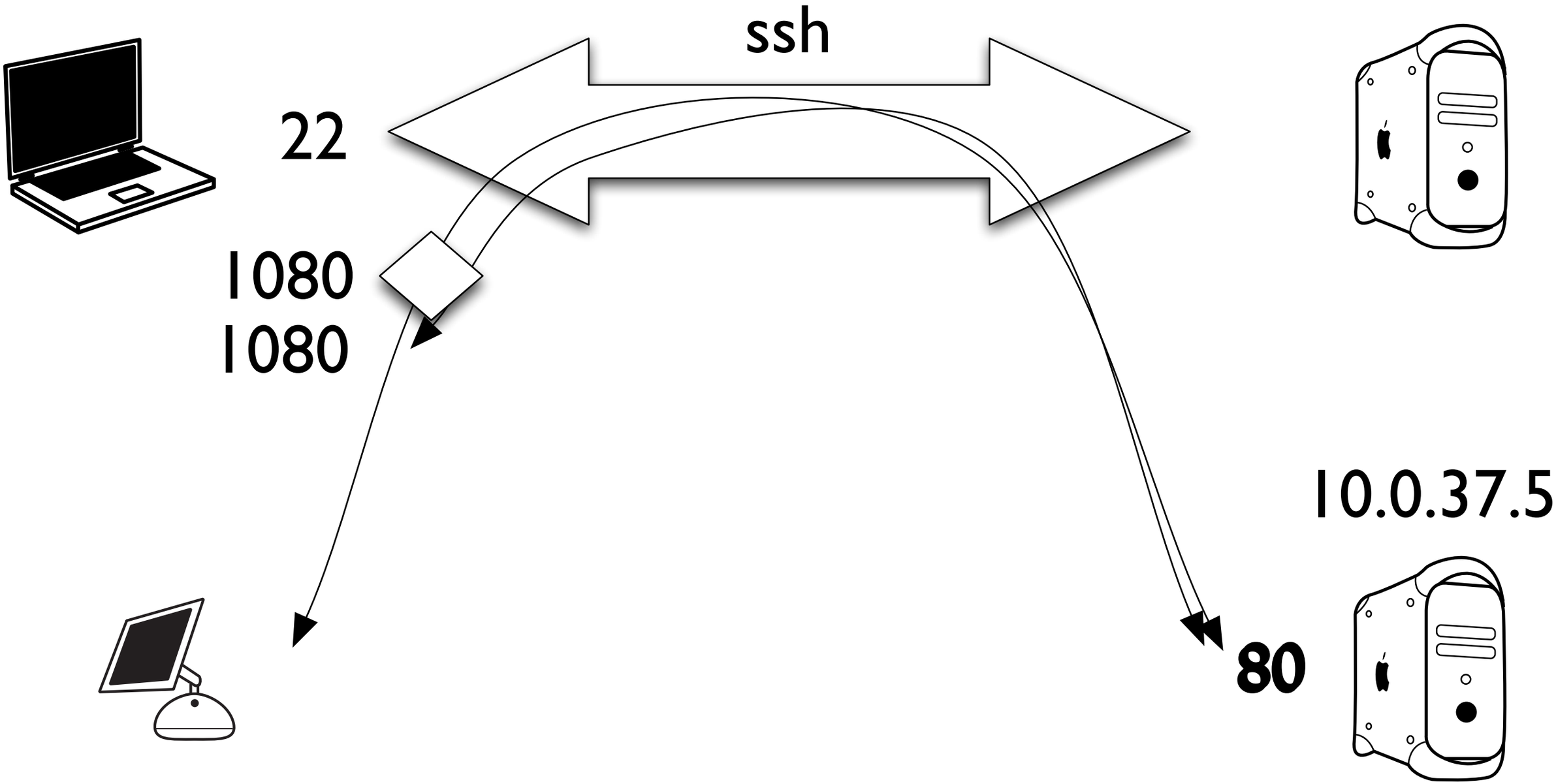
ssh mactroll@www.afp548.com -L 1025:10.0.37.5:25



ssh mactroll@www.afp548.com -L 1025:10.0.37.5:25

Reverse Tunnel

ssh mactroll@12.57.8.23 -R 1080:10.0.37.5:80



ssh mactroll@www.afp548.com -L 1025:10.0.37.5:25

VPN

PPTP

- *Least secure*
- *OSX 10.2+ and Windows 98 and greater*
- *Server - Windows NT+ and OSXS 10.2+*

L2TP/IPSec

- *Very Secure*
- *Supported by Cisco, MS, Apple*
- *OSX 10.3*
- *Server - Win2k+, OSXS 10.3, Cisco*
- *Uses L2TP to make IPSec easier*

IPSec

- *Very secure*
- *Supported by most firewall vendors*
- *Server - Unix/Linux, OSXS 10.2 and greater*
- *OSX 10.2 and greater - no Apple GUI*
- *Complicated to configure*

1. Introduction to IPSec

Why IPSec?

- *Security, Security, Security*
- *Secures all traffic, all IP protocols*
- *Allows secure connections to remote networks, even networks behind NAT*
- *Supported by most of the firewall vendors*
- *Many RFCs covering IPSec*

Common VPN Formats

Type	Apple GUI?	Easy	Secure	Vendor Support
PPTP	Yes	Yes	No	Yes
L2TP/ IPSec	Yes	Maybe	Yes	Maybe
IPSec	No	Maybe	Yes	Maybe

No Yes Maybe

L2TP/IPSec Support

- *Cisco*
- *Microsoft*
- *Apple (OS X 10.3)*
- *Free S/WAN*

IPSec Support

- *CheckPoint*
- *SonicWALL*
- *NetScreen*
- *Watchguard*
- *Linksys*
- *Draytek*
- *Free S/WAN*

Impediments to Adoption

- *Awareness of need*
- *Potentially brutal to configure*
- *Lack of IPSec pass through on network equipment*

2. Implementation

IPSec in OSX

- *First appeared in 10.2*
- *based off of the kame IPV6 stack - www.kame.net*
- *Apple GUI*
  - *None in 10.2*
  - *L2TP/IPSec only in 10.3*

Relevant Parts on OS X

- */usr/sbin/racoon*
- */usr/sbin/setkey*
- */etc/racoon/*

1. Flush any existing keys

```
sudo setkey -F
sudo setkey -FP
```

2. Specify a new policy

```
sudo setkey -C << EOF

spdadd 10.0.1.3/32 10.0.37.1/24 any -P out ipsec esp/tunnel/
10.0.1.3-17.254.0.91/require;

spdadd 10.0.37.1/24 10.0.1.27/32 any -P in ipsec esp/tunnel/
17.254.0.91-10.0.1.3/require;

EOF
```

3. Set Shared Key

```
sudo -s
echo “17.254.0.91    supersecretpass” >> /etc/racoon/psk.txt
```

4. Run racoon

```
sudo racoon -f /etc/racoon/racoon.conf
```

MIA 10.3

- *auto policy creation - allows easy IPSec gateway configuration*
- *keychain support - psk file is kept in clear text*
- *NAT traversal - using UDP to wrap IPSec packets to more easily navigate NAT connections*
- *xauth*

3. GUI Applications

Internet Connect

www.apple.com

Internet Connect

- *Included in OS X 10.3*
- *L2TP/IPSec, PPTP*
- *Simple configuration*

VPN (L2TP)

Summary | AirPort | VPN (L2TP) | VPN (PPTP) 1

L2TP over IPSec

Configuration: Other

Server address: steed.fates.org

Account Name: mactroll

Password: •••••••

☑ Show VPN status in menu bar

Status: Idle

Connect

Configurations

Steed L2TP

Description: Steed L2TP

Server Address: steed.fates.org

Account Name: mactroll

Authentication: ◉ Use Password: ••••••••••

○ RSA SecurID

Shared Secret:

+ −

OK

VPN Tracker

www.vpntracker.com

VPN Tracker

- *Most comprehensive*
- *Commercial - $200/user for Pro version*
- *IPSec*

VPN Tracker

	Name	Type	Mode	Init
☑	Home	SonicWALL	Host to Network	yes

New... Edit... Duplicate Delete

Restart IPsec for changes to take effect. Stop IPsec Restart IPsec

General

Name: Home

Connection Type: SonicWALL

☑ Initiate connection

Networking

Topology: Host to Network

Local Endpoint: ◉ Default Interface

○

Remote Endpoint: www.jodapro.com

Local Host: optional

Remote Network: 10.0.37.1 / 24 +

Authentication

◉ Pre-shared key Edit...

○ Certificates Edit...

Click the lock to prevent further changes.

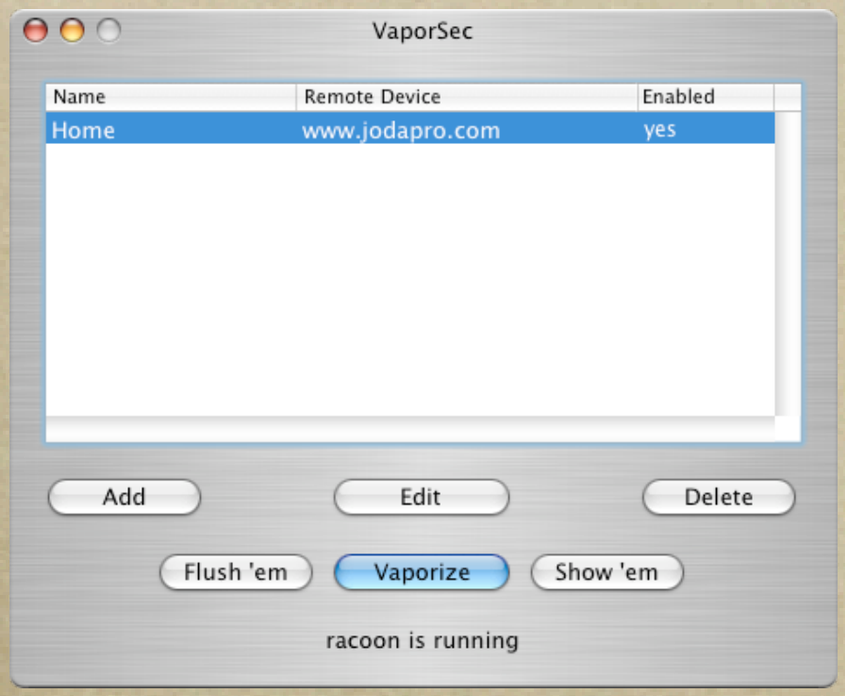
Cancel Save

VaporSec

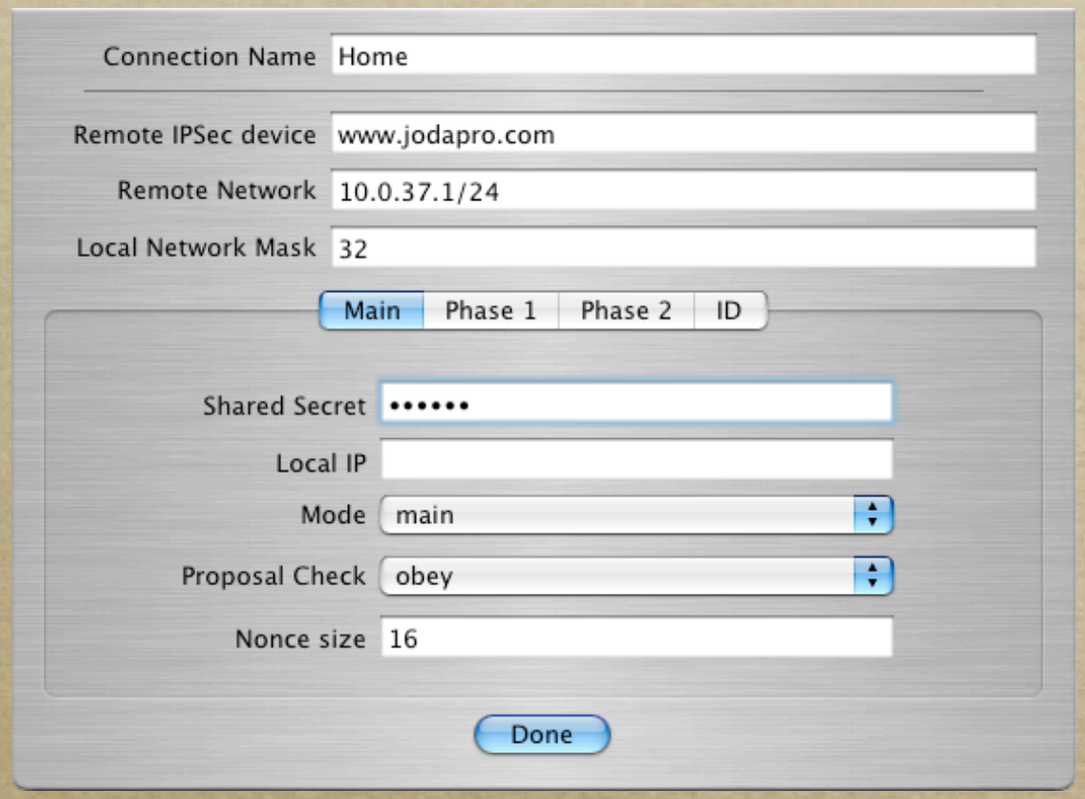
www.afp548.com

VaporSec

- *Easy to configure*
- *First GUI*
- *AppleScript Studio Application*
- *Freeware with source available*
- *IPSec*


VaporSec
Name
Remote Device
Enabled
Home
www.jodapro.com
yes
Add
Edit
Delete
Flush 'em
Vaporize
Show 'em
racoon is running


VaporSec

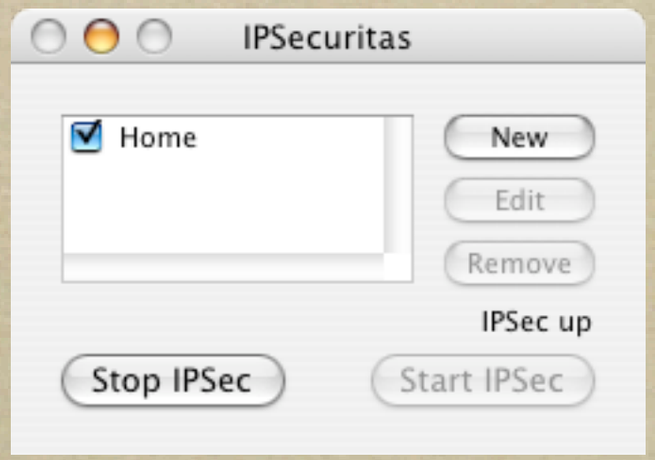

Connection Name
Home
Remote IPSec device
www.jodapro.com
Remote Network
10.0.37.1/24
Local Network Mask
32
Main
Phase 1
Phase 2
ID
Shared Secret
Local IP
Mode
main
Proposal Check
obey
Nonce size
16
Done

IPSecuritas

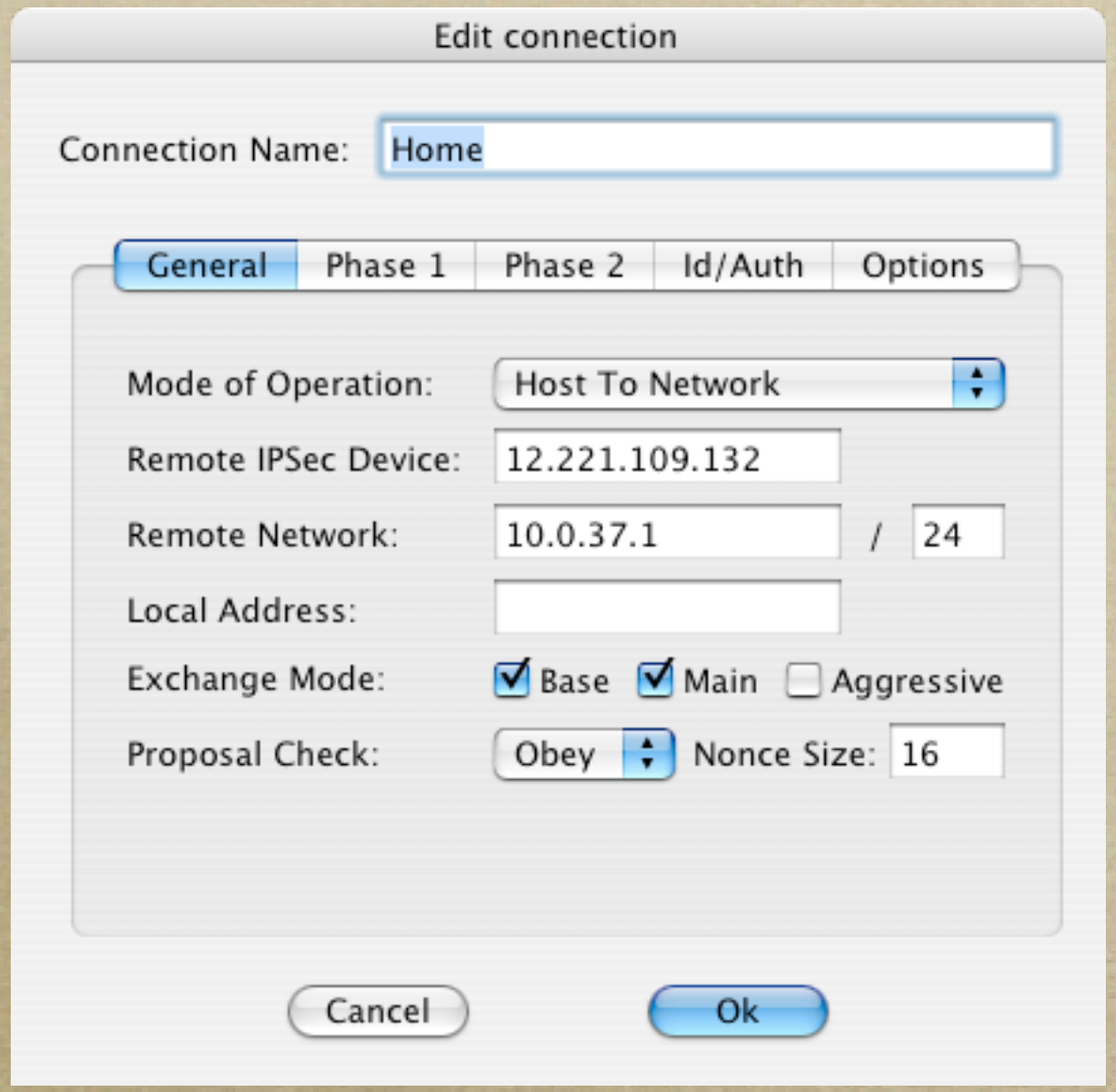
www.lobotomo.com

IPSecuritas

- *Cocoa application*
- *Recently released*
- *Freeware*
- *IPSec*


IPSecuritas
Home
New
Edit
Remove
IPSec up
Stop IPSec
Start IPSec


IPSec


Edit connection
Connection Name: Home
General
Phase 1
Phase 2
Id/Auth
Options
Mode of Operation: Host To Network
Remote IPSec Device: 12.221.109.132
Remote Network: 10.0.37.1 / 24
Local Address:
Exchange Mode: Base Main Aggressive
Proposal Check: Obey Nonce Size: 16
Cancel
Ok

4. Case Studies

I. SOHO

Simple and effective ways of securing personal networks

Equipment

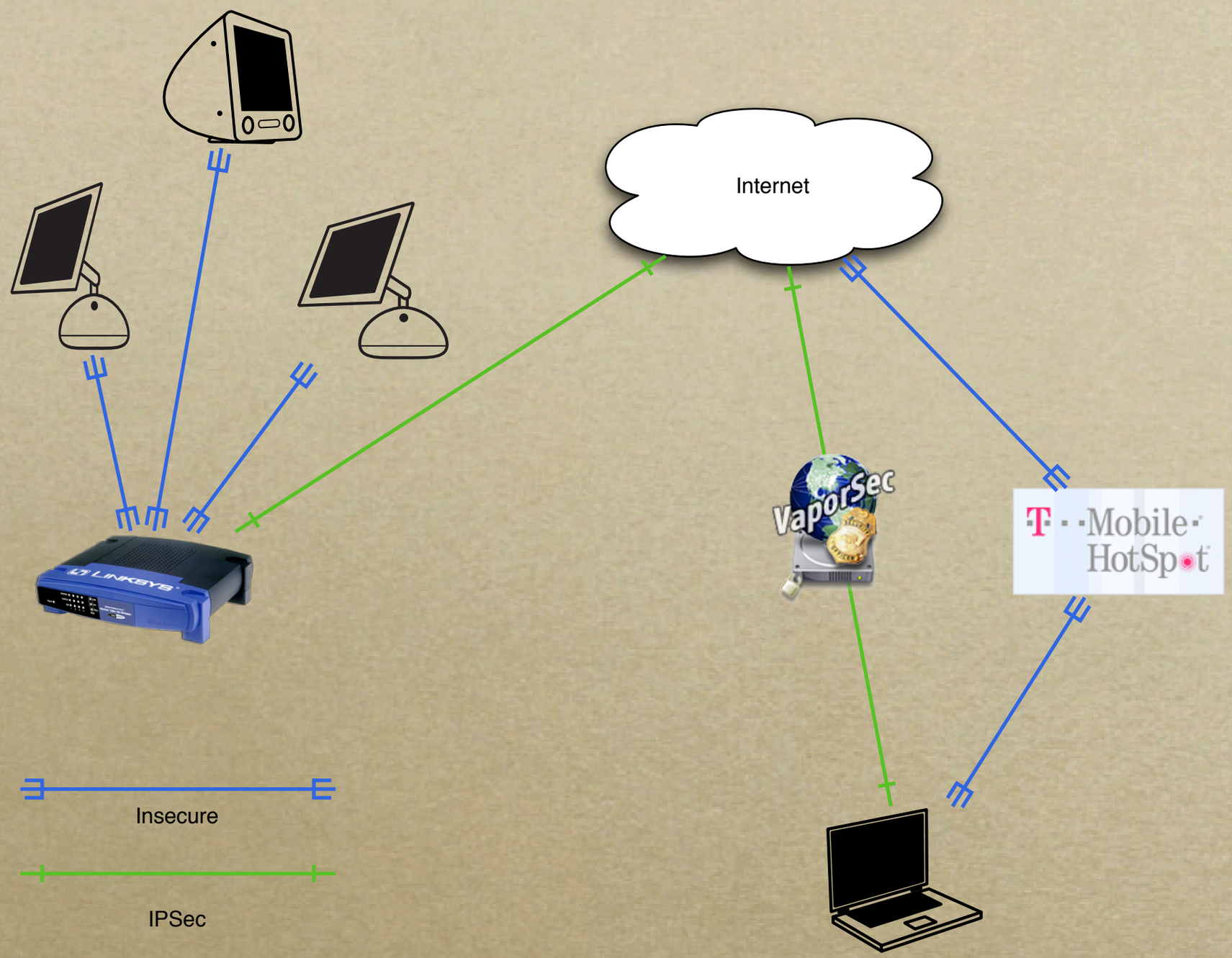
- *Inexpensive VPN Router*
- *IPSec client software*
- *Internet connection that allows IPSec passthrough*

Linksys BEFVP41
$100

Setup

- *Enable ISPec configuration on the router*
- *Configure client software*
- *Test, test, and test some more*
- *VPN from insecure network*

Time To Deploy - 1 hour



Insecure

IPSec

II. Remote Networks

Seamlessly Securing Remote LANs

Equipment

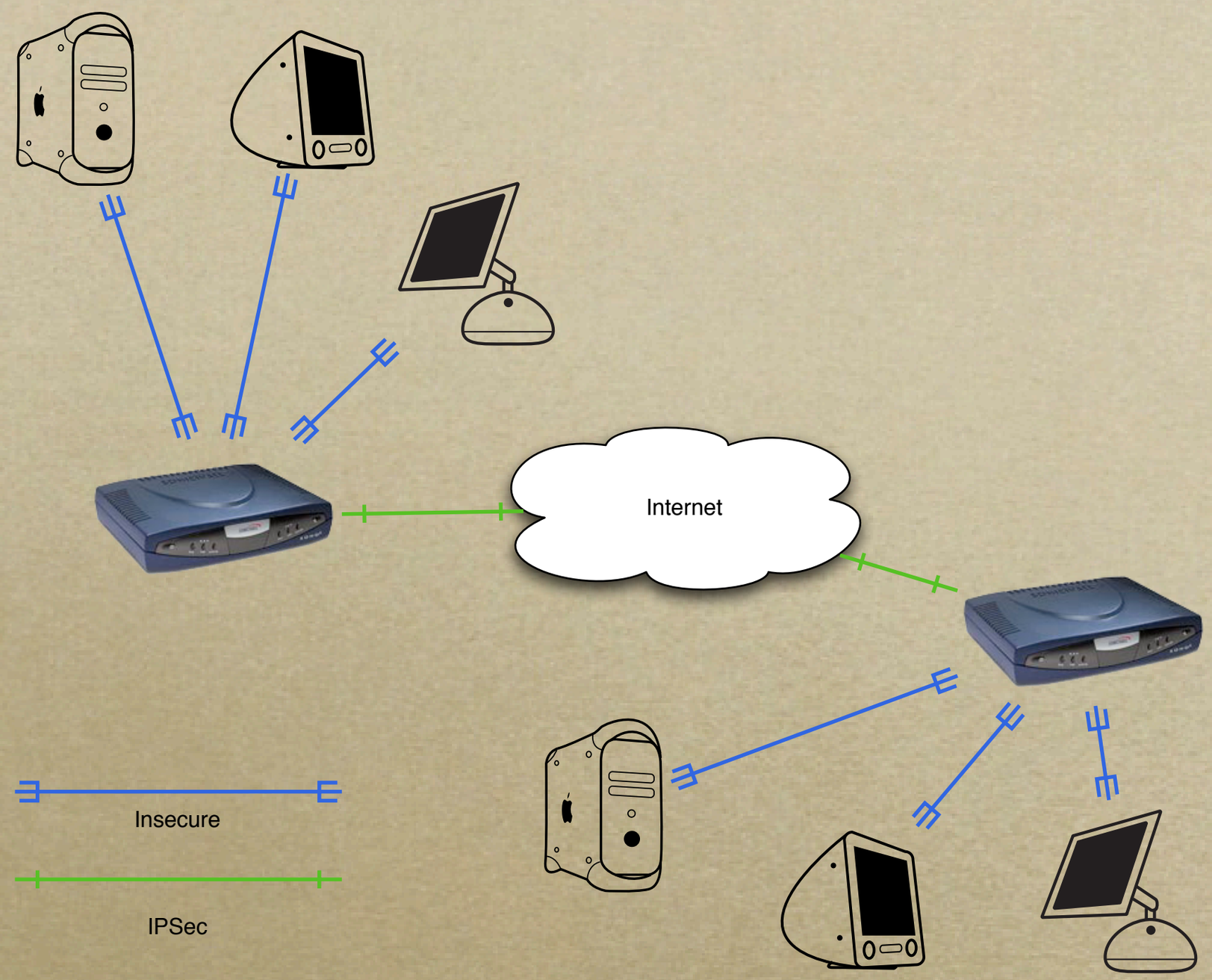
- *VPN Router or IPSec software on NAT gateways*
- *No client-side configuration*

SonicWALL SOHO3
$900

Setup

- *Configure the VPN appliances or gateway machines*
- *Turn it on*
- *Set up discovery services if needed*
- *Connect from client machine as normal*

Time To Deploy - few hours


Internet
Insecure
IPSec

Other Uses

- *Corporate LAN to remote home user - no client software needed*
- *Integrate with remote VPN users also*
- *Can be done entirely in software on OS X*

III. Enterprise

Locking Down Remote Access Users

Equipment

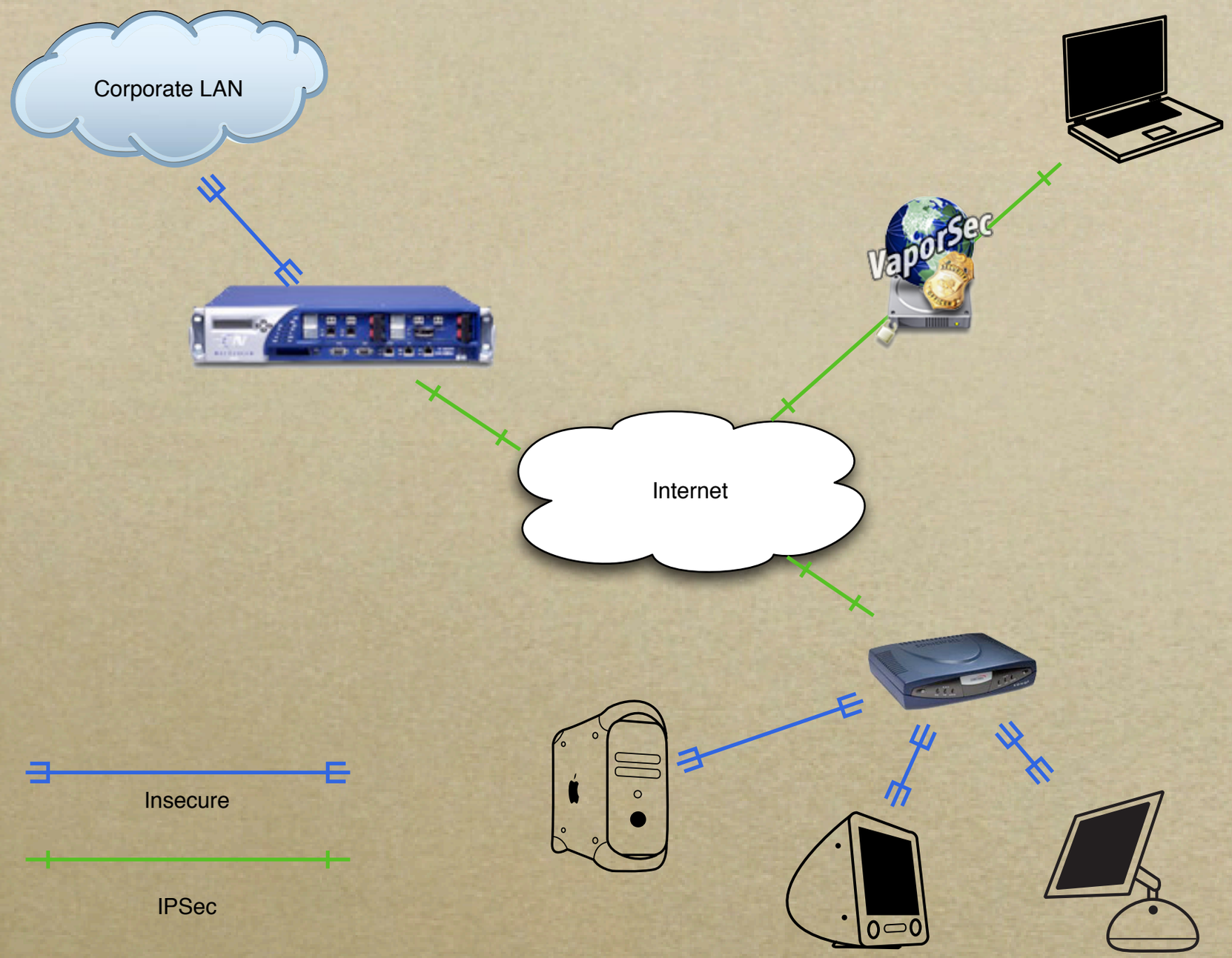
- *Dedicated VPN appliance*
- *Client software*

Netscreen 500
$25,000

Setup

- *Decide on equipment*
- *Test in lab environment*
- *Train admin staff*
- *Train users*
- *Configure clients*
- *Disallow non-encrypted access*

Time To Deploy - 6 mos.


Corporate LAN
VaporSec
Internet
Insecure
IPSec

IV. Wireless

Replacing WEP with IPSec

Equipment

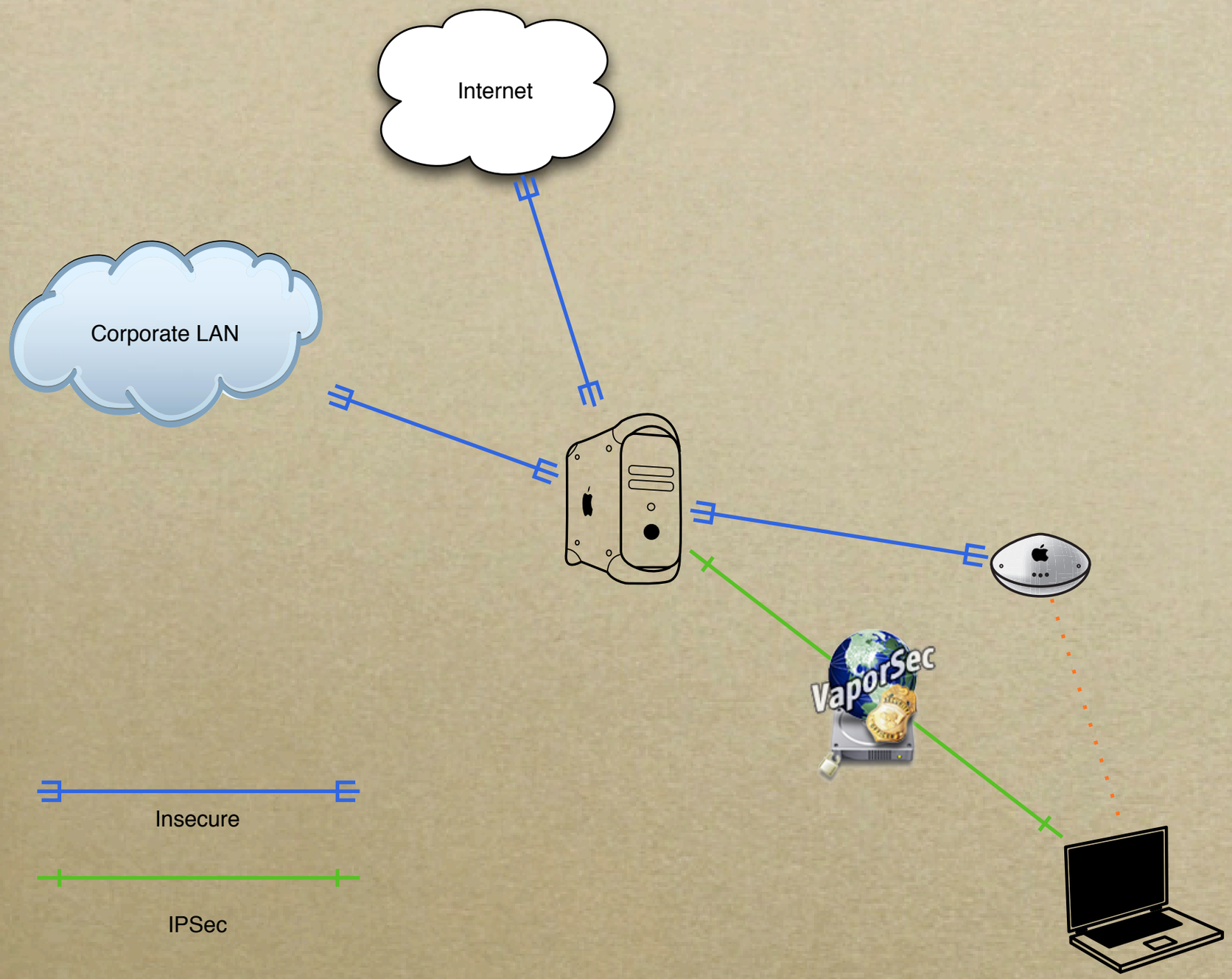
- *Software or hardware gateway*
- *Client software*

OS X Client
$129

Setup

- *Configure Gateway for NAT*
- *Enable IPSec on LAN side of NAT*
- *Use client software or hand configure clients*
- *Disallow insecure connections through NAT*

Time To Deploy - days


Internet
Corporate LAN
VaporSec
Insecure
IPSec

More Resources

- *www.afp548.com/articles*
- *www.kame.net*
- *www.netbsd.org/Documentation/network/ipsec/*
- *Google*

Questions

5. VPN on OS X Server

OSXS VPN Server

- *PPTP or L2TP/IPSec*
- *not IPSec alone*

Configuration

- *Any user can use VPN unless otherwise specified*
- *All client traffic goes across VPN regardless of destination unless specified*
- *Clients use Internet Connect to Connect*

Demo

OS X Server VPN

Questions?

VPN

SSL

Keep it secret, keep it safe

SSL

- *HTTP*
- *LDAP*
- *SMTP*
- *POP/IMAP*

Getting an SSL cert

- *Purchase - about $100/yr*
  - *www.instantssl.com*
  - *www.qualityssl.com*
- *Roll your own*

Roll your own

- *Generate Certificate Authority (CA)*
- *Generate Cert. Signing Request (CSR)*
- *Sign CSR into a Cert*
- *Install Cert*

Demo

OS X Server SSL

S/MIME

- *PKI for e-mail*
- *Similar to SSL certs*
- *Sign and/or Encrypt*

Process

- *Get cert from CA*
- *Install cert into keychain*
- *Send signed e-mail*
- *Receive signed and encrypted reply*
- *Reply signed and encrypted*

Mail.app

Re: Encryption test

Send | Reply All | Chat | Attach | Fonts | Colors | Address | Save As Draft

To: Josh Wisenbaker <josh@computertree.com>

Cc:

Subject: Re: Encryption test

Bcc:

Account: Joel Rennich <mactroll@afp548.com>

On Nov 1, 2003, at 5:50 PM, Josh Wisenbaker wrote:

> Just checking the encryption feature too. Can you read this?
>
> Josh
>
> -
> Josh Wisenbaker
> Sr. Systems Engineer
> ComputerTree Technologies
> 1-800-467-9820

Show Details

From: Josh Wisenbaker <josh@computertree.com>
Subject: **Encryption test**
Date: November 1, 2003 5:50:46 PM EST
To: Joel Rennich <mactroll@afp548.com>
Security: Encrypted, Signed

Just checking the encryption feature too. Can you read this?

Josh

-
Josh Wisenbaker
Sr. Systems Engineer
ComputerTree Technologies
1-800-467-9820

OK

Questions?

SSL

Sniffing

Listening on the wire

Packet Sniffing

- *very hard to detect*
- *very easy to do*
- *intercepts packets going across the network*

tcpdump

- *most basic form of packet sniffing*
- *installed by default on OS X*
- *all CLI*

Demo

tcpdump

Ethereal

- *Open Source*
- *free*
- *X11 GUI*
- *powerful*

Demo

Ethereal

Other sniffers

- *Etherpeek*
- *tcpflow*

How to protect yourself

- *use switches not hubs*
- *secure your protocols - SSL*
- *secure your network - VPN*

Questions?

Packet Sniffing

Thanks!

Joel Rennich

www.afp548.com
mactroll@afp548.com