Phil Steen

Phil is a Senior Solutions Architect at 318, Inc., a Santa Monica-based IT consulting firm focused on helping clients grow profitably through the smart use of technology. He started his career as a video editor and got into supporting Apple products while working as a Mac Genius, then moving on to 318, where he has been for almost 9 years.

Phil lives in Nashville, Tennessee with his wife and daughter and enjoys working on cars and 4x4ing in his time away from technology.

Caching Server,
DNS Tricks, and More

What is Caching Server?

- Stores copies of Apple-distributed software and updates on a local server. This allows clients to pull them over the local network as opposed to over the internet, thereby conserving bandwidth as well as speeding up the download process for the end user.

What is Cached?

	OS X ≥10.8.2	iOS ≥ 7	Apple TV
Software Updates	☑	☑	☑
App Store	☑	☑	NA
iBooks	☑	☑	NA
Internet Recovery	☑	NA	☑
iTunes Media	☑	☑	NA

How Caching Server Works

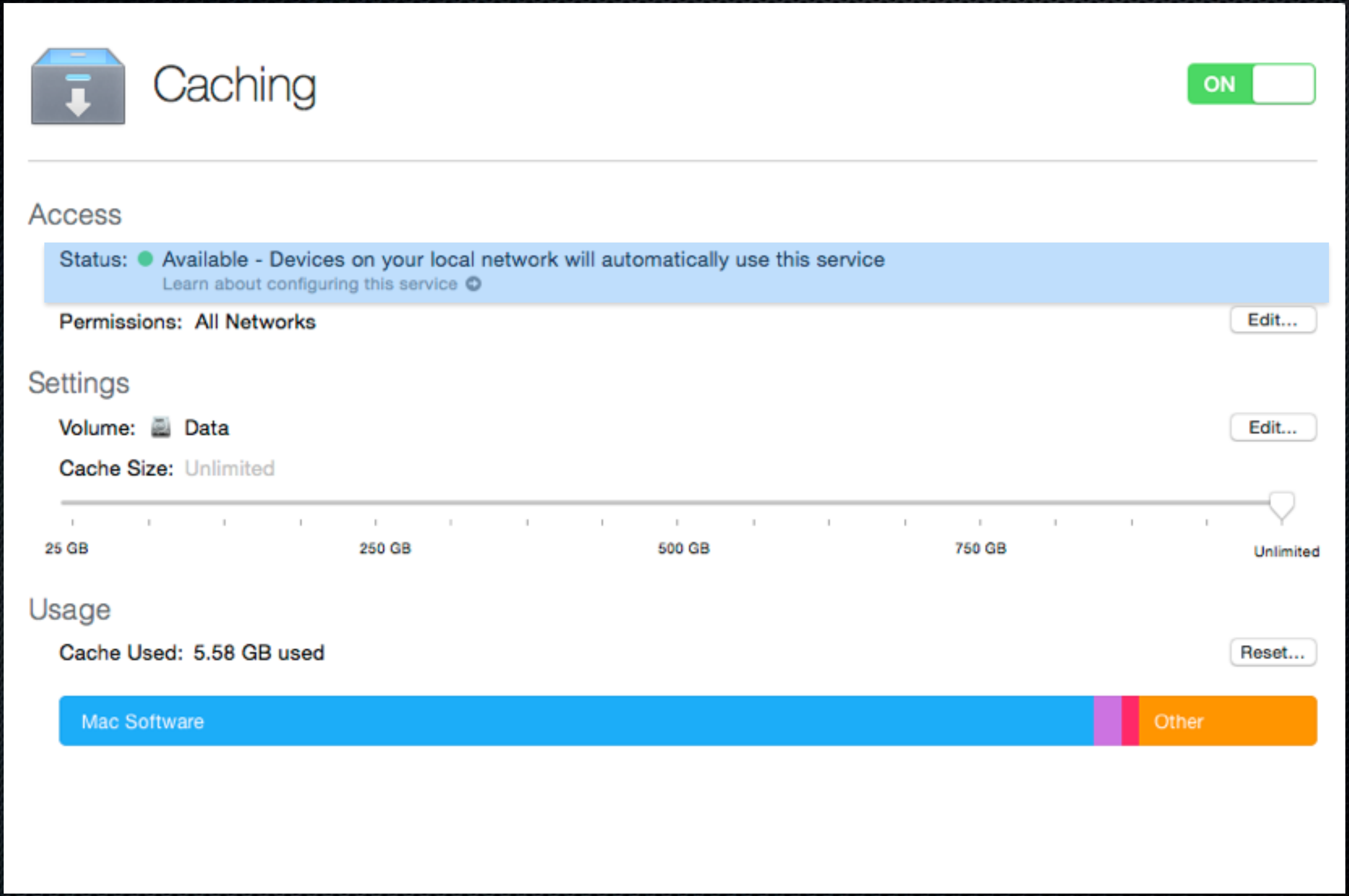
- Server registers the configured or discovered IP addresses with Apple
- The first requested download is always pulled from Apple and is then cached to the server
- Later downloads come from the server
- The server may have peers on the same network
- Clients always fallback to download directly from Apple if a local caching server can’t be reached

How Caching Server Works

- The Good:
  - No client-side configuration needed
  - Very little server configuration needed
  - Servers *may* work together as automatic peers
  - New features allow for more control over service
- The Bad:
  - Relies upon IP addressing not DNS
  - Challenging to work with IP load balancing
  - No built in pre-downloading; caching occurs as packages are requested by clients
  - No control over what is cached

- The Catch:
  - Some installs will require internal DNS TXT records

Easy Setup



Access

Status: Available - Devices on your local network will automatically use this service

Learn about configuring this service

Permissions: All Networks

Settings

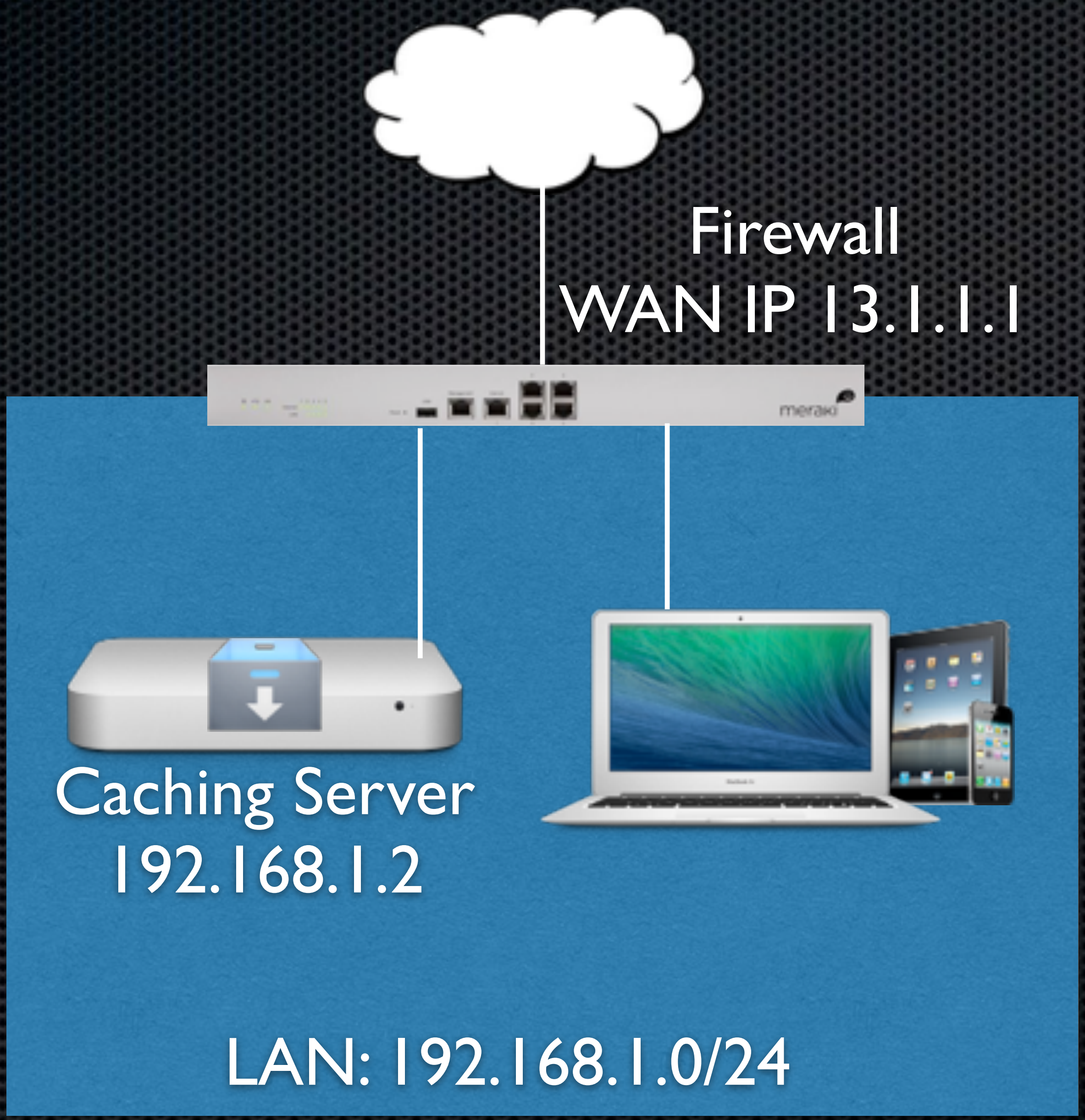
Volume: Data

Cache Size: Unlimited

Usage

Cache Used: 5.58 GB used

Scenarios - SOHO Network



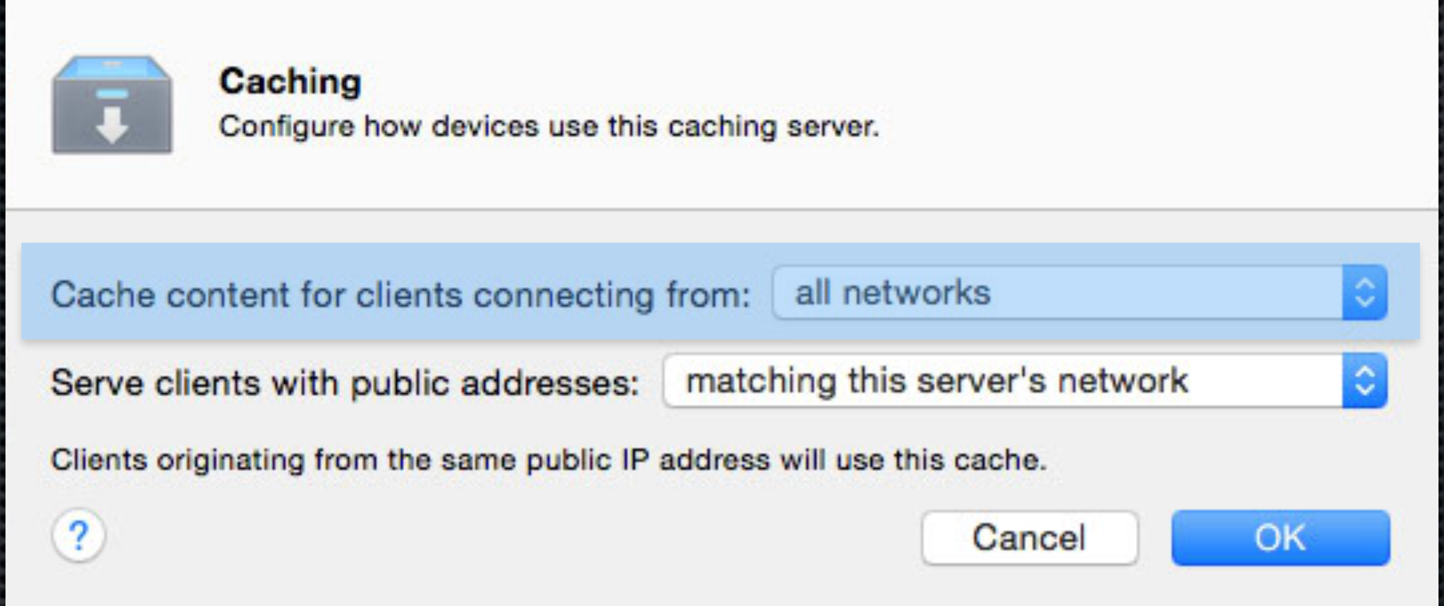
Firewall
WAN IP 13.1.1.1

Caching Server
192.168.1.2

LAN: 192.168.1.0/24

MACTECH PRO EVENTS

Scenarios - SOHO Network



Caching

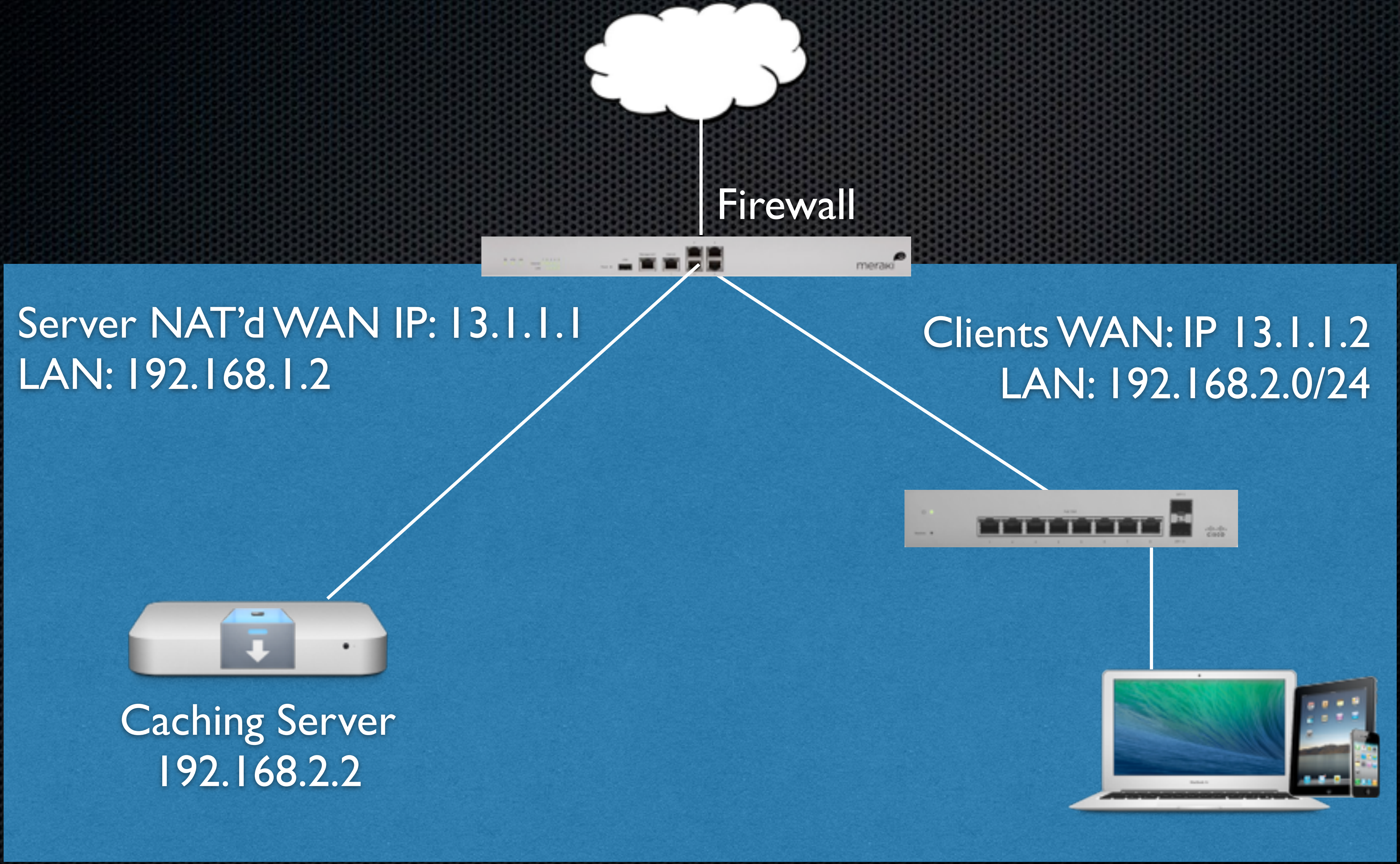
Configure how devices use this caching server.

Cache content for clients connecting from: all networks

Serve clients with public addresses: matching this server's network

Clients originating from the same public IP address will use this cache.

Scenarios - Multiple Public IPs



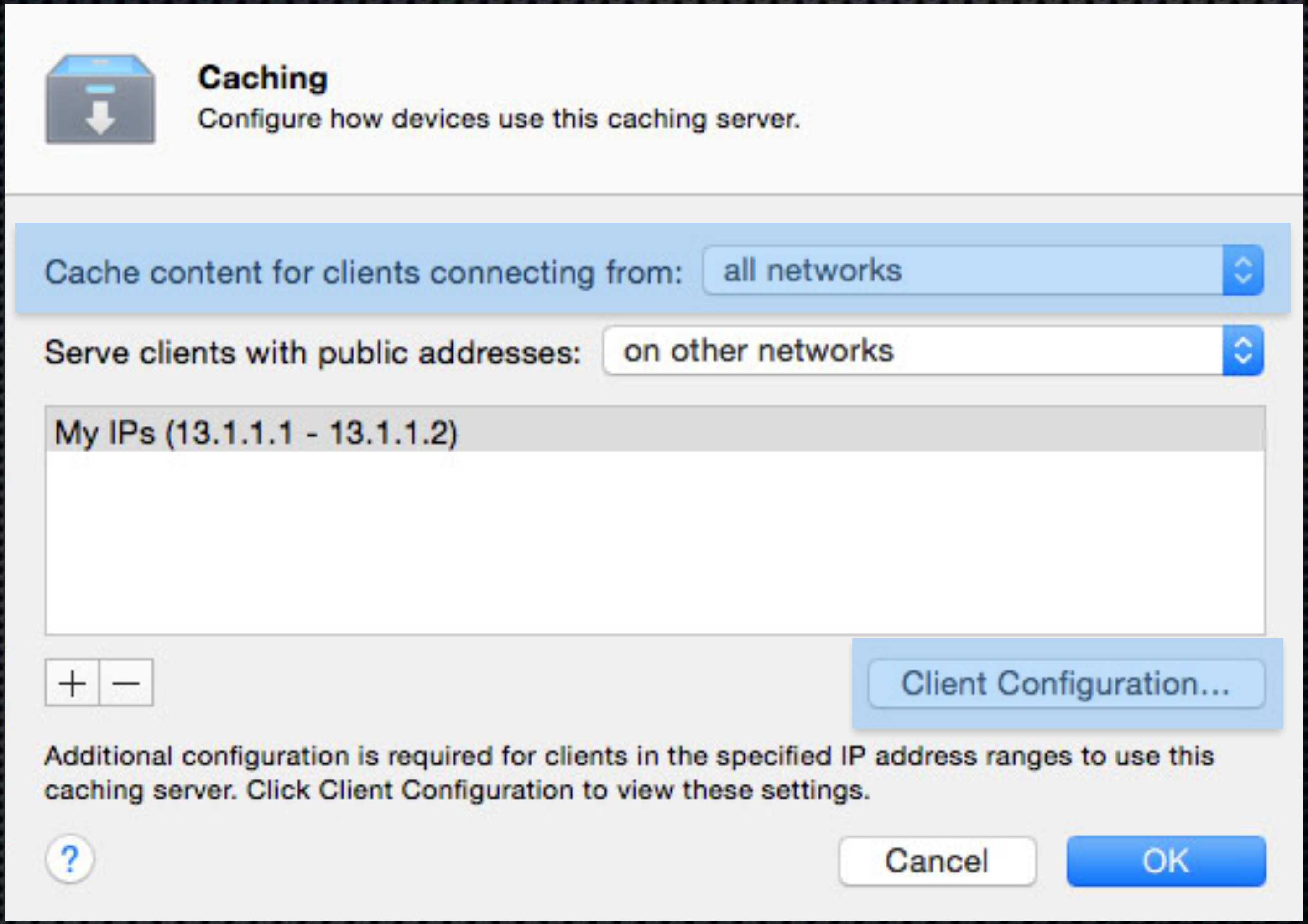
Firewall

Server NAT'd WAN IP: 13.1.1.1
LAN: 192.168.1.2

Clients WAN: IP 13.1.1.2
LAN: 192.168.2.0/24

Caching Server
192.168.2.2

Scenarios - Multiple Public IPs



Caching

Configure how devices use this caching server.

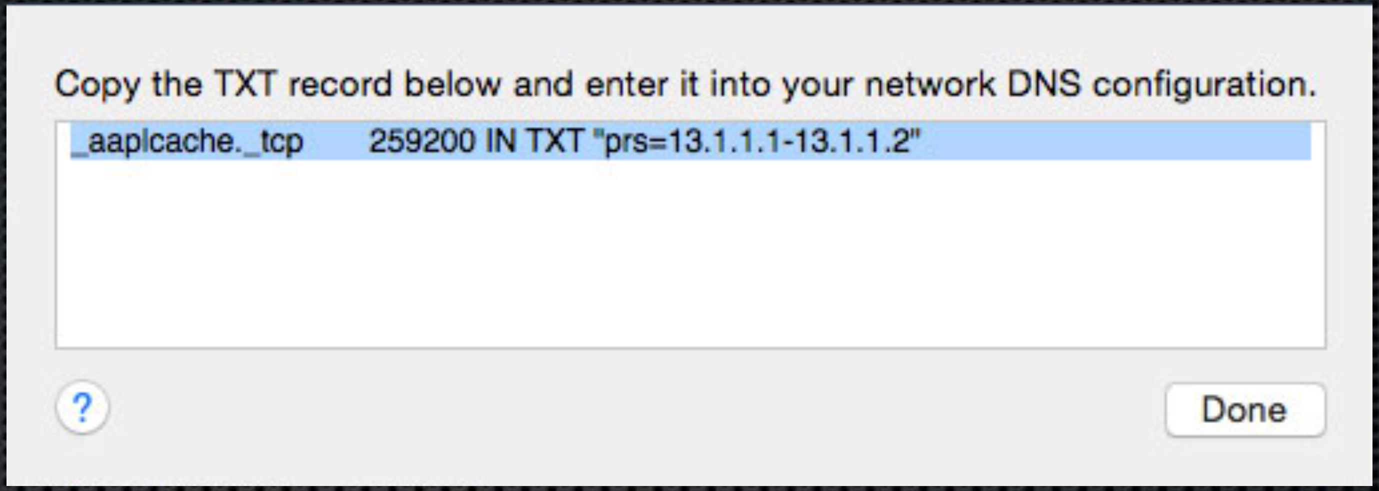
Cache content for clients connecting from: all networks

Serve clients with public addresses: on other networks

My IPs (13.1.1.1 - 13.1.1.2)

Additional configuration is required for clients in the specified IP address ranges to use this caching server. Click Client Configuration to view these settings.

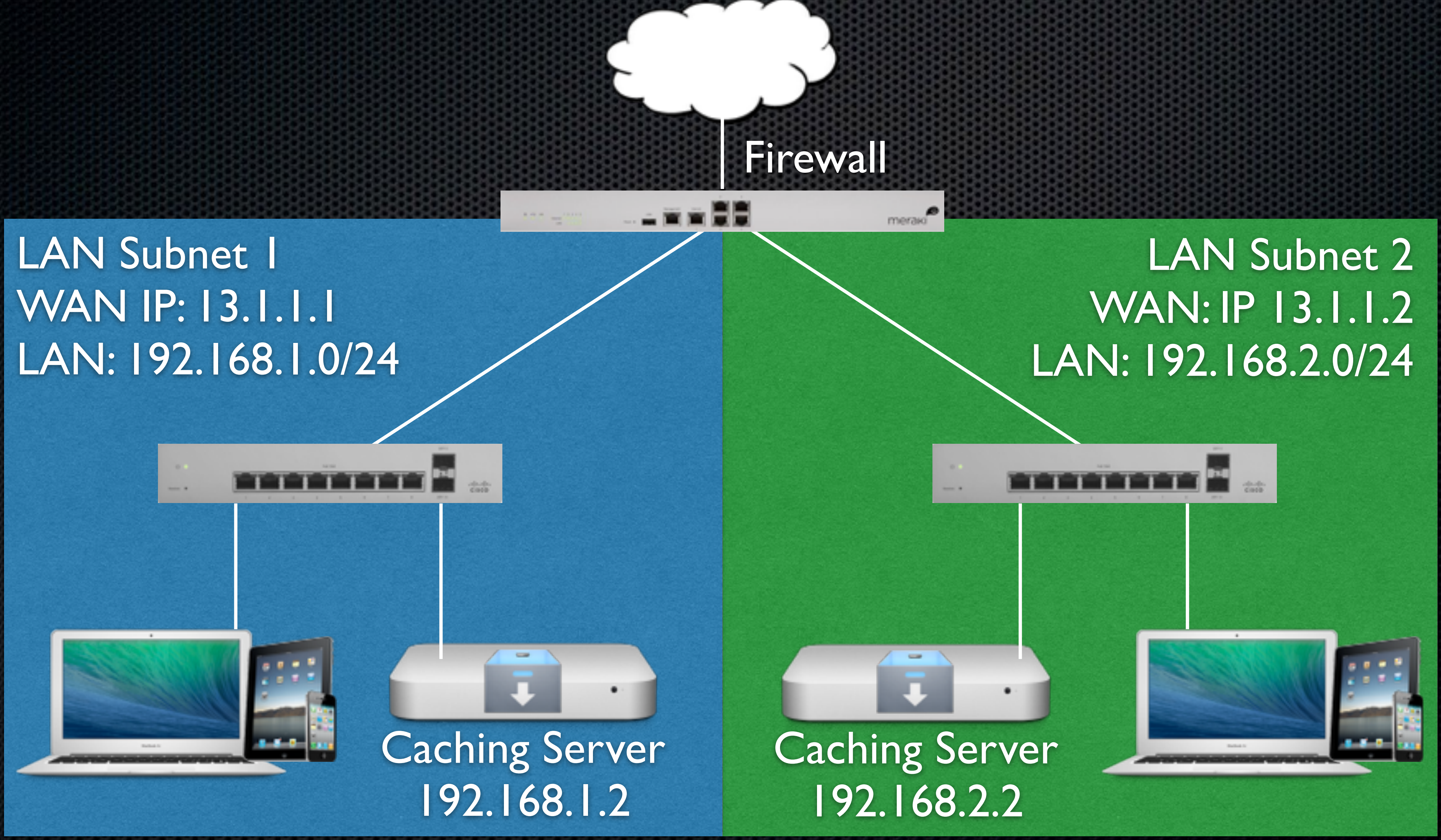
Scenarios - Multiple Public IPs



Copy the TXT record below and enter it into your network DNS configuration.

```
_aaplcache._tcp       259200 IN TXT "prs=13.1.1.1-13.1.1.2"
```

Scenarios - Multiple Public IPs with Multiple Caching Servers



Firewall

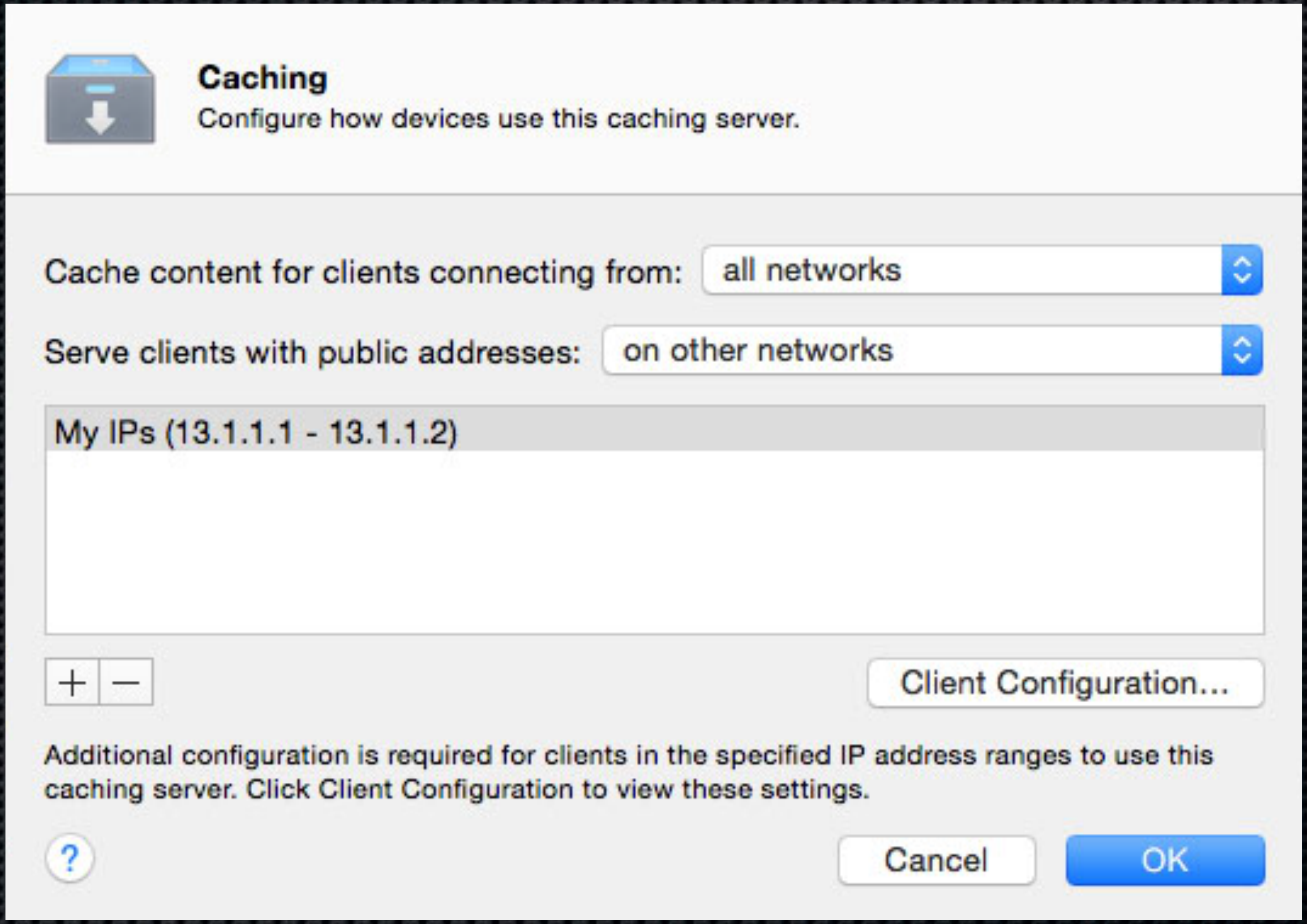
LAN Subnet 1
WAN IP: 13.1.1.1
LAN: 192.168.1.0/24

LAN Subnet 2
WAN: IP 13.1.1.2
LAN: 192.168.2.0/24

Caching Server
192.168.1.2

Caching Server
192.168.2.2

Scenarios - Multiple Public IPs with Multiple Caching Servers



Caching

Configure how devices use this caching server.

Cache content for clients connecting from: all networks

Serve clients with public addresses: on other networks

My IPs (13.1.1.1 - 13.1.1.2)

Additional configuration is required for clients in the specified IP address ranges to use this caching server. Click Client Configuration to view these settings.

Caching in "non-NAT networks"

- Configure server to use static LAN IP address (must be wired)
- Configure caching service with public range of IPs
- Copy TXT record from Server.app
- Add TXT record to db zone file: /Library/Server/named/db.domain
  - caching.apple.com zone (Server Essentials)
    - create a www host A record
    - _aaplcache._tcp.caching.apple.com TXT entry
  - your own domain zone (Advanced Server Help)
    - _aaplcache._tcp.<domain name> TXT entry
- These settings must be on the client-facing DNS server!

Caching in “non-NAT networks”

- Confirm Creation
  - dig _aaplcache._tcp.yourdomain.com. txt
  - or dig _applcache.tcp.caching.apple.com. txt
- Only use your domain if it is part of default Search Domains configured on clients, otherwise use caching.apple.com as the zone.

Advanced Options

- Not available in the GUI
  - Interface
  - LogClientIdentity
  - LogLevel
  - MaxConcurrentClients
  - MaxPeersToQuery
  - OriginDownloadTimeout
  - PeerDownloadTimeout
  - PeerFilterRanges
  - PeerNotifyTimeout
  - PeerQueryTimeout
  - PeerRetryInterval
  - Port
  - ReservedVolumeSpace

- Set via serveradmin settings caching: command

Advanced Options

- Interface - The BSD name of a network interface to be used by Caching service. Default listen on all.
- Port - The TCP port number on which Caching service accepts requests for downloads. Default is random port.
- LogClientIdentity - Determines whether or not the server should log the IP address and port number of the client requesting each asset. Default false.
- LogLevel - default, off, error, warn, info, verbose.

Logging Service

Sample log entry confirming caching functional:
(/Library/Server/Caching/Logs/Debug.log)

```
Apr  2 12:30:48 enterprise.starfleet.gov AssetCache[167]: #h5v6IzNuHHyE
25.0 MB of 25.0 MB served, 25.0 MB from cache, 0 bytes downloaded
from origin, 0 bytes from peers
```

DNS

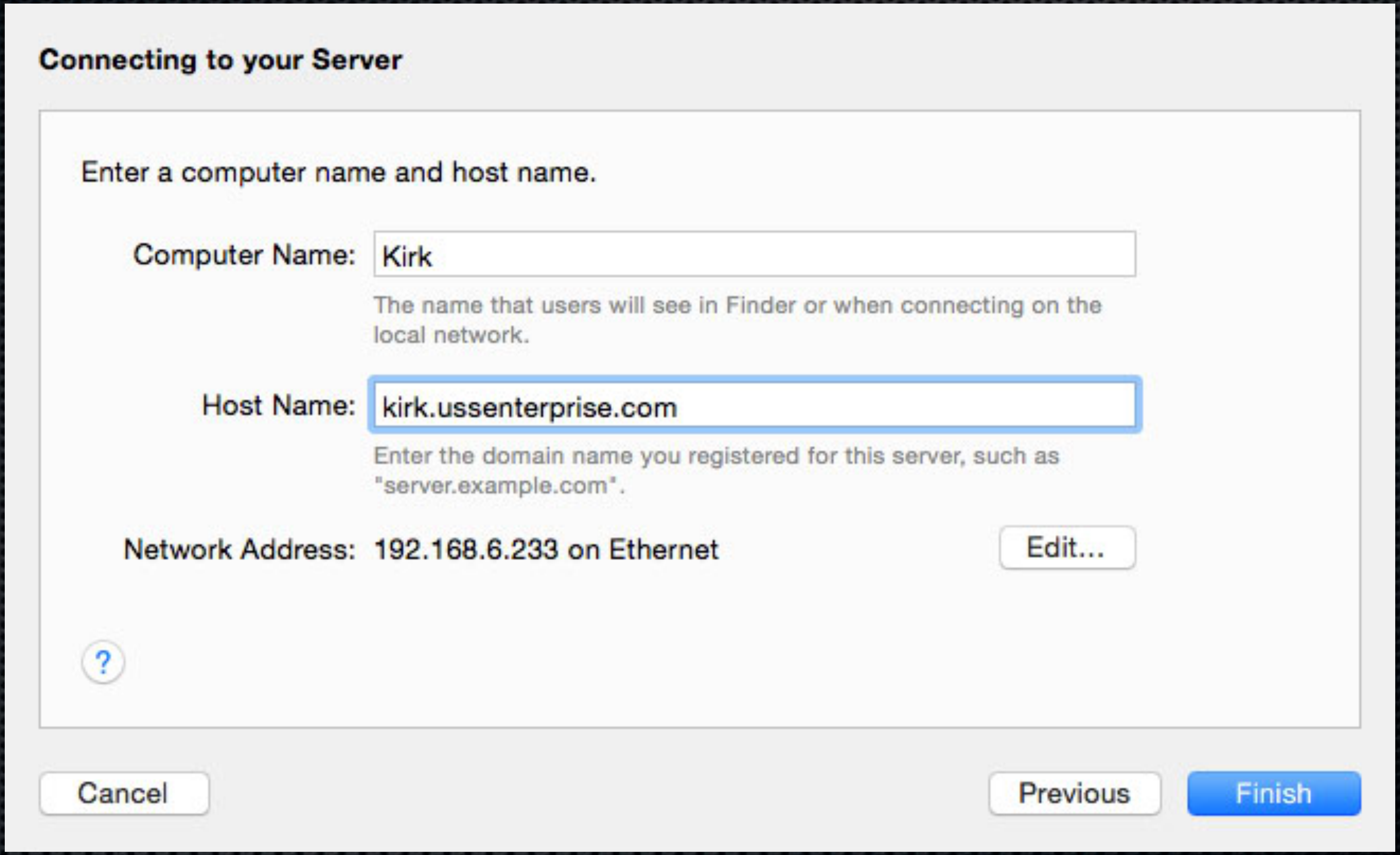
Proper Configuration of DNS

- Previously, DNS records and server hostname needed to be matched before server install and configuration
- Typical tricks included:
  - Bribing or threatening the DNS administrator
  - Self resolution just for changeip -checkhostname
- Now (since 10.7) when configuring a server:
  - If reverse DNS mismatches, Server.app auto-creates minimal DNS
  - Also happens when changing the server hostname if DNS resolution is not available

…Minimal DNS

- A DNS Zone in which the configured hostname of the server matches the zone domain
- ONLY ENTRIES are related to the server you are setting up!
- Limits future expansion - domain itself is server.domain.com

Minimal DNS



Connecting to your Server

Enter a computer name and host name.

Computer Name: Kirk

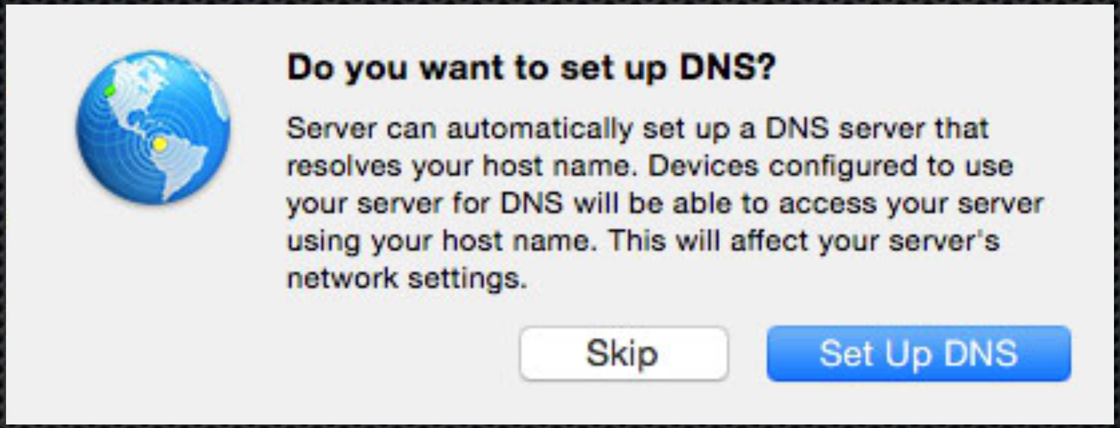
The name that users will see in Finder or when connecting on the local network.

Host Name: kirk.ussenterprise.com

Enter the domain name you registered for this server, such as "server.example.com".

Network Address: 192.168.6.233 on Ethernet

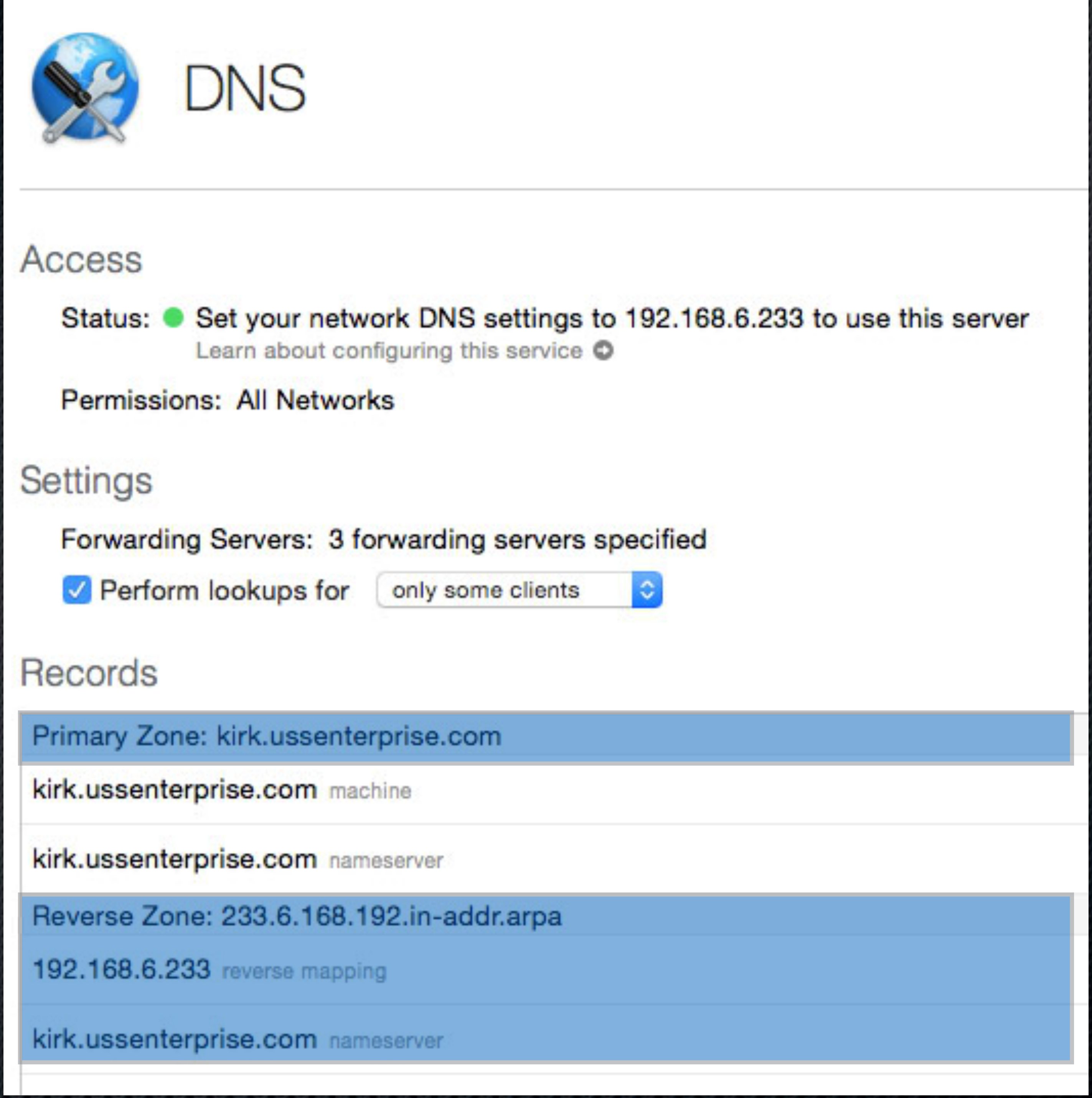
Minimal DNS



Do you want to set up DNS?

Server can automatically set up a DNS server that resolves your host name. Devices configured to use your server for DNS will be able to access your server using your host name. This will affect your server's network settings.

Minimal DNS



DNS

Access

Status: ● Set your network DNS settings to 192.168.6.233 to use this server

Learn about configuring this service

Permissions: All Networks

Settings

Forwarding Servers: 3 forwarding servers specified

☑ Perform lookups for only some clients

Records

Primary Zone: kirk.ussenterprise.com

kirk.ussenterprise.com machine

kirk.ussenterprise.com nameserver

Reverse Zone: 233.6.168.192.in-addr.arpa

192.168.6.233 reverse mapping

kirk.ussenterprise.com nameserver

Minimal DNS

- Is this good or bad? Depends upon your environment.
- Do you have control of your DNS records for your server's IP address?
- Probably good for "islands" of Macs in PC/Windows organizations with no internal resolution necessary.
- Probably OK for SOHO with minimal local services or where clients will not be looking at server for DNS

Proper Configuration of DNS

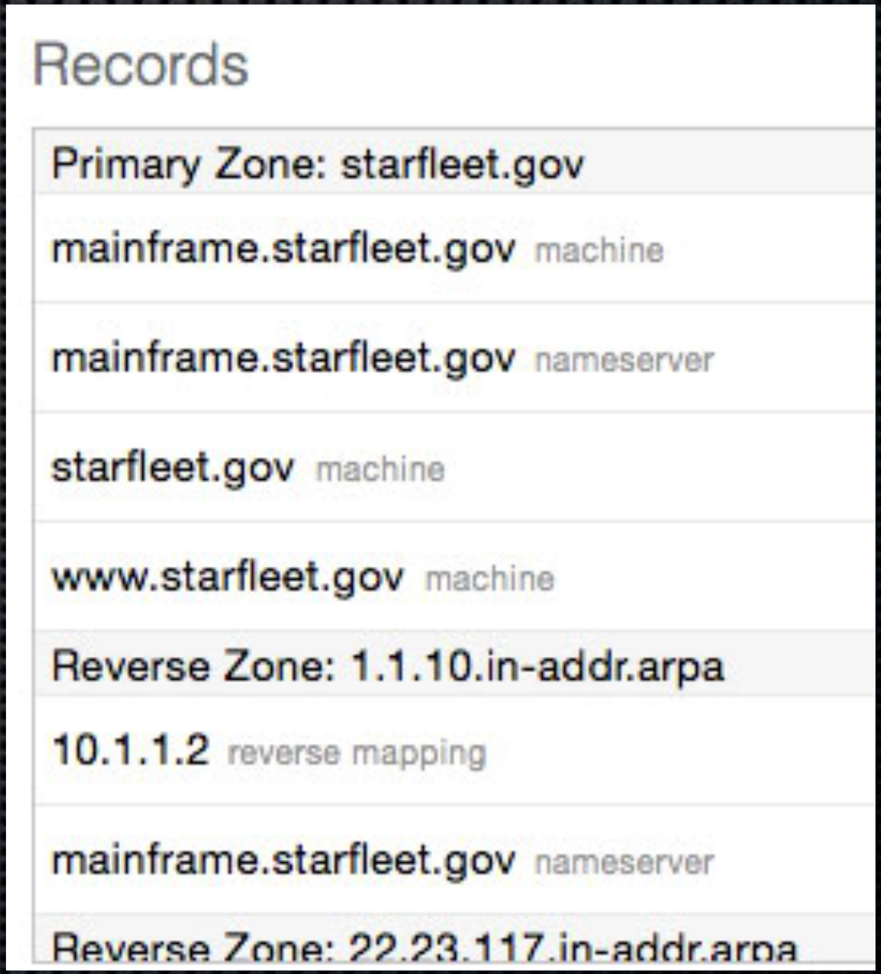
- Plan DNS in advance!
- When configuring DNS, create an A record (machine record) for the primary DNS server first as initial host record creates NS record as well
- Most OS X DNS Servers are *not* publicly accessible
  - Just don't do it man!

DNS Planning

- What services are hosted internally vs. externally?
- Will my records need to resolve externally AND internally?
- How many external resources use company domain name for access?
- Based on above, we need to choose top-level domain, subdomain, or private domain. (Hint… subdomain or private domain are easier to maintain)

DNS - Top Level Domain

- Example Zone - starfleet.gov
- Requires you to align both internal and external DNS records - you will need to make www and @ records for your website to function internally, same for any other externally hosted resources using company domain name (think of the CNAME and MX records!)
- Allows wildcard SSL certificate use for both public and private servers



Records

Primary Zone: starfleet.gov

mainframe.starfleet.gov machine

mainframe.starfleet.gov nameserver

starfleet.gov machine

www.starfleet.gov machine

Reverse Zone: 1.1.10.in-addr.arpa

10.1.1.2 reverse mapping

mainframe.starfleet.gov nameserver

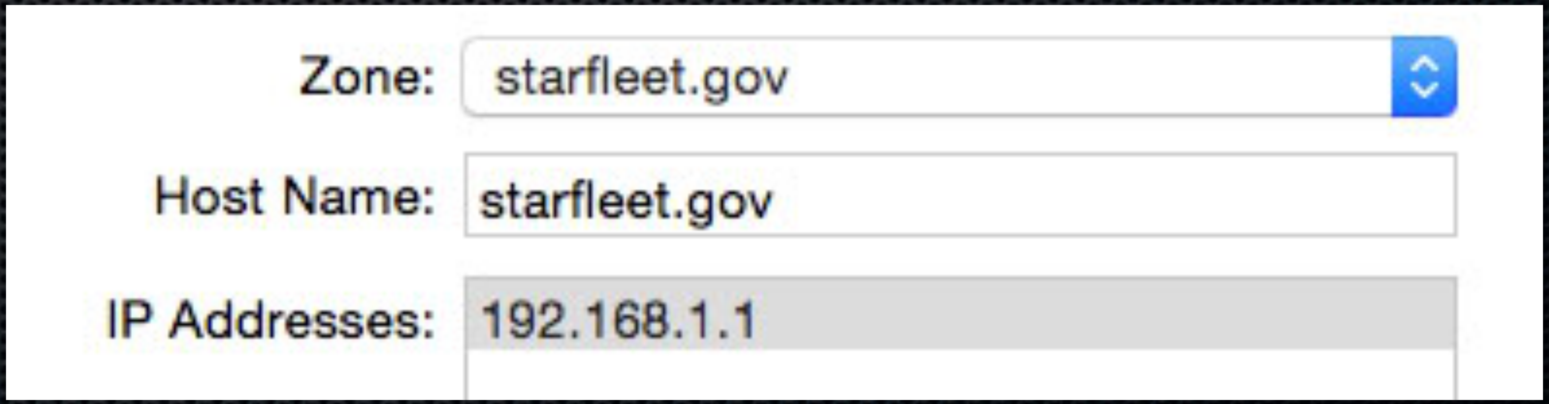
Reverse Zone: 22.23.117.in-addr.arpa

DNS - Top Level Domain

HOT TIP!

It is not obvious how to create an A record for the zone name in Server.app:

- Usually identified as @ or domain.com. (note trailing period)
- But Apple doesn't follow this standard
- To create one, make an A record for the zone in question and in the machine name, type the zone name:



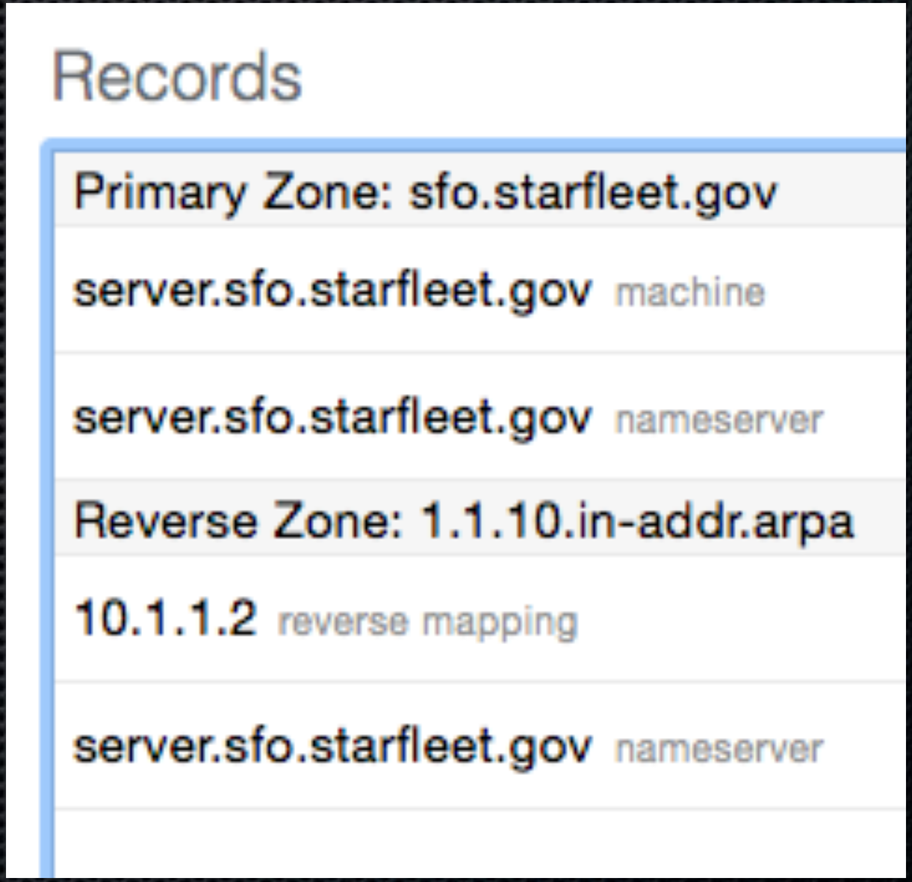
Zone: starfleet.gov

Host Name: starfleet.gov

IP Addresses: 192.168.1.1

DNS - Subdomain

- Example Zone - sfo.starfleet.gov
- Allows internal and external resolution with minimal duplicative configuration
- Allows wildcard SSL certificate use for both public and private servers
- For security, ONLY create public records for publicly accessible resources (in some instances your internal DNS will have more records than external)



Records

Primary Zone: sfo.starfleet.gov

server.sfo.starfleet.gov machine

server.sfo.starfleet.gov nameserver

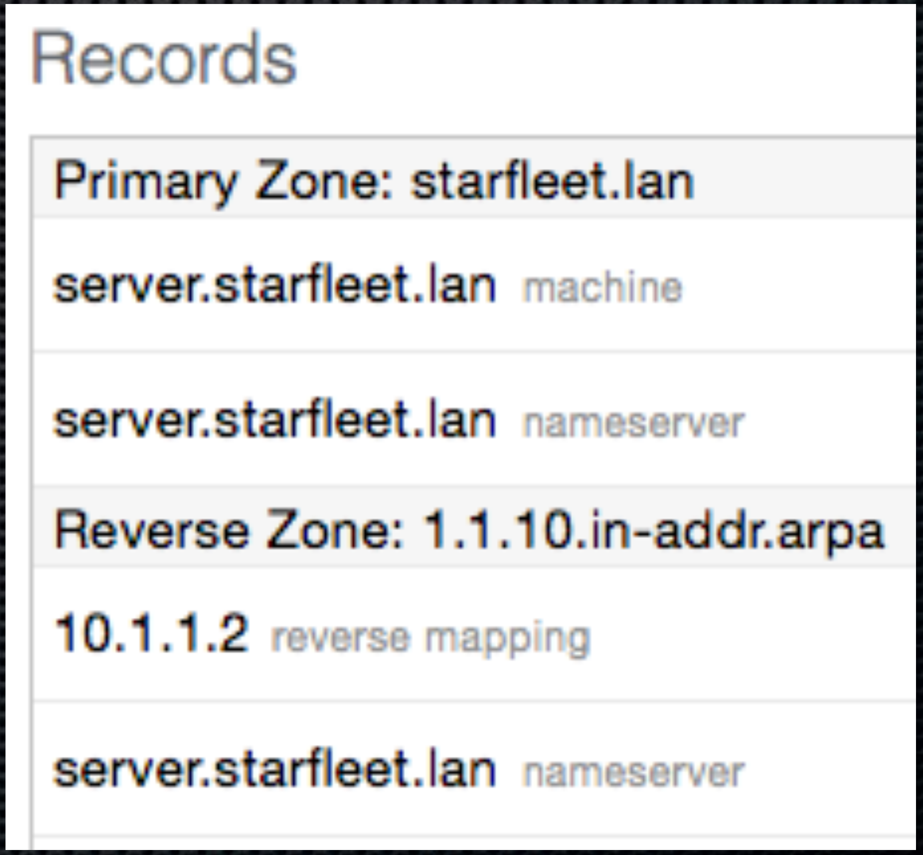
Reverse Zone: 1.1.10.in-addr.arpa

10.1.1.2 reverse mapping

server.sfo.starfleet.gov nameserver

DNS - Private Domain

- Example Zone - starfleet.lan
- Generally not publicly routable
- Most commonly seen in private or segmented networks with no external resolution necessary (think Xsan or Mac islands in PC corporations)
- Requires separate SSL certificates
- DO NOT USE .LOCAL…



Records

Primary Zone: starfleet.lan

server.starfleet.lan machine

server.starfleet.lan nameserver

Reverse Zone: 1.1.10.in-addr.arpa

10.1.1.2 reverse mapping

server.starfleet.lan nameserver

DNS Tricks and Approaches

- Multiple A records per IP address (crude load balancing)
- Primary & Secondary DNS Server configuration
  - Primary Zone -"allow zone transfers"
  - Secondary Zone -"Add Secondary Zone…"
  - Don't forget the reverse zone too!
- An Open Directory Replica is a good candidate for a Secondary DNS server because directory services relies upon DNS…

Quick Topic:
Enhancing Server Performance

Enhance Server Performance

- Link aggregation
    - Thunderbolt Ethernet or SmallTree
    - Create new Virtual Interface, add physical
    - Requires link aggregation configuration on switch!
- Access Controls to limit access by
    - Networks
    - Users/Groups
- Apple’s content servers apparently are in the range: 17.173.66.1-17.173.66.254 so prioritize traffic.

More Resources

- Built in Server app help (links in every service)
- http://help.apple.com/advancedserveradmin/mac/4.0
- Support Articles: HT200231, HT202657, PH15567
- https://www.yesdevnull.net/tag/caching/
- http://blog.fraserhess.com/2014/10/caching-server-enterprise-edition.html

Products

- CacheWarmer ($4.99) by Glencode LLC - http://blog.fraserhess.com/2014/12/introducing-cachewarmer.html

Questions?

Phil Steen

psteen@318.com