what's in a name?

taking a deeper look at the domain name system

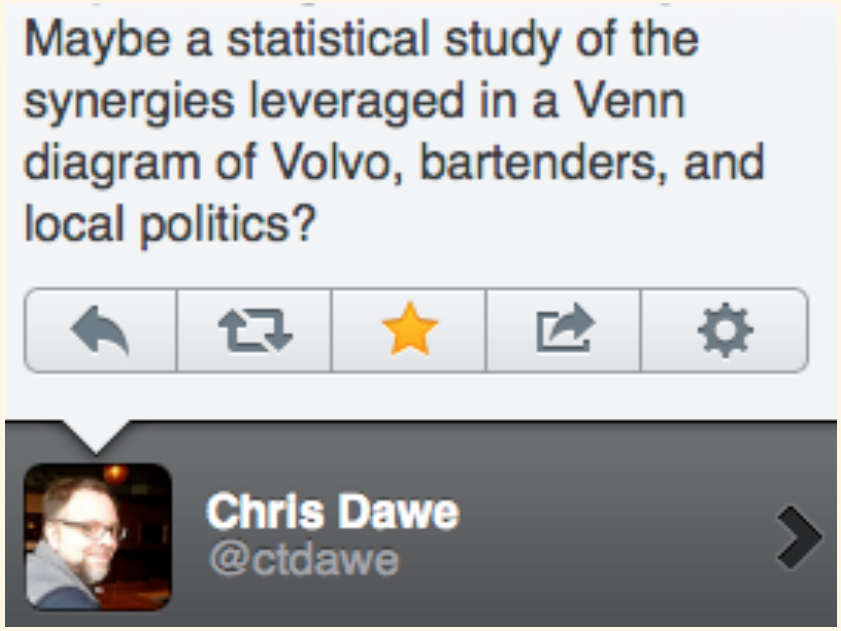
mike boylan
penn state mac admins conference

whoami

work for robert morris university, pittsburgh, pa

primarily mac and voip admin

@mboylan on twitter



the rundown

dns in a nutshell

common dns scenarios

troubleshooting dns

dns in os x server

dns in a nutshell

architecture and concepts, explained

dns is the phonebook of the internet

dns is the phonebook of the internet

at the most basic level, it turns names into numbers and numbers into names


user types apple.com into browser


apple.com translated to 17.172.224.47


networking stuff happens...

apple.com loads in the browser

apple.com translated to 17.172.224.47

how?

so much stuff!

queries

resolvers

nameservers

resolution from root

caching

zones and records

delegations

forwarding

queries

queries

“at what address is apple.com located?”

two main types of queries...

recursive query

recursive query

usually made by a client host (your mac)

asking dns server for an answer or...

please kindly return an error if you don’t know

iterative query

iterative query

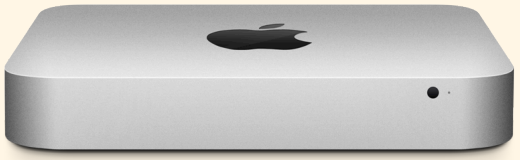
usually made by dns servers

return the best answer you have or...

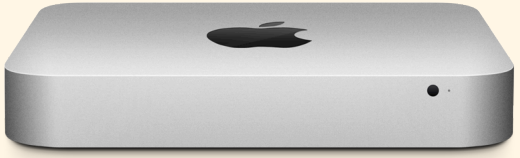
please refer me to an authoritative source

simple illustration

rmu nameserver

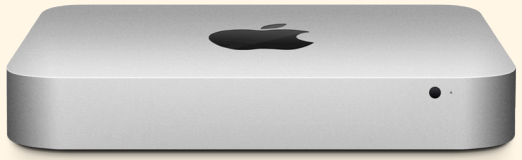


rmu nameserver



www.rmu.edu?

rmu nameserver

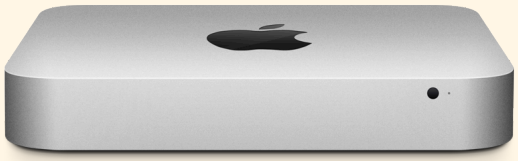


www.rmu.edu?

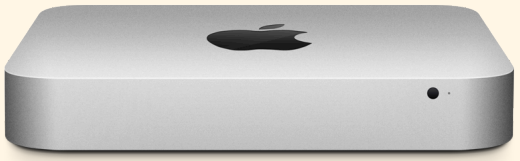
66.206.178.109

“walking the tree”

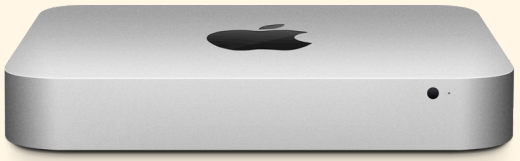
rmu server



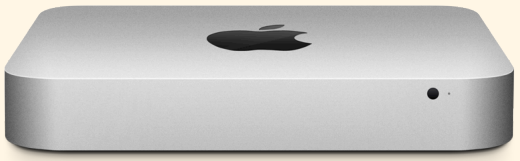
root server

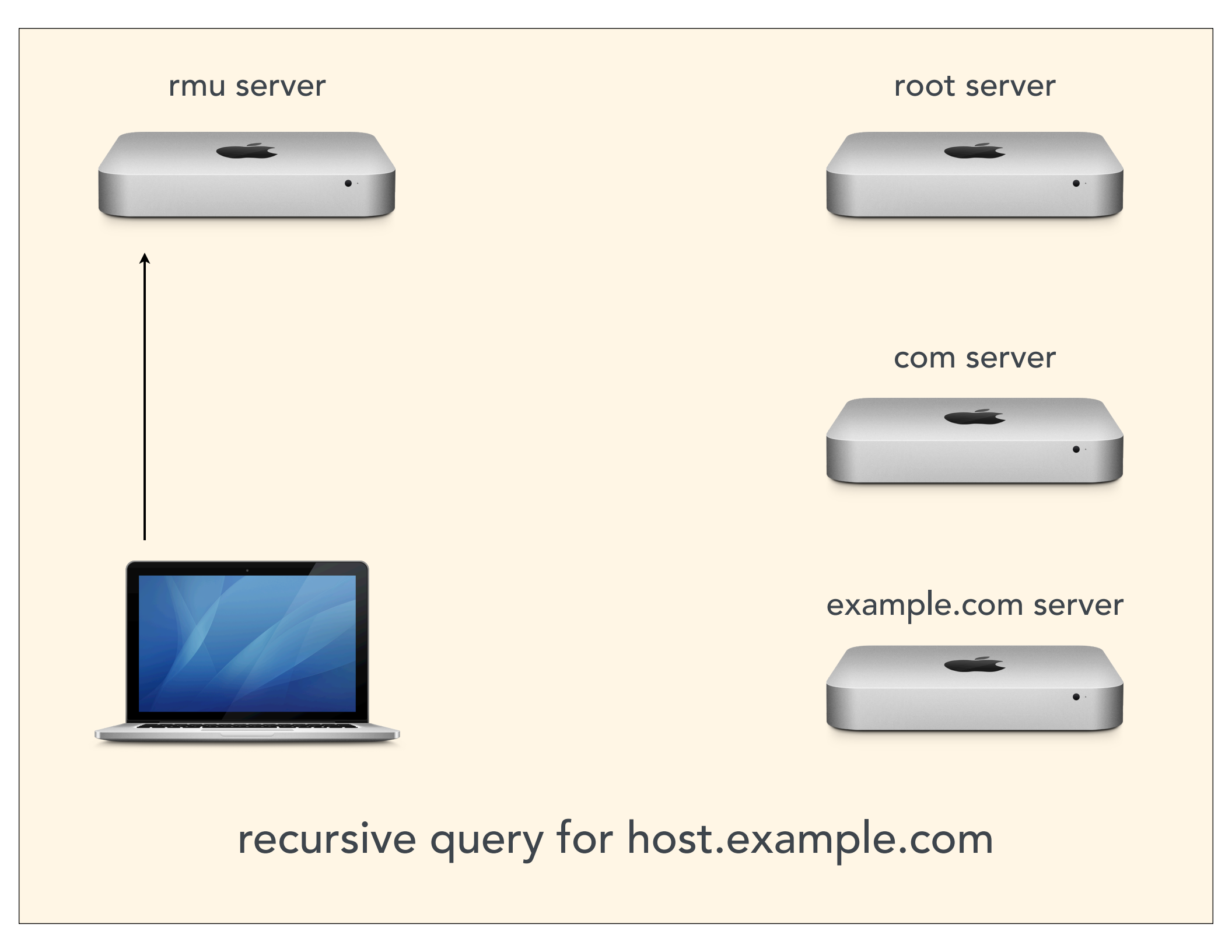


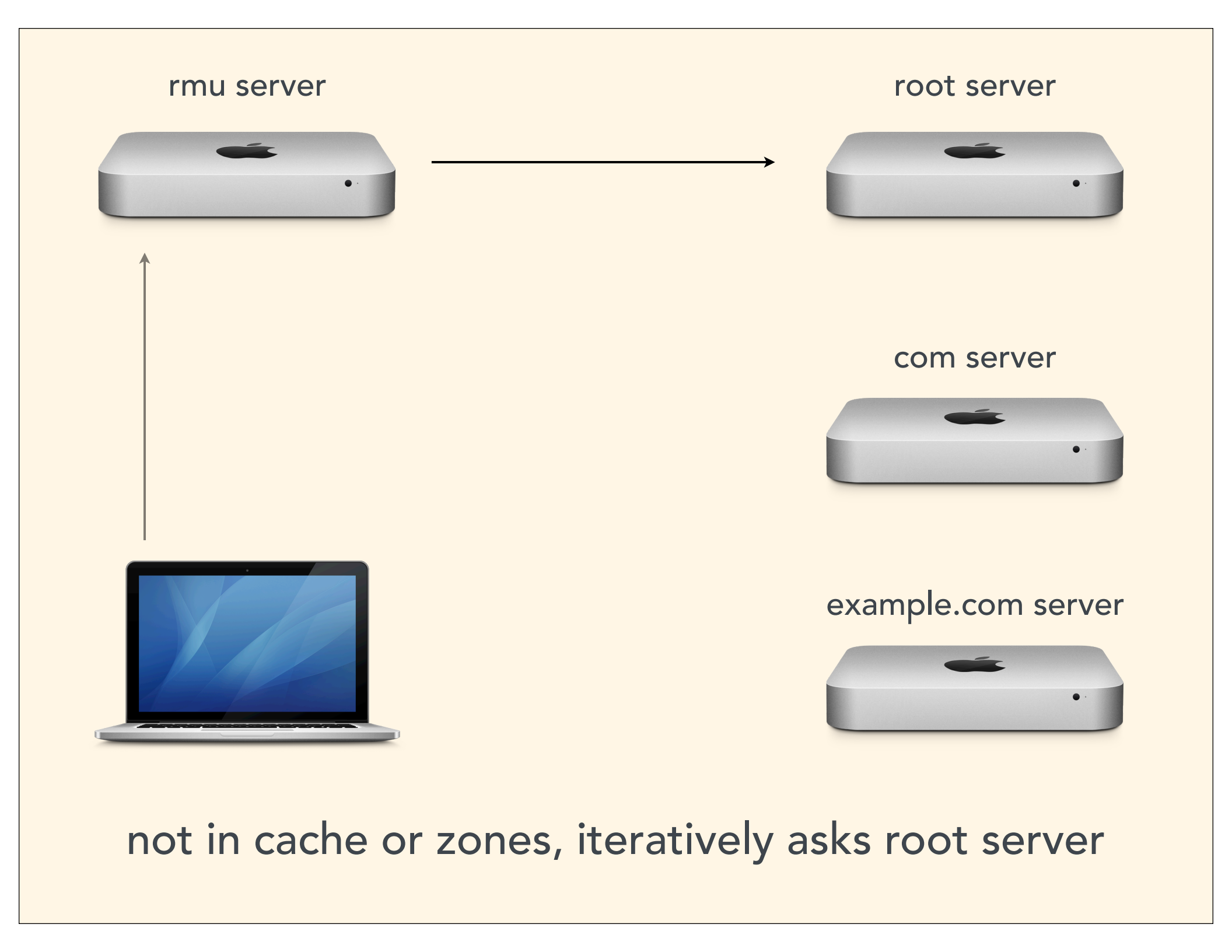
com server

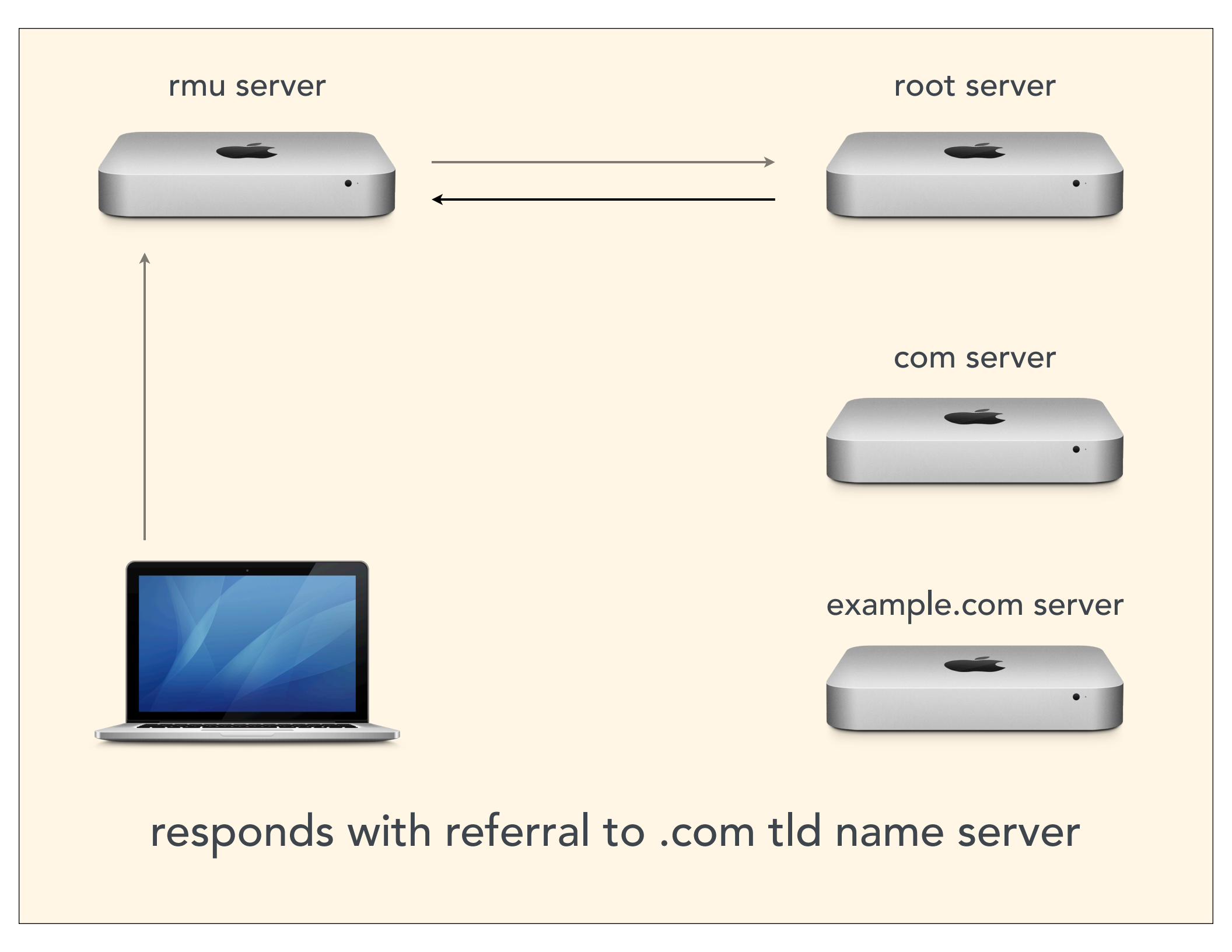


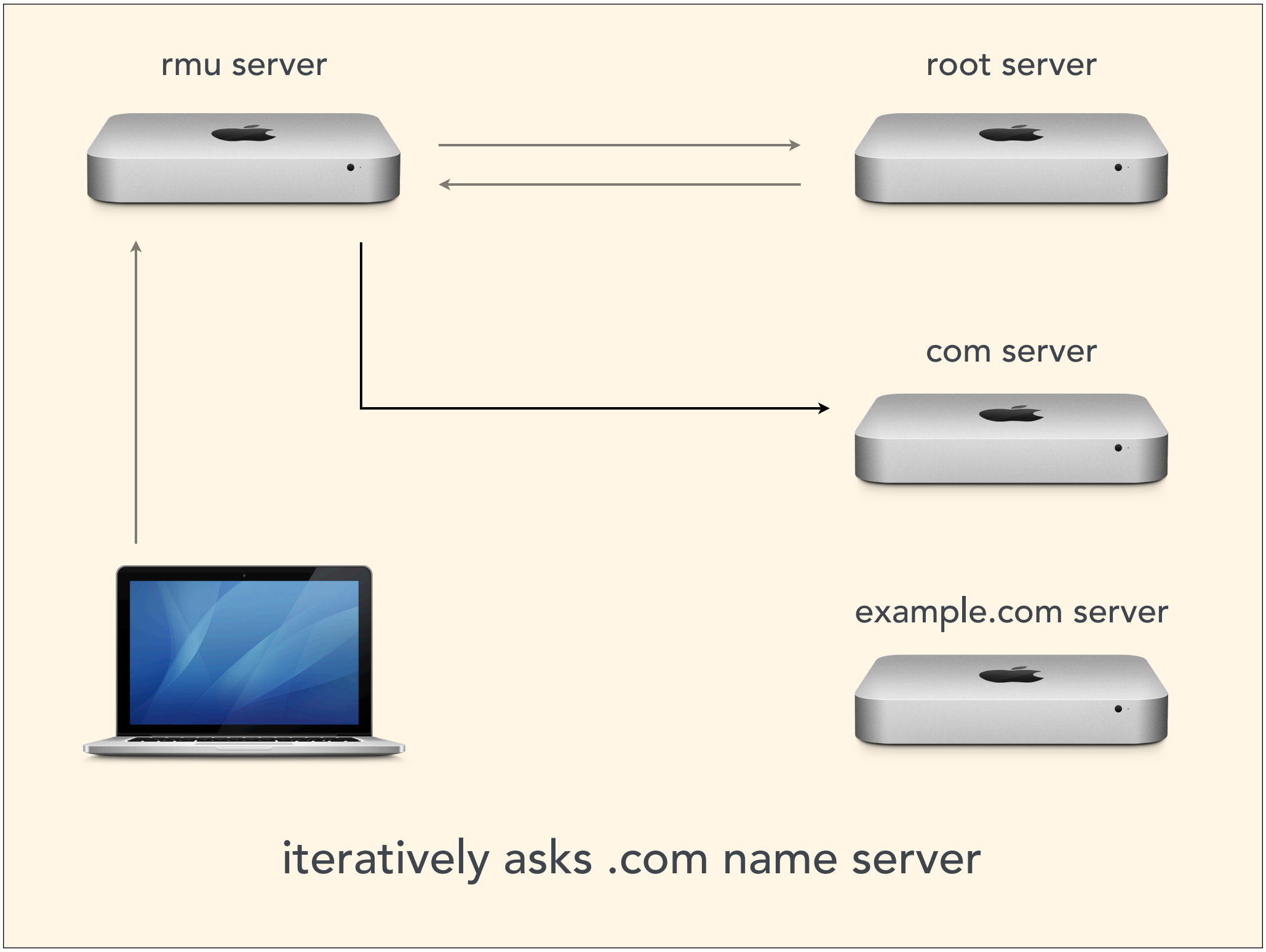
example.com server

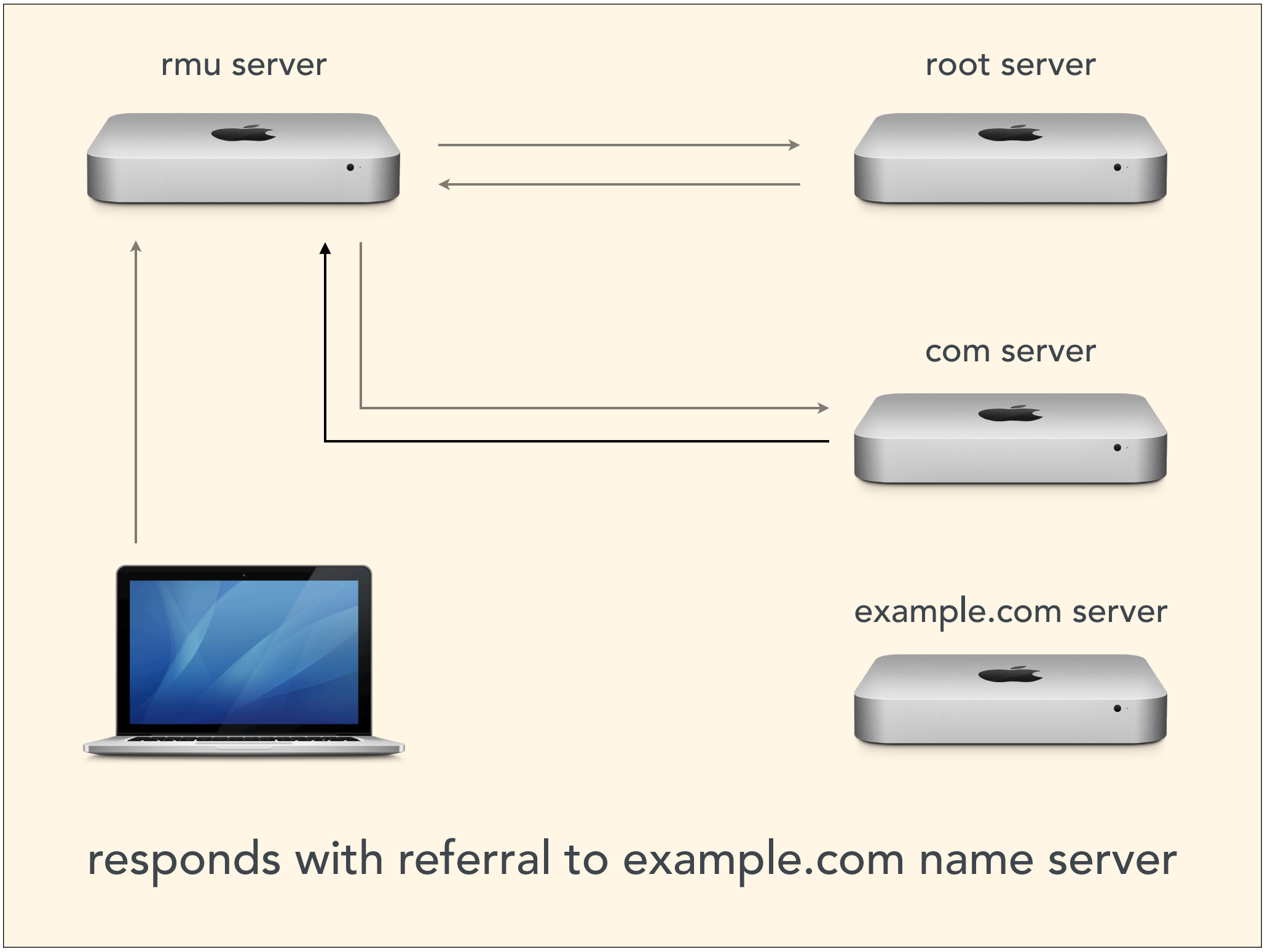



rmu server
root server
com server
example.com server
recursive query for host.example.com

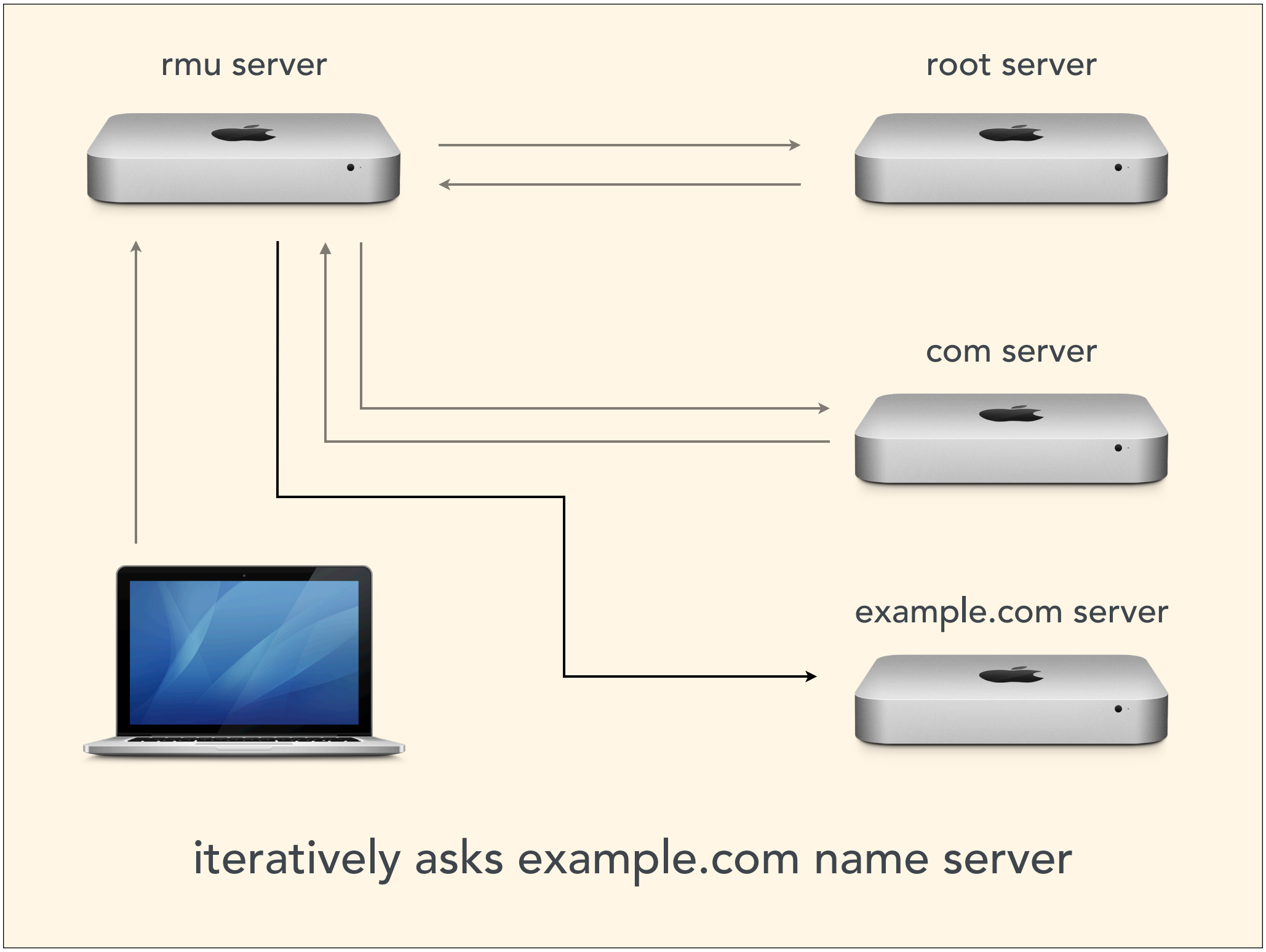

rmu server
root server
com server
example.com server
not in cache or zones, iteratively asks root server


rmu server
root server
com server
example.com server
responds with referral to .com tld name server

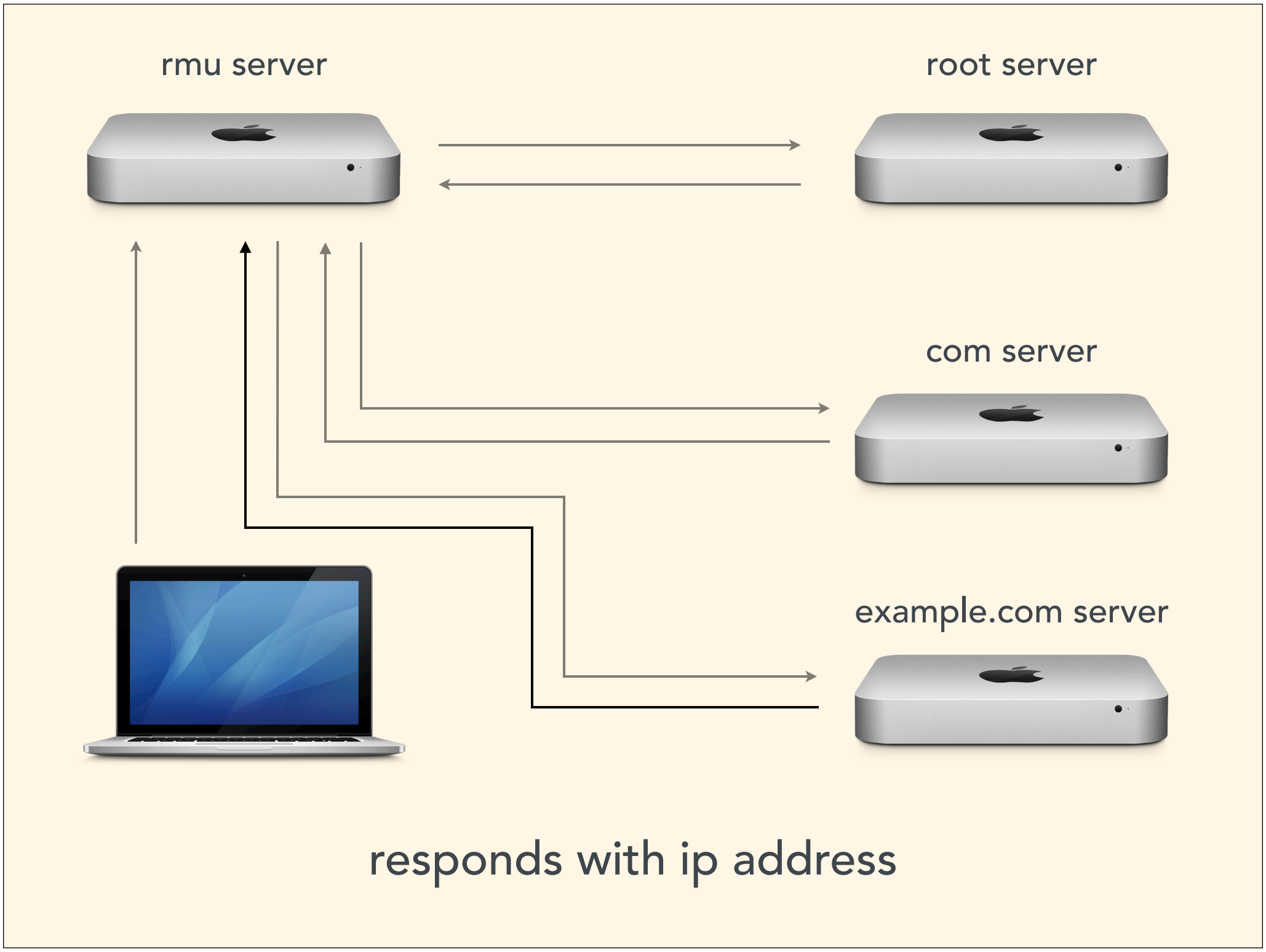

rmu server
root server
com server
example.com server
iteratively asks .com name server

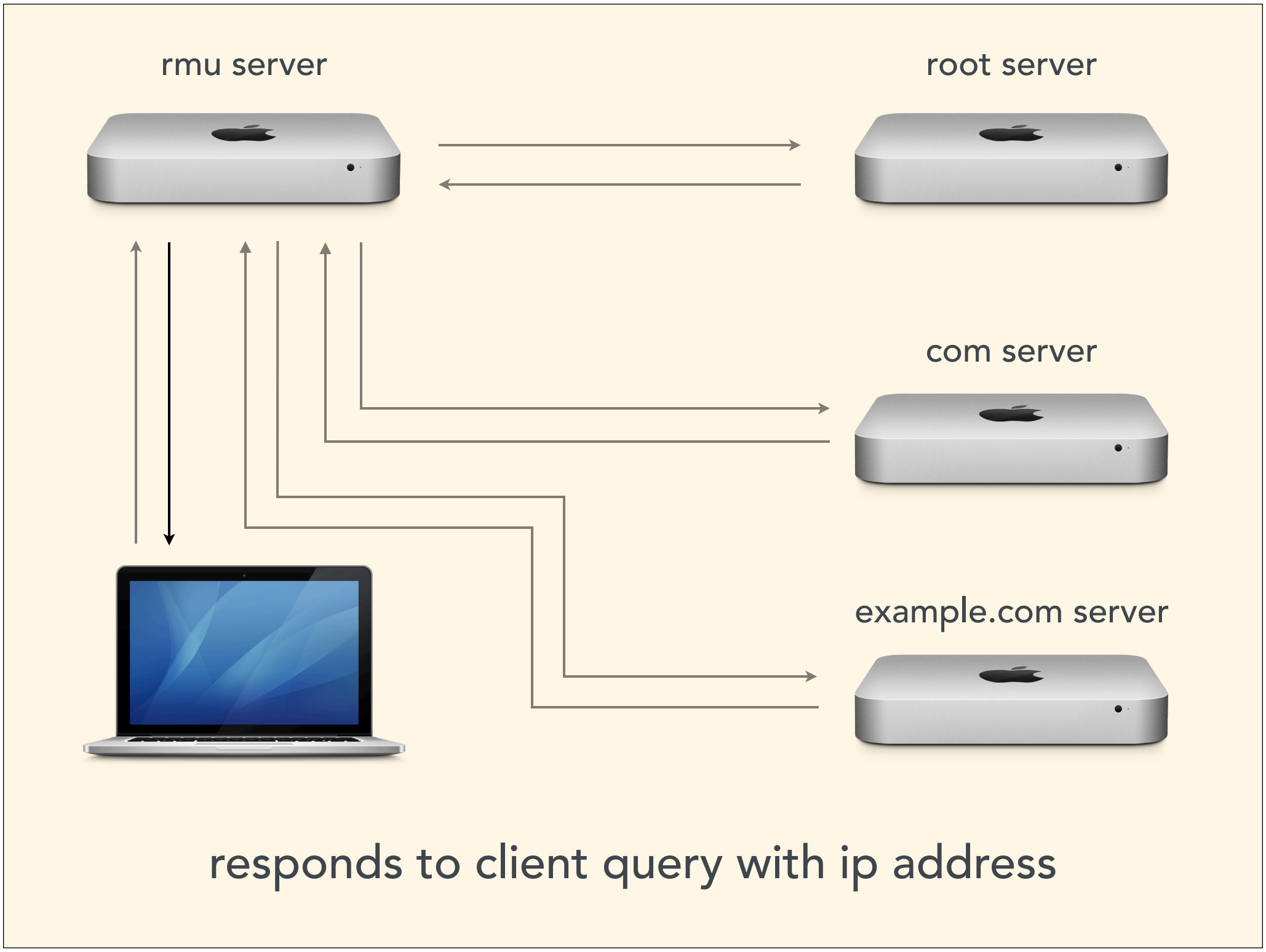


responds with referral to example.com name server



iteratively asks example.com name server


rmu server
root server
com server
example.com server
responds with ip address


rmu server
root server
com server
example.com server
responds to client query with ip address

yes, all dns servers are mac minis

loljk

dns follows a client/server model

dns follows a client/server model

resolvers are clients who issue queries

nameservers are servers (really?) with dns info*

*zone data and more...

zones

zones

domain name space = tree of domain names

tree subdivided into zones, starting with root

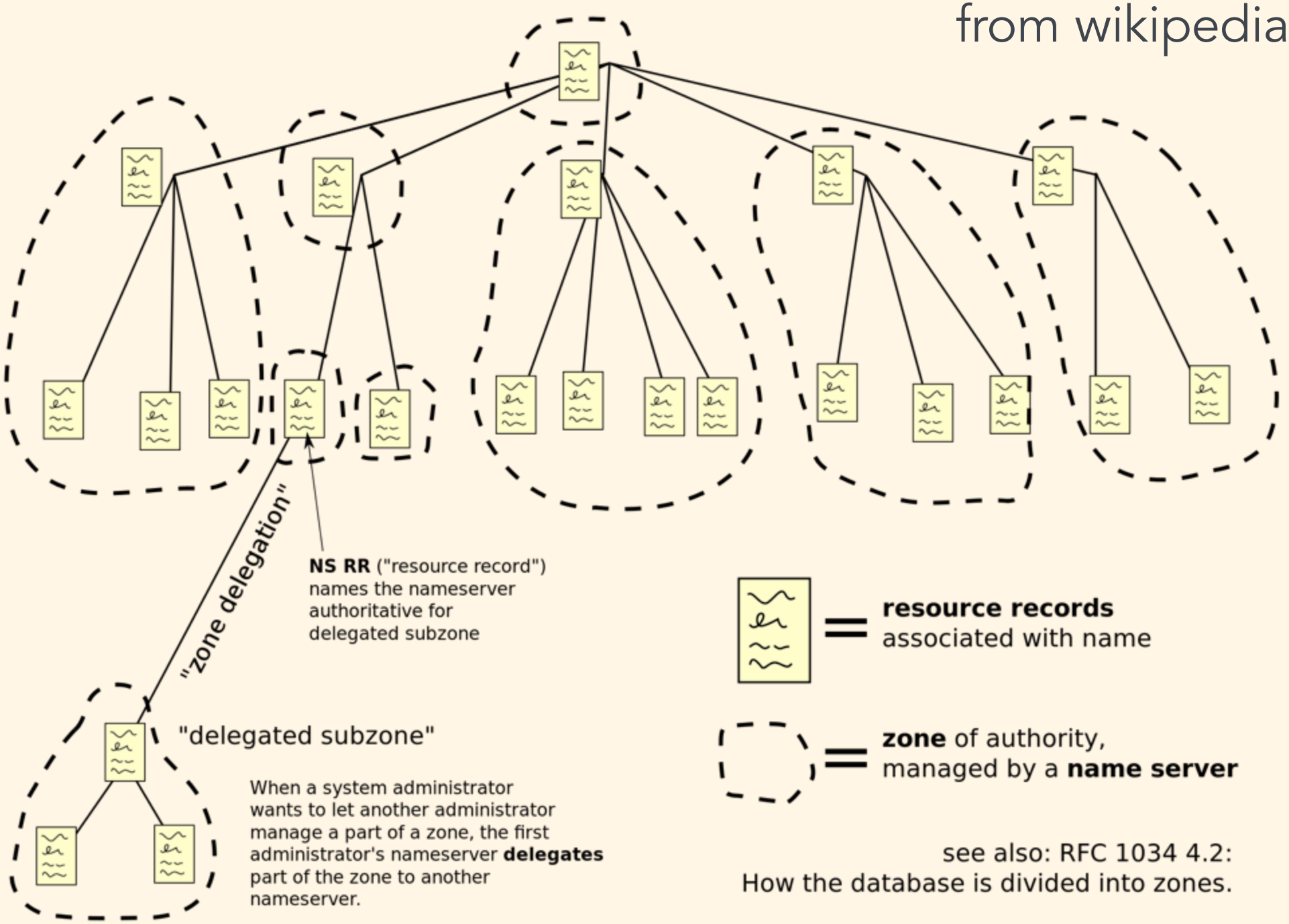
may consist of 1 domain, or many and subdomains

delegation info for subzones

contain resource records

Domain Name Space

from wikipedia



records

records

different types used for different purposes

most common:

A, AAAA, CNAME, MX, NS, PTR, SOA, SPF, SRV, TXT

nameservers

nameservers

zones holding dns record information

cache query results (TTL defines how long)

authoritative delegation info for subdomains

forwarding info for unauthoritative queries

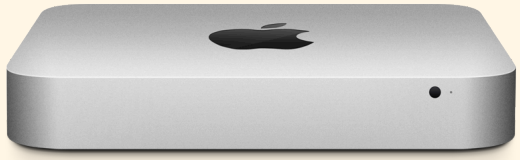
primary

hosts the zone file(s)

can host multiple zones

notifies slaves of changes

primary



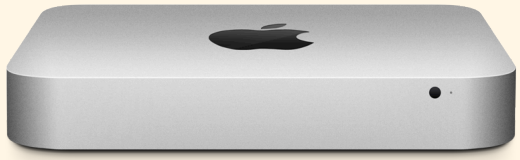
secondary (slave)

transfers the zone file(s)

can have multiple slaves

transfers are over tcp 53

secondary (slave)



the roots

the roots

<a-m>.root-servers.net.*

geographically dispersed around the world

publish root server zone file

lists authoritative dns servers for all TLDs

*not actually just 13 root name servers


Map
Satellite
Hybrid
Greenland
Iceland
Canada
Mexico
Russia
Kazakhstan
Mongolia
China
South Korea
Indonesia
Papua New Guinea
Australia
New Zealand
Spain
Algeria
Libya
Egypt
Niger
Chad
Sudan
Nigeria
Kenya
DR Congo
Tanzania
Angola
Namibia
Botswana
South Africa
Madagascar
Venezuela
Peru
Brazil
Bolivia
Argentina
North Atlantic Ocean
South Atlantic Ocean
Indian Ocean
Legend
99 Multiple instances
K Single instance
POWERED BY Google
Map data ©2013 MapLink, Tele Atlas - Terms of Use

delegations and forwarding

delegation

used to separate management of part of a zone

organization maintains all data in that subdomain

ex: mac.rmu.edu is delegated to mike boylan

forwarding

generally used for off-site queries

also used to send queries “upstream”

ex: mac.rmu.edu nameserver configured to forward non-authoritative queries to rmu.edu nameserver

question

question

is host.example.com a fqdn?

question

is host.example.com a fqdn?

technically not...

host.example.com. is... notice the trailing dot

. or “” represents dns root

fqdn

unambiguous domain name

specifies its position in the dns tree absolutely

carries a trailing period

sometimes called “rooted domain”

max length of 256 bytes

anatomy of an fqdn


host.example.com.

host.example.com.

read right to left...

root pointer

top level doman (tld)

second-level domain

[subdomain(s)]

host or resource name

snd esrever

reverse dns

reverse dns

turns numbers into names

uses a special zone called the .in-addr.arpa zone

uses PTR records

read right to left

apple.com. = 17.172.224.47

47.224.172.17.in-addr.arpa = apple.com.

reverse dns

absolutely critical for os x server services

used for rudimentary spam filtering

one half of a forward-confirmed reverse dns entry

FCrDNS: what's the name for this ip? what's the ip for this name? do they match? woohoo!

reverse dns

outermost dns servers should have “catch-all” reverse zones for RFC1918 local network addresses

prisoner.iana.org, blackhole-(1-2).iana.org designed to catch leaked queries, but often become overloaded

common scenarios

AD DNS, Round-Robin DNS, & Split-Horizon DNS

active directory dns

why is using active directory dns such a popular choice?

auto updating of ip addresses mapped to names in a dhcp environment

active directory dns & os x (server)

make sure your AD admin makes the reverse zone

os x clients unfortunately do not support secure dynamic updates

round-robin dns

one name, multiple addresses

ex: apple.com resolves to:

17.149.160.49
17.178.96.59
17.172.224.47

views or “split-horizon dns”

what you see depends on who you are

allows you to use the same dns server(s) to provide different results based on source address

subnet 1

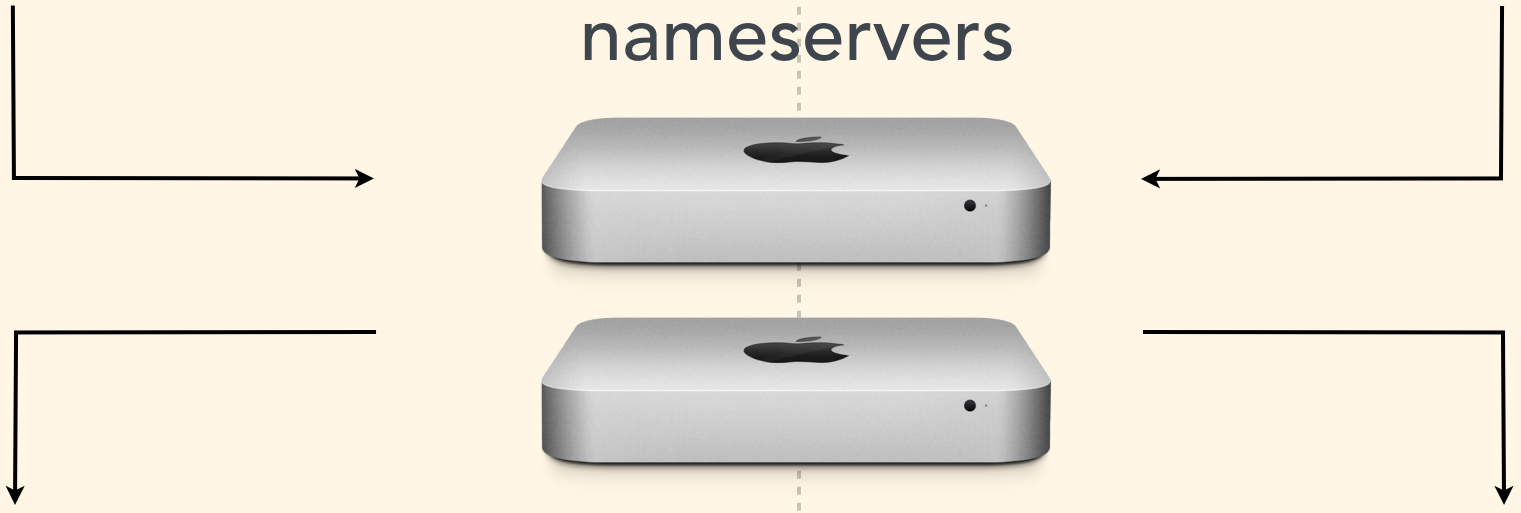
query:

hello.example.com

subnet 2

query:

hello.example.com



result:

10.10.10.10

result:

xx.xx.xx.xx

troubleshooting dns

dns doesn’t have to be a four letter word

“The strangest problems often turn out to be misconfigured DNS. DNS is critical to so many subsystems, often in obscure ways, that a problem with DNS can mask itself as other problems. This goes for a client that can’t reach its DNS servers, as well as a host with invalid DNS data describing it, or a client trying to reach a host with invalid DNS data.”

Tim Limoncelli
Time Management For System Administrators - O'Reilly Books

ISPs are evil

ISPs are evil

often resolve unresolvable domains to ad pages

“Did you mean?” -- No, I didn’t, but thanks?

can cause login delays & various other problems

fortunately, can usually “opt-out”

dns command line tools in os x

dns command line tools in os x

nslookup

host

dig

dscacheutil

scutil

changeip (Server only)

nslookup

is its own resolver

format: nslookup <name> or <ip address>

```
boylan-mbp:~ boylan$ nslookup apple.com
Server:   192.168.1.1
Address:  192.168.1.1#53

Non-authoritative answer:
Name: apple.com
Address: 17.178.96.59
Name: apple.com
Address: 17.172.224.47
Name: apple.com
Address: 17.149.160.49
```

```
boylan-mbp:~ boylan$ nslookup 17.172.224.47
Server:    192.168.1.1
Address:   192.168.1.1#53

Non-authoritative answer:
47.224.172.17.in-addr.arpa name = apple.com.
```

host

is its own resolver

format: host <name> or <ip address>

```
boylan-mbp:~ boylan$ host apple.com
apple.com has address 17.172.224.47
apple.com has address 17.149.160.49
apple.com has address 17.178.96.59
```

```
boylan-mbp:~ boylan$ host 17.172.224.47
47.224.172.17.in-addr.arpa domain name pointer apple.com.
```

dig

is its own resolver

simple format ip: dig <name> <type>

simple format name: dig -x <ip address>

specific server: dig @server...

useful options: +trace, +short, no name or ip

```
boylan-mbp:~ boylan$ dig apple.com

; <<>> DiG 9.8.3-P1 <<>> apple.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63900
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;apple.com.          IN  A

;; ANSWER SECTION:
apple.com.       2227   IN  A   17.172.224.47
apple.com.       2227   IN  A   17.149.160.49
apple.com.       2227   IN  A   17.178.96.59
```

```
boylan-mbp:~ boylan$ dig @8.8.8.8 apple.com

; <<>> DiG 9.8.3-P1 <<>> @8.8.8.8 apple.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34420
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;apple.com.          IN  A

;; ANSWER SECTION:
apple.com.       753 IN  A   17.178.96.59
apple.com.       753 IN  A   17.172.224.47
apple.com.       753 IN  A   17.149.160.49
```

```
boylan-mbp:~ boylan$ dig _ldap._tcp.ad.example.edu SRV

; <<>> DiG 9.8.3-P1 <<>> _ldap._tcp.ad.example.edu SRV
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30499
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;_ldap._tcp.ad.example.edu.    IN  SRV

;; ANSWER SECTION:
_ldap._tcp.ad.example.edu.  111 IN  SRV 0 100 389 dc01.ad.example.edu.
_ldap._tcp.ad.example.edu.  111 IN  SRV 0 100 389 dc02.ad.example.edu.
_ldap._tcp.ad.example.edu.  111 IN  SRV 0 100 389 dc03.ad.example.edu.
```

```
boylan-mbp:~ boylan$ dig _kerberos._tcp.ad.example.edu SRV

; <<>> DiG 9.8.3-P1 <<>> _kerberos._tcp.ad.example.edu SRV
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61304
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;_kerberos._tcp.ad.example.edu.  IN  SRV

;; ANSWER SECTION:
_kerberos._tcp.ad.example.edu. 600   IN  SRV 0 100 88 dc-02.ad.example.edu.
_kerberos._tcp.ad.example.edu. 600   IN  SRV 0 100 88 dc-03.ad.example.edu.
_kerberos._tcp.ad.example.edu. 600   IN  SRV 0 100 88 dc-04.ad.example.edu.
```

dscacheutil

uses osx host name/address resolution and dns query routing mechanisms

format:

dscacheutil -q host -a name <name>

dscacheutil -q host -a ip_address <ip>

```
boylan-mbp:~ boylan$ dscacheutil -q host -a name apple.com
name: apple.com
ip_address: 17.178.96.59
ip_address: 17.172.224.47
ip_address: 17.149.160.49
```

```
boylan-mbp:~ boylan$ dscacheutil -q host -a ip_address 17.172.224.47
name: st11p01ww-apple.apple.com
alias: 47.224.172.17.in-addr.arpa apple.com
ip_address: 17.172.224.47
```

scutil

used to get or set your hostname, computer name, and/or local host name.

format:

scutil --get [HostNamelComputerNamelLocalHostName]

scutil --set [HostNamelComputerNamelLocalHostName] <name>

```
boylan-mbp:~ boylan$ scutil --get ComputerName
boylan-mbp
```

changeip (server only)

used to check for FCrDNS for hostname

used to need invoked after a name or IP change

most common usage:

sudo changeip -checkhostname

```
$ sudo changeip -checkhostname
Password:

Primary address      = 10.10.10.10

Current HostName     = host.example.com
DNS HostName         = host.example.com

The names match. There is nothing to change.
dirserv:success = "success"
```

inconsistent results

inconsistent results

Apple will not confirm, but there still seems to be a tight integration between directory services caching and dns resolution

clearing the dns cache

clearing the dns cache

sudo dscacheutil -flushcache

sudo killall -HUP mDNSResponder

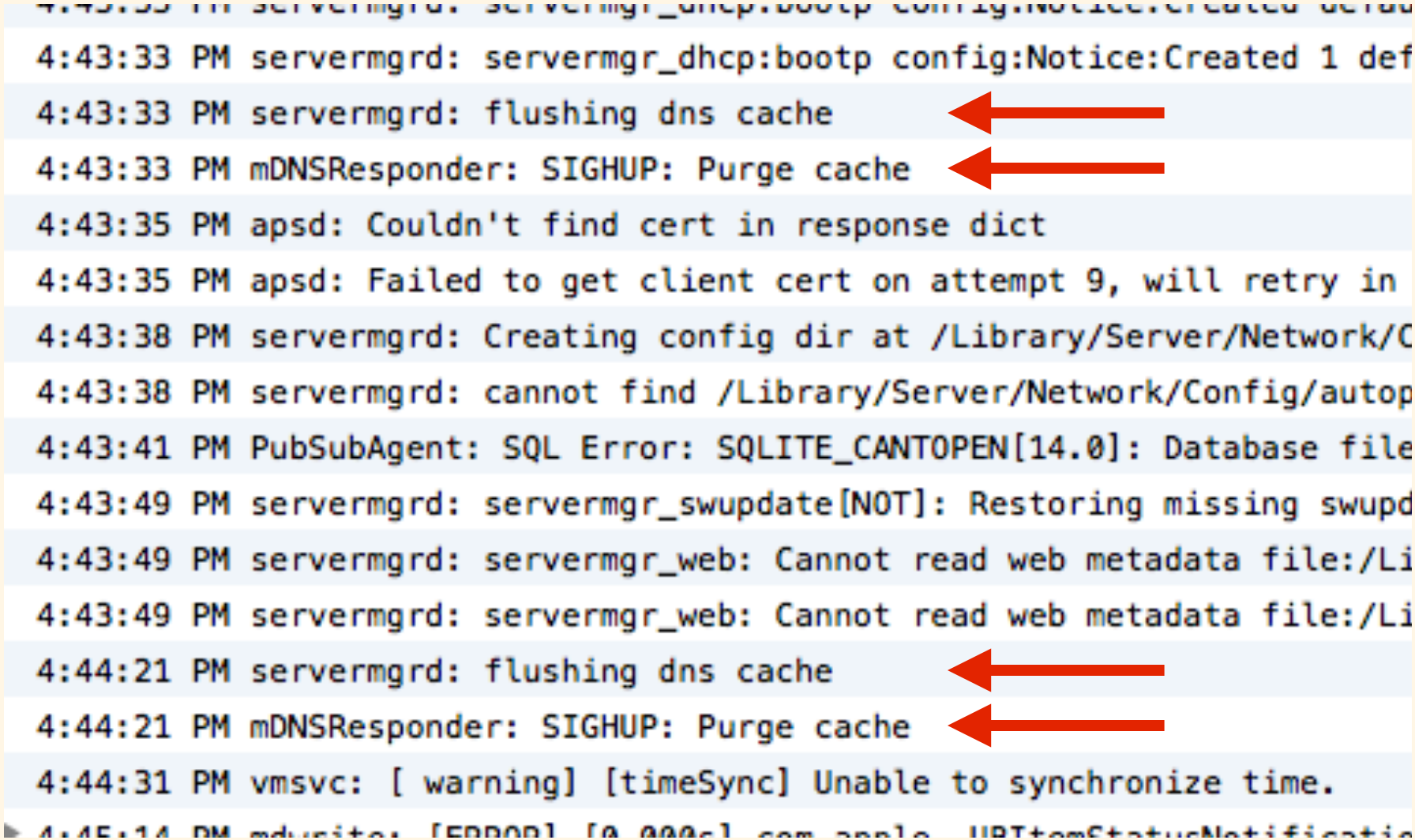
in system.log after HUPing mDNSResponder...

```
mDNSResponder[55]: SIGHUP: Purge cache
```

is that really still necessary?

is that really still necessary?

fun fact: Apple HUPs mDNSResponder multiple times during Server.app initial setup


4:43:33 PM servermgrd: servermgr_dhcp:bootp config:Notice:Created 1 def
4:43:33 PM servermgrd: flushing dns cache
4:43:33 PM mDNSResponder: SIGHUP: Purge cache
4:43:35 PM apsd: Couldn't find cert in response dict
4:43:35 PM apsd: Failed to get client cert on attempt 9, will retry in
4:43:38 PM servermgrd: Creating config dir at /Library/Server/Network/C
4:43:38 PM servermgrd: cannot find /Library/Server/Network/Config/autop
4:43:41 PM PubSubAgent: SQL Error: SQLITE_CANTOPEN[14.0]: Database file
4:43:49 PM servermgrd: servermgr_swupdate[NOT]: Restoring missing swupd
4:43:49 PM servermgrd: servermgr_web: Cannot read web metadata file:/Li
4:43:49 PM servermgrd: servermgr_web: Cannot read web metadata file:/Li
4:44:21 PM servermgrd: flushing dns cache
4:44:21 PM mDNSResponder: SIGHUP: Purge cache
4:44:31 PM vmsvc: [warning] [timeSync] Unable to synchronize time.

speaking of Server.app...

dns in os x server

from server.app setup to dns service

Server

Set up your Server

Server makes it easy to share files, host websites, publish wikis, and collaborate.
Empower your organization to do more with their devices.

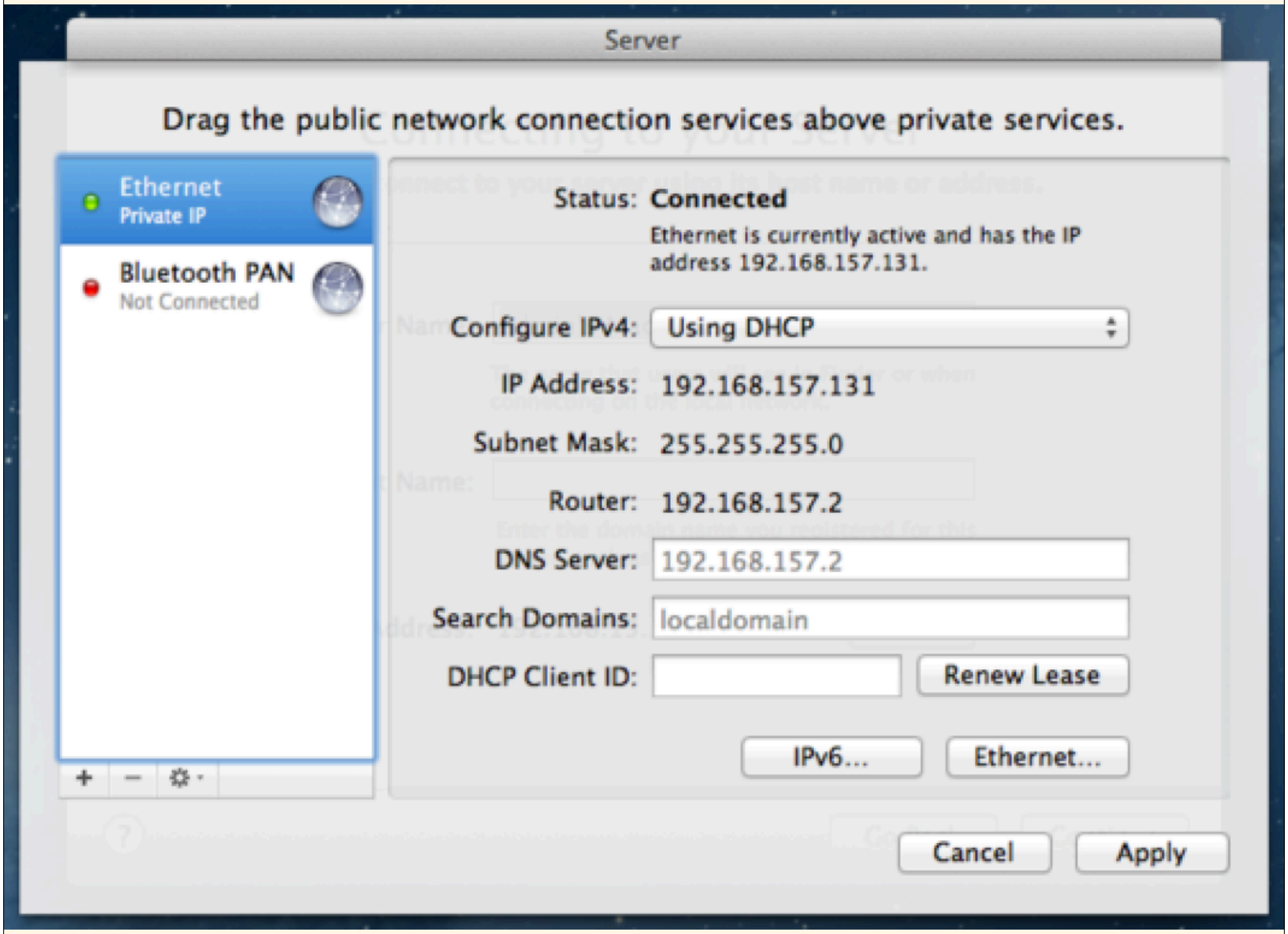
Other Server...

Quit

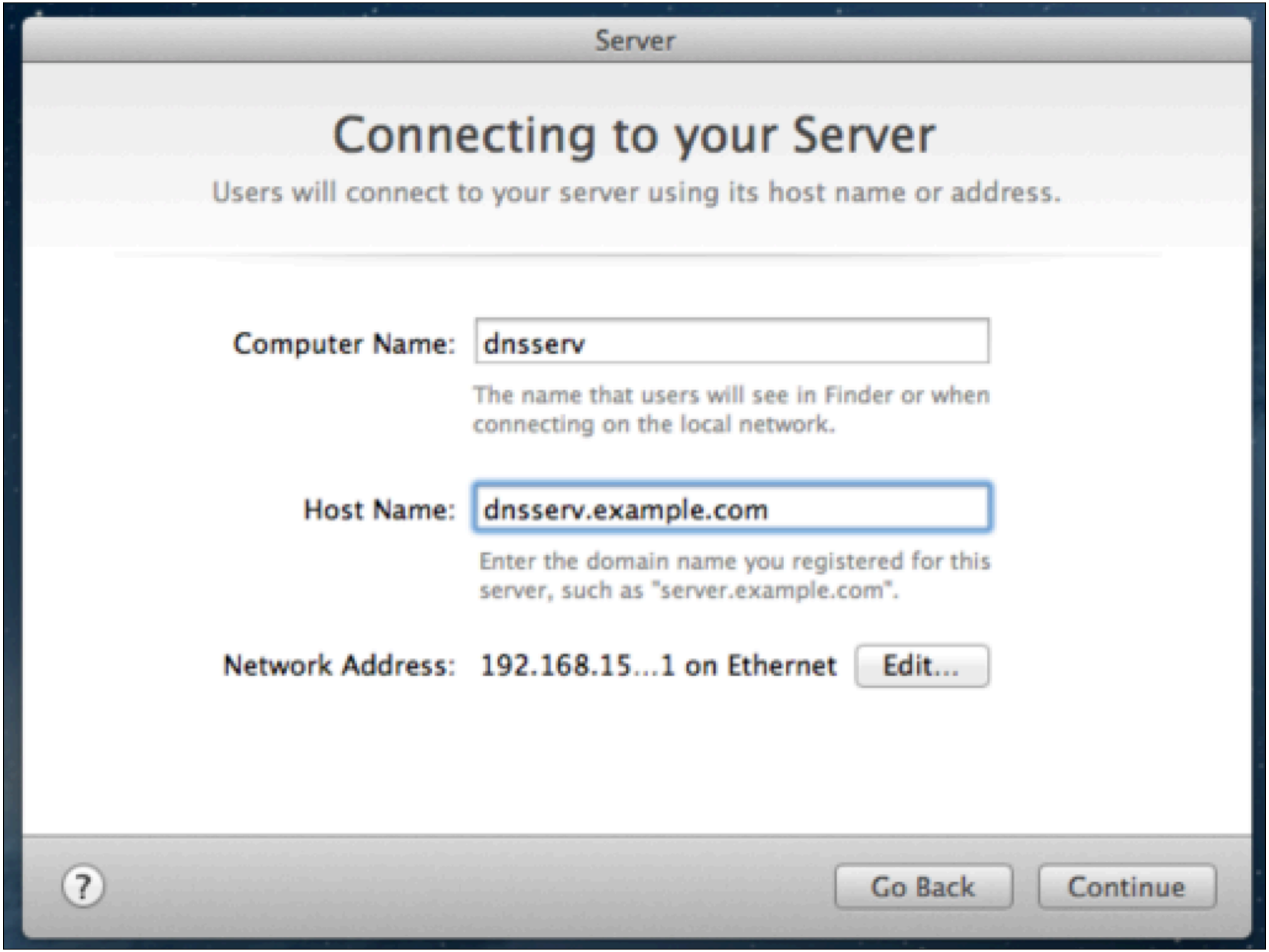
Continue

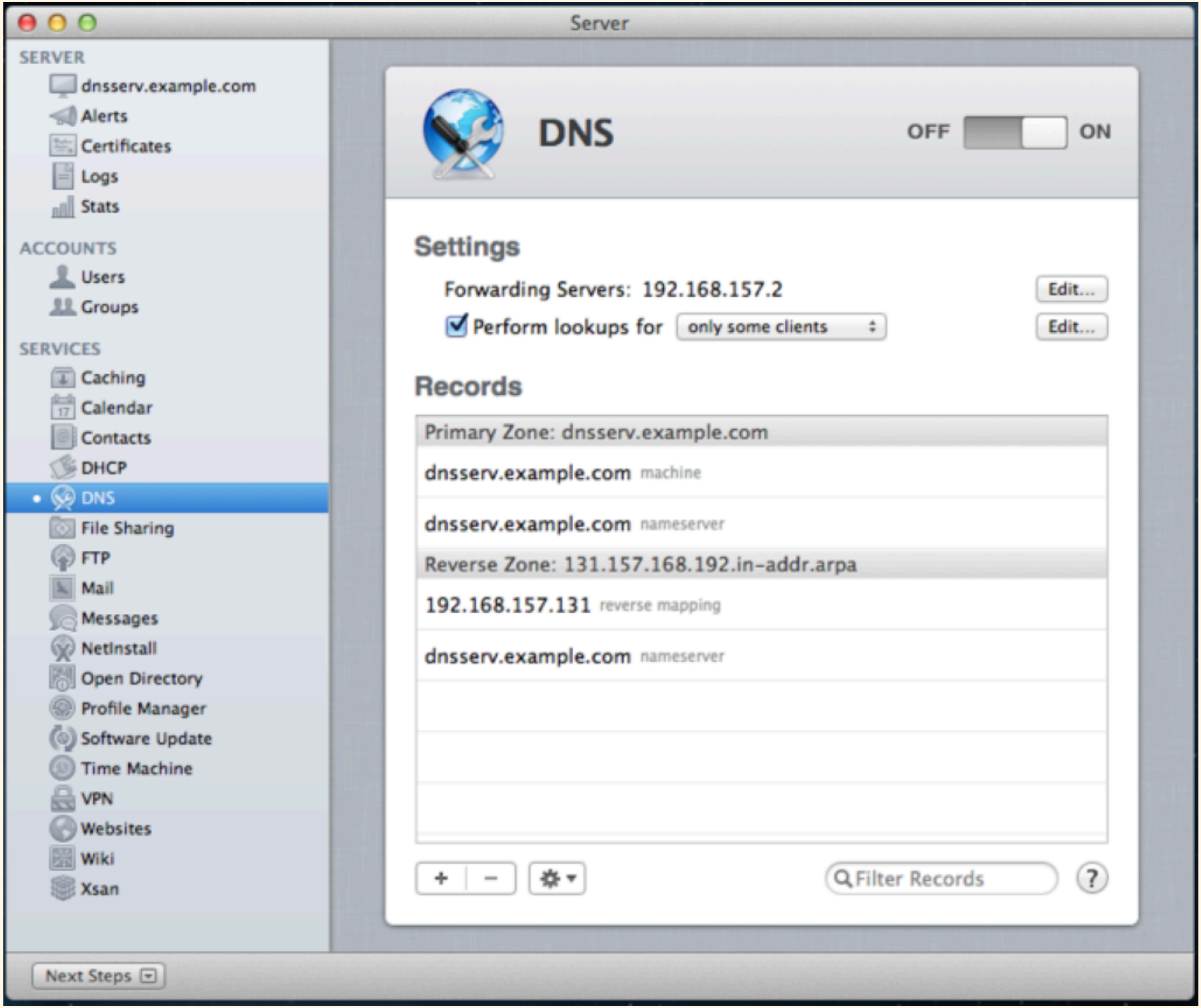

Server
Accessing your Server
Choose how users will access your server.
Local Network
Access your server on the local network using a host name ending in ".local".
Your server will not be accessible outside of your local network.
Local Network and using VPN
Access your server on the local network using a host name ending in ".private".
Users can also access your server using a Virtual Private Network (VPN).
Domain Name
Access your server on both the local network and on the Internet using a registered domain name.
?
Go Back
Continue


Server
Connecting to your Server
Users will connect to your server using its host name or address.
Computer Name:
admin's Mac
The name that users will see in Finder or when connecting on the local network.
Host Name:
Enter the domain name you registered for this server, such as "server.example.com".
Network Address:
192.168.15...1 on Ethernet
Edit...
Go Back
Continue


Server
Drag the public network connection services above private services.
Ethernet
Private IP
Bluetooth PAN
Not Connected
Status: Connected
Ethernet is currently active and has the IP address 192.168.157.131.
Configure IPv4: Using DHCP
IP Address: 192.168.157.131
Subnet Mask: 255.255.255.0
Router: 192.168.157.2
DNS Server: 192.168.157.2
Search Domains: localdomain
DHCP Client ID:
Renew Lease
IPv6...
Ethernet...
Cancel
Apply


Server
Connecting to your Server
Users will connect to your server using its host name or address.
Computer Name:
admin's Mac
The name that users will see in Finder or when connecting on the local network.
Host Name:
Enter the domain name you registered for this server, such as "server.example.com".
Network Address:
192.168.15...1 on Ethernet
Edit...
Go Back
Continue

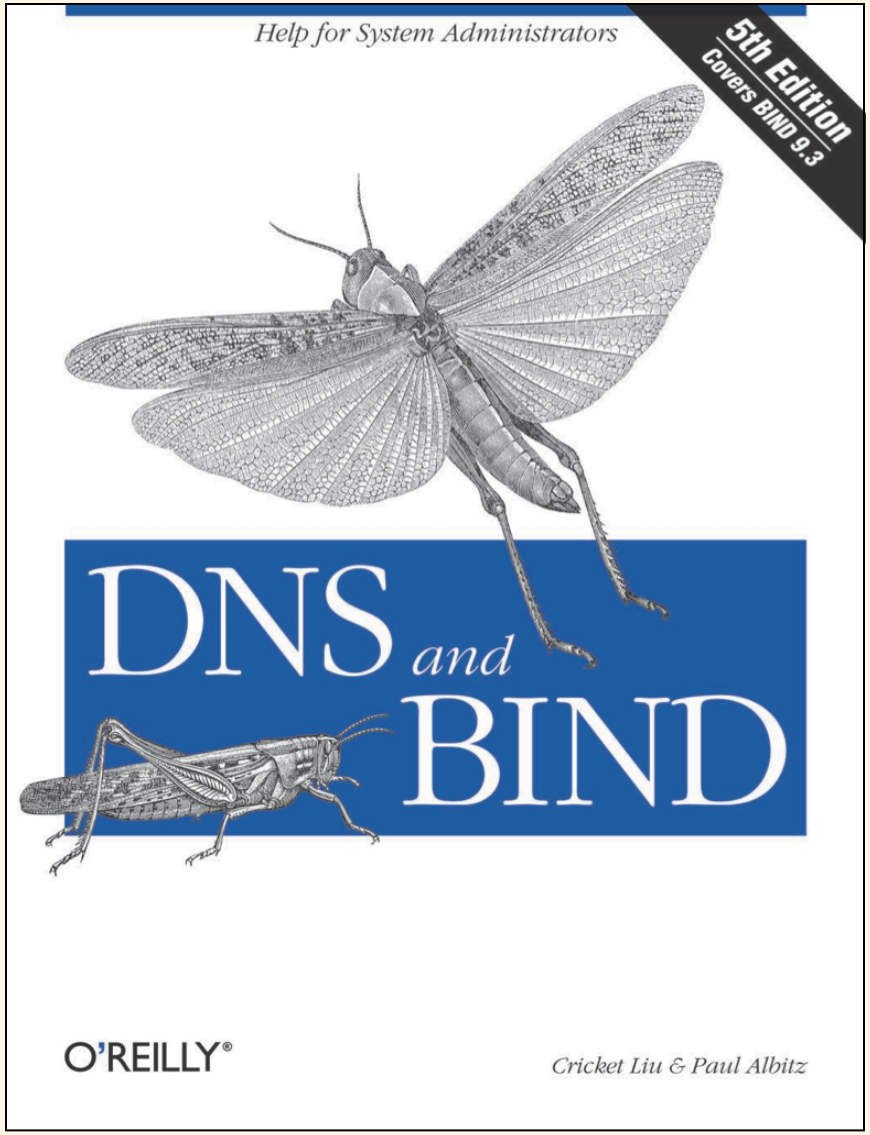

Server
Connecting to your Server
Users will connect to your server using its host name or address.
Computer Name:
dnsserv
The name that users will see in Finder or when connecting on the local network.
Host Name:
dnsserv.example.com
Enter the domain name you registered for this server, such as "server.example.com".
Network Address:
192.168.15...1 on Ethernet
Edit...
?
Go Back
Continue


Server
SERVER
dnsserv.example.com
Alerts
Certificates
Logs
Stats
ACCOUNTS
Users
Groups
SERVICES
Caching
Calendar
Contacts
DHCP
DNS
File Sharing
FTP
Mail
Messages
NetInstall
Open Directory
Profile Manager
Software Update
Time Machine
VPN
Websites
Wiki
Xsan
Next Steps
DNS
OFF
ON
Settings
Forwarding Servers: 192.168.157.2
Edit...
Perform lookups for
only some clients
Edit...
Records
Primary Zone: dnsserv.example.com
dnsserv.example.com machine
dnsserv.example.com nameserver
Reverse Zone: 131.157.168.192.in-addr.arpa
192.168.157.131 reverse mapping
dnsserv.example.com nameserver
Filter Records

okay, real demo time...

resources

additional information



ISBN 9780596100575

resources

http://work.mikeboylan.com/posts/2011/05/dns-doesnt-have-to-be-wtf.html

http://en.wikipedia.org/wiki/Domain_Name_System

http://technet.microsoft.com/en-us/network/bb629410.aspx

really geeky resources

http://tools.ietf.org/html/rfc1034

http://tools.ietf.org/html/rfc1035