Network Services: DNS, DHCP, etc..

Operating Systems and Internetworking
Week 1

Contents

Motivation for DHCP

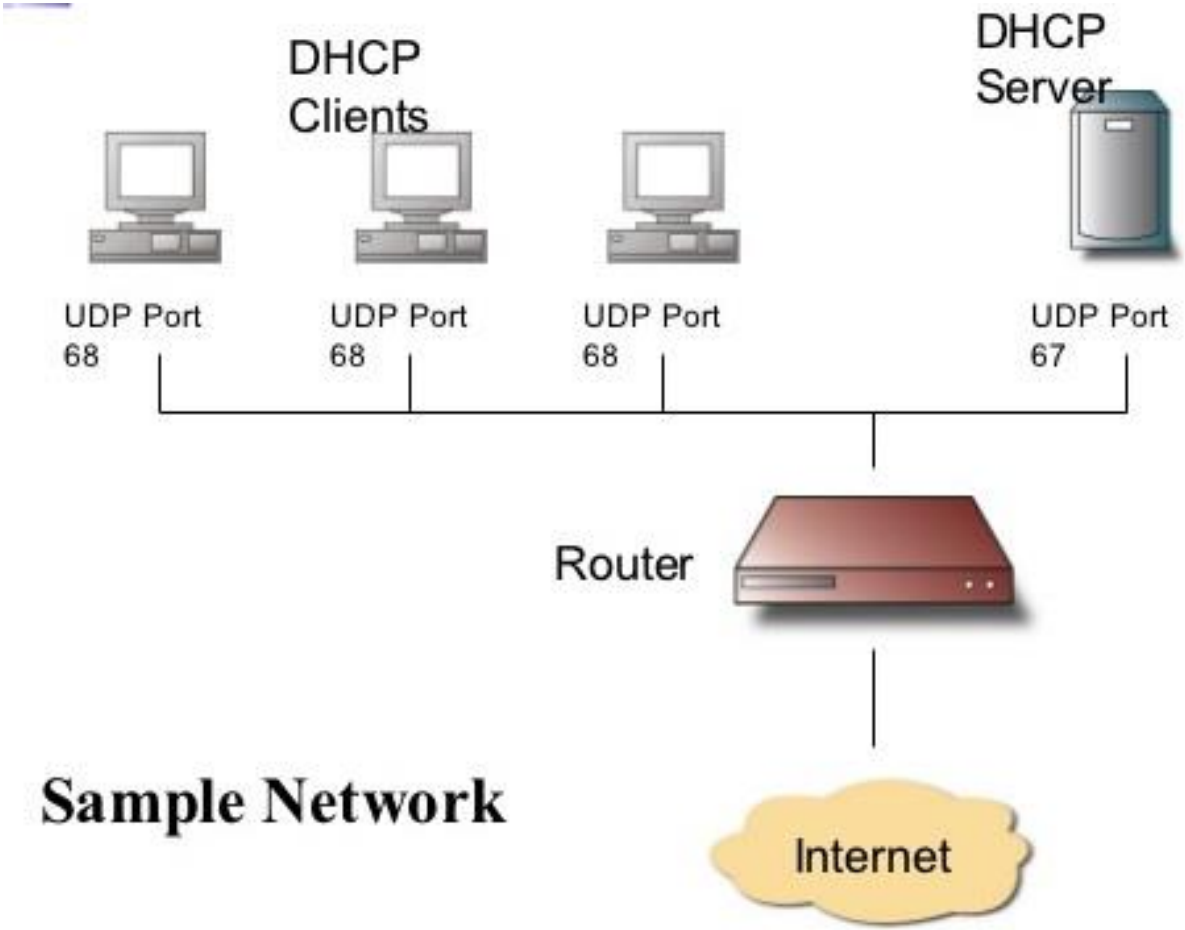
- Configuration parameters
  - IP address
  - Router address
  - Subnet mask
  - DNS server address

- What happened before?
  - Manual assignment → NETFUN networking labs
  - Bootstrap Protocol – BOOTP

DHCP – Overview

- Introduced in 1993
- An improvement over BOOTP
  - Supports temporary allocation (leases) of IP addresses
  - Clients of DHCP servers can acquire all IP configuration parameters needed to operate
  - Minimal human interaction
- Is the preferred mechanism for dynamic assignment of IP addresses
- Compatible with BOOTP clients

Networks and DHCP

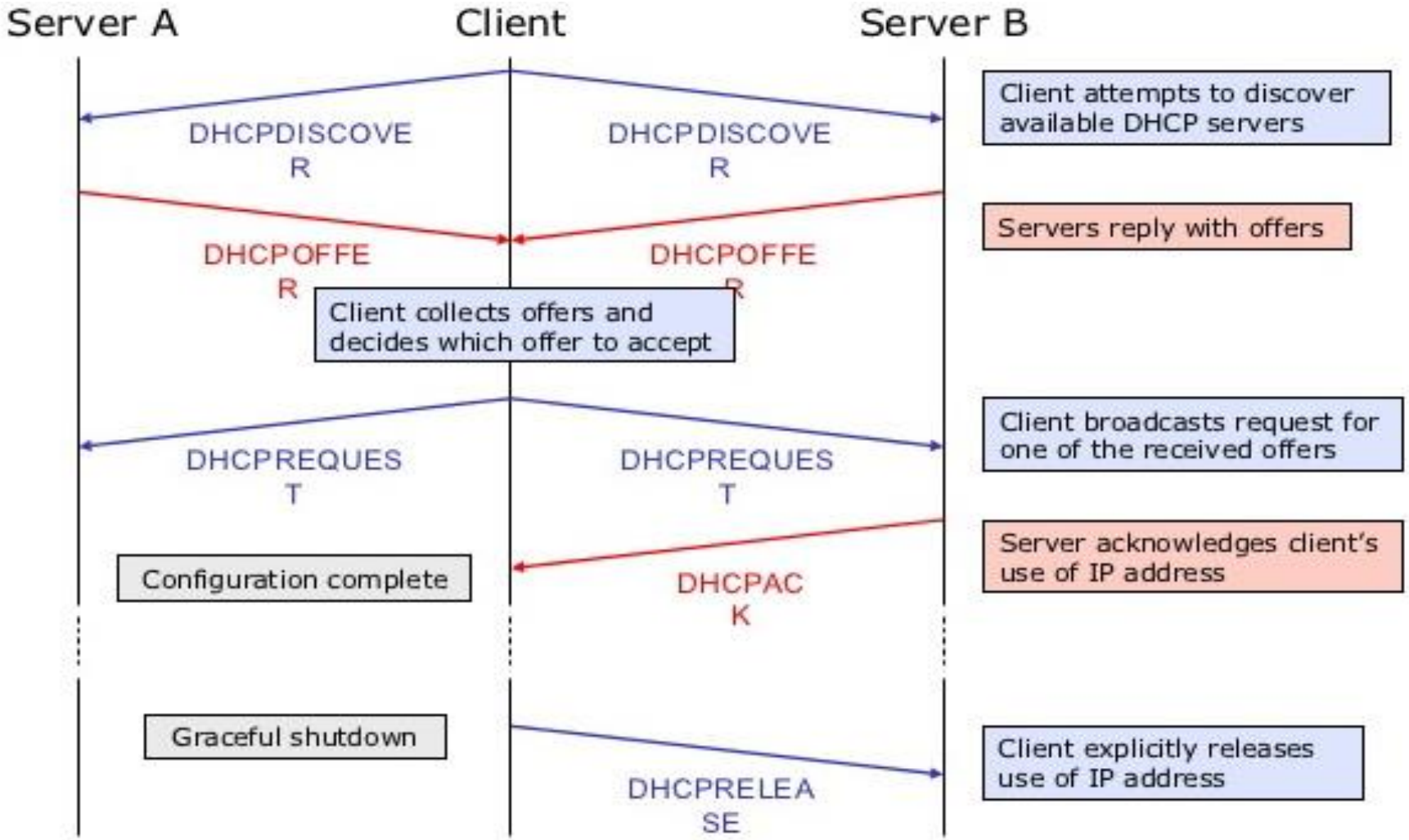


Sample Network

Terminology

- DHCP packet = DHCP Message
- DHCP Client = Client
- DHCP Server = Server
- Lease = Length of time a DHCP client can use a specific IP address

Initial Message Flow



IP release and renew

- An IP address is released when shuts down or terminates an internet connection
  - IP address returns to IP pool
  - It is available for another client to use

- A lease is renewed when 50% of the lease time is reached.
  - Request is sent to DHCP server
  - If initial DHCP server not available then request is broadcasted to all DHCP servers available

Advantages of DHCP

- Saves the network administrator from a lot of manual configuration work
  - Especially in large networks – 100+ clients
- Able to move a device from one network to another and gain instant connectivity
- More <u>efficient utilisation</u> of available IP addresses – inactive clients do not obtain IP addresses

Disadvantages

- DHCP packets are UDP packets
  - What does that mean?
  - Unreliable and insecure operations
- Potential unauthorised clients?
  - Apply MAC address filtering
- Potential malicious DHCP clients and servers
  - Supplying incorrect configuration parameters
  - Exhaustion of IP pool

DNS

The DNS is…

- Domain Name System
- What Internet users use to reference anything by name on the Internet
- The mechanism by which Internet software translates names to attributes such as IP addresses

DNS is also…

- A globally distributed, scalable, reliable database
- Comprised of three components
  - A "name space"
  - Servers – make that name space available
  - Resolvers (clients) – query the servers about the name space

DNS as a Lookup Mechanism

- Users generally prefer names to numbers
- Computers prefer numbers to names
- What is the service provided by DNS?
- DNS provides the mapping between the two
  - I know “x”, give me “y”

Global Distribution

- Data is maintained locally, but retrievable globally
  - No single computer has all DNS data
- DNS lookups can be performed by any device
- Remote DNS data is locally cacheable to improve performance

DNS – Loose Coherency

- The database is always internally consistent
  - Each version of a subset of the database (a zone) has a serial number
    - The serial number is incremented on every database change
- Changes to the master copy of the database are replicated according to timing set by the zone administrator
- Cached data expires according to timeout set by zone administrator

DNS – Scalability

- No limit to the size of the database
  - Can store 200,000,000 domain names?
  - Yes, but not particularly good idea
- No limit to the number of queries
  - Tens of thousands of queries handled easily every second
- Queries distributed among primary and secondary DNS servers and caches
  - E.g nslookup www.port.ac.uk

DNS – Reliability

- Data is replicated
  - From primary server to multiple secondary servers
- Clients can query
  - Primary server
  - Any of the copies at secondary servers
- Clients will typically query local caches
- DNS uses either UDP or TCP (port 53)
  - TCP for intra server communications
  - UDP for comms between clients and servers

Dynamicity

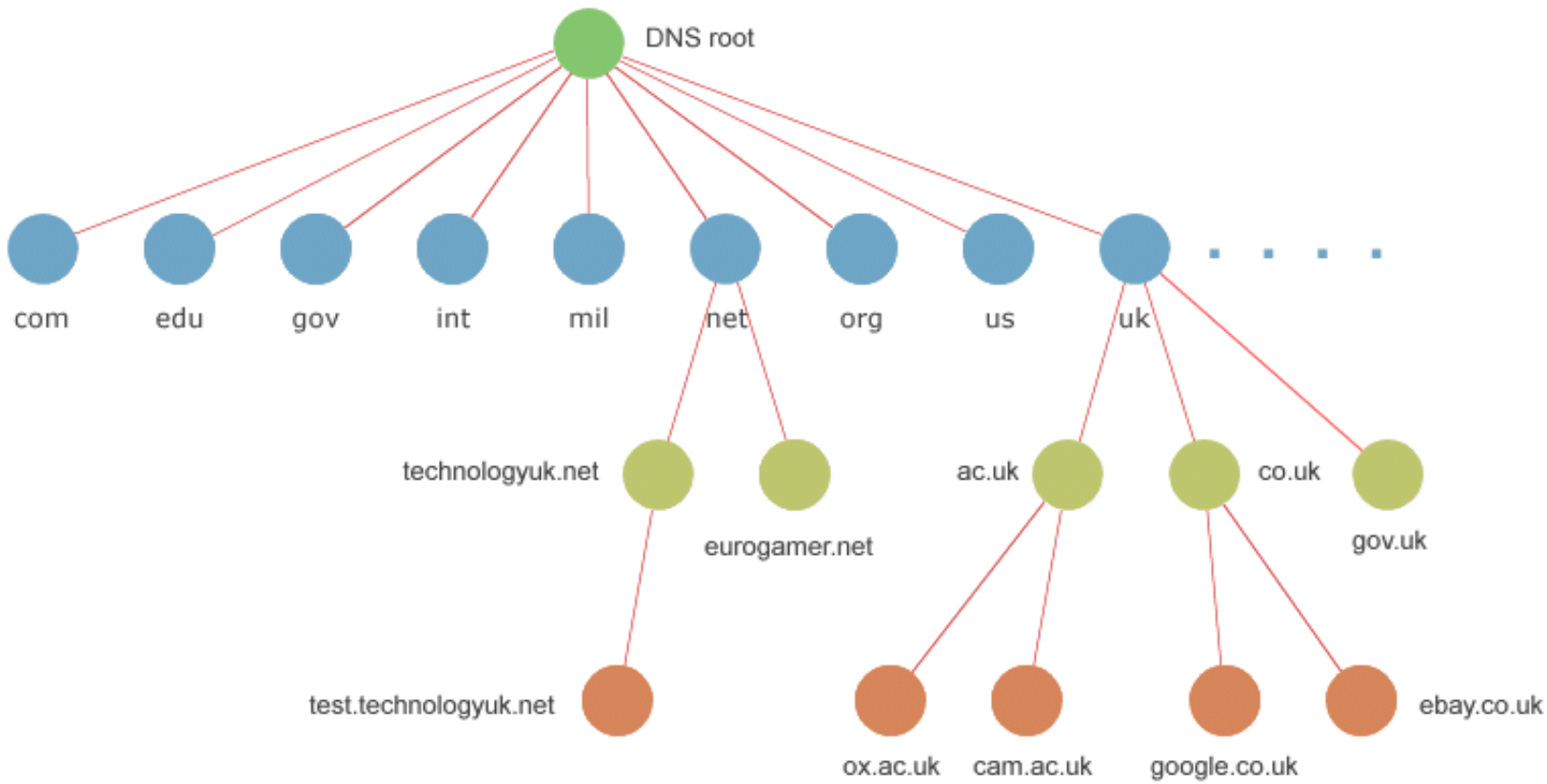
- Database can be updated dynamically
  - Add/delete/modify of any record
  - Only primary server can be dynamically updated

- Modification of the primary database triggers replication

Domain Names

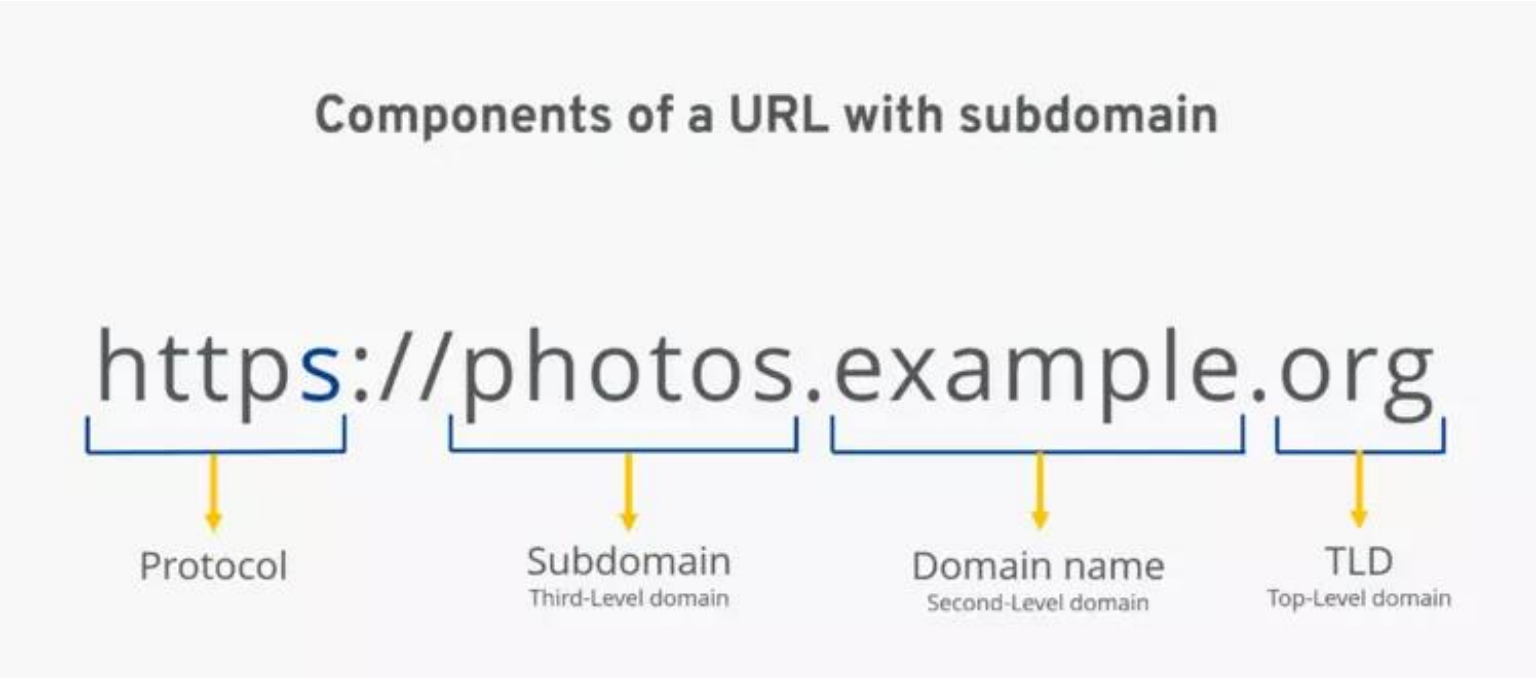
- A *domain name* is the sequence of labels from a node to the root, separated by dots (“.”s), read left to right
  - port.ac.uk
  - The name space has a maximum depth of 127 levels
  - Domain names are limited to 255 characters in length
- A node’s domain name identifies its position in the name space

Domain Name Structure



Subdomains

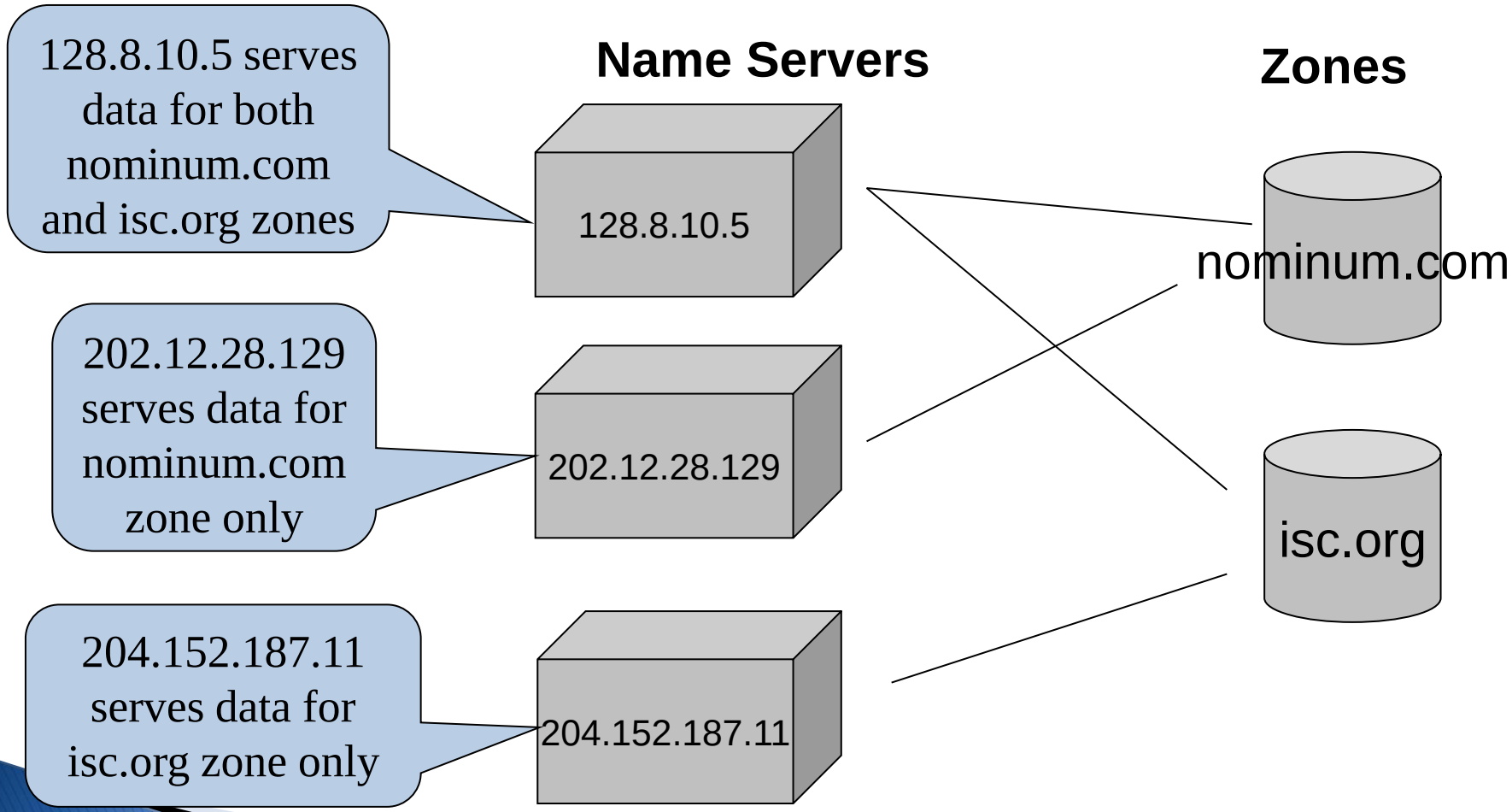
- One domain is a subdomain of another if its domain name ends in the other's domain name



(Domain) Name Servers

- Name servers store information about the name space in units called “zones”
  - The name servers that serve a complete zone are said to “have authority for” or “be authoritative for” the zone
- More than one name servers can be authoritative for the same zone
  - This ensures redundancy and spreads the load
- Also, a single name server may be authoritative for many zones

Name Servers and Zones



Types of Name Servers

- Two main types of servers
  - Authoritative – maintains the data
    - Primary – where the data is edited
    - Secondary – where data is replicated to
  - Non-authoritative (Caching) – stores data obtained from an authoritative server

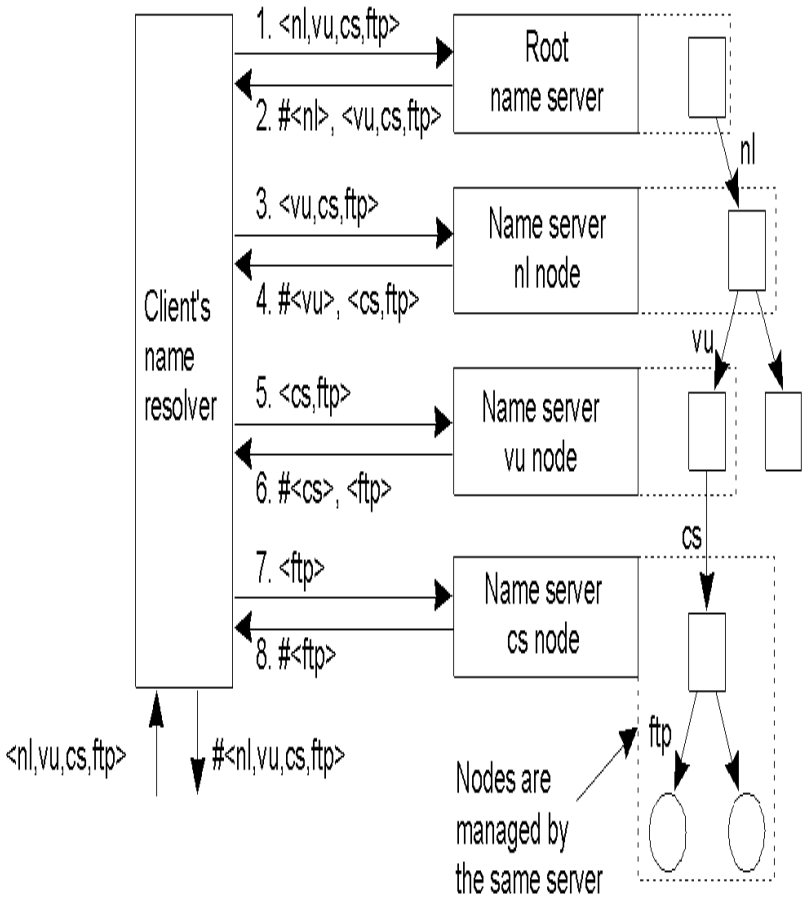
```
Non-authoritative answer:
Name:    uk.www.bbc.co.uk.pri.bbc.co.uk
Addresses:  212.58.233.252
            212.58.237.252
Aliases:    www.bbc.co.uk
            www.bbc.co.uk.pri.bbc.co.uk
```

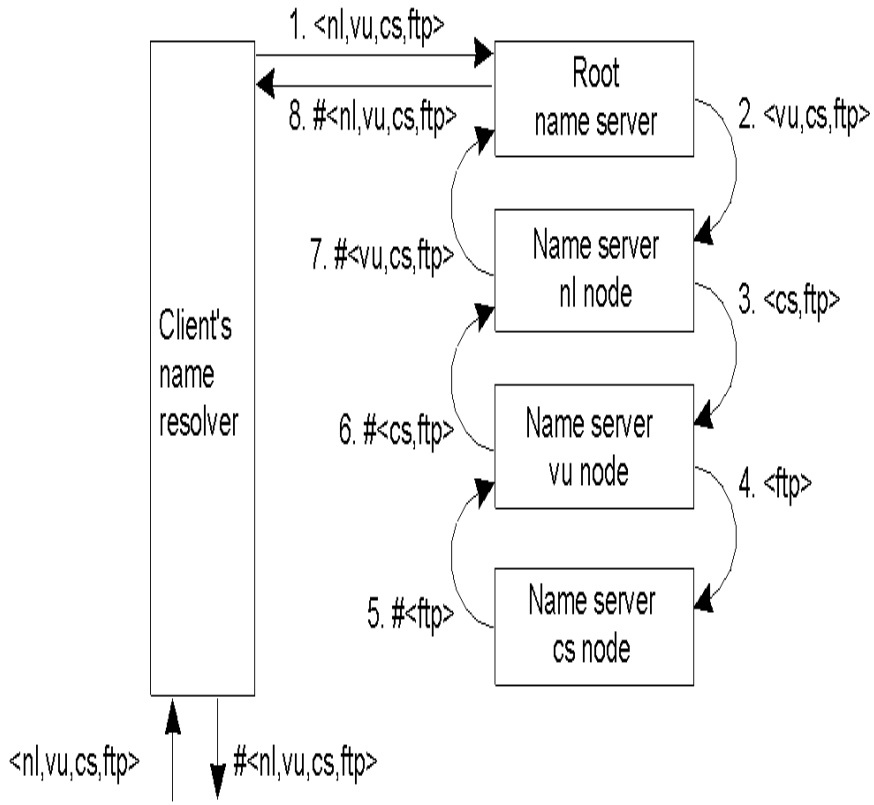
- No special hardware needed

Name Resolution

- *Name resolution* is the process by which local resolvers and name servers cooperate to find data in the name space
  - The *nslookup* command you are using this week
- Upon receiving a query from a resolver, a name server
  - 1) looks for the answer in its authoritative data and its cache
  - 2) If step 1 fails, the answer must be looked up through other servers

Iterative vs Recursive Resolution





The Resolution Process

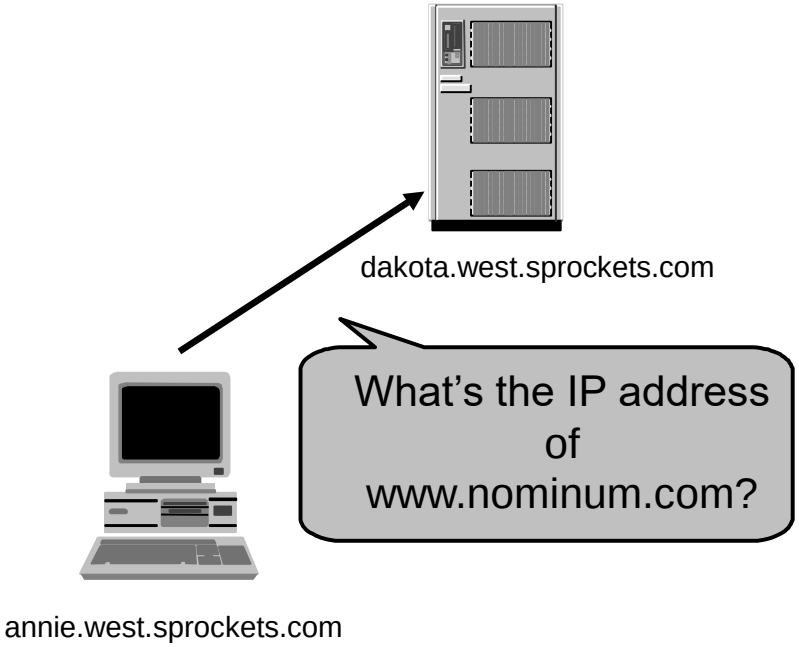
- Let's look at the iterative resolution process step-by-step:

annie.west.sprockets.com

```
ping www.nominum.com.
```

The Resolution Process

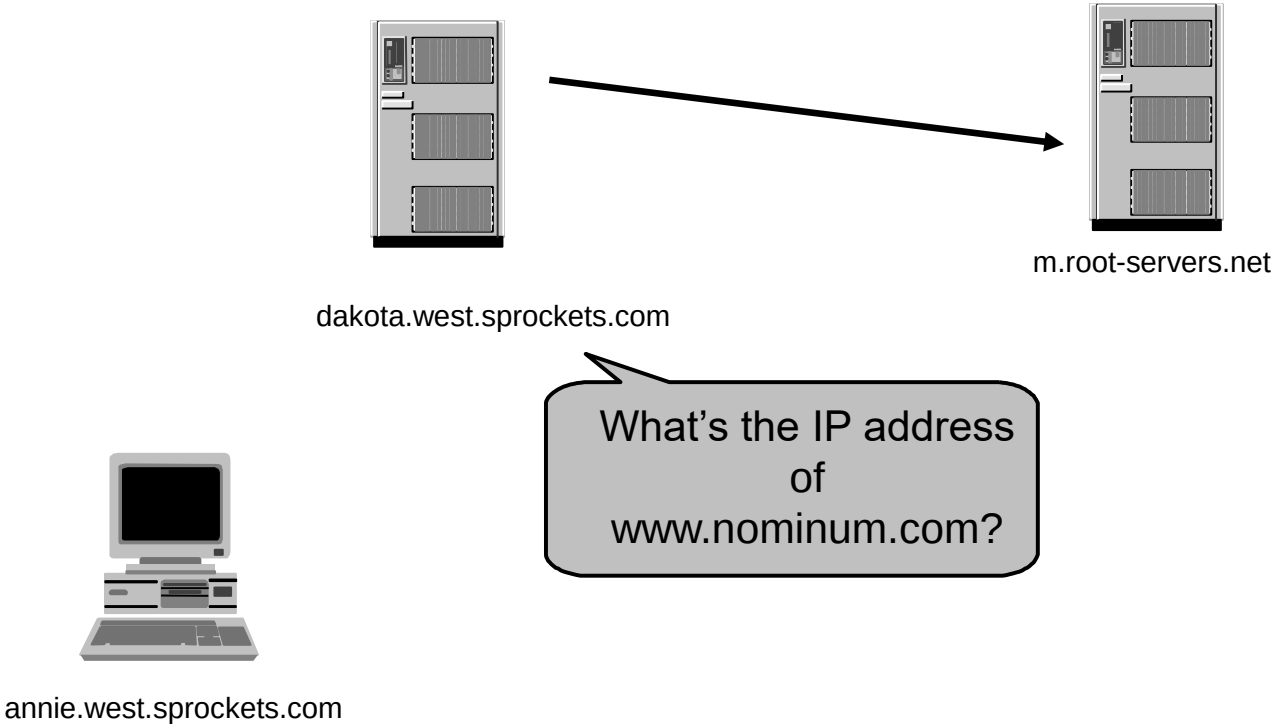
- The workstation *annie* asks its configured name server, *dakota,* for *www.nominum.com's* address




```
ping www.nominum.com.
```

The Resolution Process

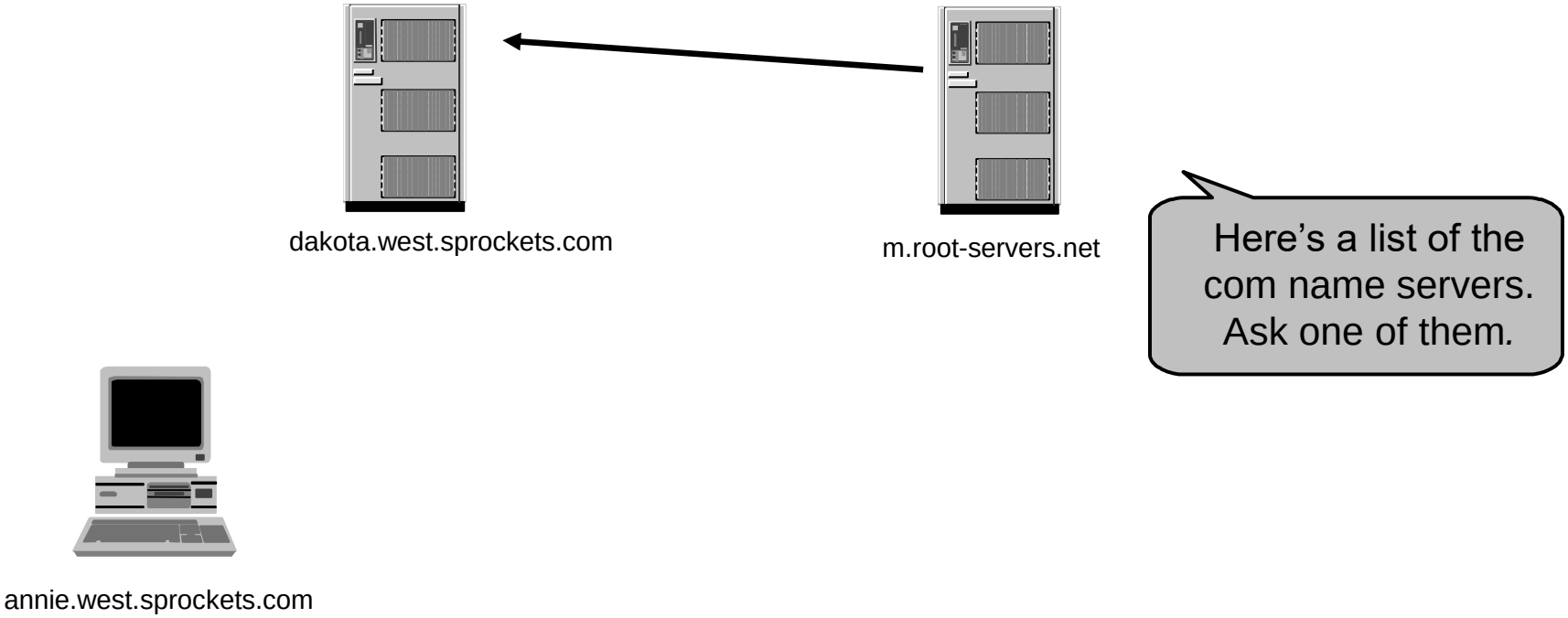
- The name server *dakota* asks a root name server, *m*, for *www.nominum.com's* address




```
ping www.nominum.com.
```

The Resolution Process

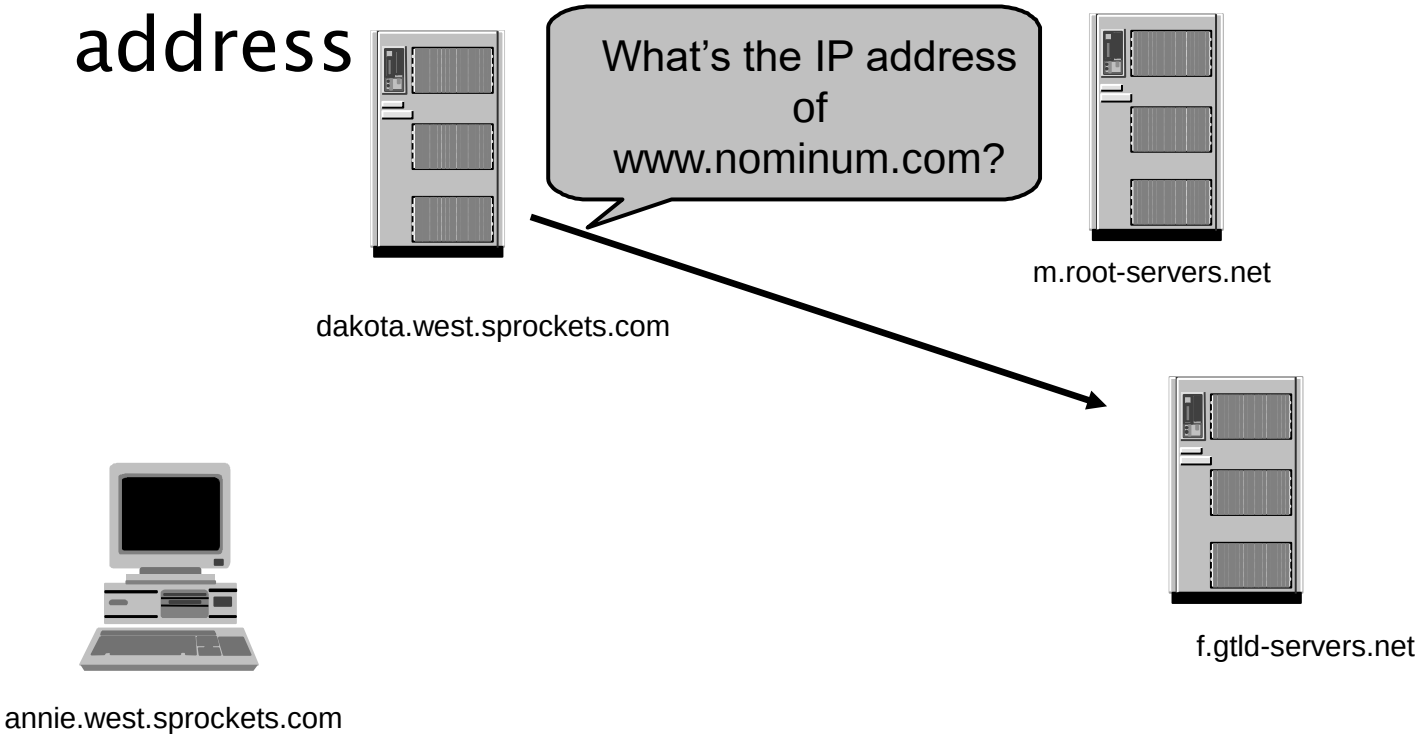
- The root server *m* refers *dakota* to the *com* name servers
- This type of response is called a “referral”




```
ping www.nominum.com.
```

The Resolution Process

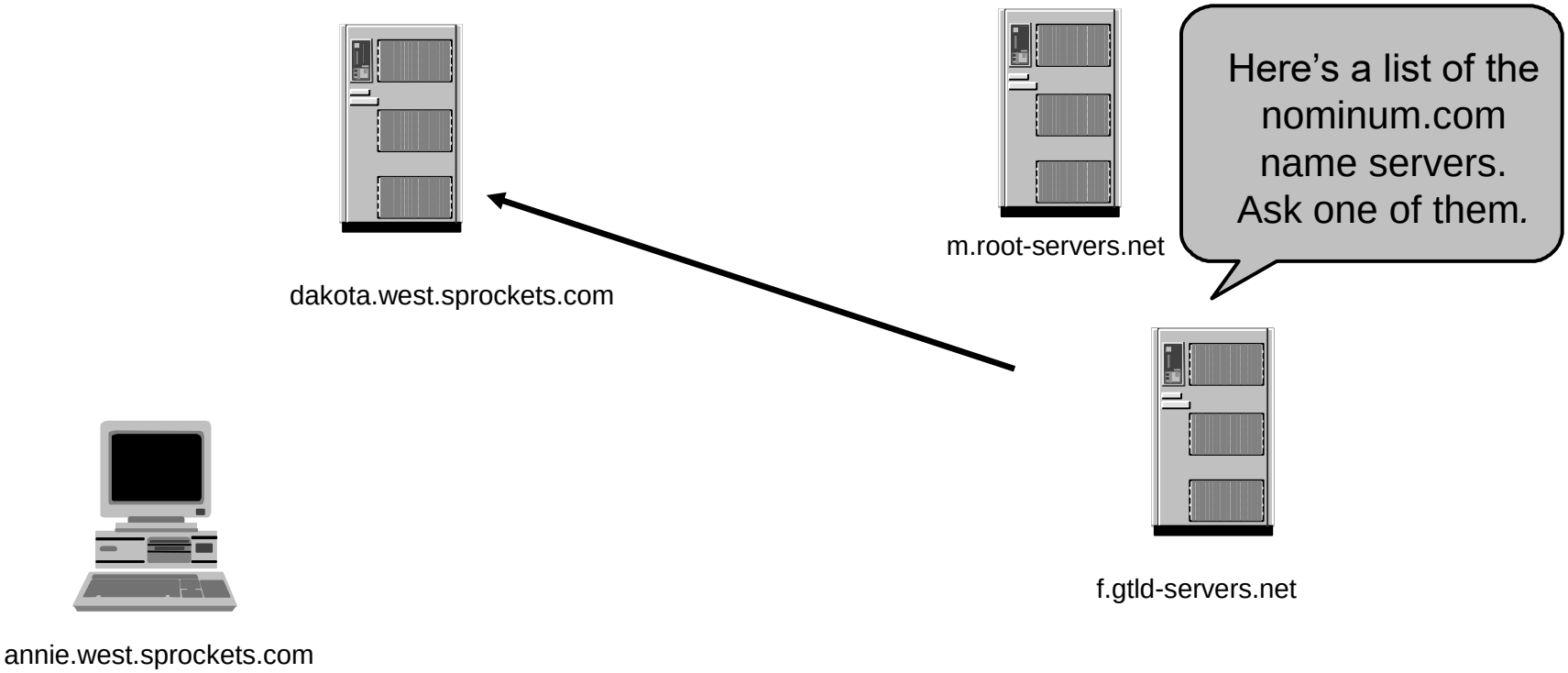
- The name server *dakota* asks a *com* name server, *f*, for *www.nominum.com's* address




```
ping www.nominum.com.
```

The Resolution Process

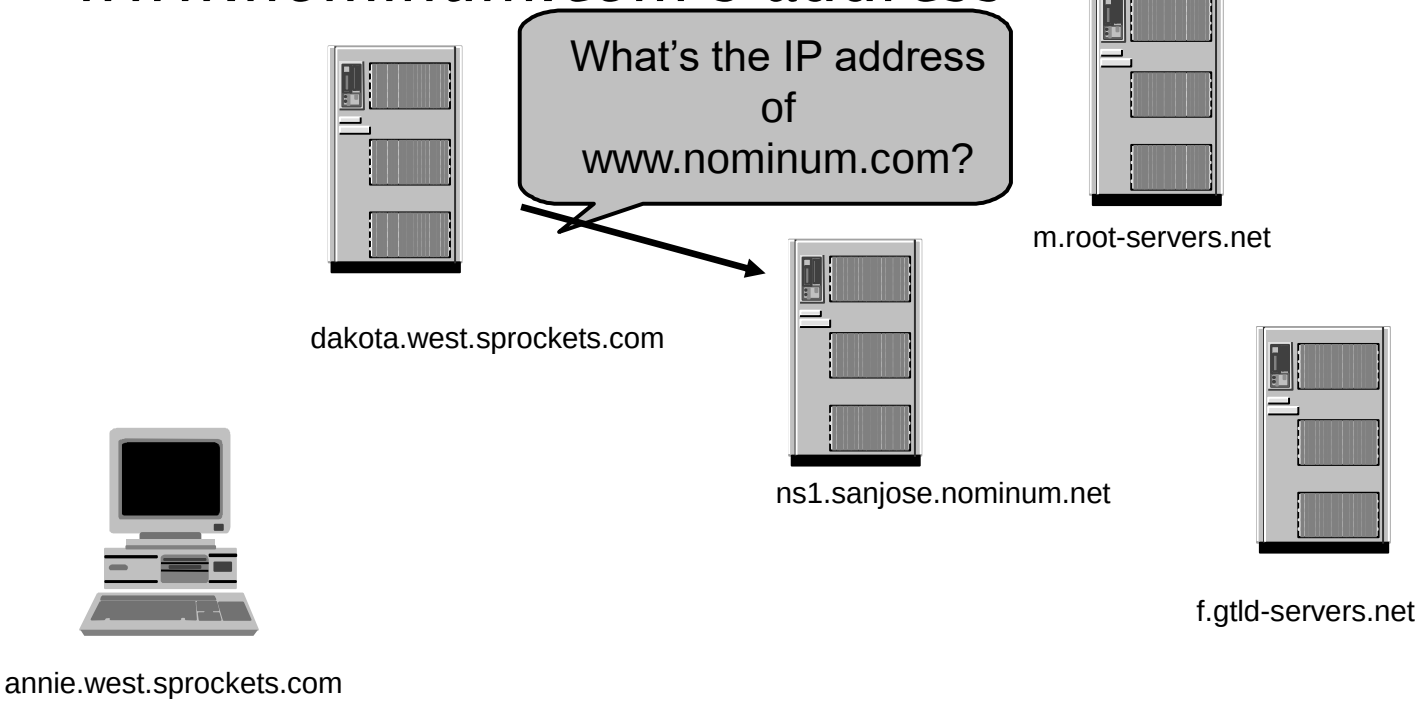
- The *com* name server *f* refers *dakota* to the *nominum.com* name servers




```
ping www.nominum.com.
```

The Resolution Process

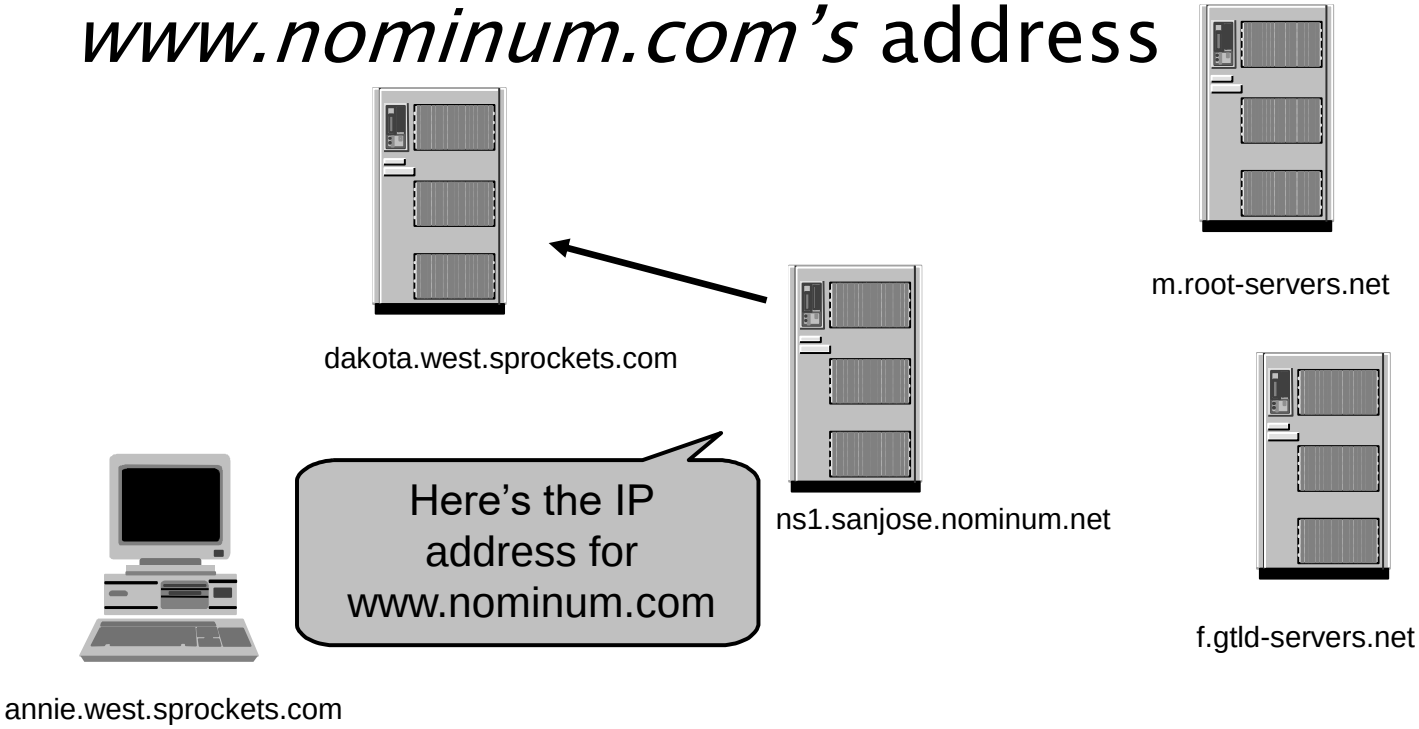
- The name server *dakota* asks a *nominum.com* name server, *ns1.sanjose*, for *www.nominum.com's* address




```
ping www.nominum.com.
```

The Resolution Process

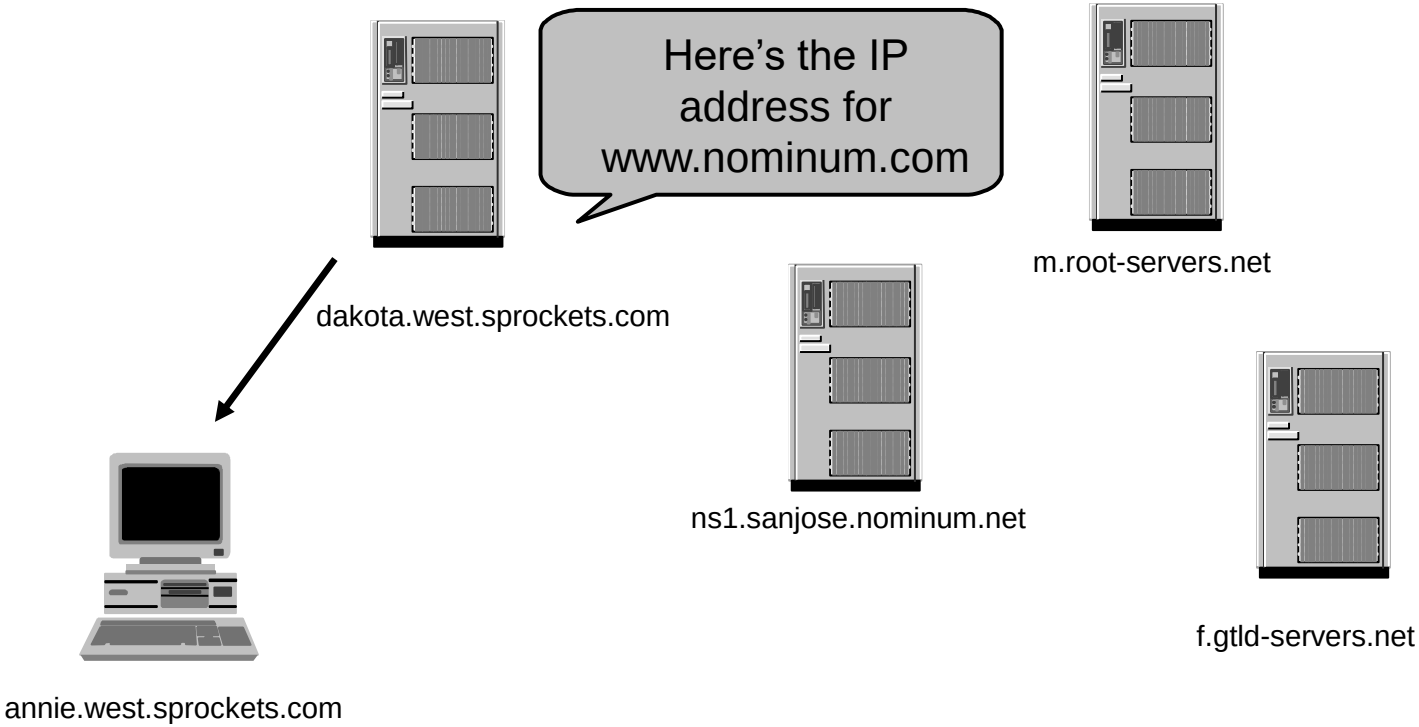
- The *nominum.com* name server *ns1.sanjose* responds with *www.nominum.com's* address




```
ping www.nominum.com.
```

The Resolution Process

- The name server *dakota* responds to *annie* with *www.nominum.com's* address




```
ping www.nominum.com.
```

Resolution Process (Caching)

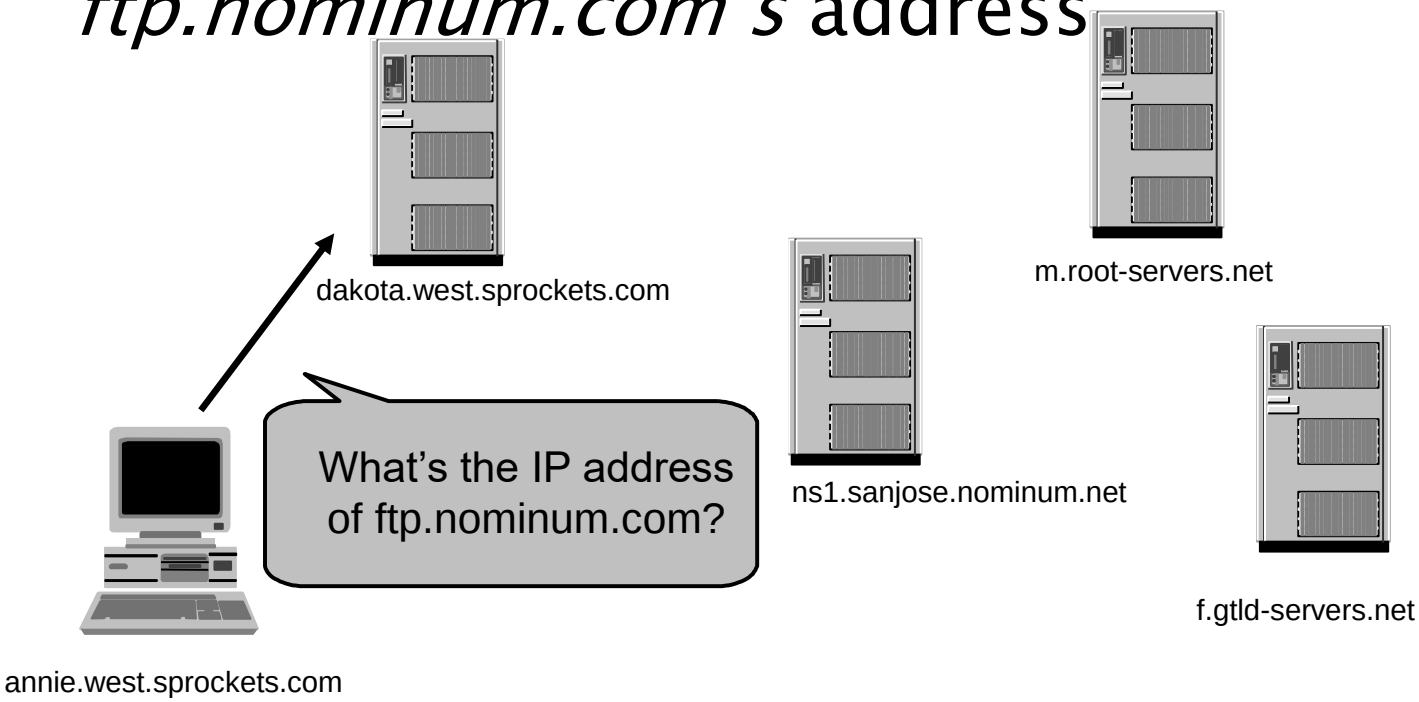
- After the previous query, the name server *dakota* now knows:
  - The names and IP addresses of the *com* name servers
  - The names and IP addresses of the *nominum.com* name servers
  - The IP address of *www.nominum.com*
- Let's look at the resolution process again

annie.west.sprockets.com

```
ping ftp.nominum.com.
```

Resolution Process (Caching)

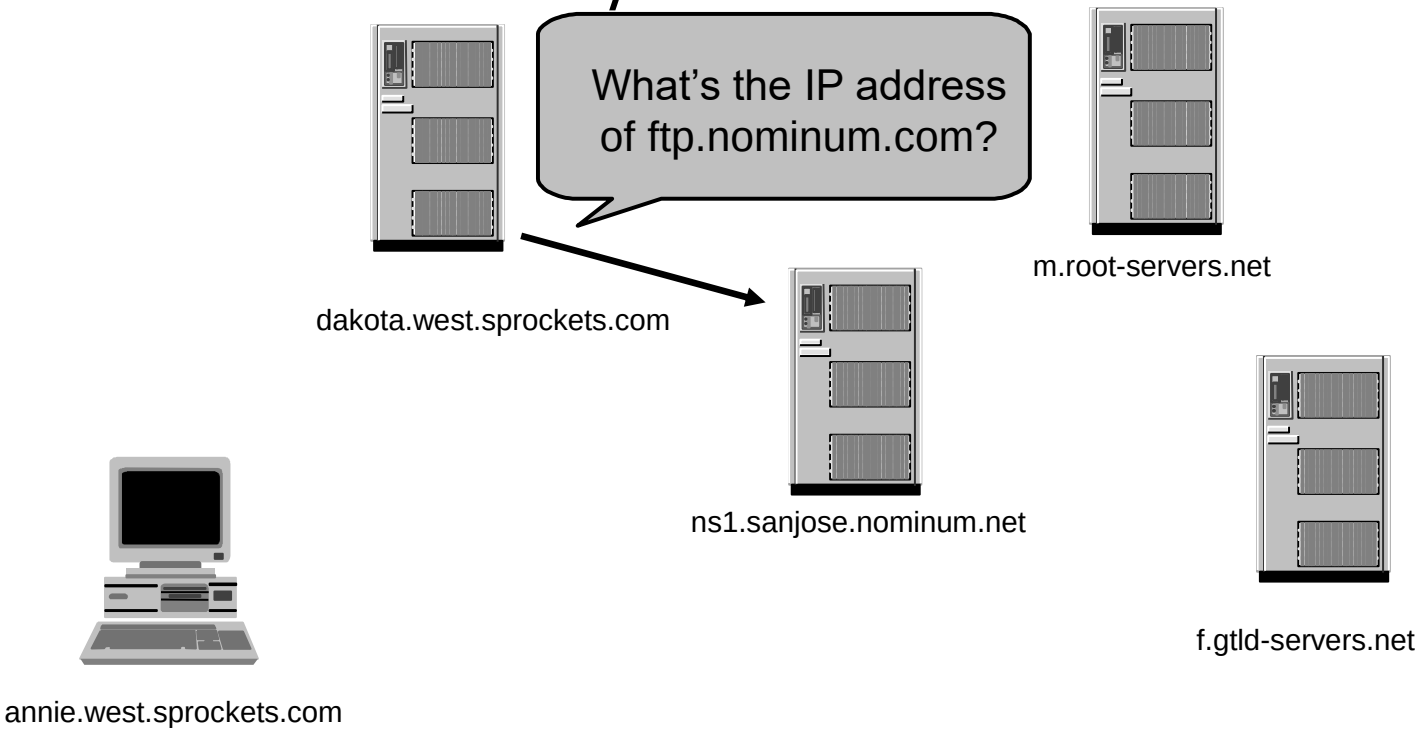
- The workstation *annie* asks its configured name server, *dakota,* for *ftp.nominum.com's* address




```
ping ftp.nominum.com.
```

Resolution Process (Caching)

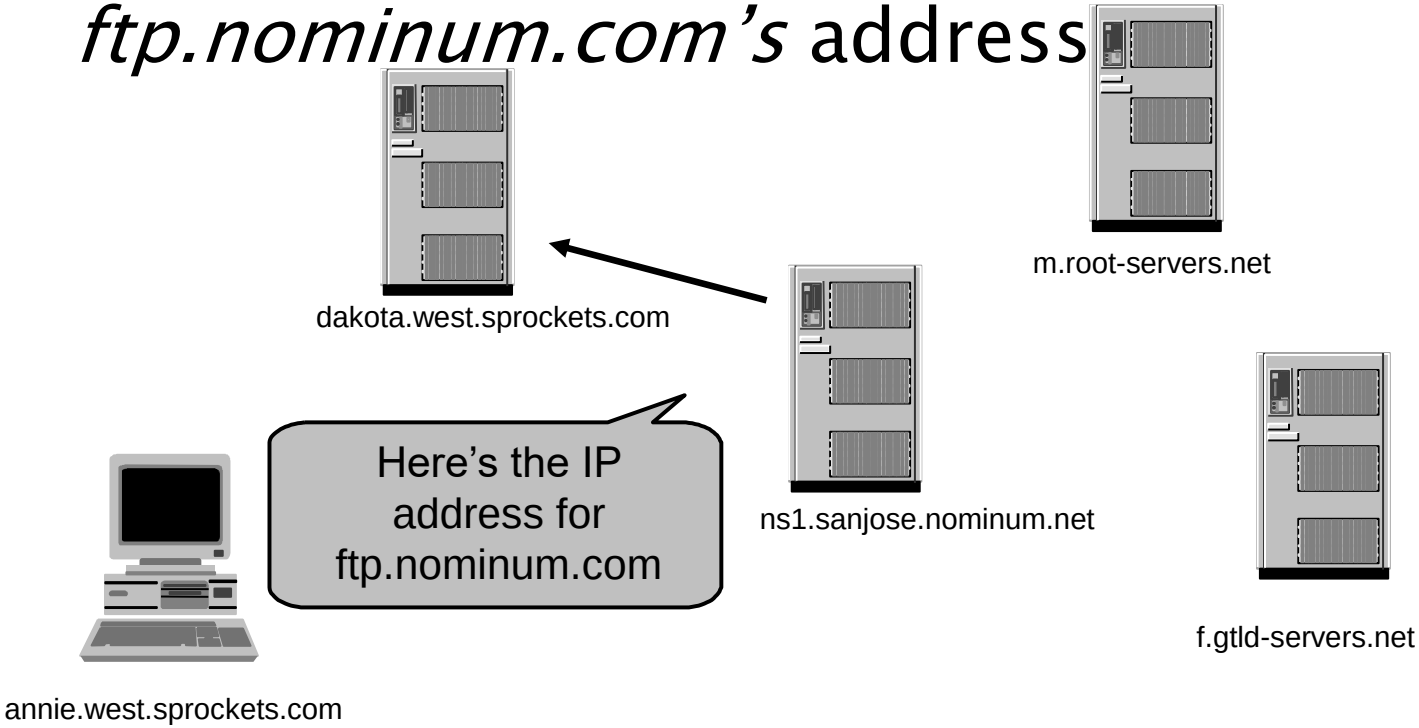
- *dakota* has cached a NS record indicating *ns1.sanjose* is an *nominum.com* name server, so it asks it for *ftp.nominum.com's* address




```
ping ftp.nominum.com.
```

Resolution Process (Caching)

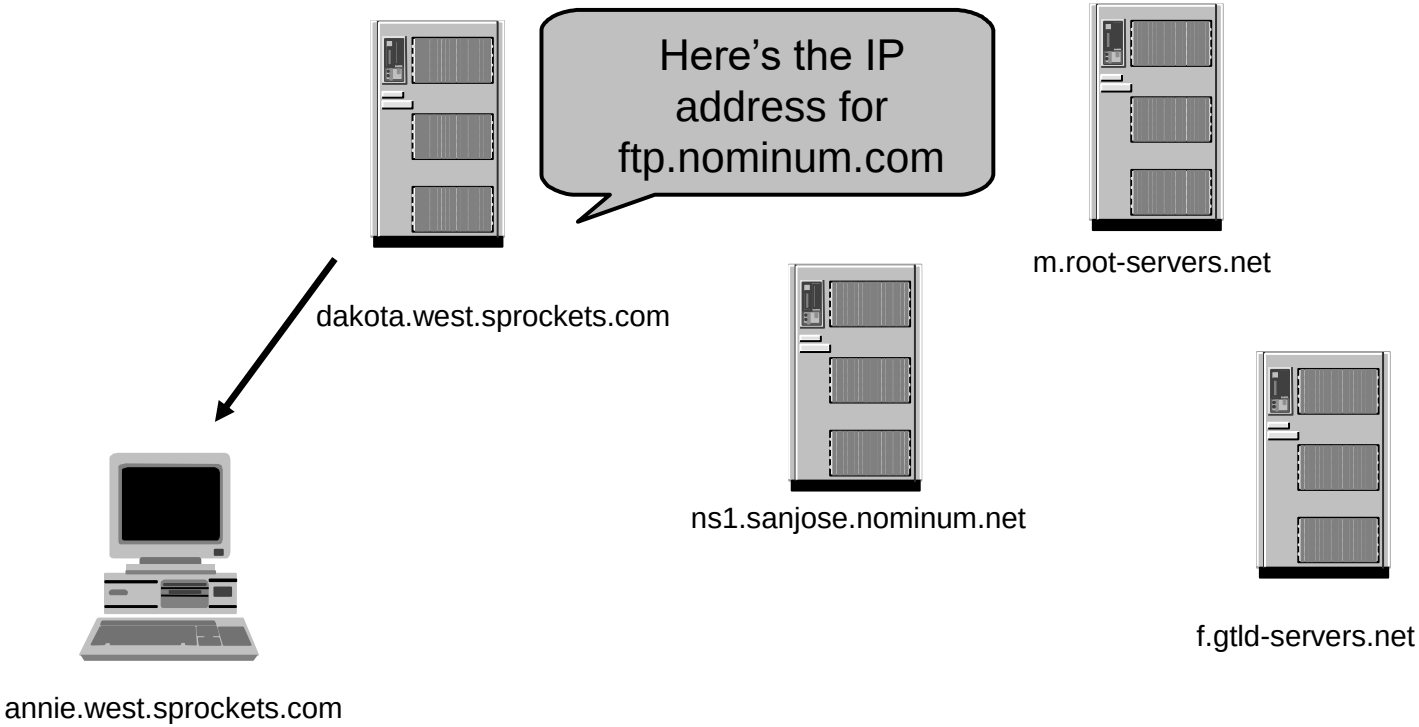
- The *nominum.com* name server *ns1.sanjose* responds with *ftp.nominum.com's* address




```
ping ftp.nominum.com.
```

Resolution Process (Caching)

- The name server *dakota* responds to *annie* with *ftp.nominum.com's* address




```
ping ftp.nominum.com.
```

The Root Nameservers (FYI only)

- The root zone file lists the names and IP addresses of the authoritative DNS servers for all Top-Level Domains (TLDs)
  - https://www.iana.org/domains/root/db
  - https://data.iana.org/TLD/tlds-alpha-by-domain.txt
- The root zone file is published on 13 servers, “A” through “M”, around the Internet
  - https://www.iana.org/domains/root/servers
- Root name server operations currently provided by volunteer efforts by a very diverse set of organisations

Root Name Server Operators

Nameserver	Operated by:
A	Verisign (US East Coast)
B	University of S. California –Information Sciences Institute (US West Coast)
C	Cogent Communications (US East Coast)
D	University of Maryland (US East Coast)
E	NASA (Ames) (US West Coast)
F	Internet Software Consortium (US West Coast)
G	U. S. Dept. of Defense (ARL) (US East Coast)
H	U. S. Dept. of Defense (DISA) (US East Coast)
I	Autonomica (SE)
J	Verisign (US East Coast)
K	RIPE-NCC (UK)
L	ICANN (US West Coast)
M	WIDE (JP)

Load Concerns (FYI only)

- DNS can handle the load
  - DNS root servers get approximately 3000 queries per second
    - Empirical proofs (DDoS attacks) show root name servers can handle 50,000 queries per second
      - Limitation is network bandwidth, not the DNS protocol
  - in-addr.arpa zone, which translates numbers to names, gets about 2000 queries per second

Performance Concerns (FYI only)

- DNS is a very lightweight protocol
  - Simple query – response
- Any performance limitations are the result of network limitations
  - Speed of light
  - Network congestion
  - Switching/forwarding latencies

Security Concerns (FYI only)

- Base DNS protocol (RFC 1034, 1035) is insecure
  - DNS spoofing (cache poisoning) attacks are possible
- DNS Security Enhancements (DNSSEC, RFC 2565) remedies this flaw
  - But creates new ones
    - DoS attacks
    - Amplification attacks
- DNSSEC strongly discourages large flat zones
  - Hierarchy (delegation) is good

Next Week…

- Routing:: IP addresses and subnets