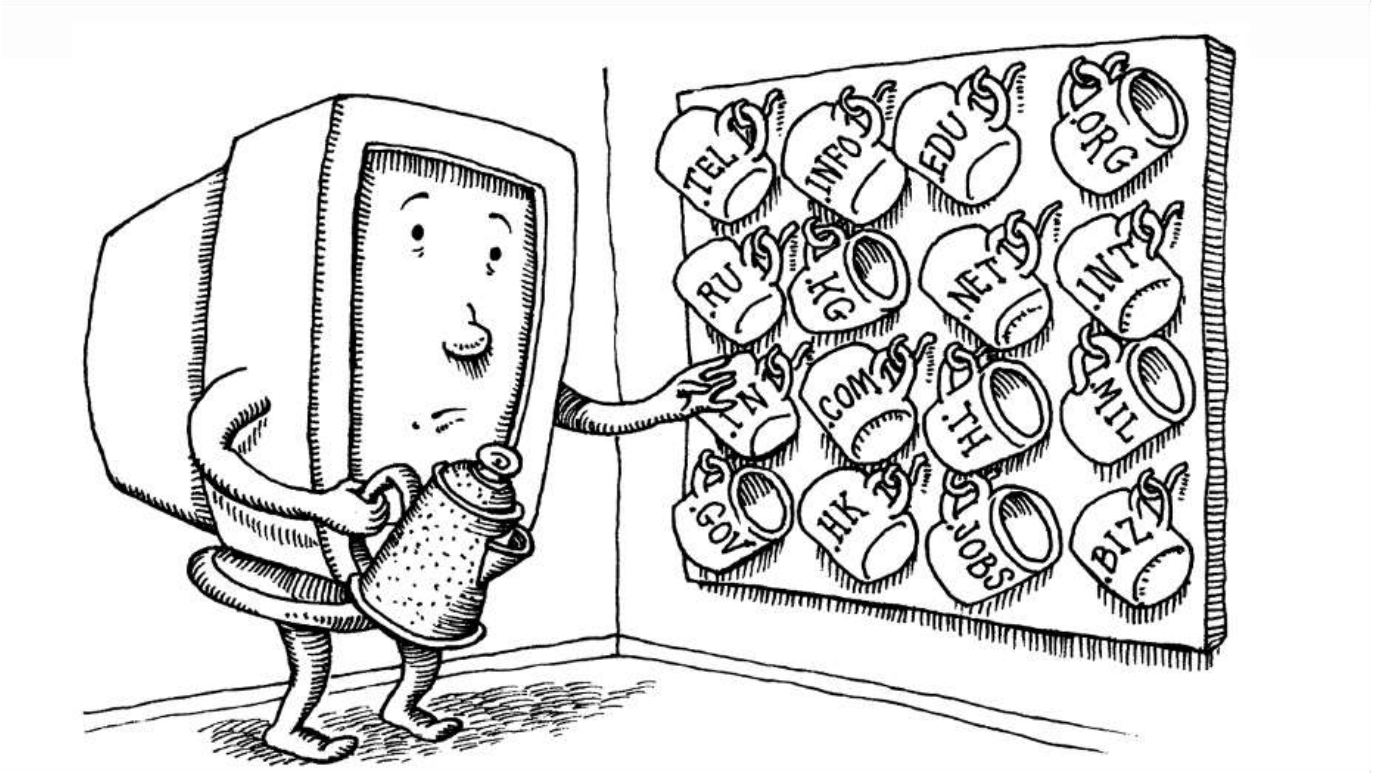
CS183

Instructor: Ali Davanian



DNS: Domain Name System

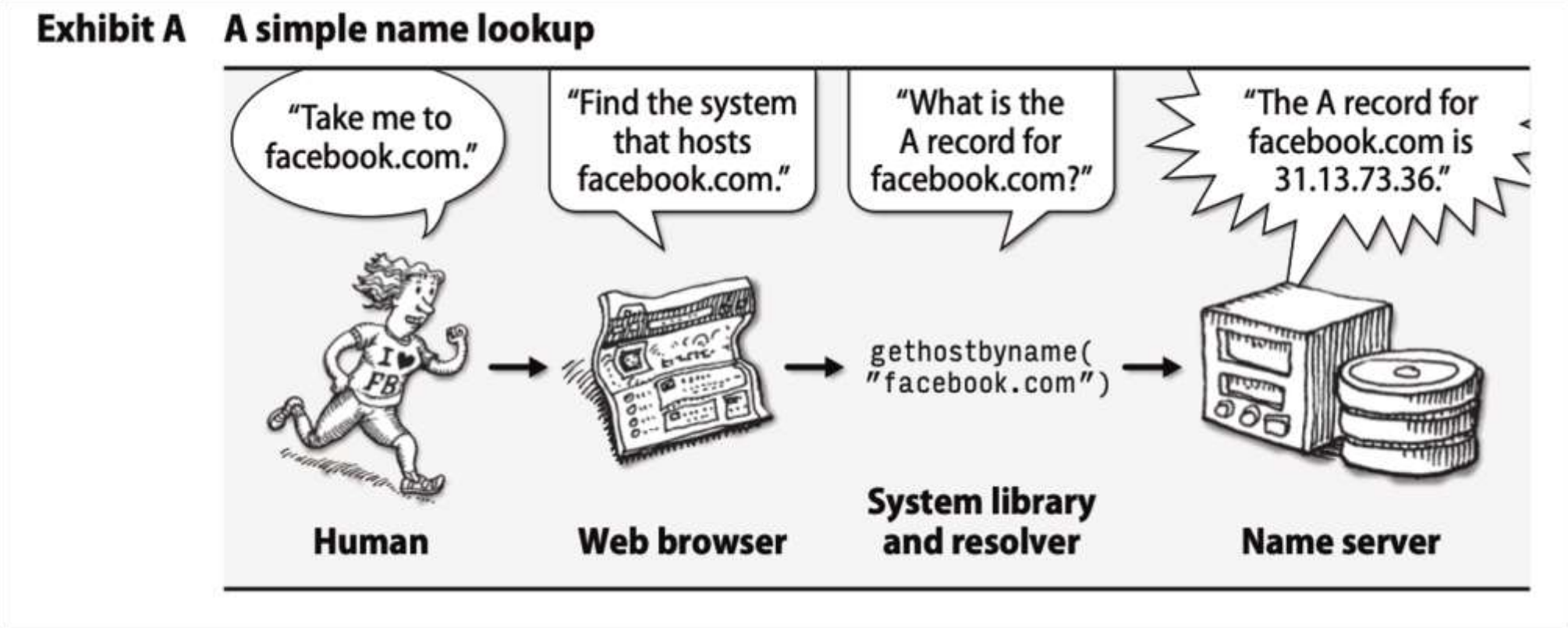
Logistics

- Pop Quiz
  - There will be a quiz on Thursday
- Helping with Projects
  - Sign up for a 5 mins chat/help on Thursday
  - https://forms.gle/Ch7bGJgfLGKiSk848 (link is available on Slack too)

Motivation behind DNS service

- Low level network layers understand only IP address
- Users and user level programs refer to resources by name
- A network service should provide mapping between names and IPs
- Domain Name System (DNS) provides mapping between names and IP
- Software programs constantly use DNS service to resolve a name to an IP

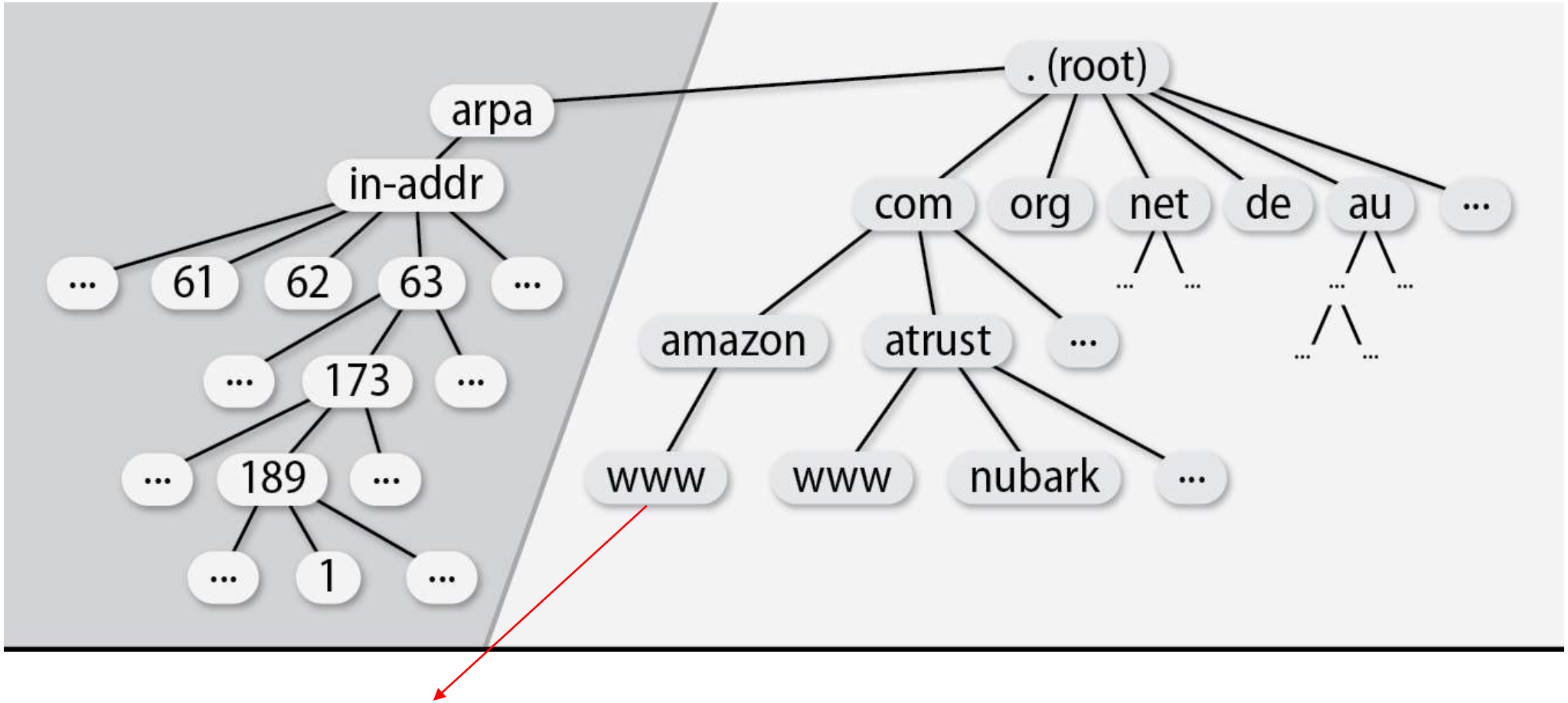
DNS name lookup



DNS architecture

- DNS has a database of names to IPs pairs
- In the simplest form, every host can keep a copy of a DNS database
  - Similar to telephone directories
  - /etc/hosts file plays this role
  - This is inefficient; DNS database is large, and records are constantly changing
- DNS is a distributed database
- DNS names are organized and maintained in a hierarchical structure
  - Higher levels provide address of lower levels

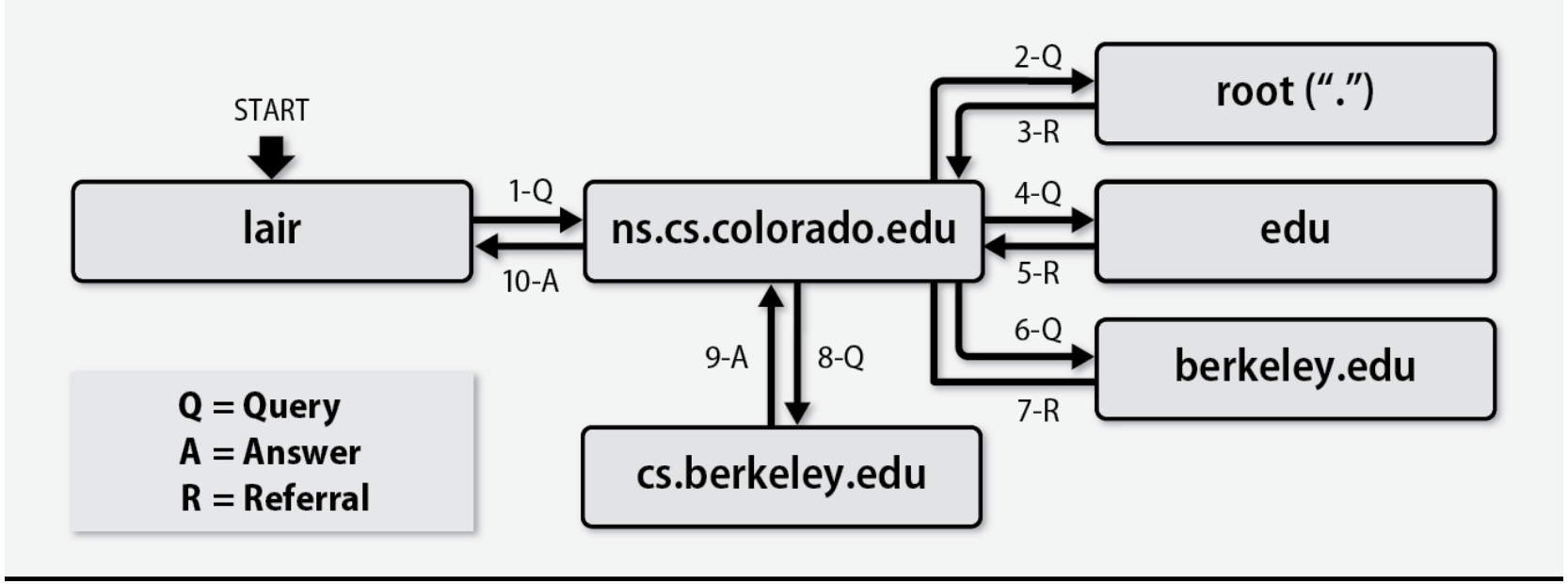
DNS Hierarchy



www.amazon.com

DNS name lookup process

- Client (with the name lair.cs.colorado.edu) wants to communicate with server vangogh.cs.Berkeley.edu

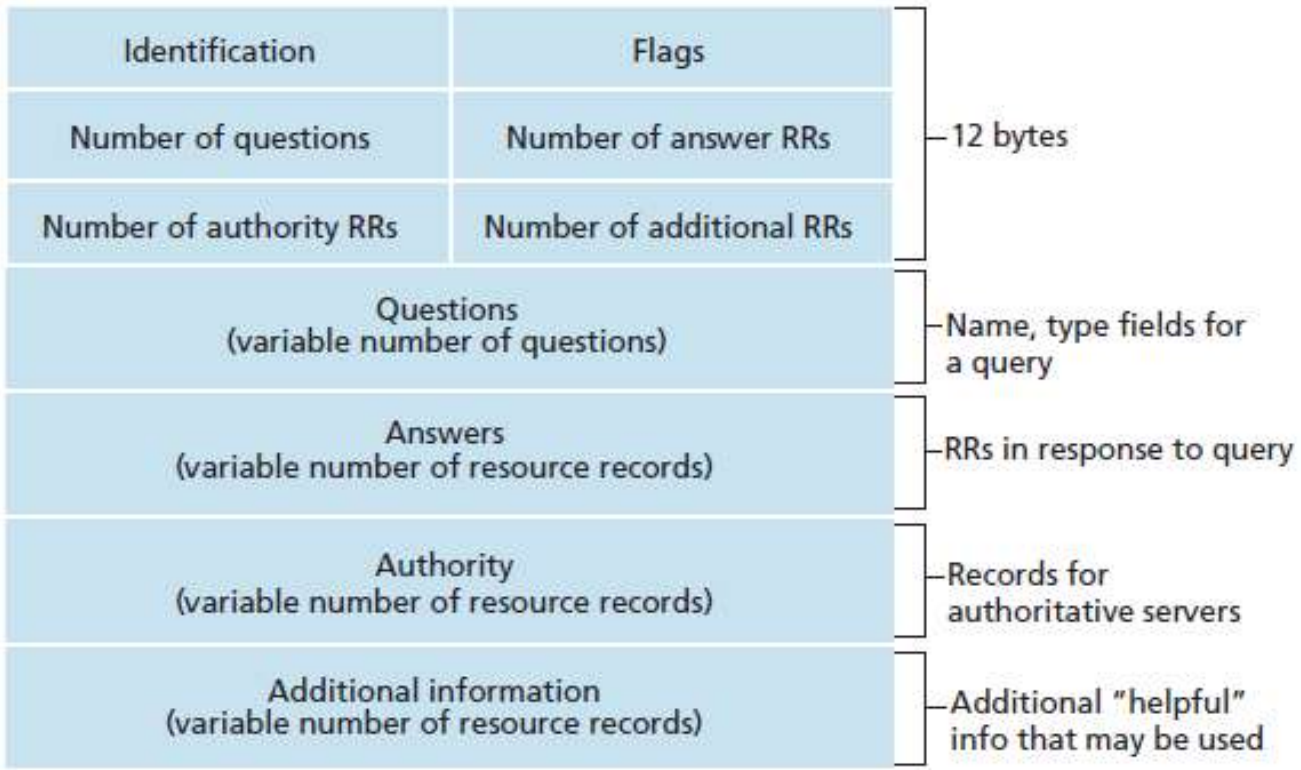


DNS terminology

- Hostname
  - The name for a host (a computer) e.g. bolt or sledge
- Fully Qualified Domain Name (FQDN
  - www.facebook.com
- Subdomain
  - cs.ucr.edu
- Name resolution or name lookup
  - The process by which a name would be resolved to a an IP
- Top Level Domain (TLD)
  - com, net, org etc.
- DNS query or DNS request
  - A message that asks for resolution of a name to an IP
- DNS response
  - A message that contains the IP for a queried name
- Domain Name Server or Name Server (NS)
  - The service provider that can resolve names to IPs
- Zone
  - A DNS database
- Recursion
  - A process in which, a server resolves a name on behalf of a client
- Bind
  - A software package that includes a DNS server and tools
- Named
  - Linux DNS server (part of the BIND package)

DNS message format

- DNS queries and responses are exchanged in a known format
  - Both clients and name servers know how to interpret the messages



Records in a DNS database

- Zones are either:
  - Forward: Names to IPS
  - Backward: IPs to names
- Each zone keeps the records of a single namespace
  - For instance cs183.local
- There are several record types

Table 17.6 DNS record types

	Type	Name	Function
Zone	SOA	Start Of Authority	Defines a DNS zone
	NS	Name Server	Identifies servers, delegates subdomains
Basic	A	IPv4 Address	Name-to-address translation
	AAAA	IPv6 Address	Name-to-IPv6-address translation
	PTR	Pointer	Address-to-name translation
	MX	Mail Exchanger	Controls email routing
Security and DNSSEC	DS	Delegation Signer	Hash of signed child zone's key-signing key
	DNSKEY	Public Key	Public key for a DNS name
	NSEC	Next Secure	Used with DNSSEC for negative answers
	NSEC3[a]	Next Secure v3	Used with DNSSEC for negative answers
	RRSIG	Signature	Signed, authenticated resource record set
	DLV	Lookaside	Nonroot trust anchor for DNSSEC
	SSHFP	SSH Fingerprint	SSH host key, allows verification via DNS
	SPF	Sender Policy	Identifies mail servers, inhibits forging
	DKIM	Domain Keys	Verify email sender and message integrity
Optional	CNAME	Canonical Name	Nicknames or aliases for a host
	SRV	Services	Gives locations of well-known services
	TXT	Text	Comments or untyped information[b]

a. The original NSEC system allows hackers handy with the **dig** command to easily list all of a zone's records. NSEC3 has fixed this weakness but is more expensive to compute; both are currently in use.

b. TXT records are increasingly being used to try out new ideas without having to get full IETF blessing for new record types. For example, SPF and DKIM records were first implemented as TXT records.

Name server configuration on a CentOS client

- DNS configuration can be automatically taken from a DHCP server
- Statically, name servers for a client can be set in /etc/resolve.conf
  - nameserver [IP]
  - [IP] can be a public DNS server such as 4.2.2.4 or 8.8.8.8
- Alternatively, you can modify /etc/sysconfig/network-scripts/ifcfg-[interface-name]:
  - DNS1=[IP1]
  - DNS2=[IP2]
- By default, a Linux client queries the name servers and then falls back to a local database stored at /etc/hosts
  - The order can be modified in /etc/nsswitch.conf

Why should we setup a DNS server?

- There are two main motivations for setting up a DNS server:
  - **Bandwidth efficiency and performance**: a local DNS server can serve as a cache, and can drop the outbound Internet traffic while improving latency
  - **Maintaining a namespace:** if you want to assign DNS names to your hosts, e.g. sledge.cs.ucr.edu
    - Some services rely on a DNS service, for instance Active Directory
    - If you want to publish a service (for instance a mail server or a website), you need a DNS server
- While cloud services usually provide you a DNS service, still you'd need to know how a DNS server can be managed

Types of name servers

Table 17.3 A name server taxonomy

Type of server	Description
authoritative	An official representative of a zone
master	The master server for a zone; gets its data from a disk file
primary	Another name for the master server
slave	Copies its data from the master
secondary	Another name for a slave server
stub	Like a slave, but copies only name server data (not host data)
distribution	A server advertised only within a domain (aka "stealth server")
nonauthoritative[a]	Answers a query from cache; doesn't know if the data is still valid
caching	Caches data from previous queries; usually has no local zones
forwarder	Performs queries on behalf of many clients; builds a large cache
recursive	Queries on your behalf until it returns either an answer or an error
nonrecursive	Refers you to another server if it can't answer a query

a. Strictly speaking, "nonauthoritative" is an attribute of a DNS query response, not a server.

Steps to setup a DNS server

- Install the DNS server
- Decide and configure the name server based on its type
  - For instance, is it an authoritative or non-authoritative server?
- Create the database and its record
  - The mapping between names and IPs
- Start the name server
  - We usually want to automatically start after the boot
- Allow the traffic pass through the Firewalls

DNS servers in Linux

- **Bind** software package provides the DNS server **named**
  - Bind tools also provide additional tools for DNS based debugging such as nslookup, dig, host and drill
- named is a system service
  - And so it has a unit file at /usr/lib/systemd/system/named.service
  - This also means that it has higher privileges than normal user processes
- named is a network service, and it listens on UDP port 53 (default DNS port)
- You can install it on CentOS via:
  - sudo yum install bind bind-utils

named configurations for a local DNS server

- named reads configurations from /etc/named.conf

```
options {
// listen-on port 53 { 127.0.0.1; };
// listen-on-v6 port 53 { ::1; };
directory "/var/named";
dump-file "/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
memstatistics-file "/var/named/data/named_mem_stats.txt";
recursing-file  "/var/named/data/named.recursing";
secroots-file   "/var/named/data/named.secroots";
allow-query     { localhost;10.0.12.0/24; };


recursion yes;


dnssec-enable yes;
dnssec-validation yes;


/* Path to ISC DLV key */
bindkeys-file "/etc/named.root.key";


managed-keys-directory "/var/named/dynamic";


pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";
};
```

Listen on all IP addresses

Only answer to 10.0.12.0/24 subnet

Resolve the names on behalf of clients

These two combined say that the database is at /var/named/cs183.local.db

```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
type hint;
file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

//forward zone
zone "cs183.local" IN {
     type master;
     file "cs183.local.db";
     allow-update { none; };
     allow-query { any; };
};

//backward zone
zone "12.0.10.in-addr.arpa" IN {
     type master;
     file "cs183.local.rev";
     allow-update { none; };
     allow-query { any; };
};
```

Maintain databases for local names

named sample zone (database) file

- The zone file located at /var/named/cs183.local.db

```
$TTL 86400
@ IN SOA dns-primary.cs183.local. admin.cs183.local. (
                                                2020011800 ;Serial
                                                3600 ;Refresh
                                                1800 ;Retry
                                                604800 ;Expire
                                                86400 ;Minimum TTL
)


;Name Server Information
@ IN NS dns-primary.cs183.local.


;IP Address for Name Server
dns-primary IN A 10.0.12.12


;Mail Server MX (Mail exchanger) Record
cs183.local. IN MX 10 mail.cs183.local.


;A Record for the following Host name
www  IN   A   10.0.12.11
mail IN   A   10.0.12.11


;CNAME Record
ftp  IN   CNAME www.cs183.local.
```

The unit file configuration

- /usr/lib/systemd/system/named.service

```
[Unit]
Description=Berkeley Internet Name Domain (DNS)
Wants=nss-lookup.target
Wants=named-setup-rndc.service
Before=nss-lookup.target
After=network.target
After=named-setup-rndc.service

[Service]
Type=forking
Environment=NAMEDCONF=/etc/named.conf
EnvironmentFile=-/etc/sysconfig/named
Environment=KRB5_KTNAME=/etc/named.keytab
PIDFile=/run/named/named.pid

ExecStartPre=/bin/bash -c 'if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then /usr/sbin/named-checkconf -z "$NAMEDCONF"; else echo "Checking of zone files is disabled"; fi'
ExecStart=/usr/sbin/named -4 -u named -c ${NAMEDCONF} $OPTIONS

ExecReload=/bin/sh -c '/usr/sbin/rndc reload > /dev/null 2>&1 || /bin/kill -HUP $MAINPID'

ExecStop=/bin/sh -c '/usr/sbin/rndc stop > /dev/null 2>&1 || /bin/kill -TERM $MAINPID'

PrivateTmp=true

[Install]
WantedBy=multi-user.target
```

Shell script to install and configure named

```
sudo iptables -F
sudo yum install bind bind-utils
sudo cp named.service /usr/lib/systemd/system/named.service
sudo wget ftp://ftp.rs.internic.net/domain/db.cache -O
/var/named/named.ca
sudo systemctl start named
sudo systemctl enable named
sudo systemctl status named
sudo cp /etc/named.conf /etc/named.bk
sudo cp named.conf /etc/named.conf
sudo cp cs183.local.db /var/named/
sudo cp cs183.local.rev /var/named/
sudo chown named:named /var/named/cs183.local.db
sudo chown named:named /var/named/cs183.local.rev
sudo named-checkconf
sudo named-checkzone cs183.local /var/named/cs183.local.db
sudo named-checkzone 10.0.12.11 /var/named/cs183.local.rev
sudo systemctl restart named
```

Disable Firewall

Copying the configurations (instead of manually adding "-4" option

Updating the top level name servers list

Start named at startup

Copying the configurations (instead of manually editing)

named service runs under named user, so we need to give this user access

Load Balancing using DNS

- A single name can be mapped to several IP addresses

```
www   IN    A    10.0.12.11
      IN    A    10.0.12.21
      IN    A    10.0.12.31
```

- Most name servers use a different order each time they receive a query
  - This can be coarsely used for load balancing; commonly referred as round robin DNS load balancing
  - (This is not enough for your final project ☺)
- A fast reliable open source software is HAProxy

DNS Security

- named allows you to limit who can interact with your server
  - allow-query, allow-recursion, allow-transfer, allow-update
- Using “bogus” feature you can define what subnets to never query
- You can use symmetric encryption between servers for secure communication
  - See TSIG and TKEY options
- DNSSEC is a set of extensions that authenticate the origin of zone data and verify its integrity using public key cryptography

Bind logging and debugging

- By default, named writes the log messages into two places:
  - /var/log/messages file
  - /var/named/data/named.run
- This can be changed by modifying the ”logging’ section of the conf file:

```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
```

- You can also activate the Debug level by passing “-dX” e.g. “-d2” to the “named” command:
  - `ExecStart=/usr/sbin/named –d2 -4 -u named -c ${NAMEDCONF} $OPTIONS`

Questions?