DNS

Linux System Administration
Fall 2023

Domain Name System

- Distributed database created to replace text file containing every host name in the world
- Hierarchical naming system
  - top level domains (e.g. `.com`, `.edu`, `.org`, `.uk`)
  - domains (`google.com`, `colorado.edu`, `janet.ac.uk`)
  - hosts (`www.google.com`, `magellan.colorado.edu`)
- Distributed database
  - Authoritative servers for each level
- FQDN - fully qualified domain name

Translating Names to IP addresses

- `/etc/nsswitch.conf` sets name resolution
  - `hosts: files dns` selects first `/etc/hosts` then `DNS`
- `/etc/hosts` for ad hoc settings
  - `100.64.42.3 machinec machinec.dundermifflin.com`
- `/etc/resolv.conf` for DNS servers
  -
```
search dundermifflin.com
nameserver 100.64.42.2
nameserver 100.64.42.6
```

BIND

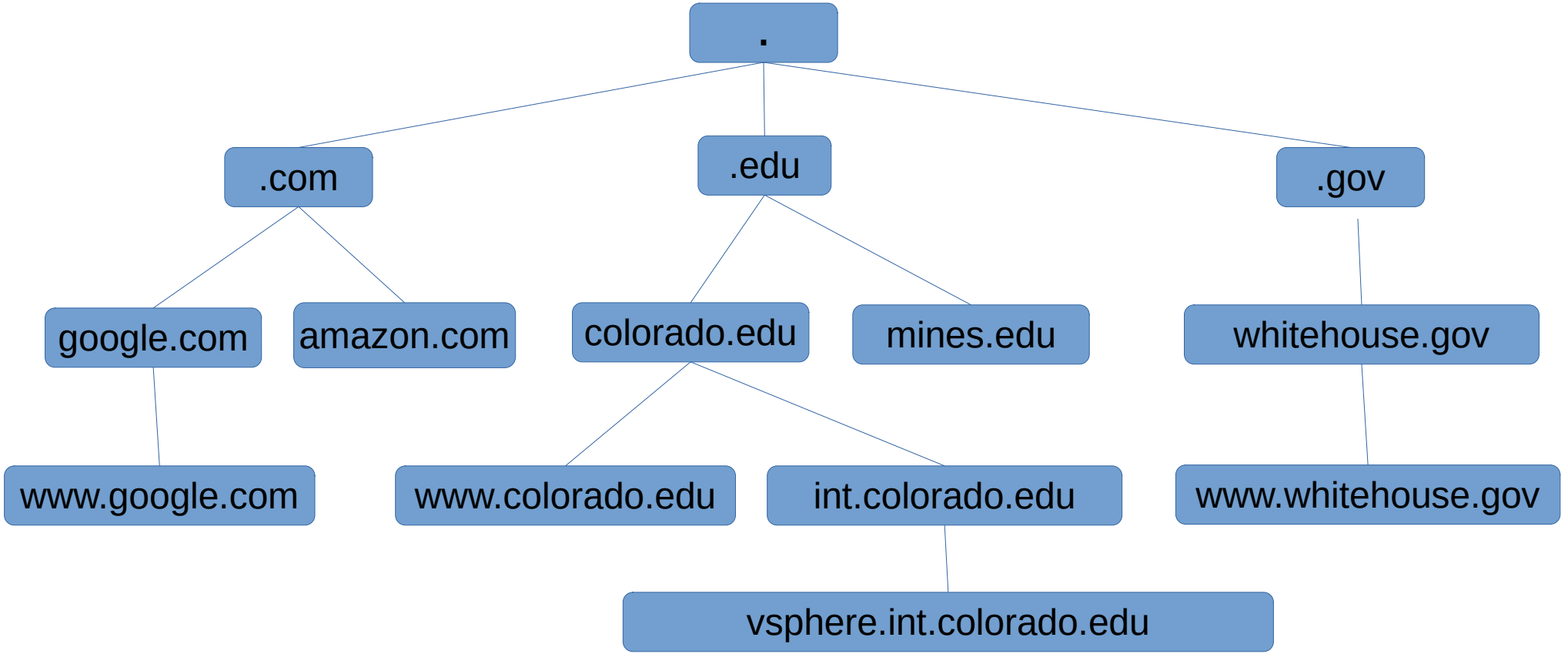
- Berkeley **I**nternet **N**ame **D**omain
  - Created early 1980s, released with BSD 4.3
  - BIND 9 released 2000 (actively maintained by ISC)
- `named` (name daemon)
  - Main configuration in `named.conf`
  - Supports primary and secondary servers
    - DNS includes a transfer mechanism to synchronize servers
  - Views allows one server to do split DNS

dig @ns type fqdn

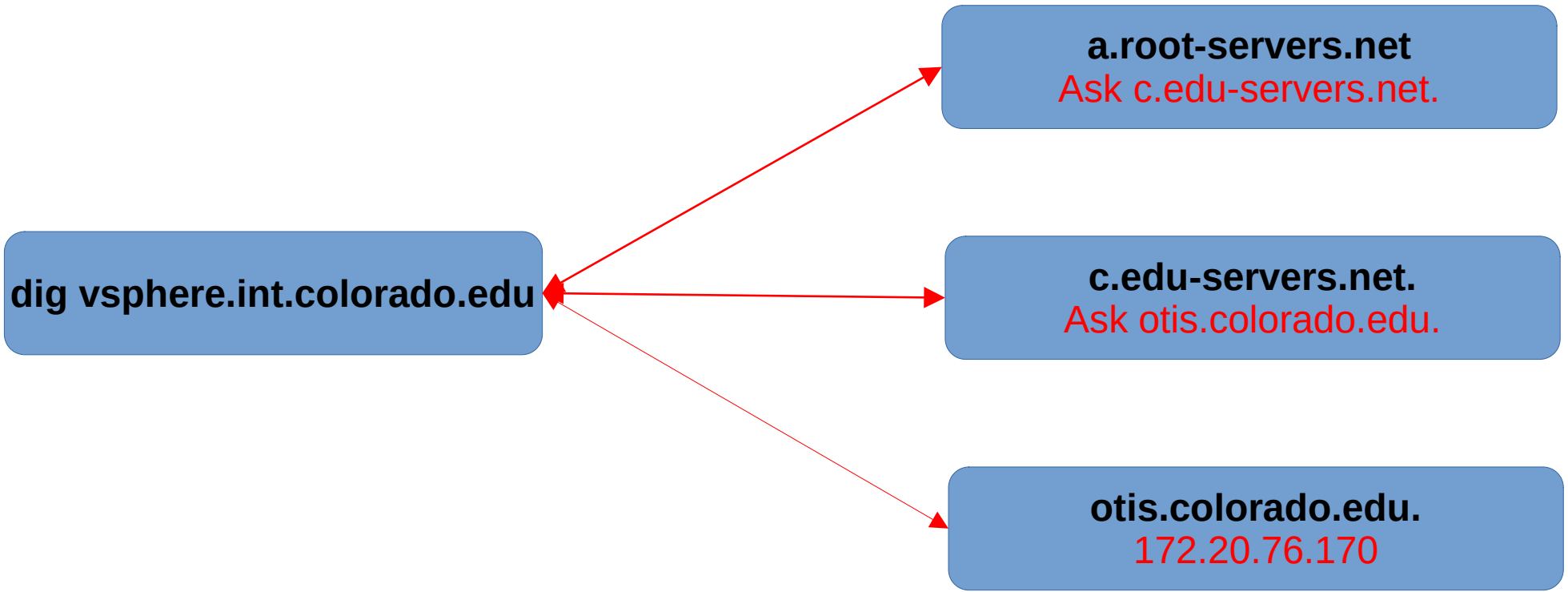
- Sections
  - Question
  - Answer
  - Authority
  - Additional
- Use -x for reverse DNS

```
dig simlab.colorado.edu
; <<>> DiG 9.16.1-Ubuntu <<>> simlab.colorado.edu
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8697
;; flags: qr rd ra; QUERY:1, ANSWER:1, AUTHORITY:3, ADDITIONAL:3

;; QUESTION SECTION:
;simlab.colorado.edu.  IN  A

;; ANSWER SECTION:
simlab.colorado.edu. 3600  IN  A 128.138.73.46

;; AUTHORITY SECTION:
colorado.edu.3600  IN  NS  oldduke.colorado.edu.
colorado.edu.3600  IN  NS  otis.colorado.edu.
colorado.edu.3600  IN  NS  boulder.colorado.edu.

;; ADDITIONAL SECTION:
otis.colorado.edu. 139621  IN  A 128.138.129.76
boulder.colorado.edu.  3324  IN  A 128.138.240.1
oldduke.colorado.edu.  139621  IN  A 128.138.130.30

;; Query time: 23 msec
;; SERVER: 192.168.11.2#53(192.168.11.2)
```

Forward DNS Hierarcy



How DNS works



How DNS works detail

dig @a.root-servers.net.
vsphere.int.colorado.edu

```
;; AUTHORITY SECTION:
edu. IN NS a.edu-servers.net.
edu. IN NS b.edu-servers.net.
edu. IN NS c.edu-servers.net.
edu. IN NS d.edu-servers.net.
edu. IN NS e.edu-servers.net.
edu. IN NS f.edu-servers.net.
edu. IN NS g.edu-servers.net.
edu. IN NS h.edu-servers.net.
edu. IN NS i.edu-servers.net.
edu. IN NS j.edu-servers.net.
edu. IN NS k.edu-servers.net.
edu. IN NS l.edu-servers.net.
edu. IN NS m.edu-servers.net.

;; ADDITIONAL SECTION:
a.edu-servers.net. IN A 192.5.6.30
b.edu-servers.net. IN A 192.33.14.30
c.edu-servers.net. IN A 192.26.92.30
d.edu-servers.net. IN A 192.31.80.30
e.edu-servers.net. IN A 192.12.94.30
f.edu-servers.net. IN A 192.35.51.30
g.edu-servers.net. IN A 192.42.93.30
h.edu-servers.net. IN A 192.54.112.30
i.edu-servers.net. IN A 192.43.172.30
j.edu-servers.net. IN A 192.48.79.30
k.edu-servers.net. IN A 192.52.178.30
l.edu-servers.net. IN A 192.41.162.30
m.edu-servers.net. IN A 192.55.83.30
```

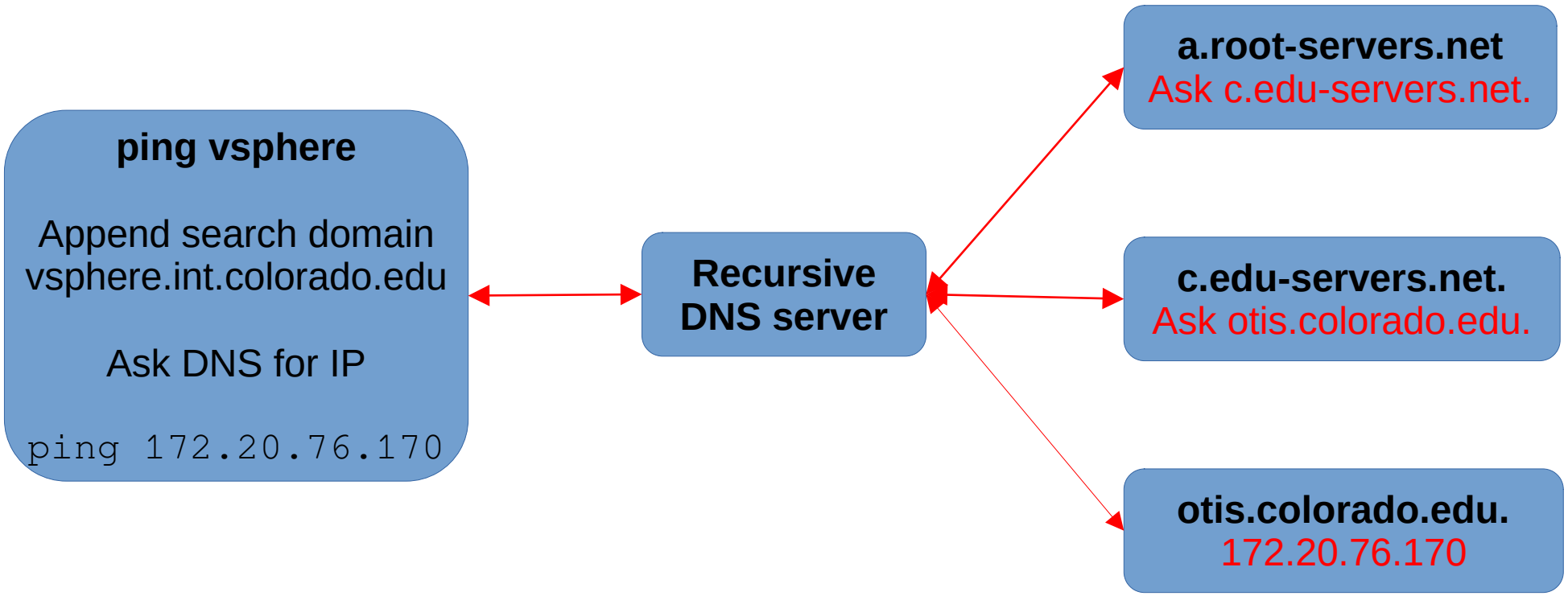
dig @c.edu-servers.net. vsphere.int.colorado.edu

```
;; AUTHORITY SECTION:
colorado.edu. IN NS boulder.colorado.edu.
colorado.edu. IN NS otis.colorado.edu.
colorado.edu. IN NS oldduke.colorado.edu.

;; ADDITIONAL SECTION:
boulder.colorado.edu. IN A 128.138.240.1
otis.colorado.edu.    IN A 128.138.129.76
oldduke.colorado.edu. IN A 128.138.130.30
```

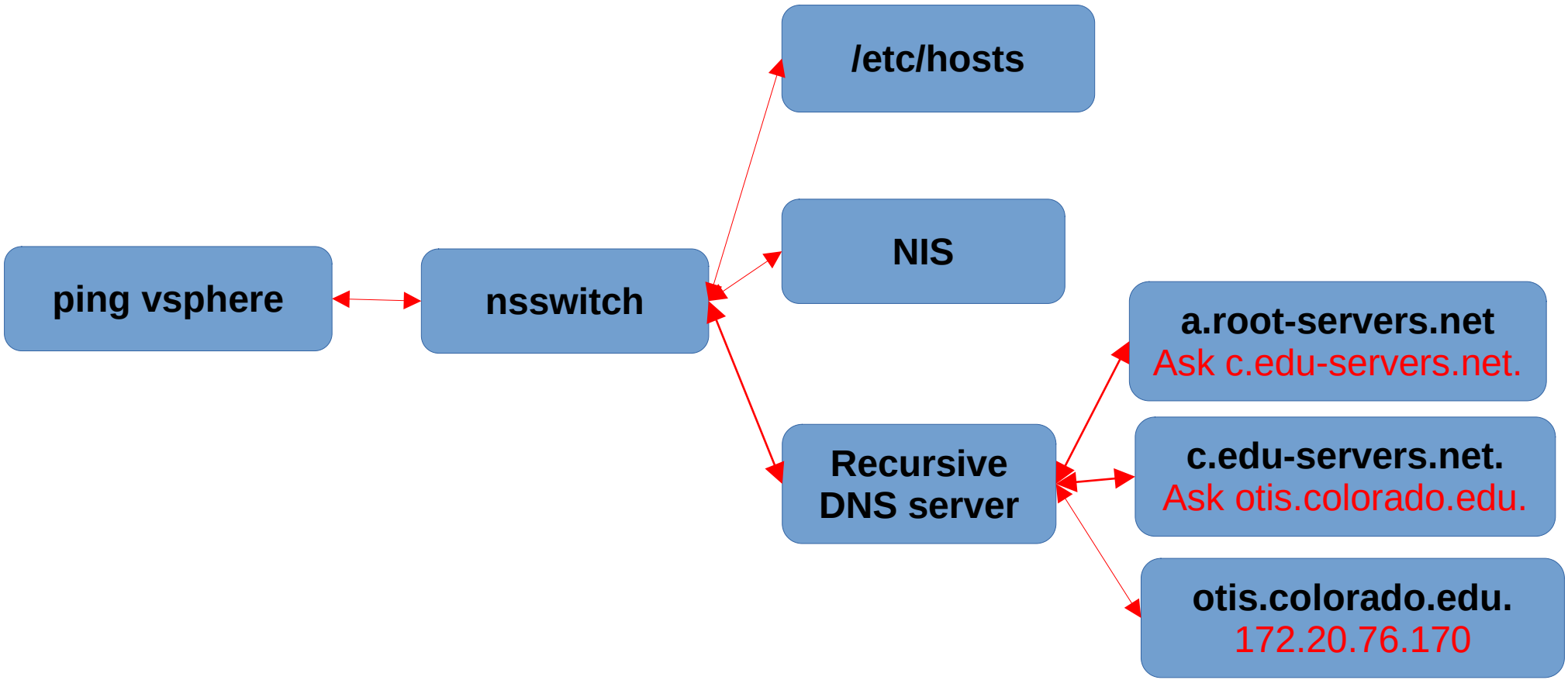
dig @otis.colorado.edu. vsphere.int.colorado.edu

```
;; ANSWER SECTION:
vsphere.int.colorado.edu. IN A 172.20.76 .170
```

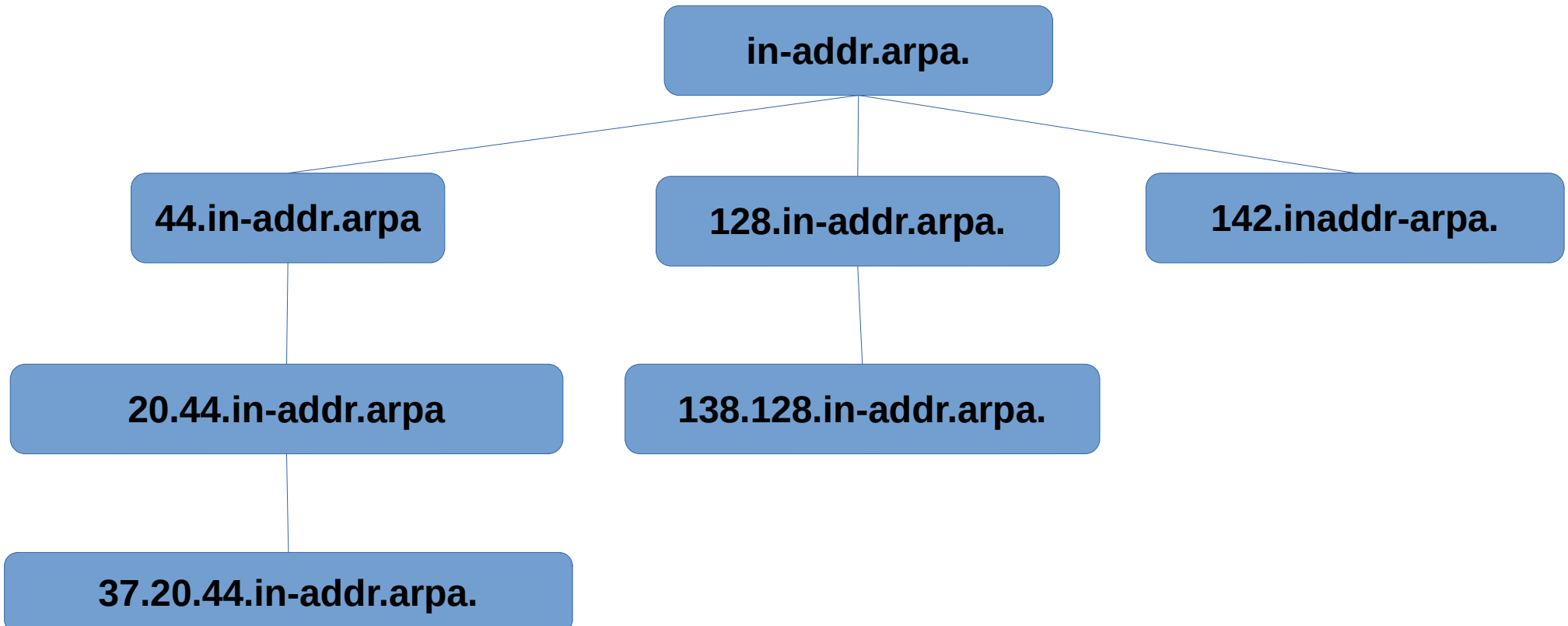
Recursive DNS



Linux/Unix DNS



Reverse DNS


in-addr.arpa.
44.in-addr.arpa
128.in-addr.arpa.
142.inaddr-arpa.
20.44.in-addr.arpa
138.128.in-addr.arpa.
37.20.44.in-addr.arpa.

DNS Server Classifications

- Authoritative
  - Has the definitive answer
- Recursive
  - Will work to get you the answer
- Master or Primary
  - Original source of resource records
- Secondary
  - Redundant backups

DNS zone

- A zone is a specific subtree of the DNS namespace
- A zone file in named.conf specifies how to resolve addresses within that zone
  - Resource records for the zone
  - References to other servers
    - Root hints
    - Forwarders

Resource Records

- **SOA** - Start of Authority
- **NS** - name server
- **A** - name to IPv4 address
- **AAAA** - name to IPv6 address
- **CNAME** - name to another name
- **PTR** - address to name
- **MX** - mail server
- and a bunch of others

Address resource records

- `name ttl IN A address`
  - if name ends in a period, it is used verbatim, otherwise the domain name is appended
  - ttl is optional
- Example in `colorado.edu`
  - `simlab 3600 IN A 128.138.73.46`

Start of Authority

- Typically the first record in a zone file
- Defines
  - Primary authoritative server
  - Email of DNS administrator
  - Timeouts for secondary servers
  - Default time-to-live

dig SOA colorado.edu

- `colorado.edu. 3600 IN SOA boulder.colorado.edu. dnsadmin.colorado.edu. 2022102815 3600 1200 2419200 3600`

  -
- SOA for `colorado.edu`
- Primary DNS server `boulder.colorado.edu`
- Administrator email `dnsadmin@colorado.edu`

- TTL 1 hour
- Serial yyyymmddhh
- Refresh 1 hour
- Retry 20 minutes
- Expire 28 days
- Negative cache 1 hour

Glue Records

- Need to define name servers for domain
- Need to specify IP for name servers
- Example: (@ is shorthand for domain)

```
@ IN SOA boulder.colorado.edu. ... (...)
  IN NS oldduke.colorado.edu.
  IN NS boulder.colorado.edu.
  IN NS otis.colorado.edu.

otis    IN A 128.138.129.76
boulder IN A 128.138.240.1
oldduke IN A 128.138.130.30
```

CNAME records

- Canonical name or alias
- Translates one name into another name
  - `machinee IN CNAME nfs.dundermifflin.com.`
- Typically requires more information to find IP
  - `www.colorado.edu. IN CNAME pantheon.map.fastly.net.`
    `pantheon.map.fastly.net. IN A 151.101.70.133`
- Note that `pantheon.map.fastly.net` address record may be in a completely different zone file
- Pay attention to trailing periods!!!

MX records

- Mail Exchange
- Server priority
  - Lower is first
  - Try in order
- What is the IP?
- Today mail also needs an SPF record
  - Sender Policy Framework

```
dig MX gmail.com
;; QUESTION SECTION:
;gmail.com. IN MX

;; ANSWER SECTION:
gmail.com. 3600 IN MX 10 alt1.gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 40 alt4.gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 30 alt3.gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 5 gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 20 alt2.gmail-smtp-in.l.google.com.

;; AUTHORITY SECTION:
gmail.com. 172800 IN NS ns2.google.com.
gmail.com. 172800 IN NS ns1.google.com.
gmail.com. 172800 IN NS ns3.google.com.
gmail.com. 172800 IN NS ns4.google.com.

;; ADDITIONAL SECTION:
ns1.google.com. 99745 IN A 216.239.32.10
ns2.google.com. 99745 IN A 216.239.34.10
ns3.google.com. 99745 IN A 216.239.36.10
ns4.google.com. 99745 IN A 216.239.38.10
```

```
dig TXT gmail.com
gmail.com.   IN TXT "v=spf1 redirect=_spf.google.com"
```

PTR records

- `address IN PTR name`
  - Used for reverse DNS
  - Address is in reverese octet order
- Example:
  - otis.colorado.edu = 128.138.129.76

    `76.129.138.128.in-addr.arpa. IN PTR otis.colorado.edu.`
  - Entry in zone file for domain `128.138.129.0/24`

    `129.138.128.in-addr.arpa. SOA (...)`

    `76 IN PTR otis.colorado.edu.`

Configuring BIND

- `options` defines global options
  - can override for individual zones and views
- `logging` configures logging
- `zone` defines a domain or subdomain
- `view` defines zones to show for split DNS
- Many more, mostly for maintainability
  - `ACL`, `masters`, etc

Key BIND `options`

- `listen-on` sets IP and port for server
- `recursion` enable recursion
- `allow-recursion` addresses from which to allow recursion
- `allow-query` addresses that may query
- `allow-transfer` addresses that may transfer entire domain
- `allow-update` addresses that may update zones
- `also-notify` send zone update notifications
- `match-clients` sets access to view
- MANY more

BIND zones

- Zone **`type`**
  - `hint` (e.g. root servers)
  - `primary` - authoritative
  - `secondary` - copy
    - Requires `primaries`
  - `forward` - cache only

- Zone **`file`**
  - Reference copy
    - Maintain this on primary
    - Store in `/etc/named` or `/etc/bind` or `/etc/bind9`
  - Secondary cache
    - Binary file
    - Used on restart
    - Stored on `/var`

Example named.conf

- **Primary**

```
options {
   listen-on port 53 { any; };
   directory "/var/named";
   allow-query { any; };
   allow-recursion { 100.64.42.0/24; };
   recursion on;
}
zone "."                        IN {type hint;    file "named.ca"; };
zone "dundermifflin.com."       IN {type primary; file "/etc/named/db.dm";};
zone "42.64.100.in-addr.arpa" IN {type primary; file "/etc/named/db.100.64.42";};
include "/etc/named.rfc1912.zones";
```

- **Secondary**

```
options {
   listen-on port 53 { any; };
   directory "/var/cache/bind";
   allow-query { any; };
   allow-recursion { 100.64.42.0/24; };
   recursion on;
 };
include "/etc/bind/named.conf.default-zones";
zone "dundermifflin.com."       IN {type secondary;primaries {100.64.41.2;};file "db.dm";};
zone "42.64.100.in-addr.arpa" IN {type secondary;primaries {100.64.41.2;};file "db.100.64.42";};
```

Example Forward DNS Zone file

- Zone is `dundermifflin.com.`

```
$TTL 1h
@ IN SOA ns1.dundermifflin.com. admin.dundermifflin.com. (
            20221017 ; serial
            3h ; refresh
            1h ; retry
           14d ; expire
            1h); negative cache
  IN NS ns1.dundermifflin.com.
  IN NS ns2.dundermifflin.com.
  IN MX 10 mail.dundermifflin.com.

ns1     IN A 100.64.42.2
ns2     IN A 100.64.42.6
router  IN A 100.64.0.42
dmz     IN A 100.64.42.1
www 10m IN CNAME web1.dundermifflin.com.
```

Example reverse DNS file

- Zone is `42.64.100.in-addr.arpa` (domain is `100.64.42.0/24`)

```
$TTL 1h
@ IN SOA ns1.dundermifflin.com. admin.dundermifflin.com. (
        20221017 ; serial
        3d       ; refresh
        1h       ; retry
       14d       ; expire
        1h)      ; negative cache
  IN NS ns1.dundermifflin.com.
  IN NS ns2.dundermifflin.com.

1 2h IN PTR dmz.dundermifflin.com.
2 2h IN PTR ns1.dundermifflin.com.
3 2h IN PTR web0.dundermifflin.com.
6 2h IN PTR web0.dundermifflin.com.
```

Reducing BIND chatter

- When `named` starts there is a LOT of stuff in the logs which can make errors hard to find
- Extraneous messages is reduced by
  - running `named` with the `-4` option (IPv4 only)
  - `empty-zones-enable no`
- When errors occur `grep named` from `/var/log/messages` or `/var/log/syslog`
  so you can see ***all*** the output
  - With `named` errors are rarely the last thing in the log

systemd-resolved

- Another of systemd's attempts at taking over the world
  - Solution in search of a problem
- Replaces `/etc/resolv.conf` with a symlink
- Maps to 127.0.0.53
  - dig shows 127.0.0.53 as DNS server
- `resolvectl` shows DNS servers and search