# Domain Name Service

Name service is delegated.

The root name server have:

```
csulb.edu IN NS garuda.csulb.edu.
139.134.in-addr.arpa IN NS garuda.csulb.edu.
garuda.csulb.edu IN A 134.139.1.2
```

or

```
csulb.edu IN NS 134.139.1.2
139.134.in-addr.arpa IN NS 134.139.1.2
```

Which delegates name service for names ending in `csulb.edu` and cables starting with `134.139` to a machine on campus.

At `garuda` responsibility is delegated to cecs:

```
cecs.csulb.edu IN NS 134.139.249.20
248.139.134.in-addr.arpa IN NS 134.139.249.20
247.139.134.in-addr.arpa IN NS 134.139.249.20
```

Suppose responsibility for names ending in `cecs.csulb.edu` and for cables starting with `134.139.248` has been delegated to our machine; how do we set up DNS?

# named

Answers queries from resolver.
Issues queries as necessary to other named's.
Answers queries as necessary for other named's.

Reads configuration out of files.

When running most DNS information is kept in memory.

Concept: each "authority" has one machine that acts as a primary server. Secondary servers cover when primary is unavailable. Secondary server frequently gets "map" from primary.

If you are the authority you can give an authoritative answer.

Optimization: Recently used information is cached by named. So the second time you are asked the same question you don't have to search.

If you answer from your cached information you can give a non-authoritative answer.

# named.conf

`/etc/named.conf` — The main file for named. It lists domains for which this named acts as primary or secondary server. Note: old versions of DNS this was `named.boot` and had a different format for the same information.

```
zone "cecs.csulb.edu" in {
    type master;
    file "named.hosts";
};
zone "249.139.134.in-addr.arpa" in {
    type master;
    file "named.rev249";
};
```

Primary for `cecs.csulb.edu` names and `134.139.249.x` numbers

Information about `cecs` is found in the file `named.hosts` Given a name, use this file to find the IP number.

Information about "249" is found in the file `named.rev249`

Given an IP number, use this file to find the IP name.

# named.conf (con'd)

```
zone "net.cecs.csulb.edu" in {
        type slave;
        file "cecsnet.bak";
        masters { 134.139.248.2 };
};
```

Secondary for cecs.
A copy of the information is stored in a file `cecsnet.bak` in case of double failure.

```
options {
    directory "/etc/namedb";
};
```

All the files mentioned are found in this directory.

```
logging {
    category lame-servers { null; };
    category cname { null; };
};
```

Special options for logging information.

# named.conf (con'd)

```
zone "." in {
        type hint;
        file "root.cache";
};
```

This file has the starting cache of name servers we know about. We need to know at least where the root name servers are, so we can use them to find other DNS servers.

```
zone "0.0.127.in-addr.arpa" in {
        type master;
        file "named.hosts.127.0.0";
};
```

You must know about yourself.

# named

`root.cache/named.ca/named.root` — The initial cache for this name server. Always includes the name of the root servers. When you boot, you get your initial information about other name servers from this file.

`A.ROOT_SERVERS.NET` is a root DNS server.
From there we can find a server for any domain.

```
.  3600000  IN NS A.ROOT_SERVERS.NET.
A.ROOT_SERVERS.NET. 3600000 A 198.41.0.4
A.ROOT-SERVERS.NET. 3600000 AAAA 2001:503:BA3E::2:30
```

A time-out value (`3600000`) is given,
for root servers a huge value suffices.

Both IP version 4 and 6 are given

Approximately 13 root servers are names,
Any local master should be named
(name service on campus will then run even if we lose our outside connection)

Download a new `named.ca` occasionally.
Currently from `rs.internic.net`

# Source of Authority record

The name of our machine and the name of the account on that machine responsible for name service. (Present in every zone file.)

```
@ IN SOA cheetah.cecs.csulb.edu.
   root.cheetah.cecs.csulb.edu. (
                2006042801    ; Serial
                28800         ; Refresh
                14400         ; Retry
                3600000       ; Expire
                86400 )       ; Minimum
```

Serial is used by the `named` and secondary to know if cache is up to date
Refresh: how often the secondaries should contact us for changes. They won't download unless a newer serial number is found.
Retry: If we are offline a secondary tries to refresh, it should wait this long before trying again.
Expire: Discard all data (that hasn't been refreshed) after this amount of time. Applies usually if the primary goes out of service.
Minimum is the default time-to-live for records that don't have any.

## Default timeout

Each zone file also has a line specifying the default time-out of records in that zone:

```
$TTL 3600000
```

## Mandatory Delegation Record

Each zone file has at least one delegation record that indicates that the current machine is the authoritative machine for that zone.

```
        IN NS cheetah.cecs.csulb.edu.
```

# Names to Numbers

`named.hosts` —
for each name there is one or more lines indicating IP addresses.
delegation of authority over sub-domains may be given here

The name varies and is the one given by the `primary` entry in `named.conf` (e.g., `named.hosts`)

```
        IN NS handles.cecs.csulb.edu.
charlotte IN   A   134.139.249.5
heart.cecs.csulb.edu. IN A 134.139.249.39
net.cecs.csulb.edu. IN NS 134.139.248.2
```

The name that led to the file is appended
(`cecs.csulb.edu`)
unless the name in the file ends with a .

`A` – address record
`charlotte.cecs.csulb.edu` IP address `134.139.249.5`

`heart.cecs.csulb.edu` IP address `134.139.249.39`

`NS` – name service record.
Service for `net.cecs.csulb.edu`
delegated to `cheetah`
Must delegate to yourself (see first line)

# Numbers to Names

`named.rev249` — addresses/names of hosts, deletation of authority.

The name varies and is the one given by the `primary` entry in `named.conf` (e.g., `named.rev249`)

Numbers are given in reverse order.

```
39  IN  PTR  heart.cecs.csulb.edu.
5.249.139.134.in-addr.arpa. IN PTR
      charlotte.cecs.csulb.edu.
```

Again, the name that lead to the entry is appended unless it ends in a .

`39.249.139.134.in-addr.arpa`: internet number of `heart`

`5.249.139.134.in-addr.arpa`: internet number of `charlotte`

Again: a self referencing NS delegation should be in every zone file.

Note: For security, some machines will block services if they are unable to get a valid machine name, hence reverse name service is mandatory.

# Other Records

Canonical name (alias)

```
www.cecs.csulb.edu. IN CNAME
                          prometheus.cecs.csulb.edu.
smtp.cecs.csulb.edu. IN CNAME
                           charlotte.cecs.csulb.edu.
cecs.csulb.edu. IN CNAME heart.cecs.csulb.edu.
```

Give machine names for particular aliases.

Mail exchanger (used by mail transport)

```
cecs.csulb.edu. IN MX 1 charlotte.cecs.csulb.edu.
```

Designate a particular machine as the mail-handler for a domain.

# Utilities

There are a couple utilities to do basic checks on your files.

`named-checkconf`
Does a simple check of the syntax of a `named.conf` file. Even if the file passes the check there is no guarantee that the entries are correct, they just have a reasonably correct format.

`named-checkzone`
Does a simple check of the syntax of a zone file. Specify the nameof the zone and the name of the file.
There are couple of options that cause some extra checks to be done, these can be useful in helping detect errors.

# Round-Robin

Many DNS servers support a round-robin for identical entries.

Suppose your forward zone file has the following three entries:

```
www IN   A   134.139.249.91
www IN   A   134.139.249.92
www IN   A   134.139.249.93
```

The first query to `named` will return the 91, the second 92, the third 93, the fourth back to 91.

This gives you a simple way to use multiple hosts to support a single "service".

Many version of `named` will also support this behavior using multiple `CNAME` entries.

# IP Version 6 Addresses

Name to number lookup: modify the existing file (`named.hosts`) adding `AAAA` records:

```
puma IN A 134.139.248.19
puma IN AAAA 0:0:0:0:0:0:868b:f813
```

Note: the legacy address of zeros followed by IP number.

Number to name requires a separate file and a zone entry in `named.conf`:

```
zone "8.f.b.8.6.8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.
     0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
  type master;
  file "named6.rev";
  allow-update { none; };
};
```

Notes: slightly different `arpa` (`ip6`)
Still reverse numbering, but in "nibbles" (half-bytes).

Reverse zone file: Same SOA structure as all zone files.
Uses reverse numbering in nibbles.
Does "auto-append" same as other reverse zone files.

```
3.1 IN PTR puma.net.cecs.csulb.edu
```