DNS

ZONES

A zone defines the contents of a contiguous section of the domain space, usually bounded by administrative boundaries. There will typically be a separate data file for each zone. The data contained in a zone file is composed of entries called Resource Records (RRs).
A domain server will probably read a file on start-up that lists the zones it should load into its database. The format of this file is not standardized and is different for most domain server implementations. For each zone it will normally contain the domain name of the zone and the file name that contains the data to load for the zone.

RESOURCE RECORDS

Records in the zone data files are called resource records (RRs).
An RR has a standard format as shown:

```
<name>   [<ttl>]   [<class>]   <type>   <data>
```

All comparisons and lookups in the name server are case insensitive.
Parenthesis ("(",")") are used to group data that crosses a line boundary. A semicolon (";") starts a comment; the remainder of the line is ignored. The asterisk ("*") is used for wildcarding. The at-sign ("@") denotes the current default domain name.

SOA (Start Of Authority)

```
<name>  [<ttl>]  [<class>]  SOA  <origin>  <person>  (
      <serial>
      <refresh>
      <retry>
      <expire>
      <minimum> )
```

The Start Of Authority record designates the start of a zone.

NS (Name Server)

```
<domain>   [<ttl>] [<class>]   NS   <server>
```

The NS record lists the name of a machine that provides domain service for a particular domain. The name associated with the RR is the domain name and the data portion is the name of a host that provides the service.
The machines providing name service do not have to live in the named domain. There should be one NS record for each server for a domain.
NS records for a domain exist in both the zone that delegates the domain, and in the domain itself.

Glue Records

If the name server host for a particular domain is itself inside the domain, then a 'glue' record will be needed. A glue record is an A (address) RR that specifies the address of the server. Glue records are only needed in the server delegating the domain, not in the domain itself.
If for example the name server for domain SRI.COM was KL.SRI.COM, then the NS record would look like this, but you will also need to have the following A record.

```
SRI.COM.  NS
 KL.SRI.COM.  KL.SRI.COM.  A 10.1.0.2.
```

A (Address)

```
<host>   [<ttl>] [<class>]   A   <address>
```

The data for an A record is an internet address in dotted decimal form.
A sample A record might look like:

```
SRI-NIC.ARPA.           A       10.0.0.51
```

There should be one A record for each address of a host.

CNAME (Canonical Name)

```
<nickname>   [<ttl>] [<class>]   CNAME   <host>
```

The CNAME record is used for nicknames. The name associated with the RR is the nickname. The data portion is the official name.

```
NIC.ARPA.       CNAME   SRI-NIC.ARPA.
```

There must not be any other RRs associated with a nickname of the same class.

MX (Mail Exchanger)

```
<name>   [<ttl>] [<class>]   MX   <preference>   <host>
```

MX records specify where mail for a domain name should be delivered. There may be multiple MX records for a particular name. The preference value specifies the order a mailer should try multiple MX records when delivering mail. Zero is the highest preference. Multiple records for the same name may have the same preference.

IN-ADDR.ARPA

The structure of names in the domain system is set up in a hierarchical way such that the address of a name can be found by tracing down the domain tree contacting a server for each label of the name. Because of this 'indexing' based on name, there is no easy way to translate a host address back into its host name.
This address mapping domain is called IN-ADDR.ARPA.
For example, the ARPANET is net 10. That means there is a domain called 10.IN-ADDR.ARPA. Within this domain there is a PTR RR at 51.0.0.10.IN-ADDR that points to the RRs for the host SRI-NIC.ARPA (who's address is 10.0.0.51). Since the NIC is also on the MILNET (Net 26, address 26.0.0.73), there is also a PTR RR at 73.0.0.26.IN ADDR.ARPA that points to the same RR's for SRI-NIC.ARPA.

PTR

`<special-name> [<ttl>] [<class>] PTR <name>`
The PTR record is used to let special names point to some other location in the domain tree. They are mainly used in the IN ADDR.ARPA records for translation of addresses to names. PTR's should use official names and not aliases.

Instructions

Adding a subdomain

1. To add a new subdomain to your domain:
2. Setup the other domain server and/or the new zone file.
3. Add an NS record for each server of the new domain to the zone file of the parent domain.
4. Add any necessary glue RRs.

Adding a host

1. To add a new host to your zone files:
2. Edit the appropriate zone file for the domain the host is in.
3. Add an entry for each address of the host.
4. Optionally add CNAME, HINFO, WKS, and MX records.
5. Add the reverse IN-ADDR entry for each host address in the appropriate zone files for each network the host in on.

Deleting a host

1. To delete a host from the zone files:

2. Remove all the hosts' resource records from the zone file of the domain the host is in.
3. Remove all the hosts' PTR records from the IN-ADDR zone files for each network the host was on.
4. Adding gateways. Follow instructions for adding a host.
5. Add the gateway location PTR records for each network the gateway is on.

Deleting gateways

1. Follow instructions for deleting a host.
2. Also delete the gateway location PTR records for each network

Components:

The DNS has three major components:

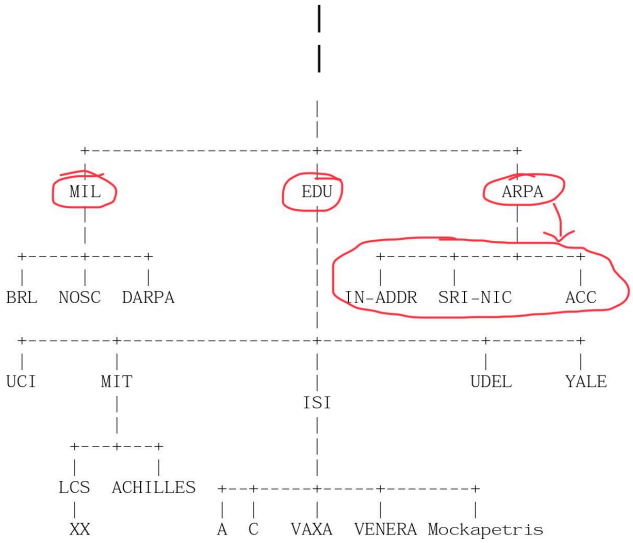
1) The **DOMAIN NAME SPACE and RESOURCE RECORDS** => specifications for a tree structured name space and data associated with the names.

Conceptually, each node and leaf of the domain name space tree names a set of information, and query operations are attempts to extract specific types of information from a particular set. A query names the domain name of interest and describes the type of resource information that is desired. For example, the Internet uses some of its domain names to identify hosts; queries for address resources return Internet host addresses.

2) **NAME SERVERS** are server programs which hold information about the domain tree's structure and set information. A name server may cache structure or set information about any part of the domain tree, but in general a particular name server has complete information about a subset of the domain space, and pointers to other name servers that can be used to lead to information from any part of the domain tree. Name servers know the parts of the domain tree for which they have complete information; a name server is said to be an AUTHORITY for these parts of the name space. Authoritative information is organized into units called ZONEs, and these zones can be automatically distributed to the name servers which provide redundant service for the data in a zone.

3) **RESOLVERS** are programs that extract information from name servers in response to client requests. Resolvers must be able to access at least one name server and use that name server's information to answer a query directly, or pursue the query using referrals to other name servers. A resolver will typically be a system routine that is directly accessible to user programs; hence no protocol is necessary between the resolver and the user program.

Resolver ←----------> Name Server



Domain Name Space and RRs

The domain name space is a tree structure. Each node and leaf on the tree corresponds to a resource set (which may be empty). The domain system makes no distinctions between the uses of the interior nodes and leaves.

Queries

Queries are messages which may be sent to a name server to provoke a response. In the Internet, queries are carried in UDP datagrams or over TCP connections. The response by the name server either answers the question posed in the query, refers the requester to another set of name servers, or signals some error condition. In general, the user does not generate queries directly, but instead makes a request to a resolver which in turn sends one or more queries to name servers and deals with the error conditions and referrals that may result. Of course, the possible questions which can be asked in a query does shape the kind of service a resolver can provide.

The four sections are:

Question **Carries the query name and other query parameters.**

Answer **Carries RRs which directly answer the query.**

Authority **Carries RRs which describe other authoritative servers. May optionally carry the SOA RR for the authoritative data in the answer section.**

Additional **Carries RRs which may be helpful in using the RRs in the other sections.**

Name Servers

Name servers are the repositories of information that make up the domain database. The database is divided up into sections called zones, which are distributed among the name servers. While name servers can have several optional functions and sources of data, the essential task of a name server is to answer queries using data in its zones.

A given name server will typically support one or more zones, but this gives it authoritative information about only a small section of the domain tree. It may also have some cached non-authoritative data about other parts of the tree. The name server marks its responses to queries so that the requester can tell whether the response comes from authoritative data or not.

How the database is divided into zones