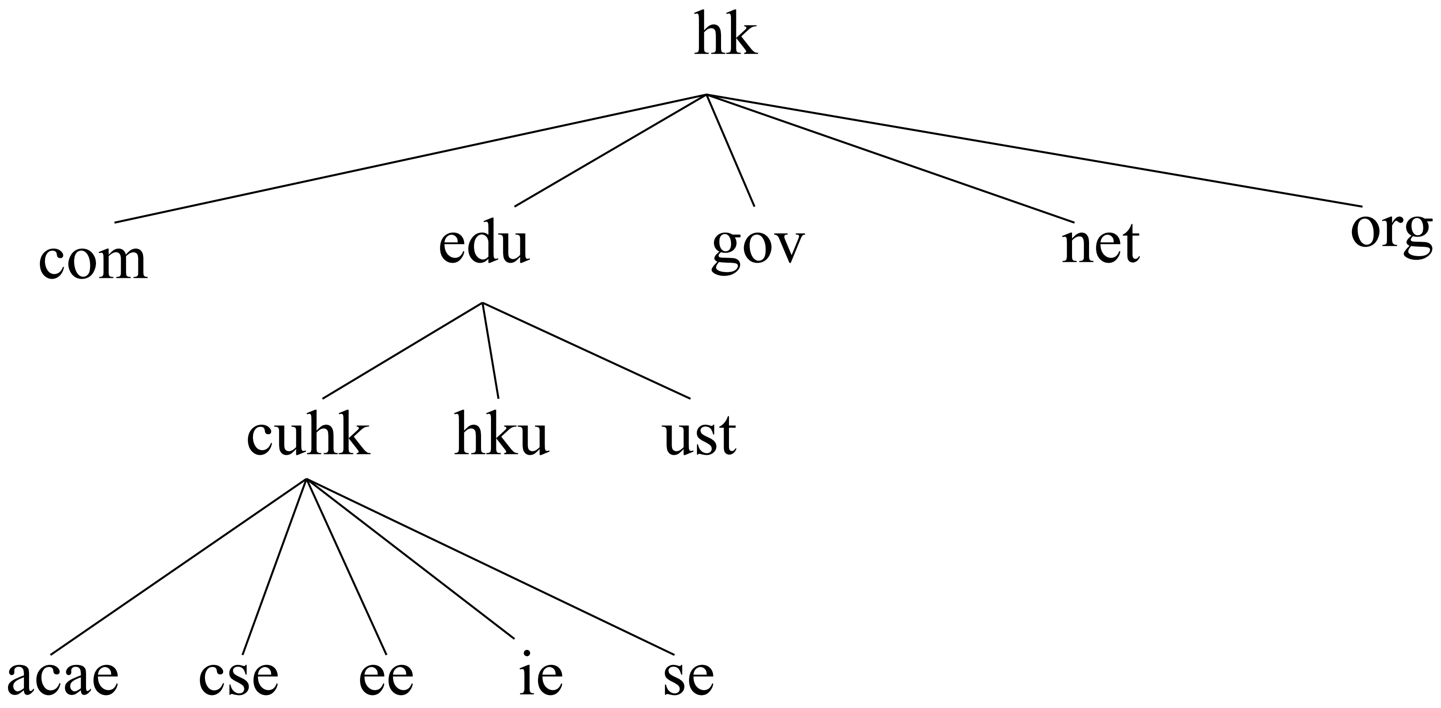
Domain Name System (DNS)

- for translating hostnames into Internet addresses
- A distributed database
- The database is pictured as an inverted tree
- Each node can be the root of a new subtree
- Each of these subtrees represents a partition of the overall database – domain in DNS
- Each domain can further divided into additional partitions, called subdomains in DNS

An example of ie.cuhk.edu.hk domain



Common Top-Level Domains

com

- Commercial organizations, such as Hewlett-Packard (*hp.com*), Sun Microsystems (*sun.com*), and IBM (*ibm.com*)

edu

- Educational organizations, such as U.C. Berkeley (*berkeley.edu*) and Purdue University (*purdue.edu*)

gov

- Government organizations, such as NASA (*nasa.gov*) and the National Science Foundation (*nsf.gov*)

Common Top-Level Domains

mil

- Military organizations, such as the U.S. Army (*army.mil*) and Navy (*navy.mil*)

net

- Networking organizations, such as NSFNET (*nsf.net*)

org

- Noncommercial organizations, such as the Electronic Frontier Foundation (*eff.org*)

See more Top-Level Domains at

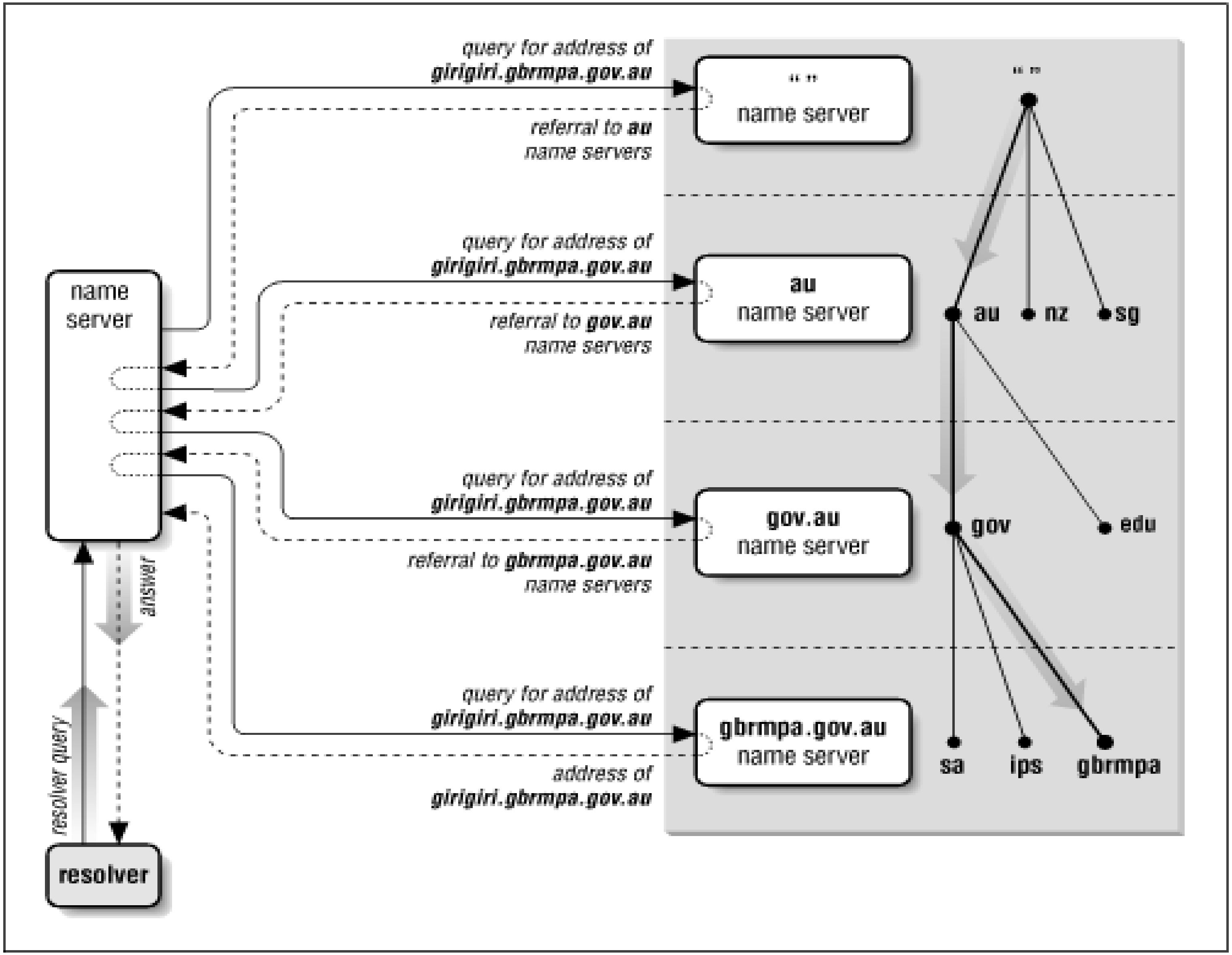
https://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

Top Level Root Servers

Root Server	Operated by
A.ROOT-SERVERS.NET	VeriSign Naming and Directory Services
B.ROOT-SERVERS.NET	Information Sciences Institute
C.ROOT-SERVERS.NET	Cogent Communications
D.ROOT-SERVERS.NET	University of Maryland
E.ROOT-SERVERS.NET	NASA Ames Research Center
F.ROOT-SERVERS.NET	Internet Systems Consortium, Inc
G.ROOT-SERVERS.NET	U.S. DOD Network - Information Center
H.ROOT-SERVERS.NET	U.S. Army Research Lab
I.ROOT-SERVERS.NET	Autonomica
J.ROOT-SERVERS.NET	VeriSign, Inc.
K.ROOT-SERVERS.NET	Reseaux IP Europeens -Network Coordination Centre
L.ROOT-SERVERS.NET	Internet Corporation for Assigned Names and Numbers
M.ROOT-SERVERS.NET	WIDE Project

Source: http://www.root-servers.org/

Resolution of girigiri.gbrmpa.gov.au on the Internet



DNS
Recursion Mode

- The DNS query in the previous slide is recursive which we usually use in our revolver. The revolver passes the final answer to its clients and does not need its clients to go through many query steps. This revolver can help to reduce the DNS traffic in a LAN and reduce the DNS query loading of the clients. DNS forwarder in firewall usually use recursive mode.

Iteration Mode

- Iteration Mode (Non-recursive Mode) query only replies the best answer it already knows- the name servers "close" to the data it is seeking and then let the clients continue to query the answers for themselves

Google Public DNS Servers

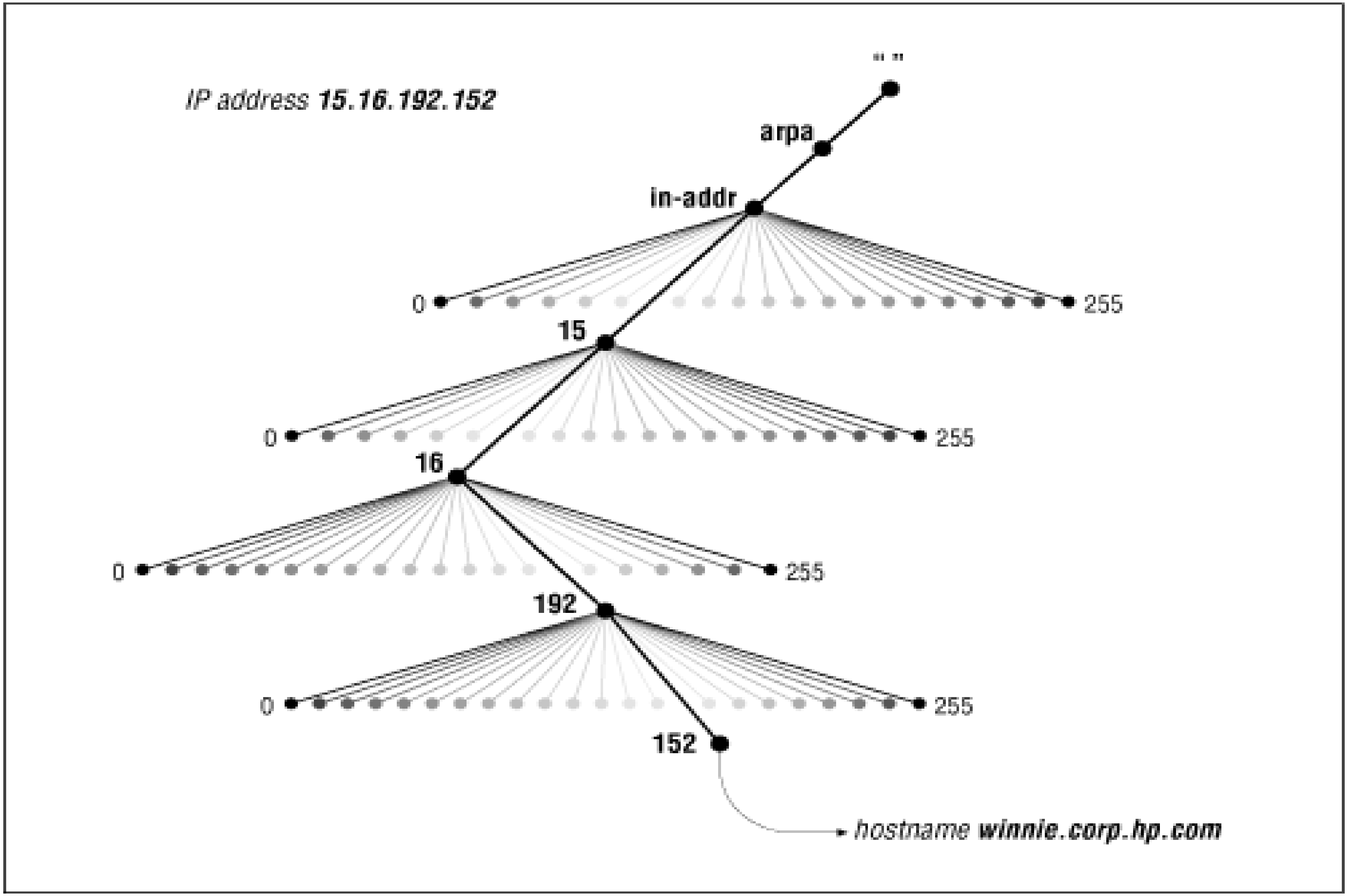
Due to security and loading concern, most networks do not provide public DNS query service in recursion mode. However, Google launched of their free DNS resolution service for the public in December, 2009. The Google Public DNS IP addresses are 8.8.8.8 and 8.8.4.4. We can use these public DNS servers for DNS setup debugging.

Google Public DNS Servers

```
csh > host www.googel.com 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

www.googel.com is an alias for www.google.com.
www.google.com is an alias for www.l.google.com.
www.l.google.com has address 74.125.71.106
www.l.google.com has address 74.125.71.99
www.l.google.com has address 74.125.71.103
www.l.google.com has address 74.125.71.104
www.l.google.com has address 74.125.71.147
www.l.google.com has address 74.125.71.105
```

addr.arpa domain tree



DNS Records

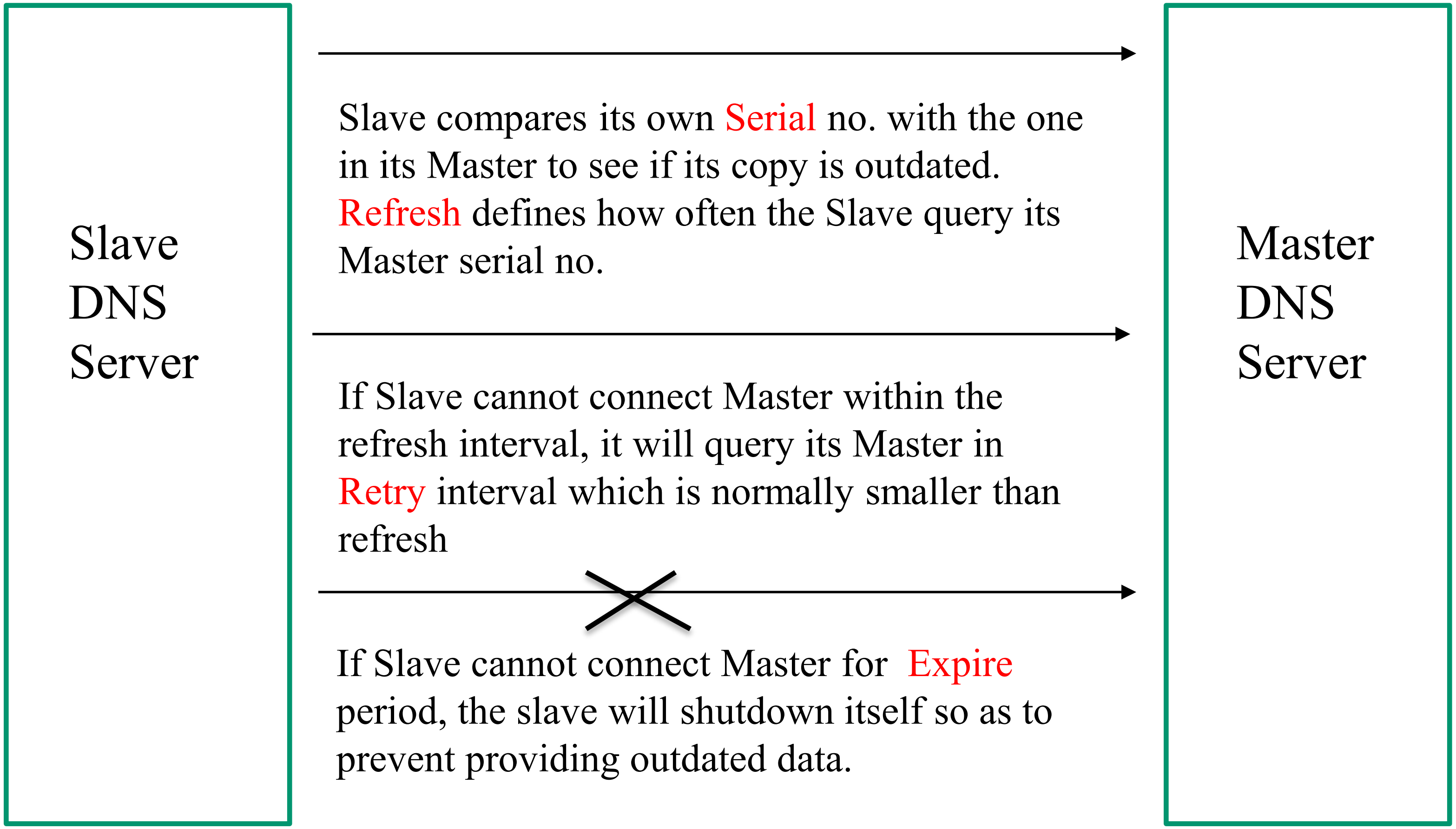
- SOA – Start Of Authority
  - Serial, Refresh, Retry, Expire, TTL
- NS – Name Server
- A – Name to Address mapping
- PRT – Address to name mapping
- CNAME – Canonical name (for aliases)
- MX – Mail eXchange
- TXT - text, records are arbitrary text strings which can be attached to given DNS nodes. Certain protocols, such as SPF (Sender Policy Framework), use this field to store protocol-specific data

DNS Records

- SOA – Start Of Authority
  - Serial

    The serial number applies to all the data within the zone. When a slave name server contacts a master server for zone data, it first asks for the serial number on the data. If the slave's serial number is lower than the master server's, the slave's zone data are out of date. In this case, the slave pulls a new copy of the zone.

SOA – Start Of Authority



Slave DNS Server

Slave compares its own Serial no. with the one in its Master to see if its copy is outdated. Refresh defines how often the Slave query its Master serial no.

If Slave cannot connect Master within the refresh interval, it will query its Master in Retry interval which is normally smaller than refresh

If Slave cannot connect Master for Expire period, the slave will shutdown itself so as to prevent providing outdated data.

Master DNS Server

DNS Records

- SOA – Start Of Authority
  - Refresh

    The refresh interval tells the slave how often to check that its data are up to date. Most users will tolerate a delay of half of a working day for things like name server data to propagate when they are waiting for their new workstation to be operational.

DNS Records

- SOA – Start Of Authority
  - Retry

    If the slave fails to reach the master name server(s) after the refresh period (the host(s) could be down), then it starts trying to connect every retry seconds. Normally, the retry interval is shorter than the refresh interval, but it doesn't have to be.

DNS Records

- SOA – Start Of Authority
  - Expire

    If the slave fails to contact the master server(s) for expire seconds, the slave expires its data. Expiring the data means the slave stops giving out answers about the data because the data are too old to be valid. The expiration time should always be much larger than the retry and refresh intervals; if the expire time is smaller than the refresh interval, your slaves will expire their data before trying to load new data.

DNS Records

- SOA – Start Of Authority
  - TTL (Time To Live)

    This value applies to all the resource records in the zone file. The name server supplies this TTL in query responses, allowing other servers to cache the data for the TTL interval. If your data don't change much, you might consider using a minimum TTL of several days. One week is about the longest value that makes sense. A value as short as one hour can be used, but it is not recommended because of the amount of DNS traffic it causes.

DNS Records

- SOA – Start Of Authority

  What values you choose for your SOA record will depend upon the needs of your site. In general, longer times cause less load on your systems and lengthen the propagation of changes; shorter times increase the load on your systems and speed up the propagation of changes.

DNS Records

- SOA – Start Of Authority

  RFC 1537 recommends the following values for top-level domain servers:

86400 ;	*Refresh 24 hours*
7200 ;	*Retry 2 hours*
2592000 ;	*Expire 30 days*
345600 ;	*Minimum TTL 4 days*

DNS Records

The TTL in SOA is interpreted as the "negative caching" time. The default TTL value is defined by $TTL directive in the first line of your zone file. E.G.

```
$TTL 28800
@           IN           SOA  …..
```

Negative Caching

“Negative caching" - the storage of knowledge that something does not exist. We can store the knowledge that a record has a particular value. We can also do the reverse, that is, to store the knowledge that a record does not exist. It is the storage of knowledge that something does not exist, cannot or does not give an answer that we call negative caching. See RFC 2308 at http://www.ietf.org/rfc/rfc2308.txt