Domain Name System - Advanced Computer Networks

Saurabh Barjatiya

International Institute Of Information Technology, Hyderabad

25 January, 2011

Contents

Structure

- Distributed database, highly volatile
- Domain names
- Top level domains
- Root DNS servers
- Resource records

Type of DNS servers

- Primary and Secondary servers
- Authoritative and Non-authoritative servers
- Recursive and non-recursive servers

Type of DNS records

- SOA records
- NS records
- A records
- AAAA records
- MX records
- CNAME records
- PTR records
- SPF records
- TXT records

List of DNS records types is available on Wikipedia at http://en.wikipedia.org/wiki/List_of_DNS_record_types

SOA records - 1

Sample SOA record

```
$TTL 3600
@ SOA ns.ipv6test.iiit.ac.in. root.ipv6test.iiit.ac.in.
    (1 15m 5m 30d 1h)
    NS ns.ipv6test.iiit.ac.in.
```

The '@' refers to the zone name, 'ipv6test.iiit.ac.in.. The SOA record type, for start of authority, tells a few important things about this zone. The data following consists of the name of the primary name server (dns1), the mail address of the administrator with the '@' replaced by a dot, and a list of ve numeric parameters used by the secondary name servers.

SOA records - 2

The serial number is used by the secondaries to decide if they need to fetch updated zone data from the primary. It must be incremented whenever the zone data on the primary is changed.

Hence often serial number is kept in form

$$yyyymmddnn$$

where nn is incremented from 00 to higher value if DNS records are changed more than once on same day.

SOA records - 3

The refresh and retry values specify the interval at which a secondary name server is supposed to contact the primary to see if the zone has changed and at what interval to retry doing so if the primary server is unreachable.

The expire value defines for how long a secondary should continue to retry reaching the primary until it considers its data entirely outdated and stop serving the zone.

SOA records - 4

The last one is called the minTTL for historical reasons but actually defines how long a cache stores negative results, i.e. the fact that a given name doesnt have a DNS entry.

Appending an m, h or d to the last four numbers specifies them in minutes, hours or days, respectively.

Reverse records

```
zone "168.192.in-addr.arpa." {
    type master;
    file "192.168.reverse.db";
};

244.201 PTR vm1.ipv4.ipv6test.iiit.ac.in.
17.202 PTR vm2.ipv4.ipv6test.iiit.ac.in.
```

'ip6.arpa.' is used for IPv6 reverse records. Details will be covered during IPv6 theory / labs.

SPF records - 1

SPF stands for Sender Policy Framework. It allows domain owners to specify which servers can send email on behalf of thier domain

SPF example - 1

"v=spf1 mx -all"
Allow domain's MXes to send mail for the domain, prohibit all others.

SPF records - 2

SPF example - 2

"v=spf1 mx -all"
The domain sends no mail at all.

SPF example - 3

"v=spf1 +all"
The domain owner thinks that SPF is useless and / or doesn't care.

For details on how to set SPF records visit
http://www.openspf.org/SPF_Record_Syntax

Miscellaneous - 1

- Public and Private (Intranet) DNS
- Split DNS
- DDNS (Dynamic DNS)
- Cache only DNS
- RFC1912 zones (named.rfc1912.zones)
- Load balancing using DNS
- Root hints file (named.root)
- BIND DNS server
- dig and nslookup
- Zone transfer (AXFR)

Miscellaneous - 2

- eDNS and OPT records
- eDNS firewall considerations
- DNS amplication attacks
- DNS cache poisioning
- /etc/hosts or bad DNS administrator
- DNSSEC

Intresting article on DNS issues is hosted at http://cr.yp.to/djbdns/notes.html