DNS

Keiichi Shima <keiichi@iijlab.net>
Slides stolen from Alisha Gurung

WHAT IS DNS??????????

What is DNS ?

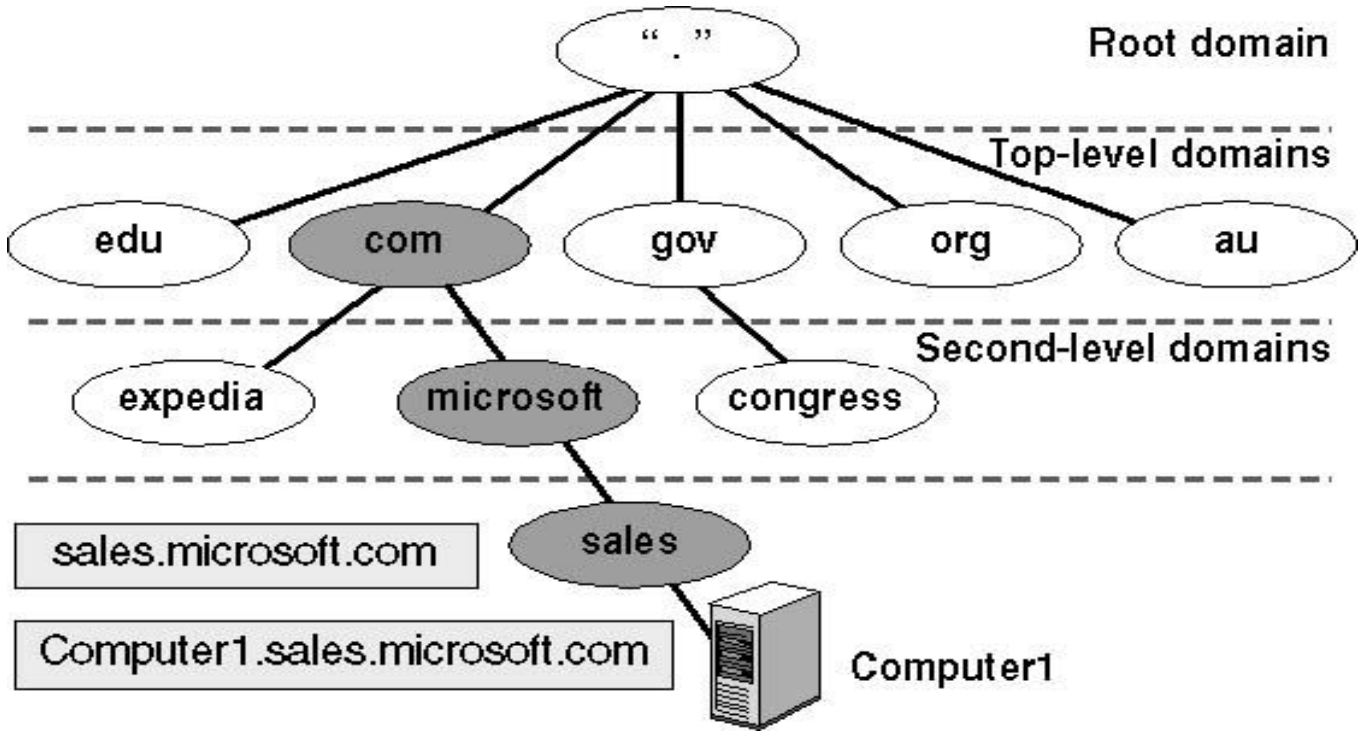
- Systems to convert domain names into ip addresses:
- For an instance;

www.druknet.bt ➔202.144.133.45

Reverse:

- **202.144.133.45➔ www.druknet.bt**

DNS Hierarchy



Root Servers

- The top of the DNS hierarchy
- There are 13 root name servers operated around the world, with names from `[a-m].root-servers.net`
- There are more than 13 physical root name servers
  - Each rootserver has an instance deployed via anycast
- Root hints file come in many names (db.cache, named.root, named.cache, named.ca)
  - Get it from ftp.rs.internic.net
- See root-servers.org for more detail

DNS QUERY-How Does It Work?

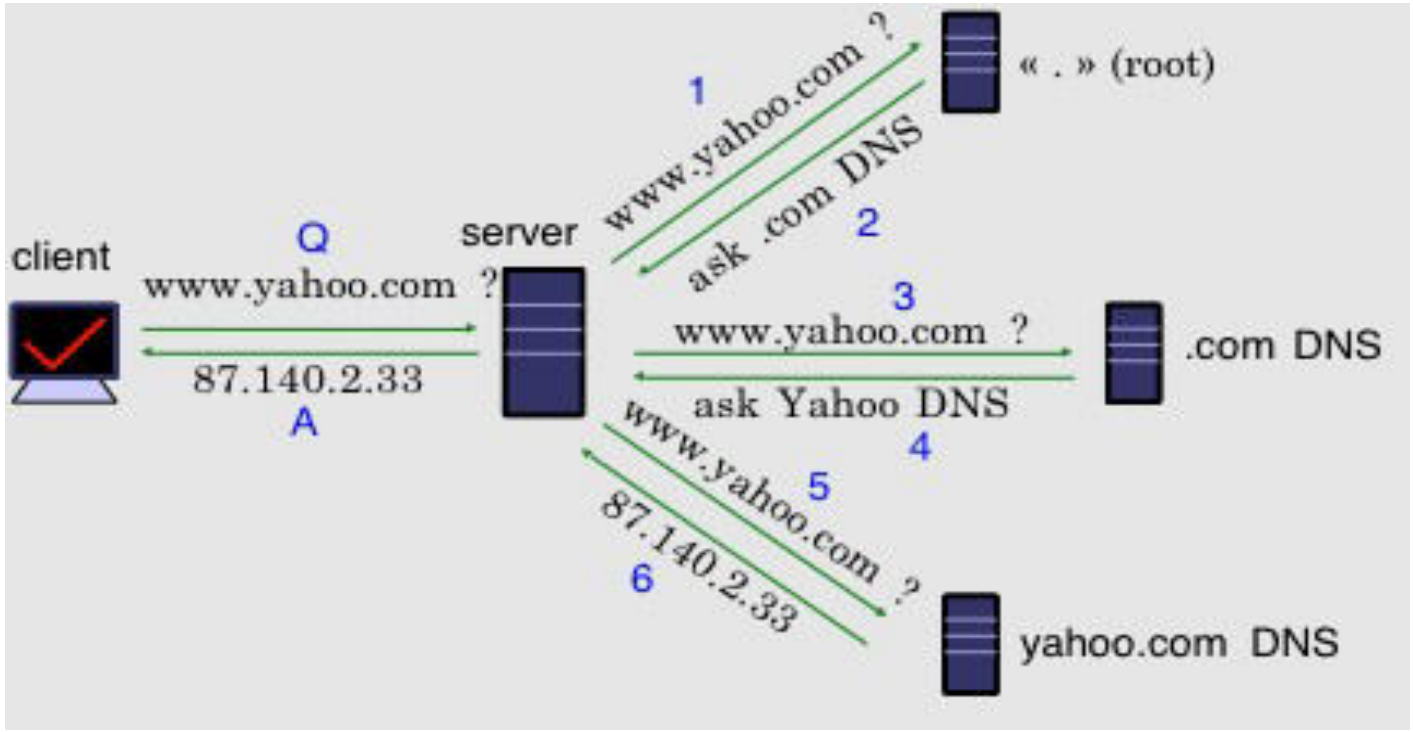


Image:(nsrc)

Simple DNS Tools

- $ host www.druknet.bt

  www.druknet.bt has address 202.144.128.145

- $ host 202.144.128.145

  145.128.144.202.in-addr.arpa domain name pointer www.druknet.bt.

- dig www.druknet.bt any

Name Servers

- **Name servers answer ‘DNS’ questions**
- **Several types of name servers**
  - → **Authoritative servers**
    - **master (primary)**
    - **slave (secondary)**
  - → **Caching or recursive server**
    - **also caching forwarders**

Caching Vs Authoritative Server

- DNS servers can be put in two categories:

  →caching and authoritative

- Caching nameservers act as query forwarders on behalf of clients, and cache answers for later.
- Can be the same software (often is), but mixing functionality (recursive/caching and authoritative) is discouraged (security risk)
- The TTL of the answer is used to determine how long it may be cached without requerying.

Authoritative DNS

- **Deliver authoritative responses for particular domains**
- **Responsible for more than one zones**
- **Two types: Primary(Master) and Slave(Secondary)**
- **Only one primary NS- changes made here**
- **Secondary/slave/ Nameserver/s retrieves a copy of the zone file from the Master(periodically based on the refresh value set In Master**
- **Primary NS can notify slaves**
-

ZONE File Sample

```
$TTL   86400 ; 24 hours could have been written as 24h or 1d
$ORIGIN example.com. @  1D  IN  SOA ns1.example.com. hostmaster.example.com. (
          2002022401 ; serial
          3H ; refresh
          15 ; retry
          1w ; expire
          3h ; minimum
         )
       IN  NS     ns1.example.com.
       IN  MX  10 mail.another.com.
ns1    IN  A      192.168.0.1  ;name server definition
www    IN  A      192.168.0.2  ;web server definition
fred   IN  A      192.168.0.4
```

Reverse Zone File Sample

- $TTL 86400 ; 24 hours, could have been written as 24h or 1d
- $ORIGIN 0.168.192.IN-ADDR.ARPA. @ 1D IN SOA ns1.example.com. hostmaster.example.com. (
- 2002022401 ; serial
- 3H ; refresh
- 15 ; retry
- 1w ; expire
- 3h ; minimum
-)
- IN NS ns1.example.com.
- 1 IN PTR ns1.example.com.
- 2 IN PTR www.example.com.
- 4 IN PTR fred.example.com.

Record Types

- Basic record types:
  - → **A, AAAA**: IPv4, IPv6 address
  - →**NS:** NameServer
  - →**MX**: Mail eXchanger
  - →**CNAME**: Canonical name (alias)
  - →**PTR**: Reverse

Delegating a Zone

- Delegation is passing of authority for a subdomain to another party
- Delegation is done by adding NS records
  - Ex: if tashicell.com wants to delegate testing.tashicell.com

```
testing.druknet.bt.   NS ns1.testing.druknet.bt.
testing.druknet.bt.   NS ns2.testing.druknet.bt.
```

- Now how can we go to ns1 and ns2?
  - We must add a **Glue Record**

Glue Record

- Glue is a ‘non-authoritative’ data
- Don’t include glue for servers that are **not in the sub** zones