GlobalLogic

A Hitachi Group Company

EDUCATION

Smart Start: Linux/Networking
Domain name system

Sergii Kudriavtsev

Agenda

* Concept of name resolution
* General network info
* Tools:
    - host
    - nslookup
    - delv
    - whois
    - dig
* dnsmasq
* DNS Transport Protocol
* Types of DNS records

Concept of name resolution

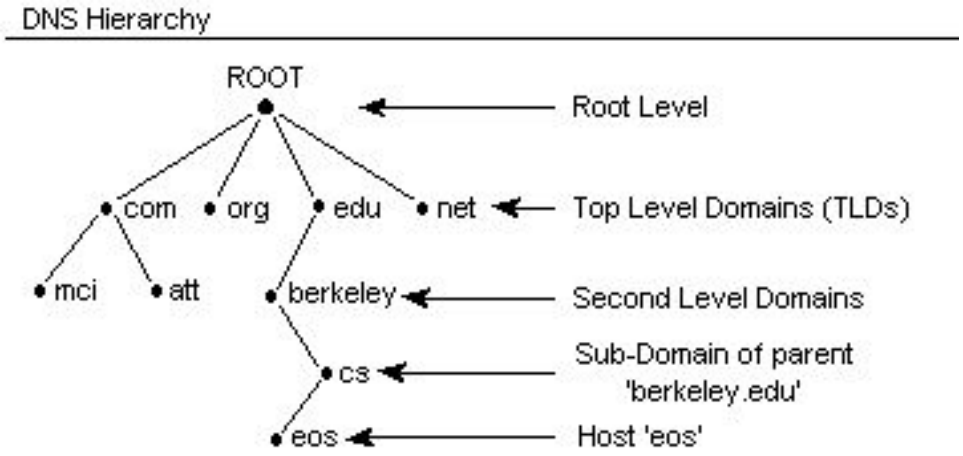
- Name resolution - process of relating easy-to-remember names with difficult-to-remember Internet Protocol (IP) addresses. The Domain Name System (DNS) provides name resolution services in most environments. These internal servers host a dynamic database of names and related IP addresses.

  - Generally, there are two common ways to resolve names to IP addresses in Linux:
    - Domain Name System (DNS): domain name to IP address
      - global, public servers that provide name resolution via the Internet.
      - DNS server can be global or local

    - hosts file: hostname to IP address
      - simplest form of name-to-address mapping
      - /etc/hosts

        ```
        127.0.0.1       localhost
        IP Hostname
        ```

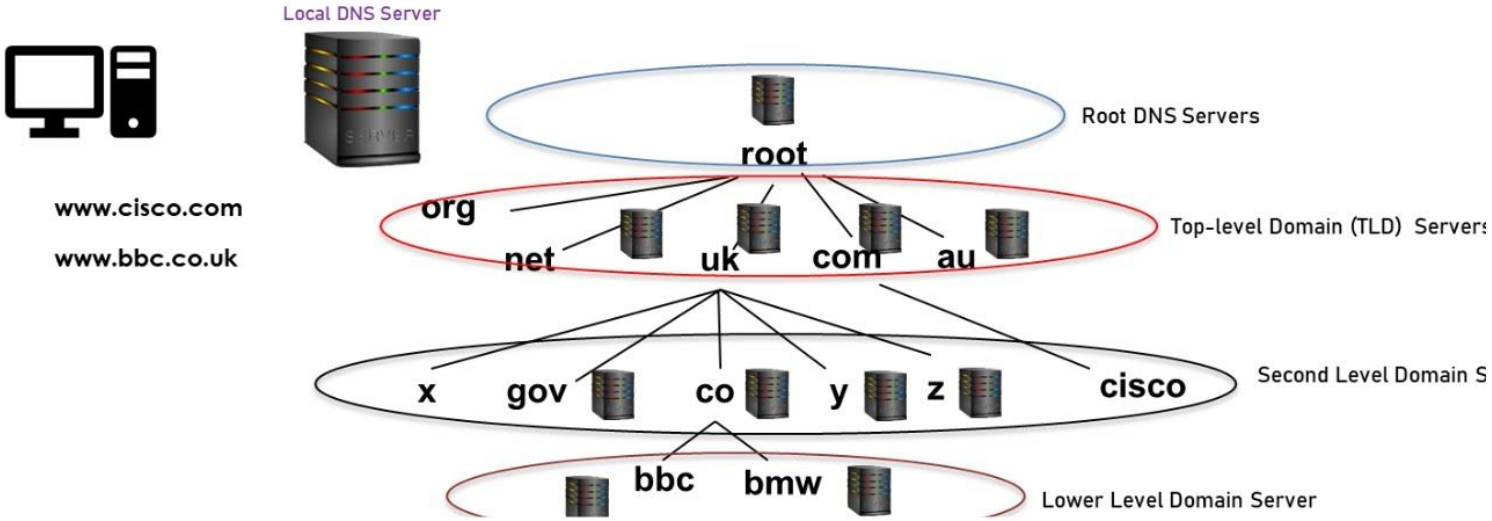
- DNS Hierarchy
  - Domain Names are hierarchical (five levels of DNS hierarchy) and each part of a domain name is referred to as either the **root**, **top level, second level** or as a **sub-domain**.
  - Distributed structure
  - Different DNS servers for each level of the DNS hierarchy.



- DNS Hierarchy
  - **Root level** - housing the DNS root zone managed by authoritative root name servers. Redirecting requests to the appropriate Top-Level Domain name servers. DNS hierarchy relies on 13 distributed Root Zone servers globally. , identified by host names like a.root-servers.net to m.root-servers.net, are managed by diverse organizations, including government entities, educational institutions, and private companies.
  - **Top Level Domains (TLD's)** - include widely recognized extensions such as .com, .net, and .org, each reflecting organizational hierarchy or geographic distinctions.
    - “com” for commercial websites.
    - “org” for organizational websites.
    - “edu” for educational websites.
    - “net” for network organizations.
    - “gov” for governmental websites.
    - “mil” for military websites.
  - **Second Level Domains** - These domains are specific to organizations or entities and serve as primary identifiers within web addresses.
  - **Sub-Domains** - additional organizational structuring of a website, enhancing flexibility in design and content management.
  - **Host Name** (a resource record) - particular device, usually a dedicated server.

- DNS hierarchy

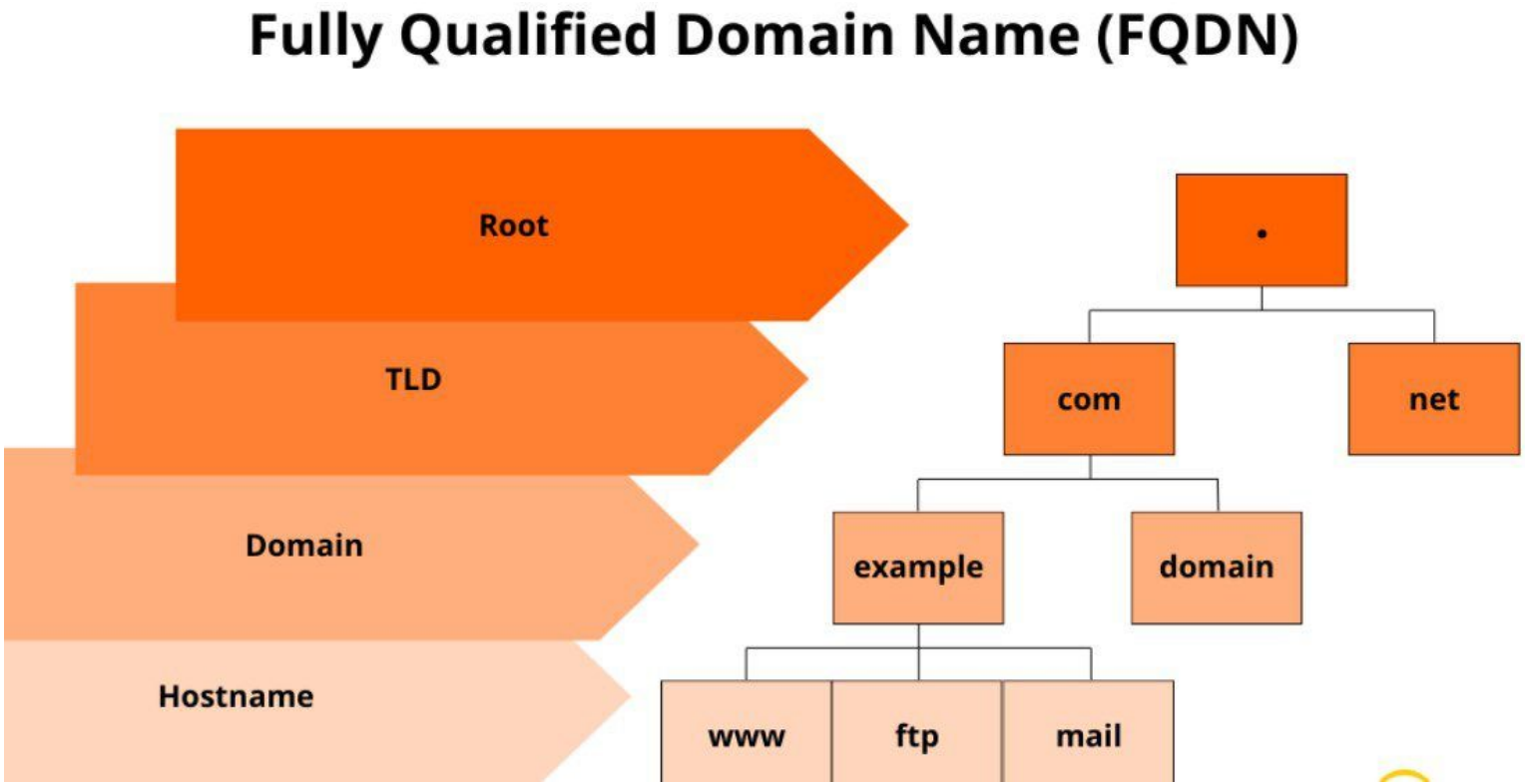
DNS hierarchical structure



- FQDN - A fully qualified domain name.
  - Conventionally written as a list of domain labels separated using the "." character.
  - The top of the hierarchy in an FQDN begins with the rightmost label:
    - glo.globallogic.com:
    - FQDN of glo.globallogic.com
      - **com** is a label directly under the root zone
      - **globallogic** is nested under the **com**
      - **glo** is nested under the **globallogic.com**
  - DNS root zone - The topmost layer of every domain name, an empty label, can be represented in an FQDN with a trailing dot (glo.globallogic.com.), often omitted by most applications.
  - The length of each label must be between **1 and 63 octets**, and the full domain name is limited to **255 octets**.
  - The characters allowed in labels are a subset of the ASCII character set, consisting of characters **a** through **z**, **A** through **Z**, **digits 0** through **9**, and **hyphen**.

- PQDN - A partially-qualified domain name
  - Relative Domain names, hostnames.
  - does not include all labels

- FQDN - A fully qualified domain name.



General network info

- General network info
  - hostname, dnsdomainname

```
$ hostname
some_hostname
$ dnsdomainname
synapse.com
$ domainname
synapse.com

cat /etc/hosts
cat /etc/hosts.allow #<service or ALL>: <IP address or hostname or subnet>
cat /etc/hosts.deny #<service or ALL>: <IP address or hostname or subnet>
```

Example:
Add to /etc/hosts.deny (block all access to host):
sshd: AL
Add to /etc/hosts.deny (allow access to host via local network):
sshd: 192.168.1.

- General network info
  - **host.conf** - resolver configuration file

    # The "order" line is only used by old versions of the C library.
    order hosts,bind
    multi on

  - **resolv.conf** - resolver configuration file

    domain synapse.com
    nameserver 192.168.0.254
    nameserver 8.8.8.8
    search synapse.com

  - **nsswitch.conf** - resolver configuration file

    hosts: files mdns4_minimal [NOTFOUND=return] dns //[STATUS=ACTION]
    networks: files

Tools: host

- host - DNS lookup utility

- ```
  $ host 8.8.8.8
  8.8.8.8.in-addr.arpa domain name pointer google-public-dns-a.google.com.
  ```
- ```
  $ host google-public-dns-a.google.com
  google-public-dns-a.google.com has address 8.8.8.8
  google-public-dns-a.google.com has IPv6 address 2001:4860:4860::8888
  ```

Tools: nslookup

- nslookup - **Querying Internet name servers utility**
-
```
$ nslookup google.com
Server:         172.17.48.16
Address:        172.17.48.16#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.209.46
```

Tools: delv

- delv - **DNS lookup and validation utility**
-
```
$ delv google.com 2>&1 | egrep -v '^[;]|^$'
google.com.             134     IN      A       216.58.209.46
```

Tools: whois

- whois - **client for the whois directory service**
- `$ whois google.com`

```
  Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-01-23T15:19:00Z <<<
```

Tools: dig

- dig - **DNS lookup utility**
  - `$ dig google.com`

```
; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1441
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             78      IN      A       216.58.215.78

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Fri Jan 31 17:58:34 EET 2025
;; MSG SIZE  rcvd: 55
```

Dnsmasq

- dnsmasq - **A lightweight DHCP and caching DNS server.**
- Features:
  - Lua scripting
  - IPv6
  - DNSSEC
  - Network booting for PXE
  - BOOTP
  - TFTP

- **Dnsmasq Subsystems:**
  - **DNS subsystem:** Provides caching of A, AAAA, CNAME and PTR, also DNSKEY and DS records
  - **DHCP subsystem:** Provide support for DHCPv4, DHCPv6, BOTP and PXE. Both static and dynamic DHCP leases can be used. Built in read-only TFTP server to support netboot.
  - **Router Advertisement subsystem** - provides basic autoconfiguration for IPv6 host

- Step 1: Install Dnsmasq
  - $ sudo apt install dnsmasq
  - Main configuration file for Dnsmasq is **/etc/dnsmasq.conf**
    port=53 # Custom port can be set (Port 53 is used for both **TCP** and **UDP** communication.)
    domain-needed # Never forward plain names (without a dot or domain part)
    bogus-priv # All reverse lookups for private IP ranges (ie 192.168.x.x, etc) which are not found in /etc/hosts or the DHCP leases file are answered with "no such domain" rather than being forwarded upstream.
    strict-order # Domain automatically added to simple names in a hosts-file.
    expand-hosts # Allows reaching hostname.hostdomain entries from /etc/hosts
    domain=example.com # Specifies domain name
    listen-address=127.0.0.1 # Set Listen address
  - $ sudo systemctl restart dnsmasq

- Step 2: Adding DNS records to Dnsmasq
  - Add DNS records in the file./etc/hosts. Dnsmasq will reply to queries from clients using these records:
  -
```
$ sudo vim /etc/hosts
10.1.3.4 server1.mypridomain.com
10.1.4.4 erp.mypridomain.com
192.168.10.2 checkout.mypridomain.com
192.168.4.3 hello.world
```
  -
```
$ sudo systemctl restart dnsmasq
```

- Step 3: Testing Dnsmasq DNS functionality
  - `$ dnsmasq --test # Check Configuration syntax`
  - `$ sudo vim /etc/resolv.conf`

    ```
    nameserver 127.0.0.1
    nameserver 8.8.8.8
    ```

  - Test using dig:

    ```
    $ dig A erp.globallogic.com
    $ dig A +noall +answer erp.globallogic.com
    ```

- Step 4: Configure Dnsmasq as DHCP Server (Optional)
  - $ Edit the file a /etc/dnsmasq.conf and provide:
    - Default gateway IP address
    - DNS server IP address (Probably Dnsmasq or different DNS server)
    - Network Subnet mask
    - DHCP Addresses range
    - NTP server
  - /etc/dnsmasq.conf Example:

```
dhcp-range=192.168.3.25,192.168.3.50,24h
dhcp-option=option:router,192.168.3.1
dhcp-option=option:ntp-server,192.168.3.5
dhcp-option=option:dns-server,192.168.3.5
dhcp-option=option:netmask,255.255.255.0
```

DNS Transport Protocol

- From the time of its origin in 1983 the DNS has used the User Datagram Protocol (**UDP**) for transport over IP. Its limitations have motivated numerous protocol developments for reliability, security, privacy, and other criteria, in the following decades.

- Conventional: DNS over UDP and TCP ports 53
  - UDP reserves port number 53
  - TCP protocol introduces reliability, security, and privacy
  - RFC 1123 specified optional Transmission Control Protocol (TCP) transport for DNS queries, replies and, particularly, zone transfers. Via fragmentation of long replies, TCP allows longer responses, reliable delivery, and re-use of long-lived connections between clients and servers. For larger responses, the server refers the client to TCP transport.
    - $ netstat -anp | grep dnsmasq

```
tcp        0      0 0.0.0.0:53          0.0.0.0:*           LISTEN      3087/dnsmasq
udp        0      0 0.0.0.0:53          0.0.0.0:*                       3087/dnsmasq
```

- UDP reserves port number 53
  - $ nslooklup google.com

```
Server:    8.8.8.8
Address 1: 8.8.8.8 dns.google

Name:      google.com
Address 1: 2a00:1450:401b:801::200e waw07s03-in-x0e.1e100.net
Address 2: 142.250.75.14 waw07s03-in-f14.1e100.net
```

Trace:

```
14:09:58.837440 IP 192.168.100.3.41638 > 8.8.8.8.53: 2+ PTR? 8.8.8.8.in-addr.arpa. (38)
14:09:58.837741 IP 192.168.100.3.41638 > 8.8.8.8.53: 2+ PTR? 8.8.8.8.in-addr.arpa. (38)
14:09:58.852716 IP 8.8.8.8.53 > 192.168.100.3.41638: 2 1/0/0 PTR dns.google. (62)
14:09:58.862138 IP 192.168.100.3.57446 > 8.8.8.8.53: 3+ AAAA? google.com. (28)
14:09:58.862494 IP 192.168.100.3.57446 > 8.8.8.8.53: 3+ AAAA? google.com. (28)
14:09:58.896244 IP 8.8.8.8.53 > 192.168.100.3.57446: 3 1/0/0 AAAA 2a00:1450:401b:801::200e (56)
14:09:58.907271 IP 192.168.100.3.56018 > 8.8.8.8.53: 4+ A? google.com. (28)
14:09:58.907570 IP 192.168.100.3.56018 > 8.8.8.8.53: 4+ A? google.com. (28)
14:09:58.923021 IP 8.8.8.8.53 > 192.168.100.3.56018: 4 1/0/0 A 142.250.75.14 (44)
14:09:58.932208 IP 192.168.100.3.42653 > 8.8.8.8.53: 5+ PTR? e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.1.0.8.0.b.1.0.4.0.5.4.1.0.0.a.2.ip6.arpa. (90)
14:09:58.932283 IP 192.168.100.3.42653 > 8.8.8.8.53: 5+ PTR? e.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.1.0.8.0.b.1.0.4.0.5.4.1.0.0.a.2.ip6.arpa. (90)
14:09:58.947644 IP 8.8.8.8.53 > 192.168.100.3.42653: 5 2/0/0 PTR waw07s03-in-x0e.1e100.net., PTR waw02s06-in-x0e.1e100.net. (159)
14:09:58.957257 IP 192.168.100.3.35878 > 8.8.8.8.53: 6+ PTR? 14.75.250.142.in-addr.arpa. (44)
14:09:58.957521 IP 192.168.100.3.35878 > 8.8.8.8.53: 6+ PTR? 14.75.250.142.in-addr.arpa. (44)
14:09:58.972717 IP 8.8.8.8.53 > 192.168.100.3.35878: 6 1/0/0 PTR waw07s03-in-f14.1e100.net. (83)
```

Types of DNS records

- From
  - SOA - A start of authority record. Is a type of resource record in the Domain Name System (DNS) containing administrative information about the zone
  - (A and AAAA) - IP addresses
  - MX - SMTP mail exchangers
  - NS - Name Servers
  - PTR - Pointers for reverse DNS lookups
  - CNAME - Domain name aliases

DNS server named forward zone configuration example:

```
$TTL    604800

@       IN      SOA     dns1.xyz1.com. admin.xyz1.com. (
                        13          ; Serial
                    604820          ; Refresh
                     86600          ; Retry
                   2419600          ; Expire
                    604600 )        ; Negative Cache TTL

; name servers - NS records
   IN  NS  dns1.xyz1.com.
   IN  NS  dns2.xyz1.com.

; name servers - A records
dns1.xyz1.com.      IN      A       192.168.56.13
dns2.xyz1.com.      IN      A       192.168.56.15

; 192.168.56.0/24 - A records
host1.xyz1.com.     IN      A       192.168.56.17
xyz1.com.           IN      CNAME   host1.xyz1.com.
host1.xyz1.com.     IN      TXT     "some text"
host2.xyz1.com.     IN      A       192.168.56.18

56.34.12.10.in-addr.arpa. IN PTR host1.example.net.
```

GlobalLogic
A Hitachi Group Company
EDUCATION

Thank You