==========
Instructor   : Jeremie Ukundwa TUYISENGE
FACULTY   : IT
Department   : SOFTWARE ENGINEERING
Date   : 11 April 2022
==========

Domain name System(Service) "DNS"

The Domain Name System (DNS) is used to resolve (translate) hostnames to internet protocol (IP) addresses and vice versa.
A DNS server, also known as a nameserver, maps IP addresses to hostnames or domain names.

- ✍️ Hostname: Human friendly (www.linux.org)
- ✍️ IP address: computer friendly (198.182.16.56)

Other Service Provided by DNS are:

1. DNS Allows machines to be grouped by name (domains)
2. DNS Provide email routing information

++

Throughout The steps provided you will learn the basics of DNS,

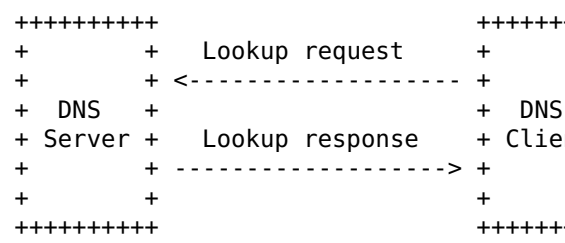
A. How DNS gets the IP address and hostname, to the concepts of forward and reverse lookup zones.
B. How to install and configure DNS,
   B.1 Define and edit zone files,
   B.2 Verify whether the DNS can resolve to the correct address with the help of commands.

++

A. How DNS gets the IP address and hostname, to the concepts of forward and reverse lookup zones.

How DNS works

When a client requests information from a nameserver(DNS Server), it usually connects to port 53, and then the nameserver resolves the name requested.



- ➡️ Sending a request from the DNS client to the DNS server is called a lookup request.
- ➡️ Getting a response from the DNS server to the DNS client is called a lookup response.
- ➡️ The system on which the DNS service is configured is called a DNS server.
- ➡️ The system that accesses the DNS server is called a DNS client.

Where does DNS get IP addresses?

You might wonder how DNS gets the IP of the corresponding hostname or domain name.
How does DNS search among different IP addresses and associate your domain name correctly?
Who stores those mappings between domain names and IP addresses?

- ☑️ When the client searches for the domain www.example.com, the request will initially go to the internet service provider's (ISP) resolver. It will respond to the user's request to resolve a domain name.

- ☑️ If the IP address is not found on the resolver, the request is forwarded to a root DNS server and later to the top-level domain (TLD) servers.
  ✍️TLD servers store information for top-level domains, such as .com or .net.

☑ Requests are forwarded to the nameservers, which know detailed information about domains and IP addresses. Nameservers respond to the ISP's resolver, and then the resolver responds to the client with the requested IP.
✍When the resolver doesn't know the IP, it stores the IP and its domain in a cache to service future queries.

Forward and reverse lookups

The forward lookup zone uses the domain name to search for IP addresses, whereas the reverse lookup zone uses IP addresses to search for the domain name.

++++++++++++++++++++ !IMPORTANT TO NOTE ++++++++++++++++++++++++++++++++

Top-level domain (TLDs)

e.g.

```
.com  : commercial organization
.net  : network of machines
.org  : non-profit organization
.mil  : US military
.gov  : US government
.co.uk: UK company
...
```

DNS sever types

```
a. Master server       : primary DNS server for a domain
b. Slave server        : receives info from the master
c. Forward server      : forwards (unresolved) DNS requests to other DNS
                         server
d. Caching only server : caches DNS info from other DNS server and uses
                         them to resolve local requests.
e. Stealth server      :
```

DNS software

```
a. BIND
b. PowerDNS
c. MaraDNS
c. MyDNS
...
..
```

++

B. Install and configure DNS

BIND (Berkeley Internet Name Domain) is a nameserver service responsible for performing domain-name-to-IP conversion on Linux-based DNS servers.

Step1: Install Bind

➡ yum install bind* -y
N.B: if it doesn't work reboot your redhat machine

Step2: Configure the /etc/named.conf file
First, add or edit the two values in the options field.
One is the DNS server address, and the other is the allow-query to any.

➡ vim /etc/named.conf

```
options {
        listen-on port 53 { 127.0.0.1; 192.168.0.2; }; # Master DNS Servers IP
        listen-on-v6 port 53 { ::1; };
        directory   "/var/named";

        allow-query     { localhost; 192.168.0.0/24; }; # IP Range of Hosts
        allow-transfer  { localhost; 192.168.0.3; }; # Slave DNS Servers IP
```

```
                recursion yes;
        }
```

N.B: 192.168.0.2 ==> DNS server address

✍ The BIND package provides the named service. It reads the configuration from the /etc/named and /etc/named.conf files.

Define the forward and reverse zones

✍ Zone is a description/definition of a domain or subdomain

Step3: Define the forward and reverse zones in the /etc/named.conf or /etc/named.rfc1912.zones (you can define zones in either of those files). In this example, I am appending zone definition details to the /etc/named.rfc1912.zones file.

➡ vim /etc/named.rfc1912.zones

```
zone "auca.com" IN {
   type master;
   file "auca.forward.zone";
   allow-update { none; };
};

zone "0.168.192.in-addr.arpa" IN {
 type master;
 file "auca.reverse.zone";
 allow-update { none; };
};
```

Create forward and reverse zone files

You also need to create forward and reverse zone files in the /var/named directory.

Note: By default, the named.conf file includes the /var/named directory for checking zone files. Sample zone files named.localhost and named.loopback are created during the installation of the BIND package.

Step4: copy sample from named.localhost and edit

➡ cp /var/named/named.localhost /var/named/auca.forward.zone

➡ vim /var/named/auca.forward.zone

```
$TTL 1D
@       IN      SOA     @  root.auca.com. (
                                202204001; serial
                                1D       ; refresh
                                1H       ; retry
                                1W       ; expiry
                                3H)      ; minimum
@       IN  NS          server.auca.com.
@       IN  A           192.168.0.2
server  IN  A           192.168.0.2
client  IN  A           192.168.0.5
```

Step5: copy sample from named.localhost and edit

➡ cp /var/named/named.localhost /var/named/auca.reverse.zone

➡ vim /var/named/auca.reverse.zone

```
$TTL 1D
@       IN      SOA     server.auca.com  root.auca.com. (
                                                202204012; serial
                                                1D       ; refresh
                                                1H       ; retry
                                                1W       ; expiry
                                                3H)      ; minimum
@       IN  NS          server.auca.com.
@       IN  PTR auca.com.
server  IN  A           192.168.0.2
client  IN  A           192.168.0.5
2       IN  PTR server.auca.com.
```

```
               5       IN  PTR client.auca.com.

Step6: changing group of zone files
        ➡cd /var/named
        ➡chgrp named auca.forward.zone
        ➡chgrp named auca.forward.zone
Step7: checking for configuration syntax
        ➡named-checkconf /etc/named.conf
        ➡named-checkzone auca.com /var/named/auca.forward.zone
        ➡named-checkzone auca.com /var/named/auca.reverse.zone
Step8: Restoring connection now
        ➡restorecon /etc/named.conf

Step9: Add the nameserver IP to /etc/resolv.conf

        ➡vim /etc/resolv.conf
                search auca.com
                nameserver 192.168.0.2
                :wq
Step10: reload (restart) NetworkManager
        ➡service NetworkManager restart

Start/restart and enable the named service
------------------------------------------

If the named service is not running or is disabled, then start and enable it.
If it is already active (running) and you made all these configurations, you need to
restart the service to make changes.

        ➡ service named status
        ➡ service named start
        ➡ service named enabled
        ➡ service named restart

     Verify the DNS name resolution
   ---------------------------------

You have installed the BIND package, configured named files, created lookup zones, and
restarted the service to make configurations take effect. Now use the nslookup and dig
commands to check whether DNS is working properly and verify whether you are getting the
intended results.

    nslookup is a program to query internet domain name servers.
    dig is a tool for interrogating DNS servers. It performs DNS lookups and displays
    the answers that are returned from the nameserver.

Query with nslookup
-------------------

        ➡ nslookup server.auca.com
          Server: 127.0.0.1
          Address: 127.0.0.1#53
          Name: server.auca.com
          Address: 192.168.0.2

        ➡ nslookup 192.168.0.2
           2.0.168.192.in-addr.arpa name = server.auca.com.

Query with dig
--------------

Here is a forward lookup, where DNS responds with 192.168.0.2 as an IP for server.auca.com:

        ➡ dig server.auca.com

=======================================

              Gracius

=======================================
```