Lab 1.3. Domain Name System (DNS)

Objectives

In this lab, we will configure a name service based on BIND. The target is to study both the basic configuration steps of the service and the protocol operation. Also, we will use client DNS tools to explore the service structure in the Internet.

Contents

Environment Preparation

In the first part (DNS Client), we will use the physical host.

For the second part of the lab (DNS Server), we will configure the network topology shown in Figure 1. As in previous labs, we will build the topology with the `vtopol` tool and an appropriate topology file. Before starting that part, configure the network interfaces as shown in the figure and check the connectivity between both machines.

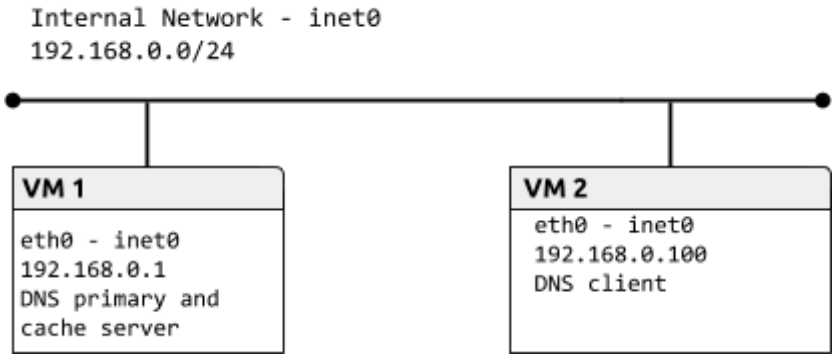

Figure 1: Topology and addressing of the network used in this lab

DNS Client

In this first part, we will use client DNS tools, which are useful both to debug the deployment of the DNS service in our local network, and to study the DNS structure in the Internet. Main tools to query a DNS service are `dig` and `host`. In this part, **we will use the physical host**. If DNS queries are blocked, then use a web interface like www.digwebinterface.com.

Exercise 1. The DNS client configuration file is `/etc/resolv.conf`. Consult the `man` page (`man resolv.conf`) and study the meaning of options `nameserver` and `search`. Check the contents of this file in the physical host of the lab.

Exercise 2. Starting from root server `a.root-servers.net` and using only the responses obtained

from each name server, get the IP address of `informatica.ucm.es`. Determine the TTL of each record and complete the following table:

Name server	Record name	TTL	Type	Data
`a.root-servers.net`	es.	172800	IN	NS a.nic.es.
a.nic.es.	ucm.es.	86400	IN	NS crispin.sim.ucm.es.
crispin.sim.ucm.es.	informatica.ucm.es.	86400	IN	CNAME ucm.es.
ucm.es.		86400	IN	A 147.96.1.15

NOTE: Use command `host -v <domain> [nameserver]`, or command `dig [@nameserver] <domain>`. More information in the `man` page of each command.

Exercise 3. Obtain information from SOA record for the `ucm.es.` zone using an authoritative server of the zone. Identify the relevant fields of the record. **NOTE**: use option `-t` with `host`, or add the record type as an argument with `dig`. foto1

Exercise 4. Determine which mail server should be used to send an e-mail to `...omaster@fdi.ucm.es`, using an authoritative server of the zone. foto2

Exercise 5. Determine the domain name for `147.96.85.71`. As in exercise 2, start from server `...root-servers.net` and use only the answers obtained from each name server.

Name server	Record name	TTL	Type	Data
`a.root-servers.net`	in-addr.arpa.	172800	IN	NS a.in-addr-servers-arpa.
a.in-addr-servers-arpa.	147.in-addr.arpa	86400	IN	NS z.arin.net.
z.arin.net.	96.147.in-addr.arpa	172800	IN	NS ucdns.sis.ucm.es.
ucdns.sis.ucm.es.	71.85.96.147.in-addr.arpa.	86400	IN	www.fdi.ucm.es

NOTE: The `host` command eases the reverse lookup when an IP address is detected as argument, creating the search domain from the IP address (that is, it reverses the byte order and adds `.in-addr.arpa.`) and establishing the default record type to PTR. Option `-x` in `dig` produces the same effect.

Exercise 6. Get the IP address of `www.google.com` without indicating any name server (the name server configured in `/etc/resolv.conf` will be used). Use `dig` command with option `+trace` and observe the queries performed. foto3

DNS Server

Forward Zone

VM1 will be the name server of the `labfdi.es` domain. The *forward* zone for `labfdi.es.` must include the records described in the following table.

Record	Description
Start of Authority (SOA)	Zone description. Freely choose the values for serial number, refresh, update, expiry and nx ttl. The primary name server of the zone is `ns.labfdi.es` and the contact e-mail is `contact@labfdi.es`.
Name Server (NS)	Name server is `ns.labfdi.es`, as specified in the SOA record
Mail server (MX)	Mail server is `mail.labfdi.es`
Canonical Name (CNAME) of server	Canonical name of `server.labfdi.es` is `mail.labfdi.es`
Address (A) of `ns.labfdi.es`	Address of `ns.labfdi.es` is `192.168.0.1` (VM1)
Addresses (A and AAAA) of web server	Addresses of `www.labfdi.es` are `192.168.0.200` and `fd00::1`
Address (A) of mail server	Address of `mail.labfdi.es` is `192.168.0.250`

NOTE: In the service configuration, don't forget that FQDN names end with the root domain ("`.`").

Exercise 1. Configure the name server. Files are in directory `/etc/bind/`, main file (`named.conf`) includes the configuration from other three files (`named.conf.options`, `named.conf.local`, `named.conf.default_zones`):

- Comment out all `include` lines in file `/etc/bind/named.conf`.
- Add a `zone` definition for the *forward* zone. The server `type` should be `master` and the zone `file` should be `db.labfdi.es`.

Listing 1. Example of zone definition in `/etc/bind/named.conf`

```
zone “labfdi.es.” {
  type master;
  file “/etc/bind/db.labfdi.es”;
};
```

NOTE: Consult `man` page of `named.conf` to learn the available options for zone definition.

NOTE: Once the configuration file is created, execute the command `named-checkconf`, to verify that the syntax is correct.

Exercise 2. Create the file for the forward zone with the records specified in the above table (you can start from one of the existing database files). Specify also the `$TTL` command.

NOTE: The zone name can be specified as `@` in the record name field.

NOTE: Once the zone file is created, execute the command `named-checkzone <zone_name> <file>`, to verify that the syntax is correct.

Exercise 3. Configure the client virtual machine to use the new name server. For this, create or modify `/etc/resolv.conf` with the new values for `nameserver` and `search`. Check the name lookup for `www.labfdi.es`.

Exercise 4. Start the DNS service with command `service bind9 start`.

Exercise 5. Use command `dig` or `host` to obtain information from the domain `labfdi.es` offered by the server.

Exercise 6. Repeat any of the previous queries and, with the help of `wireshark`:

- Check the protocol and port used by DNS client and server.
- Analyze the format (fields included and length) of the messages corresponding to DNS queries and responses.

Reverse Zone

Also, the server will include a database for reverse lookup. For that, we will define the *reverse* zone `0.168.192.in-addr.arpa.` with the PTR records corresponding to the IPv4 addresses. This zone will use the same name server and configuration parameters in the SOA record.

Exercise 1. Add another `zone` definition for the reverse zone. The server `type` should be `master` and the zone `file` should be `db.0.168.192`.

Exercise 2. Create the file for the reverse zone with the SOA and PTR records.

Exercise 3. Restart the DNS service with command `service bind9 restart` (or reload the configuration with command `service bind9 reload`).

Exercise 4. Check the reverse lookup by getting the name associated to `192.168.0.250`.