DOMAIN NAME SYSTEM (DNS)

INTRODUCTION

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. BIND is the nameserver service responsible for performing domain-name-to-IP conversion on Linux-based DNS servers.

NETWORK STRUCTURE

Working on our network diagram from the previous labsheet we will be configuring DNS on Prometheus. Routing on Prometheus and vP1 should be working so pinging between all our hosts must be possible. Your DNS Server name will be **Prometheus.yourpcname.netlab.ee.port.ac.uk** so rename Prometheus and all your VMs to include this suffix using the hostname command and editing the **/etc/hostname** file. Also change your DNS search path to yourpcname.netlab.ee.port.ac.uk. in your network card settings and in **/etc/resolv.conf**. Reboot.

INSTALLATION ON PROMETHEUS

Install BIND on Prometheus: **yum -y install bind bind-utils**

CONFIGURING DNS

Most of the configurations for bind on a DNS server are done on the named.conf file located in /etc . Here, you will configure listening ports and IP address, forward zones, reverse zones, etc.

- Open the configuration file with a text editor of your choice: **gedit /etc/named.conf**
- Configure the listening IP address by editing the following line:
  listen-on port 53 { 127.0.0.1; 148.197.28.xx; }; #Prometheus' IP address
- Allow all networks access to query the server by editing the following line:
  allow-query { localhost; 148.197.28.0/24; 148.197.30.0/24; 148.197.31.0/24; 148.197.32.0/24; };

CREATING ZONES

While still editing named.conf

- Add the following to the file for the forward lookup zone:
  zone " yourpcname.netlab.ee.port.ac.uk" IN {
  type master;
  file "/var/named/yourpcname.netlab.ee.port.ac.uk.db";
  allow-update { none; };
  };

- Add the following to the file for the reverse lookup zone for the .28 network:
  zone "28.197.148.in-addr.arpa" IN {
  type master;
  file "/var/named/148.197.28.db";
  allow-update { none; };
  };

Notes:

yourpcname.netlab.ee.port.ac.uk – Domain name
master – Primary DNS
yourpcname.netlab.ee.port.ac.uk.db – Forward lookup file
allow-update – Since this is the primary DNS, it should be none
28.197.148.in-addr.arpa – Reverse lookup name
148.197.28.db – Reverse lookup file

- Create the reverse lookup zone entries for your networks on subnets .30 .31 and .32

CREATING THE ZONE FILES

ORWARD LOOKUP ZONE FILE

By default, zone lookup files are placed under the /var/named directory. Create a zone file called yourpcname.netlab.ee.port.ac.uk.db for forward lookup under /var/named . All domain names should end with a dot (.).

- Create and edit the zone file: gedit /var/named/yourpcname.netlab.ee.port.ac.uk.db

```
@       IN      SOA     prometheus.yourpcname.netlab.ee.port.ac.uk.      root.yourpcname.netlab.ee.port.ac.uk.
(
                        1001 ;Serial
                        3H ;Refresh
                        15M ;Retry
                        1W ;Expire
                        1D ;Minimum TTL
                        )
;Name Server Information
@       IN      NS      Prometheus.yourpcname.netlab.ee.port.ac.uk.

;IP address of Name Server
Prometheus      IN      A       148.197.28.xx

;Mail exchanger
yourpcname.netlab.ee.port.ac.uk.        IN      MX      10      mail.yourpcname.netlab.ee.port.ac.uk.

;A - Record HostName To IP Address
www             IN      A       148.197.28.xx
mail            IN      A       148.197.28.xx
Prometheus      IN      A       148.197.28.xx
                IN      A       148.197.30.xx
                IN      A       148.197.31.xx

vprometheus0    IN      A       148.197.30.xx

vprometheus1    IN      A       148.197.31.xx
                IN      A       148.197.32.xx
;CNAME record
ftp     IN      CNAME   www.netlab.yourpcname.ee.port.ac.uk.
```

There are some special keywords for Zone Files
A – A record, NS – Name Server, MX – Mail for Exchange, CNAME – Canonical Name

Note: Whenever you update the zone lookup file, you need to change/increment the serial like 1002 ;Serial.

REVERSE LOOKUP ZONE FILES

Create a zone file called 148.197.28.db for the .28 reverse lookup zone under /var/named directory.

- Create and edit the zone file: gedit /var/named/148.197.28.db
- Add the following lines to the file:

```
@       IN      SOA     prometheus.yourpcname.netlab.ee.port.ac.uk.      root.yourpcname.netlab.ee.port.ac.uk.
(
                        1001 ;Serial
                        3H ;Refresh
                        15M ;Retry
                        1W ;Expire
                        1D ;Minimum TTL
                        )

;Name Server Information
@       IN      NS      prometheus.yourpcname.netlab.ee.port.ac.uk.

;Reverse lookup for Name Server
xx      IN      PTR     prometheus.yourpcname.netlab.ee.port.ac.uk.

;PTR Record IP address to HostName
xx      IN      PTR     www.yourpcname.netlab.ee.port.ac.uk.
xx      IN      PTR     mail.yourpcname.netlab.ee.port.ac.uk.
```

- Create the reverse zone files for .30, .31 and .31 networks using the above as a template.
- Restart and enable the bind service: **systemctl restart named; systemctl enable named**

FIREWALL

Allow the bind service default port access through the firewall.

- Add the port: **firewall-cmd --permanent --add-port=53/udp**
- Reload the firewall: **firewall-cmd –reload**

VERIFY ZONES

Go to vPrometheus0 Network Settings, IPv4 and configure the IP address of the DNS Server to that of your host. Switch the network card OFF and then ON again.

- Open a terminal and type: **dig www.yourpcname.netlab.ee.port.ac.uk**
- Change the DNS server on Prometheus's networking settings as well and repeat the dig command there too.
- Finally go to all your VMs one by one and ping all other VMs and the host by prefix only for example on vP0 type ping vP2. It should at the very least resolve to an IP address even if the VM isn't actually running to respond. If it does then congratulations, you have setup your very own authoritative Server for the domain "yourpcname.netlab.ee.port.ac.uk".