



NETENG Assignment 3

ENGR3821

Network Engineering

Hidden Primary DNS

24/06/2019

Consent

I, the author, give consent to ENGR3821 Topic Staff to distribute this document for the purposes of peer marking and assessment.

Table of Contents

Consent	i
Table of Contents.....	i
List of Tables	i
Table of Figures	i
Definitions.....	ii
0 Introduction.....	1
0.0 Revision History.....	1
0.1 Purpose.....	1
0.2 Scope	1
1 Installation Procedure	1
1.0 Initial Software.....	1
1.1 Configure Bind Options	2
1.2 Specify Zones.....	2
1.3 Create Zone Files	3
1.4 Check Syntax and Allow Through Firewall.....	4
1.5 Configuration of DNS Clients.....	5
2 Bibliography	6

List of Tables

Table 1 - Author and Revision History.....	1
Table 2 - neteng FQDN domain zone hosts.....	1

Table of Figures

Figure 1 - Modify the bind options	2
Figure 2 - Modify the bind local config.....	2
Figure 3 - neteng.com forward zone	3
Figure 4 - neteng.com reverse zone	3
Figure 5 - syntax checks using sudo named-check*	4
Figure 6 - Allow bind9 through the firewall.....	4
Figure 7 - Successful netplan configuration on client	5
Figure 8 - Created name servers do not appear.....	6

Definitions

Term	Definition
A	(DNS Record) Address
DNS	Domain Name Service
FQDN	Fully Qualified Domain Name
IN	(DNS Record) Internet
IP	Internet Protocol
NS	(DNS Record) NameServer
PTR	(DNS Record) Pointer
SOA	(DNS Record) Start of Authority
UFW	Uncomplicated FireWall
VM	Virtual Machine

0 Introduction

0.0 Revision History

Table 1 - Author and Revision History

Revision No.	Author	Date	Details
0	<REDACTED1>	15/06/19	Initial Documentation

0.1 Purpose

This document is intended to be a procedure of the setup required to configure a master and slave DNS server on two separate Linux Ubuntu 18.04 VMs. This document will detail testing of the restriction of connections to the primary DNS.

0.2 Scope

The setup of the DNS server(s) could not be completed due to an unknown phenomenon even on a clean install of Ubuntu 18.04 as detailed in later sections. This report shall restrict its scope such that the reproduction of the error can be created. The configuration will detail exclusively IPv4 addressing.

1 Installation Procedure

1.0 Initial Software

Bind9 is the system to be used to set up and configure the DNS servers[1]. Along with this, netplan is needed to write and manage files and network interfaces in backend Ubuntu networking software. To install these packages, use the following command.

```
sudo apt-get install bind9 netplan.io
```

Ensure the system has some sort of tool to view the current network interfaces and environment such as `ip` or `ifconfig`.

The initial addresses per zone shall be as follows:

Table 2 - neteng FQDN domain zone hosts

Server	Name	Address
Domain (FQDN) e.g.	neteng.com.	
Primary nameserver (master)	ns1.neteng.com	10.1.1.1/24
Secondary nameserver (slave)	ns2.neteng.com	10.1.1.2/24
Web server	host.neteng.com	10.1.1.100/24
FTP server	ftp.neteng.com	10.1.1.101/24
Mail Server	mail.neteng.com	10.1.1.102/24

1.1 Configure Bind Options

After installation of `bind9` and its automatic documentation and utilities, modify the file `/etc/bind/named.conf.options` with a text editor. The images in this documentation use `nano`.

For example:

```
sudo nano /etc/bind/named.conf.options
```

Create and `acl` block with the private addresses for the domain as entries. Note that the addresses of all hosts in the zone should be specified as well; this is not shown properly in the capture below. Allow recursive DNS queries from the trusted `acl` named `neteng`, for example, and apply name server settings as below.

```
acl "neteng" {
    10.1.1.1;      //primDNS,host
    10.1.1.2;      //slavDNS
};

options {
    directory "/var/cache/bind";

    recursion yes;
    allow-recursion { neteng; };    //allows recursion from trusted machine$
    listen-on { localhost; };      //name server 1
    allow-transfer { none; };

    // If there is a firewall between you and nameservers you want
```

Figure 1 - Modify the bind options

Within the options block, specify servers to forward DNS queries to in the case of failure or otherwise. The servers specified here are owned by Google, which are free to use.

```
forwarders {
    8.8.8.8;
    8.8.4.4;
}
```

1.2 Specify Zones

Using a text editor, edit the file `/etc/bind/named.conf.local` and specify the DNS zones required along with the corresponding reverse zones. Insert more zones as required such as those from ENGR3821 Workshop Unit 2. Specify the master/slave behaviour of the server, its zone file location and allow query transfer from the secondary DNS server. Note the reverse octet order of the reverse zone.

```
GNU nano 2.9.3 /etc/bind/named.conf.local

// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "neteng.com" {
    type master;
    file "/etc/bind/zones/db.neteng.com";
    allow-transfer { 10.1.1.2; };
};

zone "1.1.10.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db/10.1.1";
};

[ Read 18 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text ^T To Spell ^_ Go To Line
```

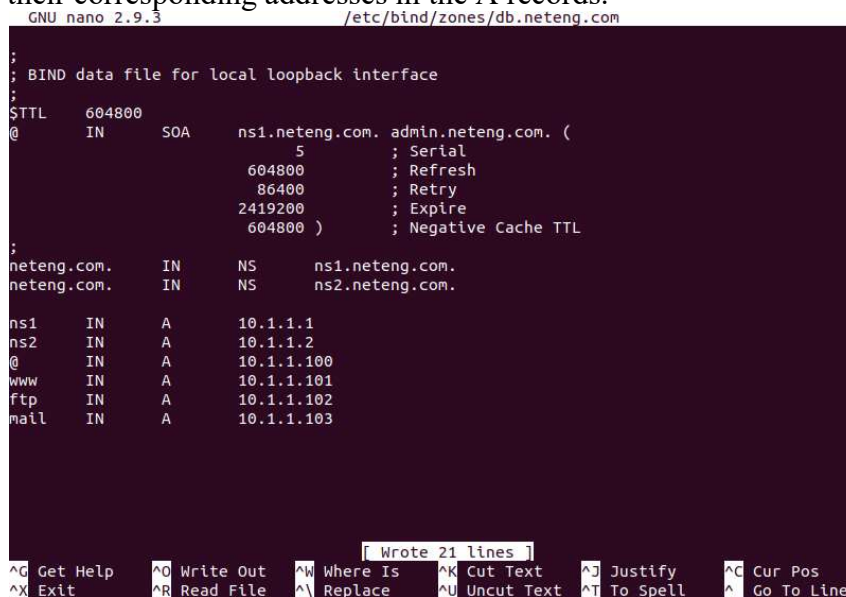
Figure 2 - Modify the bind local config

1.3 Create Zone Files

For each zone in `/etc/bind/named.conf.local`, create a file at the location specified in Step 1.2 and edit it with a text editor. For example:

```
cd /etc/bind
mkdir zones
cd zones
sudo nano db.neteng.com
```

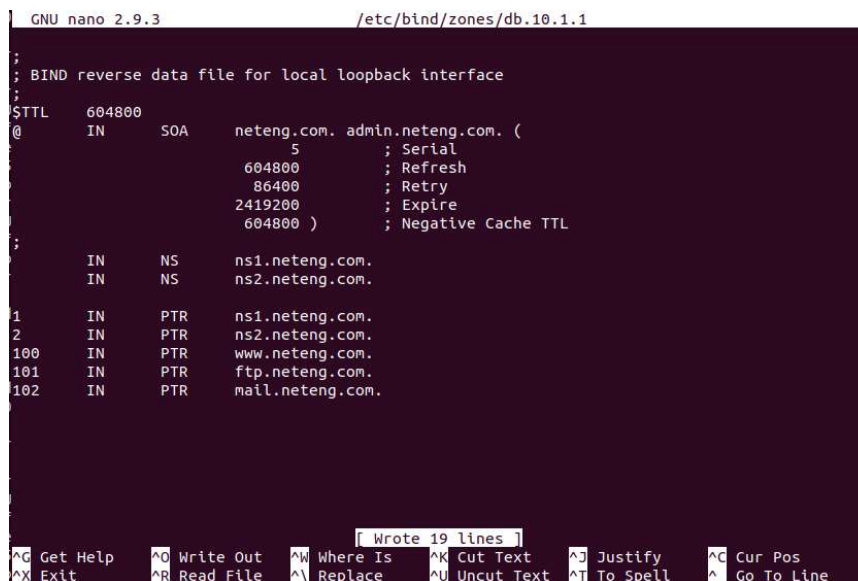
Increment the Serial value for human version control and specify the NS records to each name server. Ensure that FQDNs are used by inserting a full stop at the end of each name. Specify the hosts and their corresponding addresses in the A records.



```
GNU nano 2.9.3 /etc/bind/zones/db.neteng.com
;
; BIND data file for local loopback interface
;
$TTL 604800
@      IN      SOA      ns1.neteng.com. admin.neteng.com. (
                        5          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
neteng.com.      IN      NS      ns1.neteng.com.
neteng.com.      IN      NS      ns2.neteng.com.
;
ns1      IN      A      10.1.1.1
ns2      IN      A      10.1.1.2
@        IN      A      10.1.1.100
www      IN      A      10.1.1.101
ftp      IN      A      10.1.1.102
mail     IN      A      10.1.1.103
;
Wrote 21 lines
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^_ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

Figure 3 - neteng.com forward zone

Specify the same details in the reverse DNS zone file.



```
GNU nano 2.9.3 /etc/bind/zones/db.10.1.1
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@      IN      SOA      neteng.com. admin.neteng.com. (
                        5          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
;
      IN      NS      ns1.neteng.com.
      IN      NS      ns2.neteng.com.
;
1      IN      PTR     ns1.neteng.com.
2      IN      PTR     ns2.neteng.com.
100    IN      PTR     www.neteng.com.
101    IN      PTR     ftp.neteng.com.
102    IN      PTR     mail.neteng.com.
;
Wrote 19 lines
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^_ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

Figure 4 - neteng.com reverse zone

1.4 Check Syntax and Allow Through Firewall

Use the following commands to check the syntax and layout of each of the specified config files.

```
sudo named-checkconf
sudo named-checkzone neteng.com db.neteng.com
sudo named-checkzone neteng.com db.neteng.com
```

```
student@neteng:/etc/bind/zones$ named-checkzone neteng.com db.neteng.com
zone neteng.com/IN: loaded serial 5
OK
student@neteng:/etc/bind/zones$ named-checkzone 1.1.10.in-addr.arpa db.10.1.1
zone 1.1.10.in-addr.arpa/IN: loaded serial 5
OK
student@neteng:/etc/bind/zones$
```

Figure 5 - syntax checks using sudo named-check*

Restart the service and then allow the service through the ufw firewall.

```
sudo systemctl restart bind9
sudo ufw allow bind9
```

Ensure that ufw is enabled.

```
student@neteng:/etc/bind/zones$ sudo ufw allow bind9
Rules updated
Rules updated (v6)
student@neteng:/etc/bind/zones$ sudo systemctl ufw status
Unknown operation ufw.
student@neteng:/etc/bind/zones$ sudo ufw status
Status: inactive
student@neteng:/etc/bind/zones$ sudo ufw enable
Firewall is active and enabled on system startup
student@neteng:/etc/bind/zones$ sudo ufw status
Status: active

To Action From
--
Bind9 ALLOW Anywhere
Bind9 (v6) ALLOW Anywhere (v6)

student@neteng:/etc/bind/zones$
```

Figure 6 - Allow bind9 through the firewall

Repeat Step 1.1 and 1.4 on the secondary DNS server with Bind9 installed with the adjustments as follows:

1. In the local file change the type of each of the zones from `master` to `slave`
2. Add the line to each zone: `masters { 10.1.1.1; };`

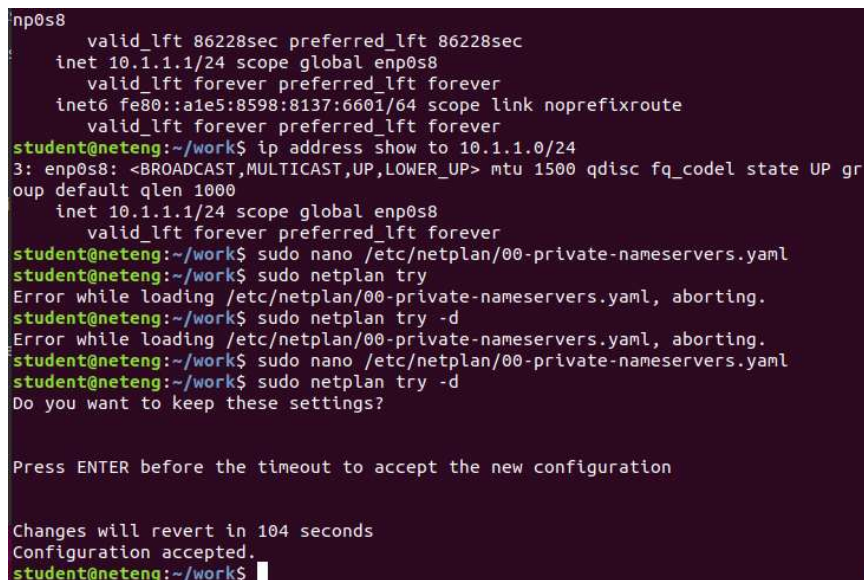
1.5 Configuration of DNS Clients

On each host machine, configure it to search for the relevant name servers in the zones specified by using `netplan` and modifying `/etc/netplan/00-private-nameservers.yaml`

```
network:
  version: 5
  ethernets:
    enp0s8:
      interface:
        nameservers:
          addresses:
            - 10.1.1.1
            - 10.1.1.2
          search: [ neteng.com ]
```

Ensure the yaml indentation is precise as this may cause errors if whitespace is not properly utilised.

Use `netplan try` with an optional `-d` (debug) flag to attempt to restart the networking features on the VM. On success, the following output should appear.



```
enp0s8
    valid_lft 86228sec preferred_lft 86228sec
    inet 10.1.1.1/24 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a1e5:8598:8137:6601/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
student@neteng:~/work$ ip address show to 10.1.1.0/24
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 10.1.1.1/24 scope global enp0s8
        valid_lft forever preferred_lft forever
student@neteng:~/work$ sudo nano /etc/netplan/00-private-nameservers.yaml
student@neteng:~/work$ sudo netplan try
Error while loading /etc/netplan/00-private-nameservers.yaml, aborting.
student@neteng:~/work$ sudo netplan try -d
Error while loading /etc/netplan/00-private-nameservers.yaml, aborting.
student@neteng:~/work$ sudo nano /etc/netplan/00-private-nameservers.yaml
student@neteng:~/work$ sudo netplan try -d
Do you want to keep these settings?

Press ENTER before the timeout to accept the new configuration

Changes will revert in 104 seconds
Configuration accepted.
student@neteng:~/work$
```

Figure 7 - Successful netplan configuration on client

Test the DNS configuration on the DNS client using the following command.

```
sudo system-resolve --status
```


The name servers should be visible under the network interface enp0s8 key for DNS Servers. However, the values 10.1.1.1 and 10.1.1.2 do not appear. Since the steps to complete the rest of the requirements of this Assignment extend from the success of this step, this marks the end of the available documentation.

```
28.172.in-addr.arpa
29.172.in-addr.arpa
30.172.in-addr.arpa
31.172.in-addr.arpa
corp
d.f.ip6.arpa
home
internal
intranet
lan
local
private
test

Link 3 (enp0s8)
  Current Scopes: DNS
  LLMNR setting: yes
MulticastDNS setting: no
  DNSSEC setting: no
  DNSSEC supported: no
  DNS Servers: 192.168.1.1

Link 2 (enp0s3)
  Current Scopes: DNS
  LLMNR setting: yes
MulticastDNS setting: no
  DNSSEC setting: no
  DNSSEC supported: no
  DNS Servers: 10.3.185.41
               192.168.1.1
lines 16-45/45 (END)
```

Figure 8 - Created name servers do not appear

END OF DOCUMENTATION

2 Bibliography

- [1] J. Ellingwood and M. Anical. (2018, 23/06/2019). *How To Configure BIND as a Private Network DNS Server on Ubuntu 18.04* Available:
<https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-18-04>