Self Hosted DNS

Homelab Club at UMD 2025-09-30

What is DNS

(D)omain (N)ame (S)ystem

Make DNS queries to lookup DNS records

A few types of DNS records:

- A: "address", hostname -> IPv4 address (32 bit)
- AAAA: "address x4", hostname -> IPv6 address (128 bit)
- PTR: "pointer" (reverse entry), IP address -> hostname
- CNAME: "canonical name" (other name), hostname -> hostname
- MX: "mail exchange", for routing SMTP (emails)
- TXT "text", confirm domain ownership + other protocols
- NS "name server", indicate which DNS server authoritative

Package Installation:

```
sudo apt update

sudo apt upgrade


sudo apt install vim

sudo apt install bind9-dnsutils

sudo apt install bind9 bind9-utils

(optional) sudo apt install bind9-doc
```

(Note: Included with bind9-utils is nslookup and dig. It has a dependency of bind9-host which includes the host command.

Note: dnsutils is the traditional package for bind9-dnsutils and may appear in other tutorials.)

Why BIND9

Benefits

- Popular option
- Customization
- Supported by the ISC
- Support on major Linux distributions

Downsides

- More complex compared to other options
- Easy to mess up if you do not pay attention

host

```
superexago@pi4-0:~ $ host google.com
google.com has address 142.251.167.138
google.com has address 142.251.167.139
google.com has address 142.251.167.113
google.com has address 142.251.167.102
google.com has address 142.251.167.100
google.com has address 142.251.167.101
google.com has IPv6 address 2607:f8b0:4002:c02::64
google.com has IPv6 address 2607:f8b0:4002:c02::8b
google.com has IPv6 address 2607:f8b0:4002:c02::71
google.com has IPv6 address 2607:f8b0:4002:c02::66
google.com mail is handled by 10 smtp.google.com.
```

nslookup

```
superexago@pi4-0:~ $ nslookup google.com
Server: 128.8.74.2
Address: 128.8.74.2#53

Non-authoritative answer:
Name: google.com
Address: 142.251.16.101
Name: google.com
Address: 142.251.16.138
Name: google.com
Address: 142.251.16.139
Name: google.com
Address: 142.251.16.113
Name: google.com
Address: 142.251.16.102
Name: google.com
Address: 142.251.16.100
Name: google.com
Address: 2607:f8b0:4004:c17::71
Name: google.com
Address: 2607:f8b0:4004:c17::8a
Name: google.com
Address: 2607:f8b0:4004:c17::8b
Name: google.com
Address: 2607:f8b0:4004:c17::66
```

nslookup (Type Flag)

```
superexago@pi4-0:~ $ nslookup -type=ns google.com
Server: 128.8.74.2
Address: 128.8.74.2#53

Non-authoritative answer:
google.com nameserver = ns4.google.com.
google.com nameserver = ns2.google.com.
google.com nameserver = ns3.google.com.
google.com nameserver = ns1.google.com.

Authoritative answers can be found from:
ns4.google.com internet address = 216.239.38.10
ns3.google.com internet address = 216.239.36.10
ns2.google.com internet address = 216.239.34.10
ns1.google.com internet address = 216.239.32.10
ns4.google.com has AAAA address 2001:4860:4802:38::a
ns3.google.com has AAAA address 2001:4860:4802:36::a
ns2.google.com has AAAA address 2001:4860:4802:34::a
ns1.google.com has AAAA address 2001:4860:4802:32::a
```

```
superexago@pi4-0:~ $ nslookup -type=mx gmail.com
Server: 128.8.74.2
Address: 128.8.74.2#53

Non-authoritative answer:
gmail.com mail exchanger = 30
alt3.gmail-smtp-in.l.google.com.
gmail.com mail exchanger = 40
alt4.gmail-smtp-in.l.google.com.
gmail.com mail exchanger = 5
gmail-smtp-in.l.google.com.
gmail.com mail exchanger = 10
alt1.gmail-smtp-in.l.google.com.
gmail.com mail exchanger = 20
alt2.gmail-smtp-in.l.google.com.

Authoritative answers can be found from:
```

nslookup (Specify DNS Server)

```
superexago@pi4-0:~ $ nslookup google.com
Server: 128.8.74.2
Address: 128.8.74.2#53

Non-authoritative answer:
Name: google.com
Address: 142.251.16.101
Name: google.com
Address: 142.251.16.138
Name: google.com
Address: 142.251.16.139
Name: google.com
Address: 142.251.16.113
Name: google.com
Address: 142.251.16.102
Name: google.com
Address: 142.251.16.100
Name: google.com
Address: 2607:f8b0:4004:c17::71
Name: google.com
Address: 2607:f8b0:4004:c17::8a
Name: google.com
Address: 2607:f8b0:4004:c17::8b
Name: google.com
Address: 2607:f8b0:4004:c17::66
```

```
superexago@pi4-0:~ $ nslookup google.com 1.1.1.1
Server: 1.1.1.1
Address: 1.1.1.1#53

Non-authoritative answer:
Name: google.com
Address: 142.251.111.100
Name: google.com
Address: 142.251.111.113
Name: google.com
Address: 142.251.111.102
Name: google.com
Address: 142.251.111.101
Name: google.com
Address: 142.251.111.139
Name: google.com
Address: 142.251.111.138
Name: google.com
Address: 2607:f8b0:4002:c03::65
Name: google.com
Address: 2607:f8b0:4002:c03::8b
Name: google.com
Address: 2607:f8b0:4002:c03::64
Name: google.com
Address: 2607:f8b0:4002:c03::66
```

dig

```
superexago@pi4-0:~ $ dig google.com

; <<>> DiG 9.18.33-1~deb12u2-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59933
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: 6340ed392721cb1f0100000068ce10848f383d532ebc0262 (good)
;; QUESTION SECTION:
;google.com. IN A

;; ANSWER SECTION:
google.com. 135 IN A 142.251.16.100
google.com. 135 IN A 142.251.16.101
google.com. 135 IN A 142.251.16.138
google.com. 135 IN A 142.251.16.139
google.com. 135 IN A 142.251.16.113
google.com. 135 IN A 142.251.16.102

;; Query time: 3 msec
;; SERVER: 128.8.74.2#53(128.8.74.2) (UDP)
;; WHEN: Fri Sep 19 22:25:08 EDT 2025
;; MSG SIZE rcvd: 163
```

ping

```
superexago@pi4-0:~ $ ping google.com
PING google.com (142.250.31.102) 56(84) bytes of data.
64 bytes from bj-in-f102.1e100.net (142.250.31.102): icmp_seq=1 ttl=101 time=6.53 ms
64 bytes from bj-in-f102.1e100.net (142.250.31.102): icmp_seq=2 ttl=101 time=6.75 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 6.534/6.640/6.746/0.106 ms
superexago@pi4-0:~ $
```

Basics of VIM

Default is normal mode, press escape to get to normal mode

- Use arrow keys to move around

Press i to get to insertion mode, acts like regular text editing mode

Command line, usually colon for short cuts, use escape then colon

- :q! quit without saving
- :wq quit and write to file
- :w write to file
- :u undo
- :0 (or any number) go to start of file or specified line number
- :$ go to end of line
- :set number to show/hide line numbers
- :syntax on/off to turn on/off syntax highlighting

Default configuration can be edited in .vimrc in home directory, add vim commands to be run whenever vim is used to open a file

Set Hostname:

Replace 127.0.1.1 with the host name of the raspberry pi

```
sudo vim /etc/hosts
```

Replace the text inside of the hostname of the raspberry pi

```
sudo vim /etc/hostname
```

Restart the raspberry pi

```
sudo shutdown -r now
```

Check if it has applied after reboot: `hostname`

Set Hostname:

Add a different hostname to /etc/hosts:

```
sudo vim /etc/hosts
```

Test output of the commands:

```
host <hostname>
nslookup <hostname>
dig <hostname>
ping <hostname>
```

Set Static IP:

Use NetworkManger to set a static IP

```
nmcli
nmcli connection show
```

Note the "name" of the connection you are using not the "device"

```
nmcli con mod "<connection-name>" ipv4.address <ip-address/<subet-mask>
nmcli con mod "<connection-name>" ipv4.gateway <gateway-ip-address>
nmcli con mod "<connection-name>" ipv4.method manual
nmcli con down "<connection-name>" && nmcli con up "<connection-name>"
nmcli
```

Bind9 Configuration files

First, look at system (system and service manager) for bind9:

```
cat /etc/systemd/system/bind9.service
```

Note:

```
EnvironmentFile=-/etc/default/named
ExecStart=/usr/sbin/named -f $OPTIONS
Alias=bind9.service
```

To check current status of the service:

```
systemctl status bind9
systemctl status named
```

Bind9 Configuration files

From what we have seen before, lets check the named service sciprt:

```
cat /etc/init.d/named | less
```

Note the comment about creating/chaining/etc/default/named (this was the EnvironmentFile=-/etc/default/named), next we will edit that file

(Note: In the bind9.service file, the =- means the file does not exist. It will not be read, and no error or warning will be logged.)

Bind9 Configuration files

Edit the named file:

```
sudo vim /etc/default/named
```

Configure the service to only run IPV4 by adding -4 to the options

Default:

```
OPTIONS="-u bind"
```

Change to:

```
OPTIONS="-u bind -4"
```

Bind9 Configuration files

Check the bind9 named configuration:

```
cat /etc/bind/named.conf
```

Note the 3 included .conf files which are used to configure Bind9

```
/etc/bind/named.conf.options
/etc/bind/named.conf.local
/etc/bind/named.conf.default-zones
```

To check if the edits made are valid use the following command:

```
sudo named-checkconf
```

named.conf.options

Editing named.conf.options

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

Put the following statement above the options {...} statement:

```
acl trusted {
     localhost;
     localnets;
};
```

none: Matches no hosts

any: matches all hosts

localhost: 127.0.0.1 and ::1, as well as the IP addresses of all interfaces on the server

localnets: 127.0.0.1 and ::1, as well as the subnets the server is on is connected to

named.conf.options

Now add configuration within the options {...} statement:

Allow DNS queries from the ACL we defined:

```
allow-query { trusted; };
allow-recursion { trusted; };  # allow query recursively for authoritative DNS servers for the domain
```

Forward requests for records that this server does not have:

```
forward only; # don’t attempt to contact other NS if forwarders not available
forwarders {
    1.1.1.1;
    8.8.8.8;
};
```

Configure for only IPv4. Change the second IP (a.b.c.d) to the IP address of your pi.

```
listen-on port 53 { 127.0.0.1; a.b.c.d; };
listen-on-v6 { none; };
```

Other configuration:

```
auth-nxdomain no;    # conform to RFC1035 – yes/no answer authoritative if NXDOMAIN
allow-transfer { none; };      # Do not transfer the zone information to the secondary DNS
```

named.conf.local

```
sudo vim /etc/bind/named.conf.local
```

Declare the zones associated with this server’s domain(s). Replace domain(s) and IP address(es) as appropriate for your setup:

```
### Forward zones
zone "homelab.local" {
     type master;
     file "/etc/bind/zones/homelab.zone";
     allow-update { none; };   # no DDNS by default
};

### Reverse Zones
#a.b.c.0/24 subnet
zone "c.b.a.in-addr.arpa" {
     type master;
     file "/etc/bind/zones/a.b.c.zone";
     allow-update {none;};          # no DDNS by default
};
```

Configure zones

Create the zone files

```
cd /etc/bind
sudo mkdir ./zones
sudo cp db.local ./zones/homelab.zone
sudo cp db.127 ./zones/a.b.c.zone
cd zones
```

Does it work?

Check your work. Is it ok?

```
named-checkzone homelab.local homelab.zone
named-checkzone c.b.a.in-addr.arpa a.b.c.zone
```

Restart the service. Ensure it is still running properly.

```
sudo systemctl restart named
systemctl status named
```

Now what happens with the following commands:

```
nslookup <hostname>
nslookup <hostname> 127.0.0.1
nslookup <hostname>.homelab.local 127.0.0.1
dig @127.0.0.1 <hostname>.homelab.local
```

Configure zones

Replace domain(s) and IP address(s) as appropriate:

```
;
; BIND data file for homelab.local
;
$TTL 604800
@    IN   SOA  druid.homelab.local. admin.homelab.local. (
                2025093000         ; Serial
                604800       ; Refresh
                86400        ; Retry
                2419200      ; Expire
                604800 )           ; Negative Cache TTL
;
; name servers - NS records
     IN   NS   druid.homelab.local.

$ORIGIN homelab.local.

; name servers -A records
druidIN   A    a.b.c.d

; a.b.c.0/24
paladin   IN   A    a.b.c.e
```

(Note: The serial chosen is the date plus a two digit integer YYYYMMDDxx. The serial needs to be incremented by at least 1 every time a change to dns is made. Any integer could work.)

(Note: $ORIGIN defines a base name from which ‘unqualified’ names (those without a terminating dot) substitutions are made when processing the zone file, (paladin -> paladin.homelab.local).)

Configure zones

Replace domain(s) and IP address(s) as appropriate:

```
;
; BIND reverse data file for c.b.a.in-addr.arpa
;
$TTL 604800
@    IN   SOA  druid.homelab.local. admin.homelab.local. (
                2025093000         ; Serial
                604800       ; Refresh
                86400        ; Retry
                2419200      ; Expire
                604800 )           ; Negative Cache TTL
;
; name servers - NS records
     IN   NS   druid.homelab.local.

$ORIGIN c.b.a.in-addr.arpa.

; Name Servers - PTR Records
d    IN   PTR  druid.homelab.local.

; PTR Records
e    IN   PTR  paladin.homelab.local.
```

Check Current DNS Server

```
cat /etc/resolv.conf
```

(Note: Do not overlook the lack of e in reolsve.conf. Use tab complete.)

(Note: Additonally note the Generated by line at the top of the file)

Setting different DNS Server:

Use NetworkManger to modify the DNS server:

```
nmcli
nmcli connection show
```

Note the "name" of the connection you are using not the "device"

```
nmcli con mod "<connection-name>" ipv4.dns "<space-separated-dns-ips>"
nmcli con mod "<connection-name>" ipv4.ignore-auto-dns yes
nmcli con down "<connection-name>" && nmcli con up "<connection-name>"
nmcli
```

(Optional) Set a search domain

```
nmcli con mod "<connection-name>" ipv4.dns-search "<domain>"
```

Does It Work Now?

Now what happens with the following commands:

```
nslookup <hostname>
nslookup <hostname>.homelab.local
dig <hostname>
dig <hostname>.homelab.local
```

General Reminders

Increment the serial each time you make changes!

Check your work:

```
named-checkconf
named-checkzone <zonename> <filename>
```

e.g.

```
named-checkzone homelab.local  homelab.zone
named-checkzone c.b.a.in-addr.arpa  a.b.c.zone
```

Trouble Shooting

Check connection to port 53:

```
telnet    <remote-server> 53

nc -vz -w 1 <remote-server> 53
nc -vuz -w 1 <remote-server> 53

sudo netstat -tulpn | grep :53
sudo lsof -Pi | grep LISTEN
sudo nmap -sS localhost
sudo nmap -sU localhost
```

Check your firewalls and ensure port 53 is allowed (e.g. iptables, nftable, firewalld, ufw)

Check named service:

```
systemctl status named
sudo journalctl -u named
```