Module: Domain Name Services (DNS)

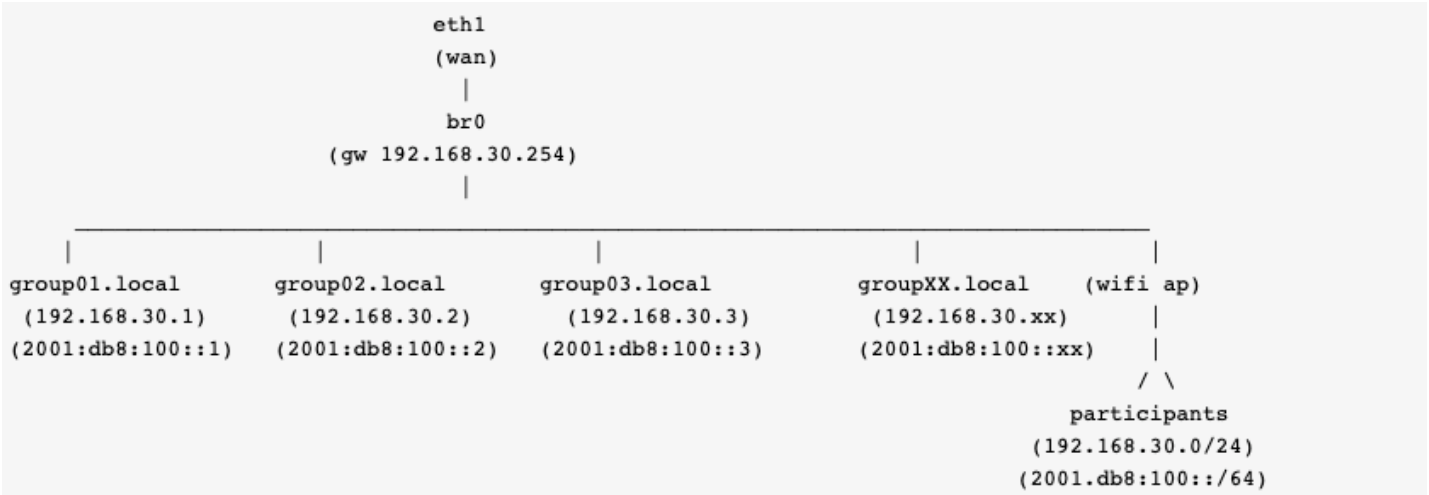
Lab Exercise – BIND Installation

Objective: Understand the concept of Domain Name System, particularly installation and setup of BIND DNS.

Background: For this lab, we will be using BIND, a free/open-source DNS application. Bind is the complete DNS software, which can be used as an authoritative or caching server or both. It is currently the most widely used DNS application on the Internet and is maintained by the Internet Systems Consortium (ISC). The current version as of writing is BIND 9.12.3-P1.

Topology

The following will be the topology used for this lab. Note that the IP addresses are examples only. When working on the lab, use the actual IP addresses as indicated by the instructors. For the purpose of this guide, the IP address of `192.168.30.X` or `2001:db8:100::X` will refer to your Virtual Machine (VM).



Lab Notes

- Confirm interface name:
    - On the VM, check the IP configuration to see the interface Name

```
ifconfig
OR
ip route show | grep " src " | cut -d " " -f 3,12
```

  - In this guide the interface name is `eth0`. Depending on the version of Ubuntu the interface name may be `enp0s3` or something different. Where `eth0` is used in this guide replace it with your interface name.

- Virtual Machine (Container) details
  - Ubuntu 16.04 LTS/LXC
  - Hostname = `groupXX.apnictraining.net`
  - Domain name = `apnictraining.net`
  - IPv4 Address = `192.168.30.xx`
  - IPv6 Address = `2001:db8:100::xx`
  - `xx` = group ID as allocated by the instructor

What You Need

- DNS Bind:
  - Current version for download from ISC is BIND 9.12.3-P1
    - Download from `http://ftp.isc.org/isc/bind9/9.12.3-P1/bind-9.12.3-P1.tar.gz`
  - Current version for installation from Ubuntu repo BIND 9.10.3-P4
- OpenSSL
  - Current version for download from OpenSSL is OpenSSL 1.1.1a
    - Download from `https://www.openssl.org/source/openssl-1.1.1a.tar.gz`
  - Current version for installation from Ubuntu repo OpenSSL 1.0.2g.
- Operating System (preferred): Linux
- Optional Software: Unbound, NSD, PowerDNS

Steps:

A. Access to the servers

1. Login to your assigned VMs (server) using a remote access tool (Terminal for Linux/Mac platform, or SSH software such as PuTTY for Windows).

```
ssh apnic@192.168.30.1 (for group01)
password: training
```

2. Add a static IPv6 Address to the `eth0` interface. First backup the `/etc/network/interfaces` file.

   ```
   sudo cp /etc/network/interfaces /etc/network/interfaces.bak
   ```

   Add the static IPv6 address details to the end of the `/etc/network/interfaces` file. Below example assigns group01 IPv6 address details:

   ```
   sudo -i
   cat >> /etc/network/interfaces <<EOL

   ### IPV6 static configuration
   iface eth0 inet6 static
   address 2001:db8:100::1
   netmask 64
   EOL
   ```

   Restart the networking services.

   ```
   sudo service networking restart
   ```

   Test connectivity with the `eth0` IPv6 address.

   ```
   ping6 2001:db8:100::1
   ```

B. Installing BIND

1. OpenSSL is required in some features of DNS such as DNSSEC. So we will first install this. (Note: OpenSSL may already be installed on the system. Here we will use the SSL version 1.0.2g from the Ubuntu Repo).

   ```
   sudo apt-get update
   sudo apt-get install -y openssl
   ```

   Confirm the version of OpenSSL

   ```
   openssl version -a
   ```

   The default location for OpenSSL is at `/usr/lib/ssl`. Check that you have this folder.

   ```
   ls -lah /usr/lib/ssl
   ```

2. To install via a package manager type the following command:

```
sudo apt-get install -y bind9 bind9utils dnsutils
```

The default location of the installation files are as follows:

```
/etc/bind for system configuration (named.conf)
/usr/local/sbin for system binaries (named, RNDC, DNSSEC)
/usr/local/bin for local/user binaries (dig, host, nslookup, nsupdate
```

The default location for BIND is at `/etc/bind`. Check that you have this folder.

```
ls -lah /etc/bind
```

3. Confirm which version of BIND is installed

```
named -v
```

Lab Exercise – Authoritative DNS Servers

Objectives

Participants should be able to configure primary and secondary name server for a given domain name and do a zone transfer between them. This should include creating, modifying, deleting RRs and incrementing Primary name server serial number. Each participant name servers should be visible from other name servers since we will use the lab root and GTLD server. A custom lab root hint will be used.

Note: Configure your VM to be the primary (also called master) of your own domain and also a slave for your partner's domain.

Steps:

1. Register your domain name and its name server's FQDN (master & slave) together with their IP addresses to the domain name registry. In our lab you should approach the instructor for registration. Instructor will also act as a GTLD server for this exercise. He will be creating the delegation of .net subdomains to every VM in the lab.

2. Edit the `named.conf.options` file to modify options.

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

To make the nameserver as an authoritative only server, change the `dnssec-validation` option

as a comment, and add `recursion no;` as follows:

3. Create a new working directory for your master server under `/var/named`

```
sudo mkdir -p /var/named/master
```

4. Create a zone file for your domain under `/var/named/master` and add necessary resource records like NS record, A record, txt record, MX record that will determine which host is receiving mail for the domain.

```
sudo vi /var/named/master/db.groupXX.net
```

For example, if you have `groupXX.net` as your domain, you must create `db.groupXX.net`, with the following base contents (sample configuration):

```
$TTL 1d
@   IN  SOA     ns.groupXX.net. email.groupXX.net.   (
          2019021901 ;serial no.
          30m        ;refresh
          15m        ;retry
          1d         ;expire
          30m        ;negative cache ttl
        )
@       IN  NS   ns.groupXX.net.
ns      IN  A   192.168.30.XX
www     IN  A   192.168.30.XX
mail    IN  A   192.168.30.XX
ns      IN  AAAA    2001:db8:100::XX
www     IN  AAAA    2001:db8:100::XX
mail    IN  AAAA    2001:db8:100::XX
groupXX.net.    MX 10   mail.groupXX.net.
groupXX.net.    IN  TXT "groupXX Authoritative DNS Server"
```

5. Modify the configuration file `/var/named/named.conf`. Please note that the primary zone is of "type master" while a secondary zone is of "type slave.” Specify your nameserver’s working directory.

```
options {
   directory "/var/named";
};

zone "groupXX.net" {
    type master;
    file "master/db.groupXX.net";
};
```

Most authoritative servers are also recursive/caching servers for their own networks. If this is the case,

also add the following zones.

```
zone "." {
    type hint;
    file "root.hints";
};

zone "localhost" {
    type master;
    file "db.localhost" ;
};
```

The `root.hints` & `db.localhost` should already be in the `/var/named` folder.

Test the changes to the configuration files, by typing in:

```
cd /var/named/master
named-checkzone groupXX.net db.groupXX.net
```

6. In `/var/named/` run bind and see if it's running properly. Error messages will give you hints where the error is.

   ```
   named -g -c named.conf
   ```

   Note This will start bind using the named.conf file.

   - "-g" to get bind to show message and run in the foreground
   - "-c" to tell bind what configuration file to use.

7. Once BIND is running, you can do some basic test using DNS tools like `dig`. Open another terminal session.

   To test your name server to display the SOA records for your domain.

   ```
   dig @192.168.30.XX groupXX.net SOA
   ```

   To test your name server to display NS records

   ```
   dig @192.168.30.XX groupXX.net NS
   ```

   To test your name server to display other resource records (A, AAAA, or MX). You can also use the -t option to set the query type.

```
dig @192.168.30.XX ns.groupXX.net A
dig @192.168.30.XX mail.groupXX.net AAAA
dig -t MX @192.168.30.XX groupXX.net
```

8. Update network settings to use the local dns server for name resolution.

   ```
   sudo vi /etc/network/interfaces
   ```

   Modify the line starting with `dns-nameservers` to look like the following:

   ```
   dns-nameservers 127.0.0.1 192.168.30.249 192.168.30.250
   ```

   Restart networking services

   ```
   sudo service networking restart
   ```

9. Test connectivity with different Fully Qualified Domain Names (FQDNs)

   ```
   ping6 mail.groupXX.net
   ping6 www.groupXX.net
   ping www.groupXX.net
   ```