Lab 3: DNS

Objective:

To help students understand how DNS works and setup a Domain Name Server.

Example Scenario:
- Domain name: **coyoteone.net**
- IP Address Range: **192.168.1.0/24**
- Servers:
  Firewall (hadrian.coyoteone.net) : 192.168.1.1
  DHCP server (dhcp.coyoteone.net) : 192.168.1.1
  DNS server (ns.coyoteone.net) : 192.168.1.1

Prerequisite: Please change all the hostname and domain name as following:
On Hadrian: localhost -> hadrian.coyoteone.net

Name Table for your network:

NO	Hostname	Domain Name	IP Address
1			
2			
3			
4			
5			
6			
.			
N			

[1] Installation: (on hadrian)

    1-1 Required packages:
- **bind**
- **bind-utils**
- **bind-libs**

    1-2 Configuration files:
        /etc/named.conf
        /var/named/named. coyoteone.net.hosts
        /var/named/named.rev.coyoteone.net.hosts
    1-3 Installation:

    [root@ns /root]# **yum –y install bind bind-utils bind-libs**

[2] Configuration:

```
[root@ns /root]# cp -aprv /usr/share/doc/bind-9.3.6/sample/etc/*     /etc/
[root@ns /root]# cp -aprv /usr/share/doc/bind-9.3.6/sample/var/named/*    /var/named/
```

Edit: /etc/named.conf
```
options
{
      query-source    port 53;
      directory "/var/named"; // the default
      dump-file            "data/cache_dump.db";
      statistics-file      "data/named_stats.txt";
      memstatistics-file     "data/named_mem_stats.txt";
};

logging
{
      channel default_debug {
           file "data/named.run";
           severity dynamic;
      };
};

key ddns_key
{
      algorithm hmac-md5;

      #use /usr/sbin/dns-keygen to generate TSIG keys  DO NOT TYPE FOLLOWING LINE
      secret  "eDMHhnGja0gsnlBXVmIPnb1RLWksR2mDpYnEwKMu0JdkFP4uA2JEktZgSTSK";
};

view   "external"
{
      match-clients              {any;};
      match-destinations         {any;};
      recursion                  no;
      allow-query-cache          {none;};
      include "/etc/named.root.hints";

      zone "coyoteone.net" {
           type master;
           file "named.coyoteone.net.hosts";
      };

      zone "1.168.192.in-addr.arpa" {
           type master;
           file "named.rev.coyoteone.net.hosts";
      };
};
```

Edit: /var/named/named.coyoteone.net.hosts

```
$TTL   86400
@              IN SOA  192.168.1.2            ns.coyoteone.net. (
                       2012041601            ; serial
                       3H                    ; refresh
                       15M                   ; retry
                       1W                    ; expire
                       1D )                  ; minimum
coyoteone.net.          IN       NS       ns.coyoteone.net.
hadrian        IN A                192.168.1.1
```

Edit: /var/named/named.rev.coyoteone.net.hosts

```
$TTL   86400
@     IN    SOA    localhost.      root.localhost. (
                   2012041601  ; Serial
                   28800       ; Refresh
                   14400       ; Retry
                   3600000     ; Expire
                   86400 )     ; Minimum
@     IN    NS     localhost.
1                  IN      PTR     hadrian.coyoteone.net.
```

[3] Firewall / SELinux Settings
[root@ns ~]# **setup**
Select "Firewall Configuration" and Select "Disabled" on SELinux Section

```
---------------------- Firewall Configuration -------------------------
|                                                                     |
|    A firewall protects against unauthorized                         |
|    network intrusions. Enabling a firewall blocks                   |
|    all incoming connections. Disabling a firewall                   |
|    allows all connections and is not recommended.                   |
|                                                                     |
|  Security Level: (*) Enabled ( ) Disabled                           |
|                                                                     |
|        SELinux:            Enforcing                                |
|                           Permissive                                |
|                           Disabled                                  |
|                                                                     |
|    ------        ---------------      -----------                   |
|    | OK |        | Customize |        | Cancel |                    |
|    ------        ---------------      -----------                   |
|                                                                     |
-----------------------------------------------------------------------
```

[4] Start the services:
Start DNS:
[root@ns /root]# **service named restart**
Start DNS on boot time:
[root@ns /root]# **chkconfig named on**

[5] Set your DNS client:
Edit /etc/resolv.conf
[root@ns /root]# **vi /etc/resolv.conf**

```
search coyoteone.net
nameserver    192.168.1.2
```

[6] Testing

Check startup log:
[root@ns ~]# **tail /var/log/messages**

```
Feb  7 03:45:29 ns named[21116]: starting BIND 9.3.3rc2 -u named
Feb  7 03:45:29 ns named[21116]: found 1 CPU, using 1 worker thread
Feb  7 03:45:29 ns named[21116]: loading configuration from '/etc/named.conf'
Feb  7 03:45:29 ns named[21116]: listening on IPv4 interface lo, 127.0.0.1#53
Feb  7 03:45:29 ns named[21116]: listening on IPv4 interface eth0, 192.168.1.1#53
Feb  7 03:45:29 ns named[21116]: command channel listening on 127.0.0.1#953
Feb  7 03:45:29 ns named[21116]: command channel listening on ::1#953
Feb  7 03:45:29 ns named[21116]: zone 1.168.192.in-addr.arpa/IN/external: loaded serial 2008041601
Feb  7 03:45:29 ns named[21116]: zone coyoteone.net/IN/external: loaded serial 2008041602
Feb  7 03:45:29 ns named[21116]: running
Feb  7 03:45:29 ns named[21116]: zone coyoteone.net/IN/external: sending notifies (serial 2012041601)
Feb  7 03:45:30 ns named[21116]: client 192.168.1.1#1092: view external: received notify for zone 'coyoteone.net'
```

Forward lookup test:
[root@ns ~]# **nslookup ns.coyoteone.net**
Server: 192.168.1.1
Address: 192.168.1.2#53

Name: ns.coyoteone.net
Address: 192.168.1.1

Reverse lookup test:
[root@ns ~]# **nslookup 192.168.1.2**
Server: 192.168.1.1
Address: 192.168.1.1#53

1.1.168.192.in-addr.arpa   name = ns.coyoteone.net.

Reload DNS databases:

[root@ns ~]# **service named reload**

Lab 3 Report:

Design your network and update your DNS.

[1] Name Table for your network:

NO	Hostname	Domain Name	IP Address
1			
2			
3			
4			
5			
6			
.			
N			

[2] /etc/named.conf file

[3] Forward lookup database file in /var/named/

[4] Reverse lookup database file in /var/named/

[5] Step by step installation procedure and what was your difficulties.