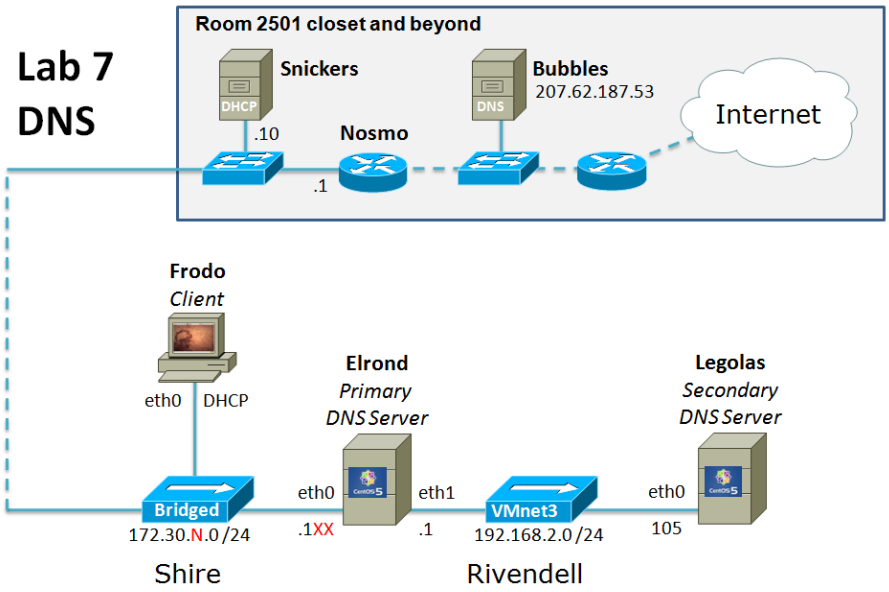
Lab 7: Domain Name System

The purpose of this lab is to configure a server as a primary DNS name server for a particular zone, a secondary name server for redundancy, then observe a zone transfer. Please read over the entire lab before proceeding with the individual steps to obtain an overview of what you are trying to accomplish.



.1XX is based on your station number and the IP Table in the Appendix
N=1 for the classroom and N=4 for the CIS lab or CTC

Supplies

- VMWare Server 1.08 or higher
- 192 VMs shown above

Preconfiguration

- Original versions of all VMs. Note, this will set the network configurations back to down or DHCP settings.

- You will need access to a DHCP server to assign addresses for the 172.30.N.0/24 network. This is already configured if the lab is done using the CIS VMware Stations in the CIS Lab (room 2504) or the CTC. If you plan to do this lab at home see: http://simms-teach.com/howtos/202-working-at-home-nat.pdf

Forum

Use the forum to ask and answer questions, collaborate, and report any equipment issues. Post tips and any lessons learned when you have finished. Forum is at: http://opus.cabrillo.edu/forum/viewforum.php?f=5

Background

The Domain Name System (DNS) is what makes life a lot easier for humans using networks. Without DNS servers, one would have to either remember the IP addresses for every host and website or attempt to keep millions of /etc/hosts file synchronized and updated. A DNS server is responsible for taking a name like **www.hp.com** or **opus.cabrillo.edu** and resolving them to the correct IP addresses. A DNS server can be responsible for the names in it's own domain and communicate with other DNS servers for other domains.

The commands we will be using for this lab are:

- named
- named-checkconf
- rndc
- host
- dig

- yum
- dhclient
- ping
- setenforce
- getenforce
- setsebool

The configuration of the **named** daemon will require root access.

Procedure

When you join Elrond to the 172.30.N.0 network, it has access to a remote DNS server, but a remote DNS server will not resolve the names local to our private subnets.

There are several mechanisms for resolving host names into IP addresses; the /etc/hosts file is just one of them. In this lab you will configure the Domain Naming Service (DNS) to perform this function.

Setup

1. Revert Elrond, Legolas and Frodo to their snapshots and power on.
2. Install the DNS service packages on both Elrond and Legolas:
    a. Cable their eth0 interfaces to the Bridged "hub"
    b. Use **dhclient eth0** to get an IP address using DHCP.

c. Install the DNS server and caching packages. Note, BIND stands for Berkeley Internet Name Domain and the DNS server daemon is called "named".
yum install bind caching-nameserver
d. Use **dhclient –r** to release their DHCP IP addresses.

3. Cable Elrond, Legolas and Frodo as shown in the map above.

Part 1

Configure the NIC's on Elrond and Legolas according to the diagram above. Use the two primary methods of name resolution (DNS server and the /etc/hosts file) to ping Legolas and google.com.

1. Log in to Elrond as root.
2. Configure Elrond to join the Shire and Rivendell networks as shown above:
   - Configure static IP addresses on eth0 and eth1
   - Configure the default gateway to 172.30.N.1
   - Configure the DNS server to be 207.62.187.53
   - Enable packet forwarding
   - Verify Elrond has Internet access
3. Verify that the necessary software was installed:
   rpm -qi bind
   rpm -qi caching-nameserver
   You should be running version 9 of the Berkeley Internet Name Domain (BIND) services.
4. Currently, what server is configured as your primary name server? (hint: check the /etc/resolv.conf file). Yes, this is the Cabrillo DNS server we configured above. Ping this name server's IP address. Is it reachable by you? If you are successful, you currently have access to a name server, otherwise you are depending on the **/etc/hosts** file for name resolution.
5. Configure Legolas to join the Rivendell network.
6. On Elrond, try pinging Legolas by it's name (**ping Legolas**). Does it work? It shouldn't because the Cabrillo name server knows nothing about the Rivendell network and there is no entry for Legolas in /etc/hosts.
7. Try it again after adding the line:
   `192.168.2.105 legolas`
   to the end of /etc/hosts. It should work now.
8. Now **ping google.com**. It should work because the Cabrillo DNS server is quite capable of resolving the name google.com to an IP address. **Note the IP address** in the ping output.
9. Remove the DNS server configuration:
   > /etc/resolv.conf
   and try pinging google.com again. It should fail now.
10. Add another entry to /etc/hosts using the IP address of the previous successful ping to google.com:
    `xxx.xxx.xxx.xxx google.com`
    and try again. It should work again now.
11. Currently, the /etc/hosts file is searched for name resolution before DNS. Since we want to test DNS, we must indicate to the system that we wish to use DNS before the /etc/hosts file to resolve host names to IP addresses. To do this, you must edit the **/etc/nsswitch.conf** file:
    Change the line: `hosts files dns`
    to read: `hosts dns files`

12. OK, edit /etc/hosts and remove the entries for legolas and google.com. We are going to make our own DNS server for Rivendell.

Part 2

We will now configure our own server to be the primary name server, and start up the DNS "named" service. You will need the caching-nameserver package that contains the configuration files for a name server.

1. Verify that the caching-nameserver package is installed:
   rpm -qa | grep caching
2. Edit the /etc/resolv.conf file to indicate yourself (127.0.0.1) as the primary name server, with "rivendell" as the domain. This file should consist of the following two lines:
   ```
   search rivendell
   nameserver 127.0.0.1
   ```
   What does the search line do? The search string is appended to names being resolved. In this case, if the user tries to look up arwen, then arwen.rivendell is tried first, then just arwen.
3. The main configuration file for the BIND DNS server implementation is the named.conf file in the /etc directory. Rather than create it from scratch, use the starter version in the Appendix.
4. Insure the permissions on this /etc/named.conf will allow named to read it.
5. Now insert the following two zones above the last line of the file:

   ```
   zone "rivendell" IN {
           type master;
           file "db.rivendell";
           allow-update { none; };
   };

   zone "2.168.192.in-addr.arpa" IN {
           type master;
           file "db.2.168.192";
           allow-update { none; };
   };
   ```

   Pay close attention to the semicolons and quote marks in this file!
   To check the syntax of this file, you can run the command:
   named-checkconf
   If there is no output from this command, the syntax is probably ok.
6. You have just declared your forward and reverse lookup zones to your DNS daemon (named), that is, when you launch it.
7. The next task is to create these two zone files. They need to reside in the directory specified at the top of your /etc/named.conf file - in the options section. What directory is that?
8. Change directory to /var/named and create the two zone database files, db.rivendell and db.2.168.192. There are starter files in the Appendix you may use for this.
9. Make sure the permissions on these files will allow named to read them.
10. Look at these files and note the small size of the domain we are covering. Notice that "Rivendell" is a top-level domain, but clearly is not registered with the DNS "root" servers listed in named.ca.
11. Edit these two files to supply the IP numbers and names appropriate to the station.

12. Modify the firewall to allow incoming DNS queries (UDP port 53), zone file transfers (TCP port 53) and allow unrestricted forwarding of DNS queries from Rivendell hosts to the Internet. In addition turn on NAT service so Rivendell hosts have Internet access:

    iptables -I RH-Firewall-1-INPUT 6 -p udp -m udp --dport 53 -j ACCEPT
    iptables -I RH-Firewall-1-INPUT 6 -s 192.168.2.0/24 -p tcp -m tcp --dport 53 -j ACCEPT
    iptables -D FORWARD 1
    iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
13. Set SELinux to Enforcing mode with **setenforce enforcing** command.
14. Use **getenforce** to verify SELinux mode
15. Now start the DNS name daemon, named, with:
    service named start
16. Check to make sure the named daemon is running using the command:
    service named status
    if it's not running, check your named.conf file for syntax errors.

Part 3

You are now ready to test your DNS service. We will use the host command, which uses DNS only for name resolution. If you want to use a regular client like ping, and you want to be absolutely sure name resolution is not happening via the */etc/hosts* file, then comment out all entries except for your loopback address from the hosts file.

Use the host command to test your DNS. Try the following commands:

host legolas.rivendell.
host legolas.rivendell
host legolas
host Elrond
host ELROND
host fang
host 192.168.2.105
host 192.168.2.200
host www.domain.foo
host opus.cabrillo.edu
host www.yahoo.com

1. Can you explain the success or failure of these commands? Note: a system does not need to be running to look up its IP address in the DNS database files.
2. If you make a change to any of your zone files, you will have to instruct the named server to re-read those files. You can do this in one of two ways:
    1. restart the server with: **service named restart**
    2. run the rndc command: **rndc reload**

    Of these two ways, the latter is the better, especially since the named service script doesn't work on older RedHat versions of Linux.

Part 4

Now let's create a secondary name server to relieve the load on the server we just configured.

1. Log on to Legolas as root.
2. Edit the */etc/hosts* file, removing all lines except for the loopback address.

3. Edit the */etc/resolv.conf* to specify the nameserver with Legolas' IP address, and use the same search name of Rivendell.
4. Create your */etc/named.conf* file (use the starter file in the Appendix) and add the following zone information just above the last line in that file:

```
zone "rivendell" {
  type slave;
  file "db.rivendell";
  masters { ip-address of master; };
        };
```

5. Insure the permissions on /var/named allow named to create new files in that directory.
6. Before bringing up the slave server, take a look at the SOA record in the primary's zone file, db.rivendell. Note the five numeric fields in the SOA record; these are used to configure the slave server in terms of when and how often it should update its zone information from the primary server. Note that 3 hours, (10800 seconds) would be a long time to wait for a refresh. You might want to drop that number to 60 seconds.
   When you change a value in a configuration file, what has to be done to get the server to recognize it?
   ANS: Rather than restarting your Primary DNS server, you can run the following command to reload the configuration and zone files: **rndc reload**
7. Open UPD port 53 using:
   iptables -I RH-Firewall-1-INPUT 6 -p udp -m udp --dport 53 -j ACCEPT
8. Set SELinux to Enforcing mode with **setenforce enforcing** command.
9. Use **getenforce** to verify SELinux mode.
10. Modify SELinux settings to allow named to write files to /var/named with:
    setsebool -P named_write_master_zones=1
11. Now start the named daemon for the Secondary server:
    service named start
12. Use the host command to test the various hosts on the network.
13. Change directory to */var/named*, and run the ls command.
    Is the db.rivendell database file there? Display it on your screen, and note the time conversions in the SOA record. Do they look right?
14. Add an address record to the database file of your primary name server:
    galadriel IN A 192.168.2.108
    What has to be done for this change to take affect? ANS: The serial number needs to be increased and an **rndc reload** done.
15. Test this new host addition with the host command:
    host galadriel
    Test both the primary and secondary name servers.
16. What has to happen to get the secondary server to pull this new information? (ANS: You have to wait for the Refresh time interval to pass.)
    The secondary server's db.rivendell file should be updated automatically if you configured this properly. You can watch the zone transfer by looking at the log files:
    tail -f /var/log/messages
    I have noted that sometimes the refresh takes up to five minutes to happen.
17. The dig command can be used to look up information about a particular name server, and about a particular request made of that name server.
    dig @207.62.187.53 opus.cabrillo.edu
    By default, dig will lookup the nameserver specified in */etc/resolv.conf*, but you can

specify any dns server after the '@' sign. The second argument is the query you are looking up. Note the different SECTIONS in the output of the dig command.

To turn in

Your *lab07* **text** file should contain the following sections.

- Standard boilerplate information:
  - CIS 192 Lab *XX*
  - *Name*
  - *Date*
  - TBA hours*: X.X*
  - Station number: CIS-Lab-*XX*
- /etc/named.conf of your primary name server
- /etc/named.conf of your secondary name server
- a copy of the db.rivendell file from your primary name server
- a copy of the db.rivendell file from your secondary name server
- the last 10 lines of the /var/log/messages file from your secondary name server, showing the zone load and transfer
- Example command summary

The command summary should be a concise set of documented examples that can be used as a resource for repeated operations in future labs.

Check your work for completeness then submit as many times as you wish up until the due date deadline. Remember, **late work is not accepted**, so start early, plan ahead for things to go wrong and use the forum to ask questions.

[p]scp lab07 cis192@opus.cabrillo.edu:lab07.*logname*

Grading rubric (30 points)

2 points for correct submittal, professional appearance and quality
5 points for a syntactically correct named.conf file for the primary server with the zone entries as specified in the lab.
5 points for a syntactically correct named.conf file for the secondary server with modifications described in the lab.
5 points for the edited db.rivendell file from the primary server
5 points for the automatically generated db.rivendell file from the zone transfer to the secondary server.
5 points for the log file showing the load time and the zone transfer to the secondary server.
3 points for complete and concise command summary

Appendix – Static IP addresses based on station number:

http://simms-teach.com/docs/static-ip-addrs.pdf

Appendix – named.conf starter file:

```
options {
        directory "/var/named";
        /*
        * If there is a firewall between you and nameservers you want
        * to talk to, you might need to uncomment the query-source
        * directive below. Previous versions of BIND always asked
        * questions using port 53, but BIND 8.1 uses an unprivileged
        * port by default.
        */
        query-source address * port 53;
};

//
// a caching only nameserver config
//
controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

// A key file needs to be referenced for use by rndc
include "/etc/rndc.key";
```

Appendix – db.rivendell starter file

```
[root@elrond named]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2010041500      ; serial number
                60              ; refresh rate in seconds
                15              ; retry in seconds
                1209600         ; expire in seconds
                300)            ; minimum in seconds
;
;
;
;Name Server Records
Rivendell.      IN NS elrond.rivendell.

;
;Address Records
localhost       IN A 127.0.0.1
legolas         IN A 192.168.2.???
elrond          IN A 192.168.2.???
;
;CNAME records
```

Appendix – db.2.168.192 starter file

```
[root@elrond named]# cat db.2.168.192
$TTL    86400
;192.168.2.* Reverse Zone Definition
;
2.168.192.in-addr.arpa. IN SOA  elrond.rivendell. root.rivendell.  (
                                      2010041500 ; Serial
                                      60         ; Refresh
                                      15         ; Retry
                                      3600000    ; Expire
                                      86400 )    ; Minimum
;
;Name Server Records
;
2.168.192.in-addr.arpa. IN NS elrond.rivendell.
;
;Address Records
???                     IN PTR  legolas.rivendell.
???                     IN PTR  elrond.rivendell.

[root@elrond named]#
```