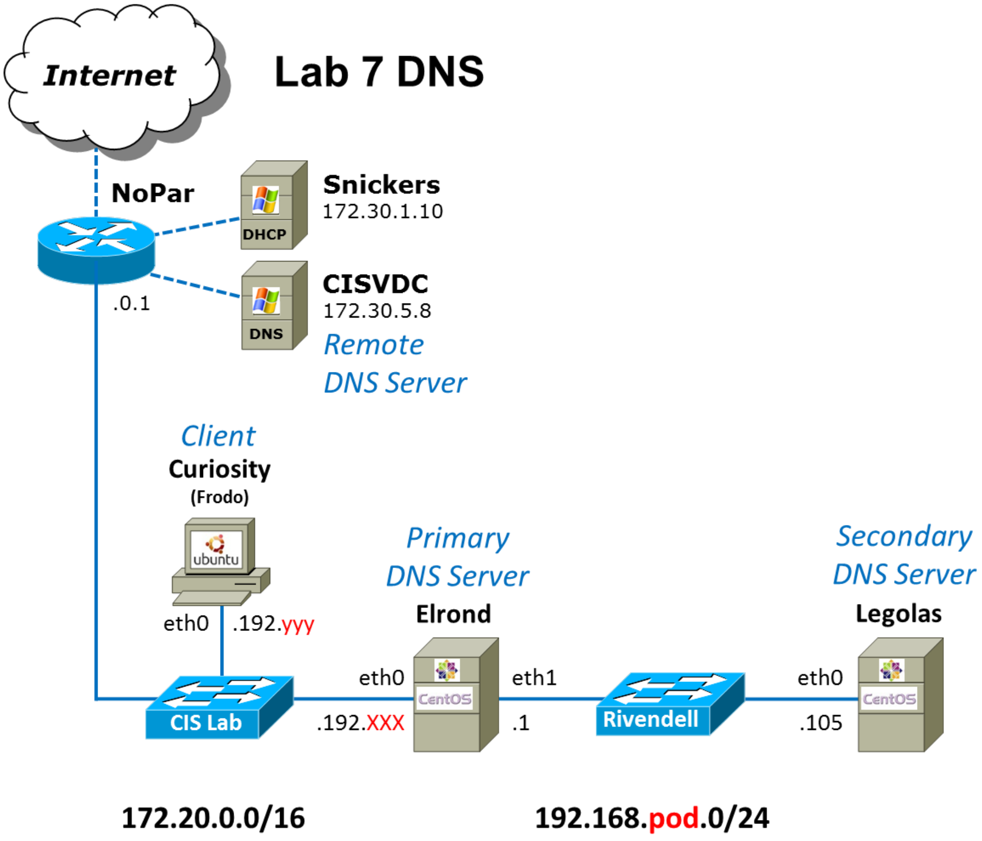
Cabrillo College

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.



xxx and yyy are for static IPs assigned to your **pod** number

Supplies

- VMware vSphere and ESXi server
- The CentOS VMs Elrond and Legolas
- The Ubuntu VM Frodo (will be renamed Curiosity)

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://oslab.cabrillo.edu/forum/

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 **oslab.cabrillo.edu** and resolving them to the correct IP addresses. A DNS server can be responsible for the names in its own domain and communicate with other DNS servers for other domains.

Procedure

When you join Elrond to the 172.20.0.0 CIS Lab network, it has access to a remote DNS server, but a remote DNS server will not resolve the names local to our private pod 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

- □ Read carefully the whole lab and make a custom network map and crib sheet of commands to use.
- □ Make a copy of the *lab07* text file in */home/cis192/depot* in your home directory on Opus.
- □ [optional] Revert VMs back to their Pristine snapshots. Starting fresh will allow you to practice the basic network setup configuration.
- □ Cable Elrond, Legolas and Curiosity (Frodo) as shown in the map above.
- □ Permanently configure on all VMs:
    - Static IP addresses on all interfaces
    - Default gateways
    - cisvdc as the name server
- □ Permanently rename pxx-frodo to be pxx-curiosity
- □ Start with default CentOS firewalls on Elrond and Legolas. If you don't have the default firewall there is a backup in */home/cis192/depot* on Opus.
- □ Permanently configure Elrond to be a gateway router.
    - Enable packet forwarding
    - Configure the default firewall to enable packet forwarding.

- Configure NAT (use SNAT) so Rivendell hosts have Internet access.

□ Disable services from previous labs if present.

Part 1

Use the two primary methods of name resolution (DNS server and the */etc/hosts* file) to ping Legolas and google.com.

□ Currently on Elrond, what server is configured as your primary name server? (hint: check the */etc/resolv.conf* file). Yes, this is the cisvdc 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.

□ On Elrond, try pinging Legolas by its name (**ping legolas**). Does it work? It shouldn't because the cisvdc name server knows nothing about the Rivendell network and there is no entry for Legolas in */etc/hosts*.

□ Try it again after adding the line:

```
192.168.pod.105 legolas
```

to the end of */etc/hosts*. It should work now.

□ Now **ping google.com**. It should work because the cisvdc server is quite capable of resolving the name google.com to an IP address. **Note the IP address** in the ping output.

□ Remove the DNS server configuration:

```
> /etc/resolv.conf
```

and try pinging google.com again. It should fail now.

□ 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.

□ 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**

□ 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.

□ Install the DNS server package on Elrond and Legolas. Note, BIND stands for Berkeley Internet Name Domain and the DNS server daemon is called “named”.

```
yum install bind
```

□ Verify that the necessary software was installed:

```
rpm -qi bind
```

You should be running version 9 or later of the Berkeley Internet Name Domain (BIND) services.

□ 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.

□ Create an RNDC key for use by the rndc tool:

```
rndc-confgen -a -r /dev/urandom
chgrp named /etc/rndc.key
chmod 640 /etc/rndc.key
```

□ 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.

□ Insure the permissions on this */etc/named.conf* will allow named to read it.

□ 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 "pod.168.192.in-addr.arpa" IN {
        type master;
        file "db.pod.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.

□ You have just declared your forward and reverse lookup zones to your DNS daemon (named), that is, when you launch it.

- □ 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?

- □ Change directory to */var/named* and create the two zone database files, *db.rivendell* and *db.pod.168.192*. There are starter files in the Appendix you may use for this.

- □ Make sure the permissions on these files will allow named to read them.

- □ 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.

- □ Edit these two files to supply the IP numbers and names appropriate to the station.

- □ Modify the firewall to allow incoming DNS queries (UDP port 53), zone file transfers (TCP port 53)

  ```
  iptables -I INPUT 4 -p udp -m udp --dport 53 -j ACCEPT
  iptables -I INPUT 4 -s 192.168.pod.0/24 -p tcp -m tcp --dport 53 -j ACCEPT
  ```

- □ Now start the DNS name daemon, named, with:

  ```
  service named start
  ```

- □ Check to make sure the named daemon is running using the command:

  ```
  service named status
  ```

  If it's not running, check */var/log/messages* for errors and re-edit your *named.conf* file for syntax errors.

- □ Configure the named service to start on boot:

  ```
  chkconfig named on
  ```

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.

- □ Install the DNS tools, like **host** and **dig**, with:

  ```
  yum install bind-utils
  ```

- □ 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.pod.105
  host 192.168.pod.200
  host www.domain.foo
  host opus.cabrillo.edu
  host www.yahoo.com
  ```

- 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.
- 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:

  Restart the server with: **service named restart**
  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.

- On Legolas, edit the */etc/hosts* file, removing all lines except for the loopback addresses (127.0.0.1 and ::1).
- Edit the */etc/resolv.conf* to specify the nameserver with Legolas' IP address, and use the same search name of Rivendell.
- 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; };
};
```

- Insure the permissions on */var/named* allow named to create new files in that directory.
- 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? ANSWER: Rather than restarting your Primary DNS server, you can run the following command to reload the configuration and zone files:

```
rndc reload
```

- Open UPD port 53 using:

```
iptables -I INPUT 4 -p udp -m udp --dport 53 -j ACCEPT
```

- Use **getenforce** to verify SELinux mode is enforcing.
- Modify SELinux settings to allow named to write files to /var/named with:

```
setsebool -P named_write_master_zones=1
```

- Create an RNDC key for use by the rndc tool:

```
rndc-confgen -a -r /dev/urandom
chgrp named /etc/rndc.key
chmod 640 /etc/rndc.key
```

□ Now start the named daemon for the Secondary server:

```
service named start
```

□ Configure the named service to start on boot:

```
chkconfig named on
```

□ Install the DNS tools, like **host** and **dig**, with:

```
yum install bind-utils
```

□ Use the **host** command to test the various hosts on the network.

□ 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?

□ Add an address record to the database file of your primary name server:

```
galadriel IN A 192.168.pod.88
```

□ What has to be done for this change to take affect? ANSWER: The serial number needs to be increased and an **rndc reload** done.

□ Test this new host addition with the host command:

```
host galadriel
```

□ Test both the primary and secondary name servers.

□ What has to happen to get the secondary server to pull this new information? (ANSWER: 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.

□ 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 @10.240.1.2 oslab.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.

- Curiosity (Frodo) */etc/network/*interfaces
- Curiosity (Frodo) */etc/hostname*
- Elrond */etc/sysconfig/iptables*
- Elrond */etc/named.conf*
- Legolas */etc/named.conf*

- Elrond */var/named/db.rivendell*
- Legolas */var/named/db.rivendell*
- Legolas */var/log/messages*, showing a complete zone transfer ("... Transfer started." to "... Transfer completed: ...")

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.

cp lab07 ~rsimms/turnin/cis192/lab07.$LOGNAME
email map/crib sheets to: **risimms@cabrillo.edu**

Grading rubric (30 points)

3 points for a complete header in your lab report
3 points for a network map/crib sheet
3 points for a correctly configured */etc/network/interfaces* on Curiosity
3 points for a correctly configured */etc/hostname* on Curiosity
3 points for a correctly configured firewall on Elrond
3 points for a correct *named.conf* file for the primary server
3 points for a correct *named.conf* file for the secondary server
3 points for the edited *db.rivendell* file from the primary server
3 points for the automatically generated *db.rivendell* file from the zone transfer to the secondary server.
3 points for the log file showing a complete zone transfer to the secondary server.

Appendix

named.conf *starter file*:

```
[root@p30-elrond named]# cat /etc/named.conf
options {
        directory "/var/named";
        query-source address * port 53;
};

controls {
        inet 127.0.0.1 allow { localhost; } keys { rndc-key; };
};

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

include "/etc/named.rfc1912.zones";

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

zone "pod.168.192.in-addr.arpa" IN {
        type master;
        file "db.pod.168.192";
        allow-update { none; };
};

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

db.rivendell *starter file*:

```
[root@elrond named]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                20yymmdd00      ; serial number
                10800           ; 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.pod.???
elrond          IN A 192.168.pod.?
;
;CNAME records
```

db.pod.168.192 *starter file*

```
[root@elrond named]# cat db.pod.168.192
$TTL    86400
;192.168.pod.* Reverse Zone Definition
;
pod.168.192.in-addr.arpa. IN SOA  elrond.rivendell. root.rivendell.  (
                                      20yymmdd00 ; Serial
                                      10800      ; Refresh
                                      15         ; Retry
                                      3600000    ; Expire
                                      86400 )    ; Minimum
;
;Name Server Records
;
pod.168.192.in-addr.arpa. IN NS elrond.rivendell.
;
;Address Records
???                     IN PTR  legolas.rivendell.
?                       IN PTR  elrond.rivendell.
```

Pod 30 Reference Implementation

Curiosity

```
cis192@p30-curiosity:~$ cat /etc/issue
Ubuntu 12.04.1 LTS \n \l

cis192@p30-curiosity:~$

cis192@p30-curiosity:~$ cat /etc/network/interfaces
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 172.20.192.210
netmask 255.255.0.0

gateway 172.20.0.1

dns-search cislab.net
dns-nameservers 172.30.5.8
cis192@p30-curiosity:~$

cis192@p30-curiosity:~$ cat /etc/hostname
p30-curiosity
cis192@p30-curiosity:~$

cis192@p30-curiosity:~$ cat /etc/init/network-manager.conf
# network-manager - network connection manager
#
# The Network Manager daemon manages the system's network connections,
# automatically switching between the best available.

description     "network connection manager"

#start on (local-filesystems
#         and started dbus
#         and static-network-up)
stop on stopping dbus

expect fork
respawn

script
        # set $LANG so that messages appearing on the GUI will be translated.
See LP: 875017
        if [ -r /etc/default/locale ]; then
                . /etc/default/locale
                export LANG LANGUAGE LC_MESSAGES LC_ALL
        fi

        exec NetworkManager
end script
cis192@p30-curiosity:~$
```

Elrond

```
[cis192@p30-elrond ~]$ cat /etc/issue
CentOS release 6.3 (Final)
Kernel \r on an \m

[cis192@p30-elrond ~]$ rpm -qa | grep bind
rpcbind-0.2.0-9.el6.x86_64
bind-libs-9.8.2-0.17.rc1.el6_4.4.x86_64
bind-utils-9.8.2-0.17.rc1.el6_4.4.x86_64
bind-9.8.2-0.17.rc1.el6_4.4.x86_64
[cis192@p30-elrond ~]$

[root@p30-elrond ~]# ls -ld /var/named/ /var/named/db*
drwxr-x---. 5 root named 4096 Apr 14 08:34 /var/named/
-rw-r-----. 1 root named  610 Apr 13 22:15 /var/named/db.30.168.192
-rw-r-----. 1 root named  608 Apr 14 08:34 /var/named/db.rivendell
[root@p30-elrond ~]#

[root@p30-elrond ~]# ls -l /etc/named.conf  /etc/rndc.key
-rw-r-----. 1 root named 574 Apr 13 22:49 /etc/named.conf
-rw-r-----. 1 root named  77 Apr 13 22:24 /etc/rndc.key
[root@p30-elrond ~]#

[root@p30-elrond ~]# chkconfig --list named
named           0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@p30-elrond ~]#


[root@p30-elrond ~]# head /etc/sysconfig/network-scripts/ifcfg-eth[01]
==> /etc/sysconfig/network-scripts/ifcfg-eth0 <==
DEVICE="eth0"
BOOTPROTO="static"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Ethernet"
IPADDR=172.20.192.211
NETMASK=255.255.0.0

==> /etc/sysconfig/network-scripts/ifcfg-eth1 <==
DEVICE="eth1"
BOOTPROTO="static"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Ethernet"
IPADDR=192.168.30.1
NETMASK=255.255.255.0
[root@p30-elrond ~]#

[root@p30-elrond ~]# head /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=p30-elrond.rivendell
GATEWAY=172.20.0.1
[root@p30-elrond ~]#

[root@p30-elrond ~]# head /etc/resolv.conf
search Rivendell
```

```
nameserver 127.0.0.1
[root@p30-elrond ~]#


[root@p30-elrond ~]# cat /etc/sysctl.conf | grep forward
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
[root@p30-elrond ~]#

[root@p30-elrond ~]# cat /etc/nsswitch.conf | grep hosts
#hosts:     db files nisplus nis dns
hosts:      dns files
[root@p30-elrond ~]#

[root@p30-elrond ~]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Sun Apr 14 00:20:28 2013
*nat
:PREROUTING ACCEPT [1860:262088]
:POSTROUTING ACCEPT [58:3698]
:OUTPUT ACCEPT [276:18920]
-A POSTROUTING -o eth0 -j SNAT --to-source 172.20.192.211
COMMIT
# Completed on Sun Apr 14 00:20:28 2013
# Generated by iptables-save v1.4.7 on Sun Apr 14 00:20:28 2013
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [240:207999]
:OUTPUT ACCEPT [22181:10557219]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -s 192.168.30.0/24 -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Sun Apr 14 00:20:28 2013
[root@p30-elrond ~]#

[root@p30-elrond ~]# cat /etc/named.conf
options {
        directory "/var/named";
        query-source address * port 53;
};

controls {
        inet 127.0.0.1 allow { localhost; } keys { rndc-key; };
};

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

include "/etc/named.rfc1912.zones";

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

zone "30.168.192.in-addr.arpa" IN {
        type master;
        file "db.30.168.192";
        allow-update { none; };
};

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

[root@p30-elrond ~]#


[root@p30-elrond ~]# cat /var/named/db.rivendell
$TTL 604800
; Rivendell Zone Definition
;
;
Rivendell.      IN SOA elrond.rivendell. root.rivendell. (
                2013041509      ; 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 192.168.30.105
elrond          IN A 192.168.30.1
galadriel       IN A 192.168.30.88

;
;CNAME records

[root@p30-elrond ~]#

[root@p30-elrond ~]# cat /var/named/db.30.168.192
$TTL    86400
;192.168.30.* Reverse Zone Definition
;
30.168.192.in-addr.arpa. IN SOA  elrond.rivendell. root.rivendell.  (
                                      2010041500 ; Serial
                                      60         ; Refresh
                                      15         ; Retry
                                      3600000    ; Expire
                                      86400 )    ; Minimum
;
```

```
;Name Server Records
;
30.168.192.in-addr.arpa. IN NS elrond.rivendell.
;
;Address Records
105                     IN PTR  legolas.rivendell.
1                       IN PTR  elrond.rivendell.

[root@p30-elrond ~]#
```

Legolas

```
[cis192@p30-legolas ~]$ cat /etc/issue
CentOS release 6.3 (Final)
Kernel \r on an \m

[cis192@p30-legolas ~]$

[cis192@p30-legolas ~]$ rpm -qa | grep bind
rpcbind-0.2.0-9.el6.x86_64
bind-9.8.2-0.17.rc1.el6_4.4.x86_64
bind-libs-9.8.2-0.17.rc1.el6_4.4.x86_64
bind-utils-9.8.2-0.17.rc1.el6_4.4.x86_64
[cis192@p30-legolas ~]$

[root@p30-legolas named]# getsebool named_write_master_zones
named_write_master_zones --> on
[root@p30-legolas named]#

[root@p30-legolas ~]# ls -l /etc/named.conf  /etc/rndc.key
-rw-r-----. 1 root named 430 Apr 13 23:01 /etc/named.conf
-rw-r-----. 1 root named  77 Apr 13 23:07 /etc/rndc.key
[root@p30-legolas ~]#

[root@p30-legolas ~]# ls -ld /var/named/ /var/named/db*
drwxrwx---. 5 root  named 4096 Apr 14 08:37 /var/named/
-rw-r--r--. 1 named named  402 Apr 14 09:11 /var/named/db.rivendell
[root@p30-legolas ~]#

[root@p30-legolas ~]# chkconfig --list named
named           0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@p30-legolas ~]#


[root@p30-legolas named]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
BOOTPROTO="static"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Ethernet"
IPADDR=192.168.30.105
NETMASK=255.255.255.0
[root@p30-legolas named]#

[root@p30-legolas named]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=p30-legolas.rivendell
GATEWAY=192.168.30.1
[root@p30-legolas named]#

[root@p30-legolas named]# cat /etc/resolv.conf
search rivendell
nameserver 127.0.0.1
[root@p30-legolas named]#

[root@p30-legolas named]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Sun Apr 14 00:50:14 2013
```

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [13934:7824133]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Sun Apr 14 00:50:15 2013
[root@p30-legolas named]#


[root@p30-legolas named]# cat /etc/named.conf
options {
        directory "/var/named";
        query-source address * port 53;
};

controls {
        inet 127.0.0.1 allow { localhost; } keys { rndc-key; };
};

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

include "/etc/named.rfc1912.zones";

zone "rivendell" {
        type slave;
        file "db.rivendell";
        masters { 192.168.30.1; };
};


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

[root@p30-legolas named]#
```