NetReg

”An automated DHCP Registration System”

Installing NetReg v1.5 HOWTO

Revision 1.51

Instructions by
Patrick M. Jaques
e-mail: pjaques@comcast.net

Last Modified on July 7, 2005

Table of Contents

Revision History

Version 1.50	June 25, 2005	- Initial release
Version 1.51	July 7, 2005	- Documentation corrections

Chapter 1. Introduction

This documentation is meant to serve as a step-by-step guide in downloading, installing and configuring a Network Registration system called NetReg on a Red Hat Linux system. Although this documentation is intended for Red Hat / Fedora Linux systems, it should work fine on other Linux distributions.

This HowTo guide only covers installing NetReg version 1.5.1 on a Linux system that has both an Apache web server and an ISC DHCP server installed as RPM packages (see ***Chapter 2. NetReg Prerequisites*****)**.

While the documentation provides a solid step-by-step instructional guide on installing NetReg, it does assume that the installer has a good understanding of Linux, DHCP, DNS Bind, Apache Webserver and TCP/IP networking.

1.1. What is NetReg?

NetReg is an automated network registration system that requires client computers that use DHCP to register their hardware (MAC) address before they can gain full network access.

1.2. How Does NetReg Work?

When a client computer running a standard DHCP client is connected to a network, it sends out a DHCP request. When a NetReg DHCP server receives this request, a lookup of the client's MAC address occurs. If the client's computer has previously registered its hardware address, it receives fully functional TCP/IP information (IP address, subnet mask, gateway address, WINS addresses, DNS server addresses, etc.), otherwise it receives an IP address within a restricted network with no, or limited access to the Internet.

How is this accomplished? The NetReg DHCP server is configured with two address pools per subnet. One pool of addresses is assigned to unregistered clients and the other pool is assigned to registered clients. The TCP/IP information passed to unregistered clients has either a non-routable IP address or an IP address that is restricted or completely blocked on your firewall, and a bogus DNS server. The bogus DNS server is designed so it resolves all names back to a Network Registration Web Server. When a user starts a web browser, the web browser connects to the NetReg server and redirects all URLs to the NetReg Registration Page. From the Registration Page, the user reads and agrees to your "Acceptable Use Policy", then enters a username/password that is authenticated against a server. If the user authenticates successfully, the computer gets registered. After the client reboots, the computer will have full access to the network and the Internet.

1.3. Why use NetReg?

DHCP is a standard protocol that automates the process of configuring network hosts by allowing hosts to obtain IP addresses and configuration parameters through the network; DHCP eliminates the need for manual configuration of hosts and manual assignments of IP addresses by network administrators. The problem with DHCP is that there is no security. Any computer can obtain access to your network through a DHCP server and for the most part is essentially anonymous. This makes tracking down malicious users more difficult.

Once a user registers their computer through NetReg's system, it links a user to a computer's hardware (MAC) address. This adds accountability to people's actions while they are connected to your network.

1.4. Potential pitfalls to NetReg.

Some clients may learn about your network configuration through others and manually configure their computer so they can bypass the NetReg system.

- Manually assigning DNS servers
- Manually assigning IP Addresses
- Manually assigning a Default gateway

So, what can you do?

- Look at your switches/router's bridge and/or IP ARP tables and compare them to NetReg's registered hardware (MAC) addresses. This will tell you if you have any rogue users that are statically assigning IP addresses and bypassing your NetReg System. You can accomplish this by scheduling a perl script that uses "Net::SNMP" to periodically check your switches/routers.

  There a few users that have posted information on how they are checking for rogue users. Use the search function at www.netreg.org and search for "rogue users".

- After identifying any rogue MAC addresses from your switch/router that were not registered by NetReg, your perl script can e-mail this information to your Network Administrator or another account. You may also be able to create a rule on your firewall that bans them from the Internet.

1.5. Recommendations

- Configure NetReg so it uses HTTP connections that run over SSL. This is not covered in this HowTO guide.
- For convenience, configure NetReg so it redirects index.html to registration.html.

Chapter 2. NetReg Prerequisites

2.1. Hardware Recommendations and Software Requirements

- Dedicated PC

  Minimum: Pentium 200MHz, 4GB HD, 32MB RAM, 10/100 Ethernet Adapter

  Recommended: P4 2.0GHz, 512MB RAM, 20 GB HD, 10/100 Ethernet Adapter **(or)** AMD Althon XP 2100+, 512MB RAM, 20 GB HD, Ethernet Adapter

- Red Hat Linux, Fedora and other Linux platforms
- Developer tools

  gcc, cc, make utilities

- DNS Server – (Bind 9/Chroot) RPM package

  bind
  bind-libs
  bind-chroot
  bind-utils

- Apache Web Server RPM package

  httpd

- DHCP Server RPM package

  dhcpd

- OpenSSL RPM package (**optional**)

  openssl
  openssl-devel

  Note: The openssl packages are only necessary if you plan on securing your NetReg web server connections by using an SSL connection.

- Perl 5 +
- An FTP, POP, IMAP, RADIUS or LDAP server for NetReg to authenticate against. Note that LDAP can be used to authenticate against Windows Active Directory servers.

2.2. Download required software for NetReg

2.2.1. Download the following software distributions

- Download netreg-1.5.1.tar.gz from http://www.netreg.org

2.2.2. Download the following perl modules from http://search.cpan.org

The following perl module versions have been tested with NetReg version 1.5.1 and are known to work. Newer versions may be available in the future and should work, but may have additional dependencies, so I make no claims that they will work.

- Download libnet-1.19.tar.gz (Net::FTP)
- Download Mail-POP3Client-2.16.tar.gz (Mail::POP3Client)
- Download Net-IMAP-Simple-0.101.tar.gz (Net::IMAP::Simple)
- Download Authen-SASL-2.09.tar.gz (Authen::SASL)
- Download Convert-ASN1-0.19.tar.gz (Convert::ASN1)
- Download IO-Socket-SSL-0.96.tar.gz (IO::Socket::SSL)
- Download Net_SSLeay.pm-1.25.tar.gz (Net::SSLeay)
- Download XML-NamespaceSupport-1.09.tar.gz (XML::NamespaceSupport)
- Download XML-SAX-0.12.tar.gz (XML::SAX)
- Download MIME-Base64-3.05.tar.gz (MIME::Base64)
- Download perl-ldap-0.33.tar.gz (Net::LDAP)
- Download RadiusPerl-0.12.tar.gz (Authen::Radius)

Note: If you plan on installing the above CPAN perl modules by using the CPAN method instead of compiling the CPAN source modules, then do not bother to download and unpack the source perl modules.

Example: # perl -MCPAN -e shell
cpan> install perl_module

Chapter 3. Unpack Software Distributions

If you plan on installing the CPAN perl modules using the CPAN method, then skip Chapter 3 and proceed to Chapter 4. Otherwise, unpack the following software distributions that you downloaded to /usr/local/src.

```
# cd  /usr/local/src
# tar  xvzf  libnet-1.19.tar.gz
# tar  xvzf  Mail-POP3Client-2.16.tar.gz
# tar  xvzf  Net-IMAP-Simple-0.101.tar.gz
# tar  xvzf  Authen-SASL-2.09.tar.gz
# tar  xvzf  Convert-ASN1-0.19.tar.gz
# tar  xvzf  IO-Socket-SSL-0.96.tar.gz
# tar  xvzf  MIME-Base64-3.05.tar.gz
# tar  xvzf  XML-NamespaceSupport-1.09.tar.gz
# tar  xvzf  XML-SAX-0.12.tar.gz
# tar  xvzf  Net_SSLeay.pm-1.25.tar.gz
# tar  xvzf  perl-ldap-0.31.tar.gz
# tar  xvzf  RadiusPerl-0.12.tar.gz
# tar  xvzf  netreg-1.5.1.tar.gz
```

Chapter 4. Install Software Distributions

4.1. Install CPAN Perl Modules

You only need to install the CPAN perl modules required by how you choose to authenticate your clients (POP, IMAP, FTP, LDAP, RADIUS). For example, if you plan on authenticating your NetReg clients using a POP connection, then you only need to install the CPAN module "Mail::POP3Client".

Authenication Type	Required CPAN modules
FTP	Net::FTP (libnet)
POP	Mail::POP3Client
IMAP	Net::IMAP::Simple
LDAP	Authen::SASL Convert::ASN1 IO::Socket::SSL Net::SSLeay XML::NamespaceSupport XML::SAX Net::LDAP
RADIUS	Authen::Radius

You can install the required CPAN perl modules using either the "CPAN method" or by "Compiling the CPAN perl module source".

4.1.1. Install using CPAN Method

```
# perl -MCPAN -e shell
  cpan> install perl_module
```

For example, to install the CPAN perl module needed for FTP authentication:

```
# perl -MCPAN -e shell
  cpan> install Net::FTP
```

4.1.2. Install by Compiling CPAN perl module source

Change into the directory you unpacked your CPAN perl module source. For example, to compile and install the Net:FTP (libnet) CPAN module:

```
# cd /usr/local/src/libnet-1.19
# perl Makefile.PL
# make
# make test
# make install
```

4.2. Install NetReg Software

Copy the following files you extracted from the netreg-1.5.1.tar.gz archive.

4.2.1. Copy NetReg webserver files

```
# cd  /usr/local/src/netreg-1.5.1
# cp -r  var/www  /var
```

4.2.2. Copy NetReg Perl Modules

```
# cd  /usr/local/src/netreg-1.5.1
# mkdir  -p  /usr/lib/perl5/site_perl/Net/NetReg
# cp -r  usr/lib/perl5/site_perl/Net/NetReg  /usr/lib/perl5/site_perl/Net
```

4.2.3. Copy dhcpd.conf file

```
# cd  /usr/local/src/netreg-1.5.1
# cp -f etc/dhcpd.conf  /etc
```

4.2.4. Copy named.conf & named.ca files

```
# cd  /usr/local/src/netreg-1.5.1
# cp -f  var/named/chroot/etc/named.conf  /var/named/chroot/etc
# cp -f  var/named/chroot/var/named/named.ca  /var/named/chroot/var/named
```

4.2.5. Copy refresh-dhcpdconf script

```
# cd  /usr/local/src/netreg-1.5.1
# cp -f  usr/local/bin/refresh-dhcpdconf  /usr/local/bin
```

4.2.6. Copy netreg registered client files

```
# cd  /usr/local/src/netreg-1.5.1
# cp -r  usr/local/etc/netreg  /usr/local/etc
```

4.3. Install Nessus Vulnerability Scanning Software

4.3.1. Download Nessus installer from http://www.nessus.org/download/

- Select "***Nessus 2.2.4 installer (all Unix systems)***"
- In order to activate Nessus, you will need to enter your e-mail address. You will receive an email with an activation code for Nessus.
- Download "***nessus-installer-2.2.4.sh***"

4.3.2. Run Nessus Installer

- Install dependencies needed

  ```
  # rpm  -ivh  sharutils-*.rpm  (or)
  # yum  install  sharutils
  ```

- Run Nessus installer

  # sh nessus-installer-2.2.4.sh

  Accept [/usr/local] as the default path.
  Enter the activation code [xxxx-xxxx-xxxx-xxxx-xxxx] you received by e-mail.

4.3.3. Install Nessus ScanLite module

- Install CPAN module dependencies:

  # perl -MCPAN -e shell

  cpan> install Config::IniFiles
  cpan> install Data::Dumper
  cpan> install Term::ReadKey
  cpan> install Net::Telnet
  cpan> install Net::Nessus:Client

  During the installation of Net::Nessus::Client you will be asked a series of questions. Accept the defaults.

- Install Net::Nessus::ScanLite Module

  # perl -MCPAN -e shell
  cpan> install Net::Nessus::ScanLite

4.3.4. Add 'nessusd' to your startup script

Add the command '**nessusd -D**' to /etc/rc.local init script.

4.3.5. Create a SSL cert for Nessus

Run 'nessus-mkcert' and follow the prompts in creating a SSL certificate for Nessus.

4.3.6. Create a User for Nessus

- Run 'nessus-adduser'

  Create a login user name and password for Nessus.

- Edit Variables.pm in /usr/lib/perl5/site_perl/Net/NetReg.

  a) Set the variable $NESSUS_USER to the user name you specified with 'nessus-adduser.

  b) Set the variable $NESSUS_PASS to the password you specified with 'nessus-adduser'.

  c) Set the variable $USE_NESSUS to "1".

Chapter 5. Configure Software

5.1. Configure NetReg

5.1.1. Create a new index.html

So it automatically redirects you to **registration.html**. Change the below yellow highlight so it reflects your NetReg server's fully qualified domain name (FQDN) or IP Address.

```
<html>
<head>
  <title> Online Network Registration</title>
  <meta http-equiv="pragma" content="no-cache">
  <meta http-equiv="refresh" content="0;url=http://192.168.100.110/registration.html">
</head>
<body>

    Redirecting... please wait. If you are not redirected automatically, then click
    <a href="/registration.html"> here</a>.
</body>
</html>
```

5.1.2. Configure how NetReg will authenticate your users

Edit **Variables.pm** in **/usr/lib/perl5/site_perl/Net/NetReg**.

- If you want NetReg to authenticate against a POP server:
  - ✓ Change $AUTH_METHOD to "**POP**".
  - ✓ Change $POPSERVER to the hostname or IP Address of your mail server.
- If you want NetReg to authenticate against a FTP server:
  - ✓ Change $AUTH_METHOD to "**FTP**".
  - ✓ Change $FTPSERVER to the hostname or IP Address of your FTP server.
- If you want NetReg to authenticate against a IMAP server:
  - ✓ Change $AUTH_METHOD to "**IMAP**".
  - ✓ Change $IMAPSERVER to the hostname or IP Address of your IMAP server.
- If you want NetReg to authenticate against a Radius server:
  - ✓ Change $AUTH_METHOD to "**RADIUS**".
  - ✓ Change @RADIUS_SVRS to the IP Address of your Radius servers. If you have more than one Radius server then enter the server's IP address in quotes separated by a comma.

    Example: **@RADIUS_SVRS = ("10.1.1.1","10.2.1.1");**

- If you want NetReg to authenticate against a LDAP server:
  - ✓ Change $AUTH_METHOD to "**LDAP**".
  - ✓ Change @LDAP_SERVERS to the hostname or IP Address of your LDAP servers. Example: **@LDAP_SERVERS = ("10.3.1.1", "10.4.1.1");**
  - ✓ Change $LDAP_BASE to your LDAP user base. For example: "**ou=users,dc=yourdomain,dc=edu**";
  - ✓ Change $LDAP_AUTH_ATTR to the user attribute, which is either "**uid**" or "**cn**". To authenticate against Microsoft's Active Directory, change $LDAP_AUTH_ATTR to "cn".
  - ✓ Change $LDAP_USE_ADS to **1** if you wish to use Microsoft's Active Directory Server as your authentication source.
  - ✓ Change $LDAP_ADS_DOMAIN to your domain. For example: **$LDAP_ADS_DOMAIN = "yourdomain.edu";**

  The above examples show you how to authenticate against Microsoft's Active Directory. To authenticate against other LDAP entities, there are other LDAP variables that you may need to change in Variables.pm.

5.1.3. Change NetReg Default DHCP paths (Optional)

If your install the RPM package for DHCP Server (DHCPd) that comes with your Linux distribution, then you should not need to edit the default paths for dhcpd.conf and dhcpd.lease.

In the event that you need to change the default paths, you will need to edit **Variables.pm** in **/usr/lib/perl5/site_perl/Net/NetReg**. Below are the defaults:

```
$LEASESPATH      = "/var/lib/dhcp";
$LEASESFILE      = "dhcpd.leases";
$DHCPDCONFPATH   = "/usr/local/etc/netreg/dhcpd";
$DHCPDCONFFILE   = "dhcpd.conf";
$SUBNETFILE      = "/usr/local/etc/netreg/subnet.dat";
```

5.1.4. Configure subnets managed by NetReg

Edit **subnet.dat** in **/usr/local/etc/netreg** so it reflects all the subnets on your network that utilize DHCP. The format of subnet.dat is:

- Subnet/mask length for registered clients
- Location of subnet (description)
- Total number of leases for registered clients for that subnet.
- Subnet/mask length for unregistered clients if different, otherwise blank.

Suppose your network consisted of 3 VLANS using a different subnet for registered and unregistered DHCP clients. Registered clients receive a 10.x.x.x IP address and unregistered clients receive a 172.x.x.x IP address. Below is what your subnet.dat could resemble:

10.1.0.0/16: Dorms Blds: 5100: 172.16.0.0/16:
10.2.0.0/16: Classrooms: 5100: 172.17.0.0/16:
10.3.0.0/16: Admin Blds: 5100: 172.18.0.0/16:

5.1.5. Make refresh-dhcpdconf script Executable

In order for NetReg to allow clients to register their computer so they can obtain full access to your campus network, the 'refresh-dhcpdconf' script needs to be marked as executable. To do this enter the following command:

chmod 755 /usr/local/bin/refresh-dhcpdconf

5.2. Configure Apache Webserver

5.2.1. Create user/group for Apache/DHCPd & NetReg

- Create user & group called **netreg** with no logon abilities using "**Users and Groups**" for RedHat systems or using '**adduser**' for other Linux distributions.
- Edit **/etc/httpd/conf/httpd.conf** file and change the following lines:

From:

```
User    apache
Group   apache
```

To:

```
User    netreg
Group   netreg
```

5.2.2. Configure Apache httpd.conf restrictions

Configure Apache's httpd.conf file so your registration server's web directories are properly restricted. To restrict access of NetReg's webserver to specific networks, modify the following lines under Apache's <Directory> statements in httpd.conf.

```
Order deny,allow
deny from all
allow from 10.1 10.2 10.3 127.0.0.1
```

This restricts access so NetReg's web server can only be accessed from 10.1.0.0, 10.2.0.0, and 10.3.0.0 subnets and from the web server's localhost.

5.2.3. Restrict Apache cgi-bin directory

To allow a directory to be password restricted by a .htaccess file, you first need to ensure that the httpd.conf allows user authentication to be set up in a .htaccess file. This is controlled by the **AuthConfig** override. The **httpd.conf** file should include AllowOverride AuthConfig under the <Directory "/var/www/cgi-bin"> directive

```
<Directory "/var/www/cgi-bin">
    AllowOverride AuthConfig
    Options None
</Directory>
```

5.2.4. Configure ServerName in httpd.conf file

Edit /etc/httpd/conf/httpd.conf file and set ServerName to your NetReg server's FQDN.
Example: ServerName **netreg.yourdomain.edu**

5.2.5. Add ErrorDocument lines to httpd.conf

ErrorDocument 403 /registration.html
ErrorDocument 404 /registration.html

5.2.5. Create a .htaccess file

Place this file (**.htaccess**) in your **/var/www/cgi-bin/admin** to protect NetReg's administrative script.
----------Example: **.htaccess** file----------

AuthUserFile /etc/httpd/conf/htusers
AuthName "NetReg Administration"
AuthType Basic
AuthAuthoritative on
require valid-user

5.2.6. Create a user Authentication File

Create a user authentication file called 'htusers' and place it in /etc/httpd/conf.

Ex. **htpasswd –c /etc/httpd/conf/htusers netreg**

The –c argument tells **htpasswd** to create a new users file for Apache in the specified directory. When you run this command, you will be prompted to enter a password for 'netreg', and then confirm it. Other users can be added to the existing file in the same way without the –c argument.

5.2.7. Change ownership/access rights on Apache's directories

chown -R root:netreg /var/www
chown -R root:netreg /etc/httpd

5.3. Configuring ISC DHCPd

5.3.1. Modify the dhcpd.conf.

Modify the **dhcpd.conf** file in **/etc/netreg** so it reflects your network infrastructure. The below example dhcpd.conf file provides DHCP support to one network, which is 192.168.100.0, although it could support many networks/subnets and shared networks.

----------Example dhcpd.conf—(single network)----------

```
## ISC DHCPD v3 Configuration file
## for NetReg version 1.5
## Belongs at /etc/dhcpd/dhcpd.conf

max-lease-time 120;
default-lease-time 120;
option domain-name "yourdomain.edu";
server-identifier netreg.yourdomain.edu;
ignore bootp;
ddns-update-style ad-hoc;
ddns-updates off;

# Define subnet pools for known/unknown clients

subnet 192.168.100.0 netmask 255.255.255.0 {
        authoritative;
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.100.255;
        option routers 192.168.100.10;

        # Unregistered clients pool
        pool {
                range 192.168.100.200 192.168.100.209;
                option domain-name-servers 192.168.100.110; #Bogus DNS
                one-lease-per-client true;
                max-lease-time 120;
                default-lease-time 120;
                allow unknown clients;
        }

        # Registered clients pool
        pool {
                range 192.168.100.210  192.168.100.219;
                option domain-name-servers 192.168.100.10; # Real DNS
                option netbios-name-servers 192.168.100.10;
                one-lease-per-client true;
                max-lease-time 28800;
                default-lease-time 28800;
                deny unknown clients;
        }
}
include “/usr/local/etc/netreg/dhcpd/netreg.registered”;
```

5.3.2. Change the owner/permissions on dhcpd.registered files.

In order for clients to be able to register their computers with the NetReg system, NetReg needs to have read/write access to where the DHCP server stores client registrations. NetReg stores client registrations in **/usr/local/etc/netreg/dhcpd**.

```
# chown -R root:netreg /usr/local/etc/netreg
# chmod 664 /usr/local/etc/netreg/dhcpd/*
```

When a client register's their computer's hardware address through NetReg's registration web server, it puts the hardware address in 'dhcpd.registered.new'. NetReg's refresh-dhcpdconf script check every minute whether 'dhcpd.registered.new' has been updated and if so, it stop's the dhcpd service, copies 'dhcpd.registered.new' to 'dhcpd.registered' and then restarts the dhcpd service.

Note: When installing NetReg for the first time, make sure you delete any information stored in netreg.registered, netreg.registered.new and netreg.registered.bak.

5.4. Configuring DNS Bind

Since almost all new Linux distributions use Bind 9 in a chroot configuration for security reasons, for this reason this is the only configuration covered by NetReg v1.5.1 Instructions.

NetReg's DNS server is a bogus DNS server designed to resolve all Internet names back to NetReg's Web Server registration page for all unregistered DHCP clients. NetReg v1.5.1 adds a new feature that allows certain domains to be resolved so unregistered clients can retrieve Windows updates or virus definition updates.

5.4.1. Configure named.conf

Edit **named.conf** in **/var/named/chroot/etc.** Change the forwarders IP address highlighted in yellow to the IP address of your real DNS server.

----------Example named.conf----------

```
// BIND 9.x named.conf (CHROOT)
// For NetReg version 1.5
// Belongs at /var/named/chroot/etc/named.conf
// 192.168.100.10 = your real DNS IP

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

controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

## Allowed Windows Zones

zone "microsoft.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "akadns.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "akadns.net" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "akamai.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "akamai.net" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "download.windowsupdate.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "msft.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "msft.net" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
```

```
zone "nsatc.net" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "nsatc.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "ntservicepack.microsoft.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "windows.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "windows.net" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "windowsupdate.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "windowsupdate.microsoft.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "windowsupdate.net" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "wustat.windows.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "footprint.net" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "edgesuite.net" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "speedera.net" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "speedera.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};

## Allowed Apple Zones

zone "apple.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};

## Allowed Antivirus Zones

zone "sophos.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "mcafee.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "symantec.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
```

```
## Allowed Misc Zones

zone "dell.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "dell4me.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};
zone "powerpcs.com" {
      type forward; forwarders { 192.168.100.10; }; forward only;
};

## Wilcard zone

zone "." {
        type master;
        file "named.ca";
};

include "/etc/rndc.key";
```

5.4.2. Configure the DNS Bind cache file

Edit '/var/named/chroot/varnamed/named.ca' and change the yellow highlighted lines to the IP address of your NetReg (bogus) DNS server.

----------Example named.ca----------

```
; Bind 9.x (CHROOT) -- Zone file -- for NetReg version 1.5
; Belongs at /var/named/chroot/var/named/named.ca
;
$TTL 3600
. IN SOA localhost. root.localhost. (
        2005061501 ; serial
        10800      ; refresh
        3600       ; retry
        604800     ; expire
        86400      ; default_ttl
)
                   IN    NS    localhost.

; Allowed Windows Zones

microsoft.com.     IN    NS    localhost.
akadns.com.        IN    NS    localhost.
akadns.net.        IN    NS    localhost.
akamai.com.        IN    NS    localhost.
akamai.net.        IN    NS    localhost.
msft.com.          IN    NS    localhost.
```

```
msft.net.                   IN      NS      localhost.
nsatc.net.                  IN      NS      localhost.
nsatc.com.                  IN      NS      localhost.
windows.com.                IN      NS      localhost.
windows.net.                IN      NS      localhost.
windowsupdate.net.                  IN      NS      localhost.
ntservicepack.microsoft.com.        IN      NS      localhost.
windowsupdate.com.                  IN      NS      localhost.
windowsupdate.microsoft.com.        IN      NS      localhost.
download.windowsupdate.com.         IN      NS      localhost.
wustat.windows.com.                 IN      NS      localhost.
footprint.net.              IN      NS      localhost.
edgesuite.net.              IN      NS      localhost.
speedera.net.               IN      NS      localhost.
speedera.com.               IN      NS      localhost.

; Allowed Apple Zones

apple.com.                  IN      NS      localhost.

; Allowed antivirus zones

sophos.com.                 IN      NS      localhost.
mcafee.com.                 IN      NS      localhost.
symantec.com.               IN      NS      localhost.

; Allowed misc zones

dell.com.                   IN      NS      localhost.
dell4me.com.                IN      NS      localhost.
powerpcs.com.               IN      NS      localhost.

; Wildcard Zones
; 192.168.100.110 = your NetReg box IP

netreg                      IN      A       192.168.100.110
*.com.                      IN      A       192.168.100.110
*.net.                      IN      A       192.168.100.110
*.edu.                      IN      A       192.168.100.110 (Not Needed)
*.org.                      IN      A       192.168.100.110 (Not Needed)
*.                          IN      A       192.168.100.110
```

Chapter 6. Scheduling NetReg Update Script

6.1. Scheduling the refresh-dhcpdconf script.

Schedule the **refresh-dhcpdconf** script so it runs every minute. Since the DHCP server only reads its conf file when it is started, you will need a cron job that checks to see if the server needs to restart, reloading its updated configuration. The refresh-dhcpdconf script helps do this but cron will need to run this script every minute or two. We have cron running the script every minute as root like so in /var/spool/cron/root. FYI: Don't edit /var/spool/cron/root directly, use crontab –e.

```
0-59/1 * * * * /usr/local/bin/refresh-dhcpdconf
```

Within a minute, refresh-dhcpdconf will check if the netreg.registered.new has been updated. If netreg.registered.new is newer than netreg.registered, it updates netreg.registered and restart the DHCP server.

You have now successfully built a Network Registration server utilizing NetReg v1.5.1. Please reboot your server or manually start the '**dhcpd'** and '**httpd**' services.

Chapter 7. Acknowledgements

Many thanks go to the developers and contributors of the NetReg project. Their dedication has helped many network administrators take solace in knowing who are using our networks.

Programming:

Peter Valian valianp@southwestern.edu

Documentation:

Todd K Watson tkw@southwestern.edu
Peter Valian valianp@southwestern.edu
Patrick Jaques pjaques@comcast.net

Code Contributors:

Allie M. Tate allie@lsu.edu
Bobby Clark bobby.clark@eku.edu
Robert Lowe robert.h.lowe@lawrence.edu