Example Linux Networking Commands

Terminals, GUIs, run levels, miscellaneous

```
startx       (start up gnome desktop)
```

Alternate command Terminals

```
Ctrl-alt-1
Ctrl-alt-2
Ctrl-alt-3
Ctrl-alt-4
Ctrl-alt-5
Ctrl-alt-6

Graphical desktop
Ctrl-alt-7

shutdown now
init 0       (fastest way to shut down)
init 1       (minimal system)
init 3       (normal system)

su           (gets you to root, without path so must use \sbin\ifconfig)
su -         (gets you to root with root's path)

/sbin/route –n > myresults       (output overwrites file)
/sbin/route –n >> myresults      (output appended to file)
```

Mount external media

```
mount /dev/sda1 /mnt/usb-stick
umount /mnt/usb

mount /dev/fd0 /mnt/floppy
mount –r –t iso9660 /dev/cdrom /mnt/cdrom
umount /mnt/floppy

mount /dev/cdrom /mnt/cdrom
umount /mnt/cdrom
```

To show a running process

```
ps –e | grep ppp
```

To show parent processes

```
ps -ef
```

Users and groups (note, new users can't log in without passwd used to set password)

```
groupadd –g 192 cis192
groupdel cis192
useradd –g cis192 frank
useradd –g users –u 510 sarah
id frank
passwd frank
userdel frank
```

Configuring NICs

---

lspci (gives you hardware clue for which driver to select and install)
lsmod (view already installed drivers)

http://www.tldp.org/HOWTO/text/Ethernet-HOWTO
http://www.tldp.org/HOWTO/Hardware-HOWTO/nic.html

(to research Linux network driver info)

Network drivers (hopefully already in /lib/modules/2.4.20-8/kernel/drivers/net)

- e100 - for Intel Ethernet PRO 100 NIC
- 8139too - for D-Link NIC with RealTek 8129/8139 chipsets
- 3c59x - for 3Com 3c905x NICs
- tulip - for Lite-on Communications LNE 100TX cards with DEC chipsets

insmod 3c59x (installs driver, leave off the .o on driver name)
or modprobe 8139too (if driver has dependencies)

lsmod (verify new network drive is running)
/sbin/ifconfig eth1 172.30.4.106 netmask 255.255.255.0 broadcast 172.30.4.255
(ifconfig command still classful so must add broadcast)

/sbin/route add default gw 172.30.4.1 (adds default gateway)

ifconfig –a (shows all interfaces)

Other related commands:
ifconfig lo 127.0.0.1 (configure loopback)
rmmod e100 (removes intel NIC driver)
dmesg (shows ton of HW info)

more /var/log/dmesg (hardware loading info)
more /proc/modules (same as lsmod)
more /proc/interrupts (IRQs)
more /proc/ioports (IO ports)

ifconfig eth0 up
ifconfig eth0 down

/etc/init.d/network stop
/etc/init.d/network start
/etc/init.d/network status

Configuring client DNS

Edit (vi or gedit) /etc/resolv.conf and add:

nameserver 207.62.187.54 (IP address of primary name server)
nameserver XXX.XXX.XXX.XXX (IP address of secondary name server)

```
search cabrillo.edu       (domain suffix to add for short names)

or echo "nameserver 207.62.187.54" > /etc/resolv.conf

cat /etc/resolv.conf


Individual hosts can be locally added to the /etc/hosts file
127.0.0.1     donkey localhost.localdomain localhost
192.168.2.106 elrond
```

Configuring NICs permanently

```
To load NIC driver at system bootup
Edit /etc/modules.conf
       To look like:
       alias eth0 8139too
       alias eth1 3c59x
       alias eth1 e100


To set IP configuration:
Edit /etc/sysconfig/network-scripts/ifcfg-eth0       (or eth1)
       To look like:
       DEVICE=eth0
       USERCTL=no
       ONBOOT=yes
       BOOTPROTO=none
       BROADCAST=192.168.1.255
       NETWORK=192.168.1.0
       NETMASK=255.255.255.0
       IPADDR=192.168.1.5

To configure gateway:
Edit /etc/sysconfig/network
       To look like:
       NETWORKING=yes
       HOSTNAME=station01.mordor.rivendell.middleearth
       GATEWAY=172.24.1.100
       NISDOMAIN=cismud.net

To make static routes permanent:
Edit /etc/sysconfig/static-routes
       To look like:
       eth0 host 172.30.4.28 gw 207.62.106.30
       eth0 net 192.168.2.0 netmask 255.255.255.0 gw 172.30.4.107

To stop and start network:
/etc/init.d/network stop
/etc/init.d/network start
service network restart

Watchout for Redhat network utilities which if exist take priority:
/etc/sysconfig/networking/profiles/default/
       hosts
       ifcfg-eth0
       ifcfg-eth1
       network
       resolv.conf
```

Cheater baby configuration (watch out for classful broadcasts)

```
netconfig                  (TUI wizard for eth0)
netconfig –d eth1          (TUI wizard for eth1)
```

Configuring routes

To display routing table
```
route -n
```

Configure default gateways with:
```
route add default gw 192.168.2.6
route del default gw 192.168.2.6
```

Configure specific routes with:
```
route add –net 192.168.3.0 netmask 255.255.255.0 gw 172.30.4.106
route del –net 192.168.3.0 netmask 255.255.255.0 gw 172.30.4.106

route add –net 192.168.3.0 netmask 255.255.255.0 dev eth1
route del –net 192.168.3.0 netmask 255.255.255.0 dev eth1
```

Flush the routing table cache:
```
route -CF
```

To enable IP forwarding
```
Echo 1 > /proc/sys/net/ipv4/ip_forward
```

To disable IP forwarding
```
Echo 0 > /proc/sys/net/ipv4/ip_forward
```

To make routing permanent add:
```
Net.ipv4.ip_forward=1 to /etc/sysctl.conf
```

---

ssh and scp

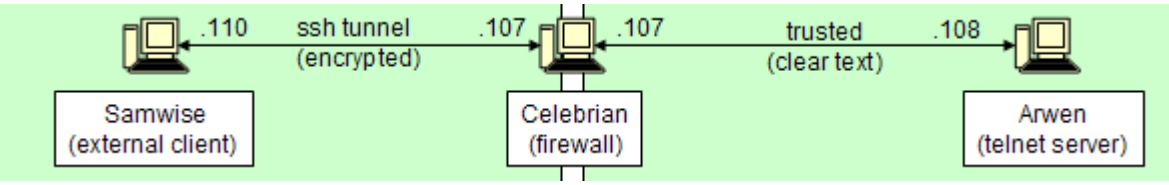
Copy lab1.txt from remote computer to “here”
```
scp root@172.30.4.106:lab1.txt .
```

Copy a file to Opus
```
scp iptables.simmsr cis192@opus.cabrillo.edu:
scp email cis192@opus.cabrillo.edu:email.simmsr
```

To run a command on a Linux computer and append output to a local file:
```
ssh cis192@opus.cabrilo.edu “quiz simmsr”
ssh root@elrond “route –n” >>  results.txt
ssh root@sauron “ping –c3 172.168.4.109” >> results.txt

scp guest@instructor:/tmp/bind* .
scp guest@gandalf:/tmp/dhcp* /root/
```

---

ssh port forwarding



To set up a "port forwarding" secure tunnel from an external client's local port 8000 through port 23 on a "firewall" server (172.30.4.107) to a specific internal telnet server (192.168.2.108) use:
`ssh -L 8000:192.168.2.108:23 172.30.4.107` (on the client)

Then to then access the telnet server (192.168.2.108) from the client outside the firewall use:
`telnet localhost 8000`

Testing

```
ping –b 172.30.1.255                    (broadcast ping)
ping 172.30.4.1                         (pings from eth0)
ping –I 192.168.2.106 172.30.4.106      (ping from specific interface ip to remote ip)
ping –c3 172.30.4.107                   (ping 3 times only then stop)
```

Note: ls –l /bin/ping shows ping in red because it runs as root

```
ethereal            (to run sniffer in GUI)
```

In Ethereal to capture a stream, select a packet then select:
`analyze > Follow TCP Stream` (from the menus)

Example capture filter to use in the capture setup window:
`src host 192.168.2.168 or 172.30.4.110`

Example display filter:
`ip.src == 15.27.245.100`

Monitoring log files on Linux
`tail -f /var/log/iptables`

Check for installed software

```
rpm –qa | grep telnet
rpm -qa | grep j2sdk
rpm -qa | grep postgres
```

```
rpm –ql dhcp              #files installed by rpm
rpm –ql dhcp              #information on rpm
```

Setup telnet server

```
rpm –qa | grep telnet     (look for telnet-server-0.17-28.i386.rpm)
rpm –ihv telnet-server*
```

To enable telnet server and restrict it to a single client:

Modify /etc/xinetd.d/telnet as follows :

```
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        only_from       = 192.168.2.107
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        disable         = no
```

To activate these config file changes

- xinitd can be restarted (slight impact to all services)
  `/etc/init.d/xinetd restart`
- or touched gently to re-read its config files with
  `ps –e | grep xinitd` (note *pid* of xinitd procees)
  `kill –1 pid` (replace “pid” with real pid from previous command)
  `-- or --`
  `killall -1 xinitd`

---

iptables firewall

Simple minded firewall wizard:

```
lokkit
```

To remove the older ipchains module:

```
lsmod           (look for ipchains)
rmmod ipchains  (if it is there)
```

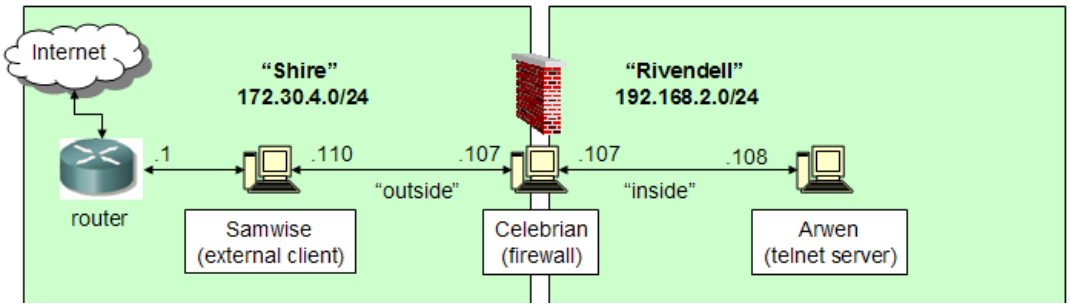
To view current firewall settings:

```
iptables –L
```

To save and restore firewall tables:

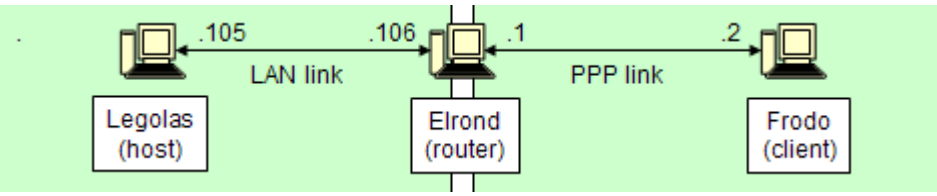
```
iptables-save > iptables.bak            (this is a little weird)
```

```
cat iptables.bak | iptables-restore –c     (this is very weird)

To setup firewall to block everything:
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

To setup firewall to accept everything:
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

To flush rules:
iptables -F
```




```
Celebrian configuration:
New connections from within firewall OK
iptables -A FORWARD -s 192.168.2.0/24 -d 0/0 -m state --state NEW -j ACCEPT

External packets to our Telnet server on port 23 OK
iptables -A FORWARD -s 0/0 -d 192.168.2.108 -m state --state NEW,ESTABLISHED,RELATED -
p tcp --dport 23 -j ACCEPT

Already established and related traffic OK
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

OK for firewall to output packets
iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

OK for firewall to accept packets from internal servers:
iptables -A INPUT -i eth0 -s 192.168.2.0/24 -d 192.168.2.107 -m state --state NEW -j
ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

To allow gedit to wrok (which need loopback):
Ipables –A INPUT –I lo –j ACCEPT




--------------------

iptables NAT

--------------------

To load NAT iptables module
modprobe iptable_nat
```

```
Create a pseudo public address (with IP aliasing) for external telnet server access
ifconfig eth1:0 172.30.4.5 netmask 255.255.255.0 broadcast 172.30.4.255

Translate incoming pseudo destination address to the telnet server:
iptables -t nat -A PREROUTING -d 172.30.4.5 -j DNAT --to-destination 192.168.2.108

Translate outgoing packet source addresses from the internal telnet server to the
pseudo address
iptables -t nat -A POSTROUTING -s 192.168.2.108 -j SNAT --to-source 172.30.4.5

Translate other outgoing packets from other internal servers to have source IP of
firewall public address
iptables -t nat -A POSTROUTING -s 192 168.2.0/24 -j SNAT --to-source 172.30.4.107

------------------------

iptables logging

------------------------

edit /etc/syslog.conf and add kern.info /var/log/iptables near top

more /etc/syslog.conf     (to check if vi edits worked)

> /var/log/iptables       (to create empty log file)

service syslog restart    (to restart logging)

to log INPUT and FORWARD entries
iptables -A INPUT -j LOG --log-level info --log-prefix "iptables INPUT: "
iptables -A FORWARD -j LOG --log-level info --log-prefix "iptables FORWARD: "

tail -f /var/log/iptables         (to monitor log)




------------------------------------------------------------

VI commands (when desparate and gedit is not available)

------------------------------------------------------------

j = scroll down
k = scroll up
l = scroll right
i = input mode
dd = delete line
o = start input mode after this line
esc = go to command mode
:w! = exit and save
:q! = quit without saving
x = delete

--------------------------------------

Setting up a serial connection

----------------------------------
```



Part I – set up the server (Elrond):

```
ls –l /dev/ttyS?        (lists the serial devices ttyS0 to ttyS9)
setserial /dev/ttyS0    (shows UART, port and IRQ for COM 1)
/etc/inittab            (used by INIT process for specific run level)
```

Note: want UART to be 16550A for high speed connection

The following entry is placed near the end of the /etc/inittab file. It will respawn (restart) agetty which is used to open the specified tty port and initiate a login:

```
s1:35:respawn:/sbin/agetty 38400 ttyS0
```

```
telinit q       (tells init to re-examine the updated /etc/inittab file)
chmod u+s /usr/sbin/pppd  (permission change so normal users run pppd)
```

Part II – set up the client (Frodo) and login to the server (Elrond):

```
minicom –s  (to reconfigure minicom for /dev/ttyS0 instead of /dev/ttyS1
default)
minicom –o  (to run the terminal emulator for logging into Elrond, -o
suppresses modem commands)
```

Minicom provides terminal emulation and modem control. It is initially used on Frodo to login into Elrond over the serial cable as any terminal would log into a mini-computer. Note use TERM=ansi77 if not running from an xterm (i.e. gnome desktop).

Part III - using pppd for layer 2 part of network connection

Pppd functions as both a server and client on both ends to create the pppd network connection over the same serial link. This results in ppp0 interfaces showing up in ipconfig output. We need a way to get pppd to run when loggin in to the server (Elrond) from the client (Frodo). To do this we put the following pppd command into the Elrond's /home/guest/.bash_profile so it will run someone logs into Elrond's guest account:

```
/usr/sbin/pppd -detach crtscts proxyarp 10.0.0.1:10.0.0.2 /dev/ttyS0 38400
```

Note on pppd options and args:

```
-detach - keeps init from continuously spawning new instances of pppd
crtscts – use HW flow control
proxyarp – provides arp functionality to work with other Ethernet LANs
10.0.0.1:10.0.0.2 - local gets 10.0.0.1, remote peer (Frodo) gets 10.0.0.1
38400 – buad rate
```

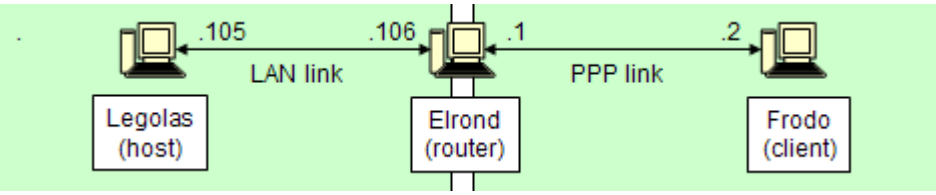
On the client Frodo, we use

```
minicom –o        (to login to Elron, -o suppresses modem commands)
Ctrl-A z q        (to quit minicom)
```

pppd –detach crtscts /dev/ttyS0 38400 & (preload this, needs fast typing)

At this point we have a network connection with ppp0 interfaces showing on both ends with the ip addresses shown above being used. Routing and IP forwarding can be set up as with any other network.

Automating a serial connection



To create a user on Elrond server that uses the pppd command as the shell use:
useradd -u 100 -g 100 -c "PPP Account" -d /etc/ppp -s /usr/sbin/pppd ppp
passwd ppp (to set the password for user ppp)

On Elrond, put the following options for the pppd daemon in the /etc/ppp/options file:

```
-detach                 (stop spawning additional pppd processes)
crtscts                 (use HW flow control i.e. RTS/CTS)
lock                    (exclusive access to serial port)
proxyarp                (arp handling for coexisting with Ethernet LAN's )
10.0.0.1:10.0.0.2       (local:remote IP addresses to configure)
/dev/ttyS0              (serial port to use)
38400                   (baud rate)
```

On the client Frodo create the following ppp-on script:

```
pppd updetach crtscts defaultroute /dev/ttyS0 38400 connect \
"exec chat -v TIMEOUT 3 ogin:--ogin: ppp assword: secret"
      updetach
      updetach – pppd will detach once connection is established
      defaultroute - adds static default route using peer as the gateway
      \ - negates the carriage return to get this all on one line
      connect – runs the script that follows
      "exec chat …." – script using chat command to login to ppp user account
Chmod 7555 ppp-on       (makes script executable)
./ppp-on                (runs script)
```

At this point we have a network connection with ppp0 interfaces showing on both ends with the ip addresses shown above being used. Routing and IP forwarding can be set up as with any other network.

```
-------------------------

Install firefox

-------------------------


www.mozilla.org and download latest
tar –xzvf firefox-1.5.0.2.tar.gz
cd firefox
./firefox

To update task bar icon
Right-click on WWW icon on taskbar
Change to firefox in firefox directory
```

```
-----------------------------

Samba

-----------------------------

RPMs:
      samba-common-*
      samba-client-*
      samba-swat-*

      (Install common first)

      rpm –ihv samba-common-*       #to install
      rpm -qi samba                 #to query installed rpm
      rpm –qa | grep samba          #to see what rpms are installed


Configure /etc/samba/smb.conf

      workgroup = WORKGROUP
      server string = Cool Virtual Samba Server
      hosts allow = 192.168.2. 172.30.4. 127.
      encrypt passwords = yes
      smb passwd file = /etc/samba/smbpasswd


      Add share definitions to end of config file:

      [var]
          comment = Linux Log files
          path = /var
          writable = yes
          browseable = yes
          hide dot files = yes
          guest ok = yes

To check smb.conf for errors
      testparm

Add a shared user

      smppasswd –a cis192           #to add user
      smbpasswd –x cis192           #to delete user

service smb start
service smb stop
service smb restart

smbclient -L celebrian -U cis192%password      #to see shares
smbclient -L frodo -U cis192%password

mount -t smbfs -o username=cis192,password=cis192     #to mount share
         //frodo/SharedDocs /mntpoint
```

DHCP

```
rpm –ihv dhcp-3.0pl2-6.14.i386.rpm
```

Configure DHCP:

```
vi /etc/dhcpd.conf
touch /var/lib/dhcpd/dhcpd.leases
```

```
[root@celebrian root]# cat /etc/dhcpd.conf
ddns-update-style interim;
ignore client-updates;
option time-offset              -25200; # Pacific Daylight Time
#
#   R I V E N D E L L
#
subnet 192.168.2.0 netmask 255.255.255.0 {
        option routers                  192.168.2.107; # Default GW
        option subnet-mask              255.255.255.0;
        option domain-name              "Rivendell";
        option domain-name-servers      207.62.187.54;

        range dynamic-bootp             192.168.2.50 192.168.2.99;
        default-lease-time              21600;
        max-lease-time                  43200;

        # give the relay agent a fixed address
        host Arwen {
                hardware ethernet       00:03:FF:9E:8E:68;
                fixed-address           192.168.2.150;
        }
}
#
#   S H I R E
#
subnet 172.30.4.0 netmask 255.255.255.0 {
        option routers                  172.30.4.1;
        option subnet-mask              255.255.255.0;
        option domain-name              "Shire";
        option domain-name-servers      207.62.187.54;

        range dynamic-bootp             172.30.4.50 172.30.4.99;
        default-lease-time              21600;
        max-lease-time                  43200;
}
#
#   M O R D O R
#
subnet 192.168.3.0 netmask 255.255.255.0 {
        option routers                  192.168.3.150;
        option subnet-mask              255.255.255.0;
        option domain-name              "Mordor";
        option domain-name-servers      207.62.187.54;

        range dynamic-bootp             192.168.3.50 192.168.3.99;
        default-lease-time              21600;
        max-lease-time                  43200;
}
[root@celebrian root]#
```

Start and stop DHCP:

```
service dhcpd start
service dhcpd stop
service dhcpd restart
service dhcpd status

ps –e | grep dhc

/var/lib/dhcp/dhcpd.leases      (server lease log)
```

To permanently run when computer boots up:

```
chkconfig –-level 35 dhcpd on

chkconfig –-list dhcpd
ls /etc/rc.d/rc3.d/
```

Configure DHCP relay agent:

```
vi /etc/sysconfig/dhcrelay
INTERFACES=”eth0 eth1”      (one for server, one for clients)
DHCPSERVER=192.168.2.107
```

Stop and start DHCP relay agent:

```
service dhcrelay start
service dhcrelay stop
service dhcrelay restart

ps –e | grep dhc
```

DHCP client :

```
dhclient                    (request IP address)
dhclient –r                 (release IP address)
/var/lib/dhcp/dhclient.leases      (client lease log)
```

```
-------------------

DNS Server

-------------------
```

Check for and install DNS

```
rpm –qa | grep bind
rpm –qa | grep bind-utils
rpm –qa | grep caching

rpm –ihv bind-9.2.2-21.i386.rpm
rpm -ihv caching-nameserver-7.2-7.noarch.rpm
```

DNS configuration

```
/etc/named.conf                 (overall config file)
```

```
[root@arwen root]# cat /etc/named.conf
// generated by named-bootconf.pl

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; };
};

zone "rivendell" {
        type slave;
        file "db.rivendell";
        masters {192.168.2.107; };
};
```

```
      include "/etc/rndc.key";
      [root@arwen root]#
```

```
/var/named/db.rivendell       (one of the zone files)
```

```
      [root@celebrian root]# cat /var/named/db.rivendell
      $TTL 604800
      ; Rivendell Zone Definition
      ;
      ;
      Rivendell.      IN SOA hostname.rivendell. root.rivendell. (
                      2001080109      ;       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 hostname.rivendell.
      ;
      ;Address Records
      localhost       IN A    127.0.0.1
      legolas         IN A    192.168.2.105
      elrond          IN A    192.168.2.106
      celebrian       IN A    192.168.2.107
      arwen           IN A    192.168.2.108
      galadriel       IN A    192.168.2.104
      ;
      ;CNAME records
```

```
named-checkconf               (checks DNS files)
```

Operation

```
rndc reload             #reloads zone files
rndc flush              #flushes cache
```

Start and stop DNS

```
service named start
service named stop
service named restart

chkconfig –level 35 named on        #always start at bootup

ps –e | grep named                  #check if DNS service running
```

Monitor DNS log file

```
tail –f /var/log/messages
```

DNS utilities

```
host Legolas
dig @celebrian legolas
```

```
-----------------

NFS

-----------------
rpm -q portmap nfs-utils

To access shares on remote computers:


      showmount –e hershey                    #show avalable mounts on hershey


      Temporary
      mount hershey:/home/cis192 /home        #mount remote share to local directory
      mount                                   #to verify
      umount /home                            #unmount share

      mount shadowfax:/home/cis192/images /tmp/images

      Permanent
      Edit /etc/fstab and add:
            hershey:/home/cis192 /home nfs defaults 0 0

            mount                             #to verify


To make shares for others

      Edit /etc/exports file and add:
            /home/cis192   192.168.2.0/255.255.255.0(ro,no_root_squash,sync)
            /home/guest    *(rw,sync)


      service nfs start

      exportfs –rv                            #after modifying /etc/exports
```

```
----------

NIS

----------

NIS client

      domainname cismud.net

      - or –

      Add “NISDOMAIN=cismud.net” to /etc/sysconfig/network


Configuration files

      /etc/nsswitch.conf

      #hosts:     db files nisplus nis dns
      hosts:      dns files nis

      /etc/yp.conf file

      service ypbind start
      service ypbind status

      Configure ypbind to start automatically on boot:

      chkconfig –-level 35 ypbind on
      chkconfig –-list
      chkconfig –-list ypbind

NIS Server

      ypserv is the daemon
      /etc/ypserv.conf is config file
      /var/yp has makefile and map files
            Host.byaddr
            Hosts.byname
            hosts
```