

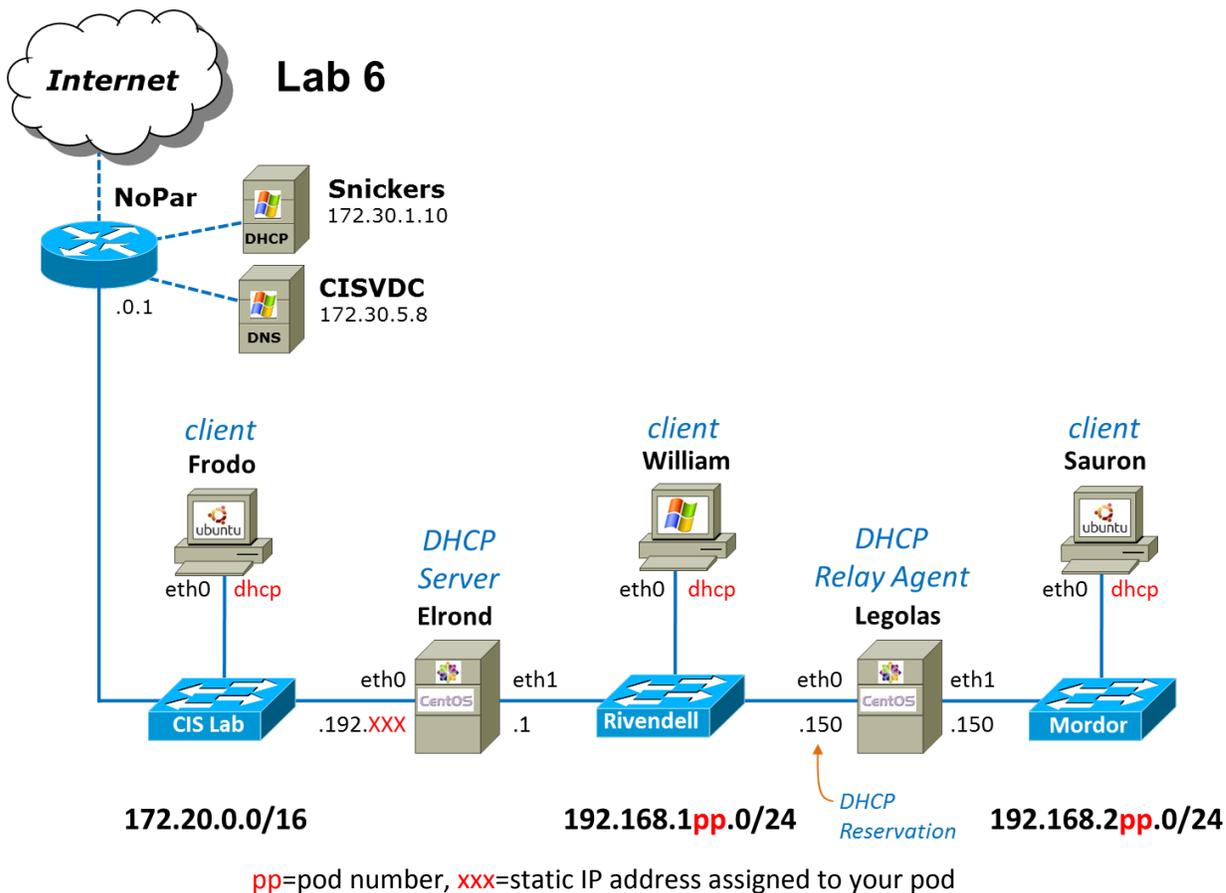
CIS 192 Linux Lab Exercise

Lab 6: Dynamic Host Configuration Protocol

Spring 2013

Lab 6: Dynamic Host Configuration Protocol

The purpose of this lab is to configure a DHCP server for multiple subnets. You will configure additional options along with an IP address and netmask, and you will configure a host reservation to guarantee that a particular host will always get a specific IP address. You will also configure a relay agent for relaying IP addresses from your server to clients in Mordor, the 192.168.2.0 network.



DHCP Service Specifications

Global			
default-lease-time	60 minutes (3600 seconds)		
maximum-lease-time	120 minutes (7200 seconds)		
option domain-name-servers	172.30.5.8, 10.24.1.2		
ddns-update-style	none		
ignore-client-updates	✓		
Scopes			
	CIS Lab	Rivendell	Mordor
subnet	172.20.0.0/16	192.168.1pp.0/24	192.168.2pp.0/24
range	See: Static IP Assignments Table	.50-.99	.50-.99
option domain-name	cislab.net	Rivendell	Mordor
option domain-search	"cislab.net";	"rivendell", "cislab.net";	"mordor", "cislab.net";
option routers	172.20.0.1	192.168.1pp.1	192.168.2pp.150
Authoritative		✓	✓
Reservations			
host	na	ppp-legolas	na
hardware Ethernet	na	00:0c:29:yy:yy:yy	na
fixed-address	na	192.168.1pp.150	na

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/>

Supplies

- Virtualization: VMware ESXi/vSphere (for VLab Pod)
- Centos 6.3 VMs: Elrond and Legolas
- Ubuntu 12.04 LTS VMs: Frodo and Sauron
- Windows XP VM: William
- Virtual networks: Rivendell and Mordor

Preparation

- [Optional] Revert VMs to their "Pristine" snapshots.
- Make a network map and crib sheet with everything you need to do this lab productively.
- On Opus, make a copy of the *lab6* report template file in */home/cis192/depot* in your home directory. Edit the header of this file with your own information and record all the information requested.
- Cable the VMs according to the diagram.

Elrond Setup

Challenge: See if you can do each of the following configuration steps using your crib sheets from previous labs and lesson slides. If you get stuck you can peek at the reference implementation in the Appendix.

- Permanently configure eth0 with your first static IP address for your pod. Save the remainder for a pool of CIS Lab network addresses for your DHCP server to use.
- Permanently configure eth1 as shown on the diagram.
- Permanently configure Nopar as the default gateway.
- Permanently configure the DNS nameserver and search domain(s).
- Permanently configure ip_forward to enable packet forwarding.
- Permanently modify the firewall to:
 - Allow packet forwarding.
 - Allow DHCP requests with:
iptables -I INPUT -p udp -m udp --dport 67 -j ACCEPT
- Permanently provide NAT services for Rivendell and Mordor hosts.
- Permanently add a static route to Mordor.
- Install the dhcp package so Elrond can provide dhcp services.
- Get the MAC address of the Legolas eth0 to make a dhcp reservation.
- Configure the global section and scopes for the CIS Lab and Rivendell networks in */etc/dhcp/dhcpd.conf*. This should include a reservation for the eth0 interface on Legolas.
- Start the dhcpd service with: **service dhcpd start**
- Configure it to start on boot: **chkconfig dhcpd on**
- If this command FAILS, then review the */var/log/messages* file. You must re-edit */etc/dhcp/dhcpd.conf*, fix any mistakes, and try again.

Test DHCP Service

- If the DHCP daemon starts up successfully, you are ready to test the service.
- Power on Frodo, what IP address did you get? Note: there is another DHCP server (Snickers) on the CIS Lab subnet, so Frodo may obtain an address from the other DHCP server. How will you know? Hint: the other DHCP server's pool of addresses does not include any 172.20.192.xxx addresses.
- On Frodo, release the current DHCP address with **dhclient -v -r eth0**, then request again with **dhclient -v eth0**.
- On Frodo, use **ifconfig**, **route -n** and **cat /etc/resolv.conf** to verify IP settings, default gateway and DNS have been set up properly. Note: Frodo uses dnsmasq so */etc/resolv.conf* will point to itself.
- Power on William, use **ipconfig /all** to see the IP address you got. Use **ipconfig /release** and **ipconfig /renew** to release and then request a new DHCP address.

Legolas Network Settings

Challenge: See if you can do each of the following configuration steps using your crib sheets from previous labs and lesson slides. If you get stuck you can peek at the reference implementation in the Appendix.

- Permanently configure eth0 for dhcp.
- Permanently configure eth1 as shown on the diagram.
- On Legolas, do a **service network restart**. Does Legolas get its reserved IP address?
- On Legolas, do a **dhclient -v -r eth0** followed by a **dhclient -v eth0** to release then request a new DHCP address.

- On Legolas, use **ifconfig**, **route -n** and **cat /etc/resolv.conf** to verify IP settings, default gateway and DNS have been set up properly and has Internet access.

Legolas configuration continued

Configure Legolas and a DHCP relay.

- Permanently configure `ip_forward` to do packet forwarding.
- Permanently modify the firewall to:
 - Allow packet forwarding.
 - Allow DHCP requests with:
iptables -I INPUT -p udp -m udp --dport 67 -j ACCEPT
- Install the `dhcp` package so Legolas can provide dhcp relay services.
- Before starting your DHCP Relay server, you will need to edit the configuration file:
/etc/sysconfig/dhcrelay
assign the two shell variables in this file as follows:
`INTERFACES="eth0 eth1"`
`DHCPSEVER=192.168.1pp.1`

The DHCP Relay agent needs to listen on the interface with which it will talk to the DHCP server as well as the interface on which it will listen for client requests.

- Start the `dhcrelay` service: **service dhcrelay start**
- Configure it to start on boot: **chkconfig dhcrelay on**
- Power on the Mordor client Sauron and verify it got a correct address.

Logs

Review the leases on the DHCP server and clients.

- On the clients, review the lease and reservation information recorded in the client database file:
 - Sauron (Ubuntu): */var/lib/dhcp/dhclient.leases*
 - Legolas (CentOS): */var/lib/dhclient/dhclient.leases*
 - Note that this information records the address of the DHCP server that handed them out.
- Review the DHCP Server's database file on Elrond, */var/lib/dhcpd/dhcpd.leases*, for a recording of the leases and their expiration dates.

To turn in

Record the following in your lab06 report:

1. Elrond's */etc/dhcp/dhcpd.conf* contents
2. Legolas' */etc/sysconfig/dhcrelay* contents
3. Sauron lease:
 - a. Snip one from Elrond's */var/lib/dhcpd/dhcpd.leases*
 - b. Snip one from Sauron's */var/lib/dhcp/dhclient.leases*
4. Legolas lease (reservation):
 - a. Snip one from Legolas' */var/lib/dhclient/dhclient.leases*
5. William lease:
 - a. Snip one from Elrond's */var/lib/dhcpd/dhcpd.leases*
6. Snipped `dhcpd` log entries showing:

- a. dhcpd service restarting
- b. providing an IP address to William
- c. providing an IP address to Sauron

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 lab06 /home/rsimms/turnin/cis192/lab06.$LOGNAME`
- Email your network map/crib sheet to: rsimms@cabrillo.edu

Grading rubric (30 points)

2 points for complete header including time spent and station info
4 points for map/crib sheet

2 points for correctly configuring the DHCP server globals
2 points for correctly configuring the DHCP server CIS Lab scope
2 points for correctly configuring the DHCP server Rivendell scope
2 points for correctly configuring the DHCP server Mordor scope

2 points for correctly configuring the DHCP relay agent

2 points for a single Sauron lease (on Elrond)
2 points for a single Sauron lease (on Sauron)
2 points for a single Legolas eth0 lease (reservation)
2 points for a single William lease

2 points for dhcpd log entries on Elrond (dhcp server restarting)
2 points for dhcpd log entries on Elrond (servicing William)
2 points for dhcpd log entries on Elrond (servicing Sauron)

Extra Credit

(1 point each)

Having done the lab, can you answer the following questions?

1. From the DHCP server's perspective does a reservation expire?
(Hint: check the DHCP server's database file, *dhcpd.leases* for the reservation.)
2. Does the DHCP service need a static route to Mordor when a relay agent on Legolas is available? Why?
3. If port 67 had not been opened on Elrond's firewall would clients still be able to obtain IP addresses? Why? (Hint: close UDP port 67 on Elrond and Legolas and observe what happens with tcpdump.)

Appendix - Pod 28 Reference Implementation

Elrond

```
[root@p28-elrond ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
BOOTPROTO="static"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Ethernet"
IPADDR=172.20.192.196
NETMASK=255.255.0.0
[root@p28-elrond ~]#
```

```
[root@p28-elrond ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE="eth1"
BOOTPROTO="static"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Ethernet"
IPADDR=192.168.128.1
NETMASK=255.255.255.0
[root@p28-elrond ~]#
```

```
[root@p28-elrond ~]# cat /etc/sysconfig/network-scripts/route-eth1
192.168.228.0/24 via 192.168.128.150
[root@p28-elrond ~]#
```

```
[root@p28-elrond ~]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=p28-elrond.rivendell
GATEWAY=172.20.0.1
[root@p28-elrond ~]#
```

```
[root@p28-elrond ~]# cat /etc/resolv.conf
search cislab.net
nameserver 172.30.5.8
[root@p28-elrond ~]#
```

```
[root@p28-elrond ~]# cat /etc/sysctl.conf
< snipped >
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
< snipped >
[root@p28-elrond ~]#
```

```
[root@p28-elrond ~]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Tue Mar 26 10:51:31 2013
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [43:5308]
-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 67 -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 Tue Mar 26 10:51:31 2013
```

```
# Generated by iptables-save v1.4.7 on Tue Mar 26 10:51:31 2013
*nat
:PREROUTING ACCEPT [1:239]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A POSTROUTING -o eth0 -j MASQUERADE
COMMIT
# Completed on Tue Mar 26 10:51:31 2013
[root@p28-elrond ~]#
```

```
[root@p28-elrond ~]# cat /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#   see 'man 5 dhcpd.conf'
#
option domain-name-servers 172.30.5.8, 10.240.1.2;
default-lease-time 3600; # 60 minutes
max-lease-time 7200; # 2 hours
ddns-update-style none;
#
#   R I V E N D E L L
#
subnet 192.168.128.0 netmask 255.255.255.0 {
    authoritative;
    option routers 192.168.128.1; # Default GW
    option subnet-mask 255.255.255.0;
    option domain-name "rivendell";
    option domain-search "cislabs.net";
    range 192.168.128.50 192.168.128.99;

    # reservations
    host p28-legolas {
        hardware ethernet      00:50:56:B7:CF:0B;
        fixed-address           192.168.128.150;
    }
}
#
#   M O R D O R
#
subnet 192.168.228.0 netmask 255.255.255.0 {
    option routers 192.168.228.150; # Default GW
    option subnet-mask 255.255.255.0;
    option domain-name "mordor";
    option domain-search "cislabs.net";

    range 192.168.228.50 192.168.228.99;
}
#
#   C I S L A B
#
subnet 172.20.0.0 netmask 255.255.0.0 {
    option routers 172.20.0.1;
    option subnet-mask 255.255.0.0;
    option domain-name "cislabs.net";

    range 172.20.192.198 172.20.192.202;
}
}
```

Legolas

```
[root@p28-legolas ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Ethernet"
[root@p28-legolas ~]#
```

```
[root@p28-legolas ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE="eth1"
BOOTPROTO="static"
NM_CONTROLLED="no"
ONBOOT="yes"
TYPE="Ethernet"
IPADDR=192.168.228.150
NETMASK=255.255.255.0
[root@p28-legolas ~]#
```

```
[root@p28-legolas ~]# cat /etc/sysconfig/iptables
# Generated by iptables-save v1.4.7 on Mon Apr 1 17:47:28 2013
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [20753:20325551]
:OUTPUT ACCEPT [3631:1122553]
-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 67 -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 Mon Apr 1 17:47:28 2013
[root@p28-legolas ~]#
```

```
[root@p28-legolas ~]# cat /etc/sysctl.conf
< snipped >
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
< snipped >
[root@p28-legolas ~]#
```

```
[root@p28-legolas ~]# cat /etc/sysconfig/dhcrelay
# Command line options here
DHCRELAYARGS=""
# DHCPv4 only
INTERFACES="eth0 eth1"
# DHCPv4 only
DHCPSEVERERS="192.168.128.1"
[root@p28-legolas ~]#
```