Lesson Module Status

- Slides
- Whiteboard with 1st minute quiz

- Flashcards
- Web Calendar summary
- Web book pages
- Commands
- Howtos

- Lab tested
- Lab template in depot
- Extra credit lab tested
- Lab template in depot

- Backup slides, Confer links, handouts on flash drive
- 9V backup battery for microphone

Course history and credits

Jim Griffin

- Jim created the original version of this course
- Jim's site: http://cabrillo.edu/~jgriffin/

Rick Graziani

- Thanks to Rick Graziani for the use of some of his great network slides
- Rick's site: http://cabrillo.edu/~rgraziani/

CIS 192 – Lesson 7

Instructor: **Rich Simms**
Dial-in: **888-450-4821**
Passcode: **761867**


Solomon


Sean C.


Chris


Corey


Bryan


Sean F.


Tony


David


Donna


Dave


Evan


Gabriel


Elia


Tajvia


Carlos

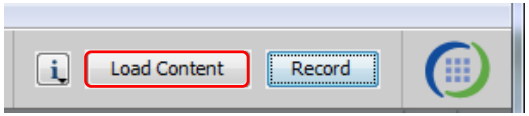

Adam


Ben


Laura

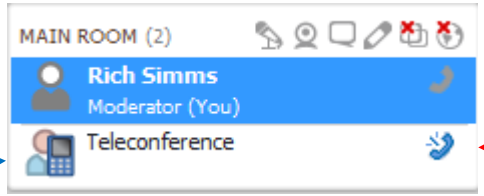
Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit

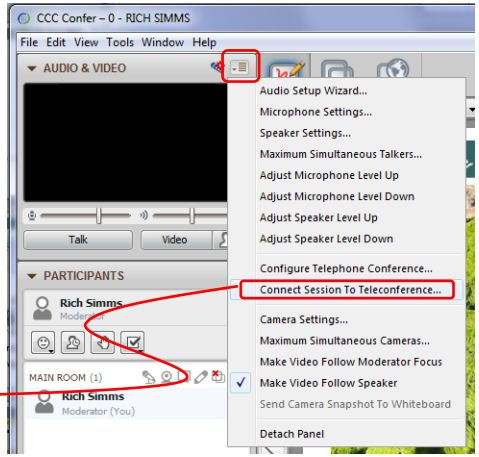
[ ] Preload White Board with *cis*lesson??*-WB*



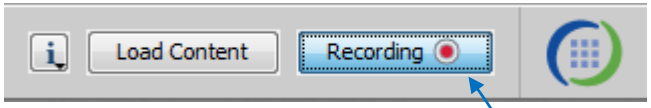
[ ] Connect session to Teleconference

Session now connected to teleconference





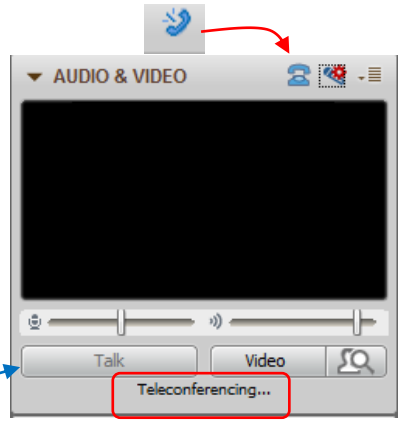
[ ] Is recording on?



Red dot means recording

[ ] Use teleconferencing, not mic

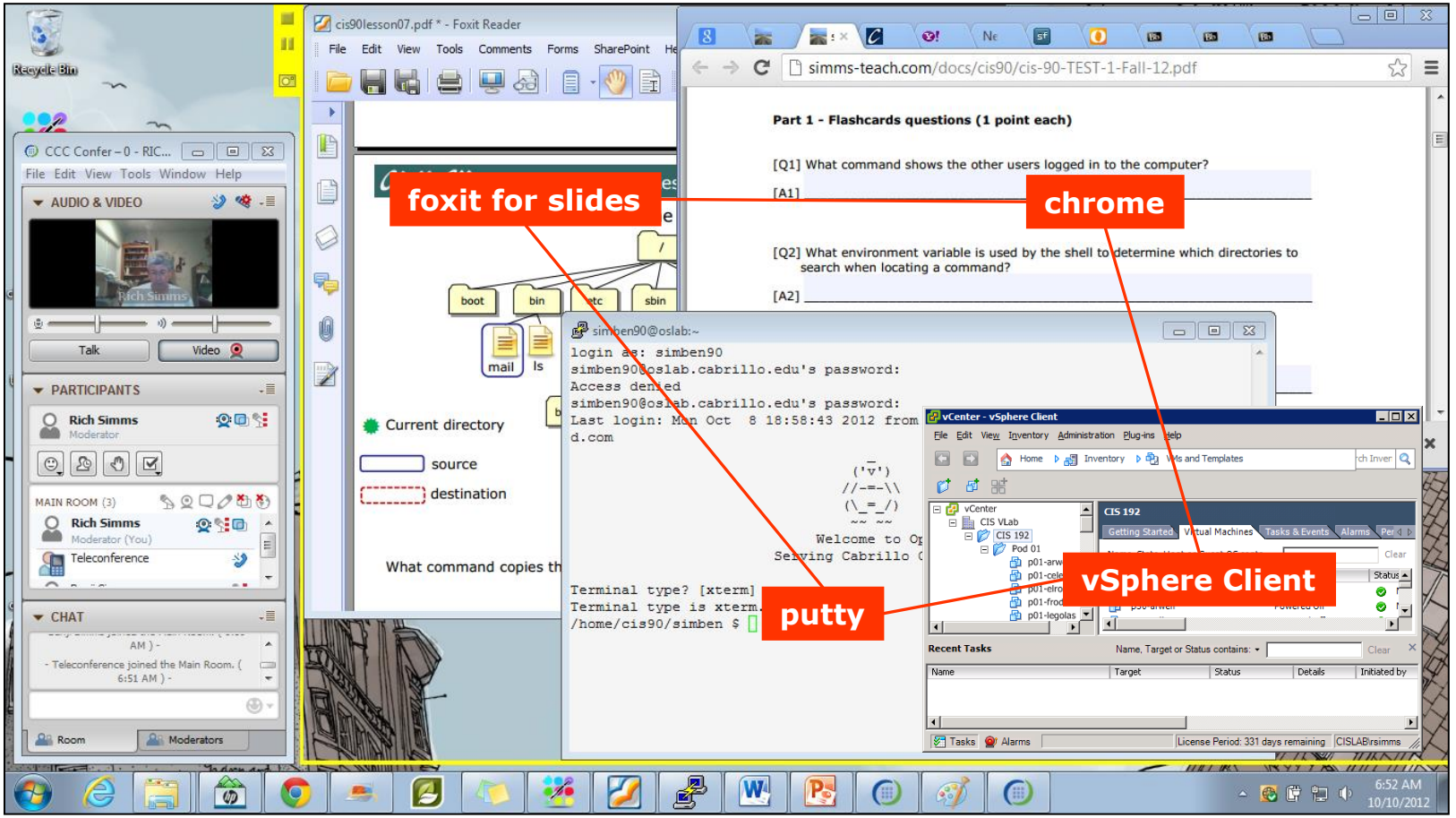
Should be greyed out



CCC Confer

Don't Forget

- [ ] **Video (webcam) optional**
- [ ] **layout and share apps**

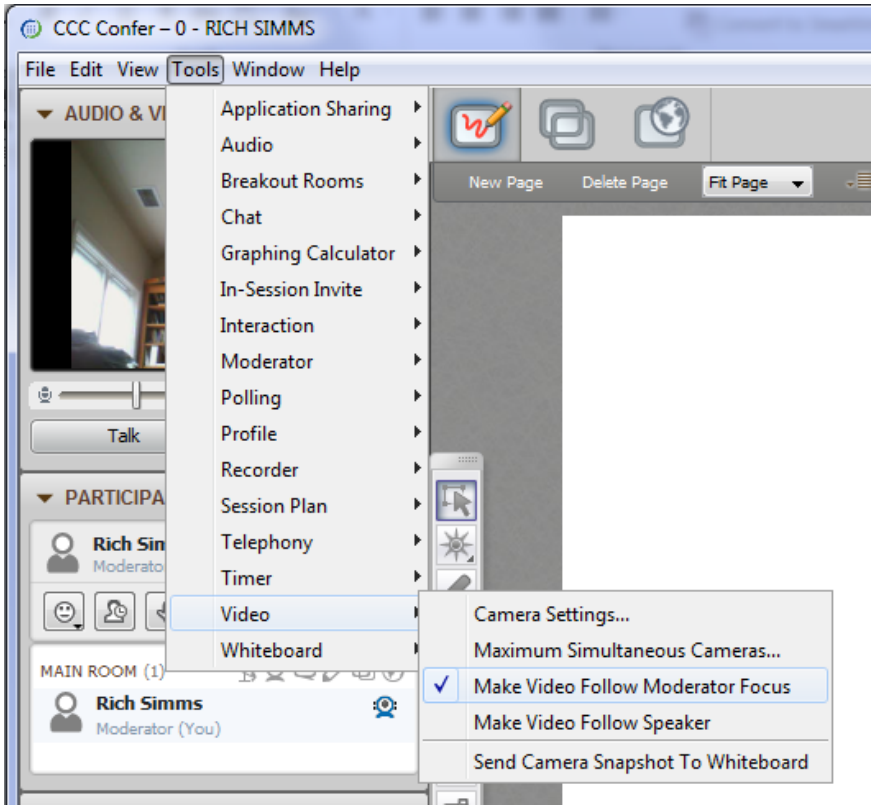


CCC Confer

[ ] Video (webcam) optional

[ ] Follow moderator

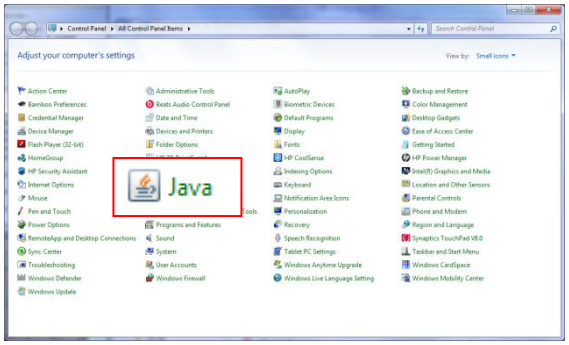
[ ] Double-click on postages stamps



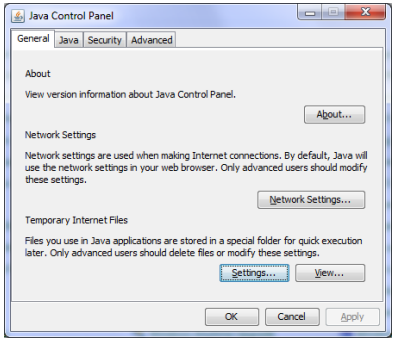
Universal Fix for CCC Confer:

1) Shrink (500 MB) and delete Java cache
2) Uninstall and reinstall latest Java runtime

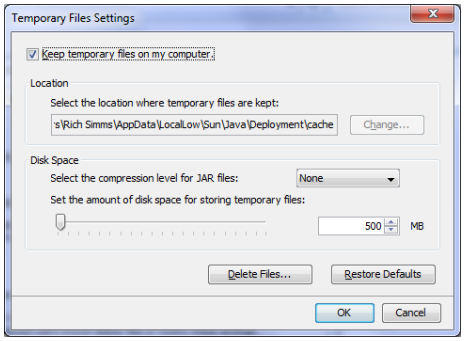
Control Panel (small icons)



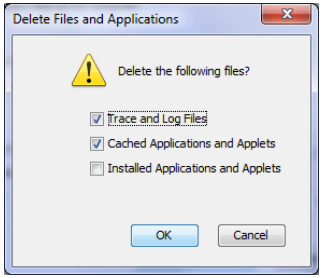
General Tab > Settings…



500MB cache size



Delete these



Google Java download

First Minute Quiz

Please answer these questions **in the order** shown:

Use CCC Confer White Board

For credit email answers to:
risimms@cabrillo.edu
within the first few minutes of class

DHCP

Objectives	Agenda
• Connect two computers on a serial line. • Connect two LANs together through a serial line using Point to Point protocol.	• Quiz • Questions on previous material • Housekeeping • Skills practice • DHCP overview • DHCP Client • DHCP Server • DHCP Relay • Wrap • Lab workshop

Questions

Questions

Lesson material?

Labs?

How this course works?

Chinese Proverb	他問一個問題，五分鐘是個傻子，他不問一個問題仍然是一個傻瓜永遠。 *He who asks a question is a fool for five minutes; he who does not ask a question remains a fool forever.*

Housekeeping

- Kindle found last week in 2501
- Firewall Lab 5 due today -- don't forget to include FORWARD log entries in the last section of the Lab Report.
- First extra credit lab X1 (SSH tunneling) available
- Spring Break next week

Grades Web Page

http://simms-teach.com/cis192grades.php

Code Name	Grading Choice	Quizzes & Tests													Forum				Labs										Final	Extra Credit	Total	Grade
		Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	T1	T2	T3	F1	F2	F3	F4	L1	L2	L3	L4	L5	L6	L7	L8	L9	L10				
Max Points		3	3	3	3	3	3	3	3	3	3	30	30	30	20	20	20	20	30	30	30	30	30	30	30	30	30	30	60	90	560	
Aragorn	Grade	2		3											20				30	30	23									3		
Bilbo	Grade	3	3	3											20				29	28	29									11		
Denethor	P/NP	3	3	3											16				8	13	26									6		
Dwalin																																
Elrohir																																
Elrond																																
Faramir																																
Frodo																																
Gwaihir																																
Ioreth																																
Legolas																																
Nazgul																																
Pippin																																
Samwise																																
Saruman																																
Strider	Grade	3	3	2											20				29	30										4		
Theoden	Grade	3	3	3											20				30	29	27									3		
Treebeard	Grade																															

Please check your:

- Grading Choice
- Quiz points
- Forum points
- Test points
- Lab points
- Extra Credit points

Don't know you secret LOR code name?

… then email me your student survey to get it!

Help with labs

Like some help with labs?

I'm in the CIS Lab Monday afternoons
- See schedule at http://webhawks.org/~cislab/

or see me during office hours

or contact me to arrange another time online

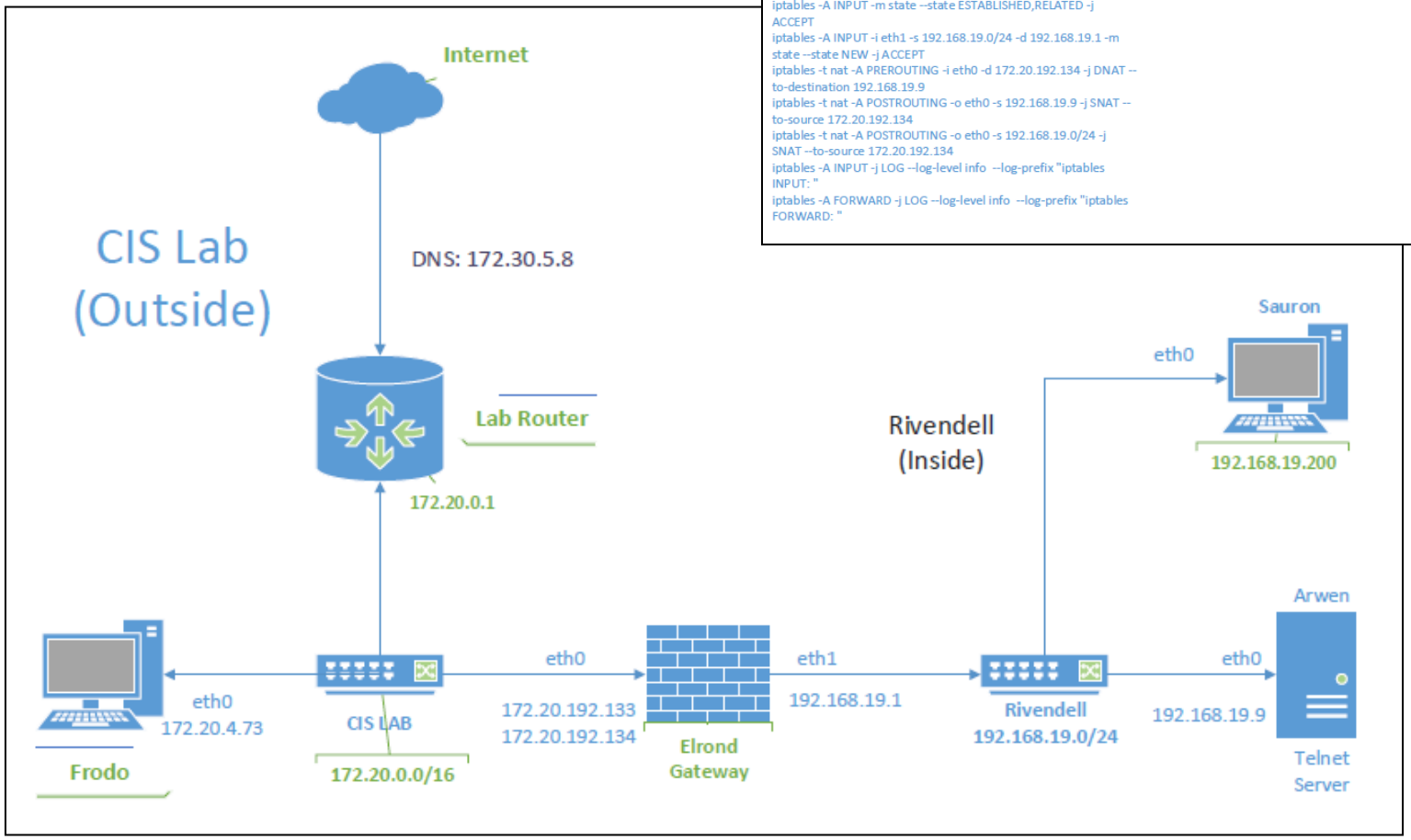
Lab Map/Crib Gallery

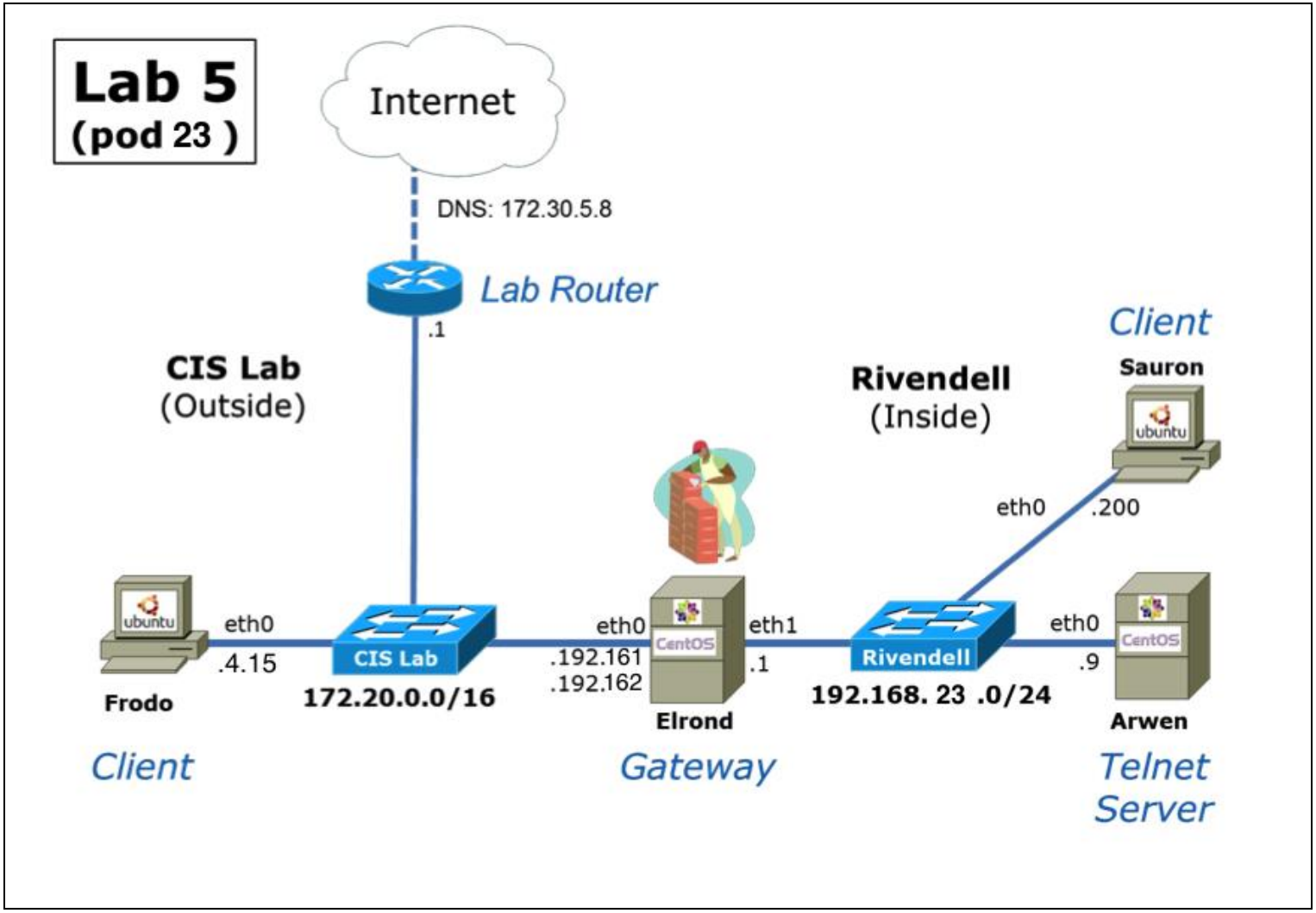
Elrond Crib Sheet

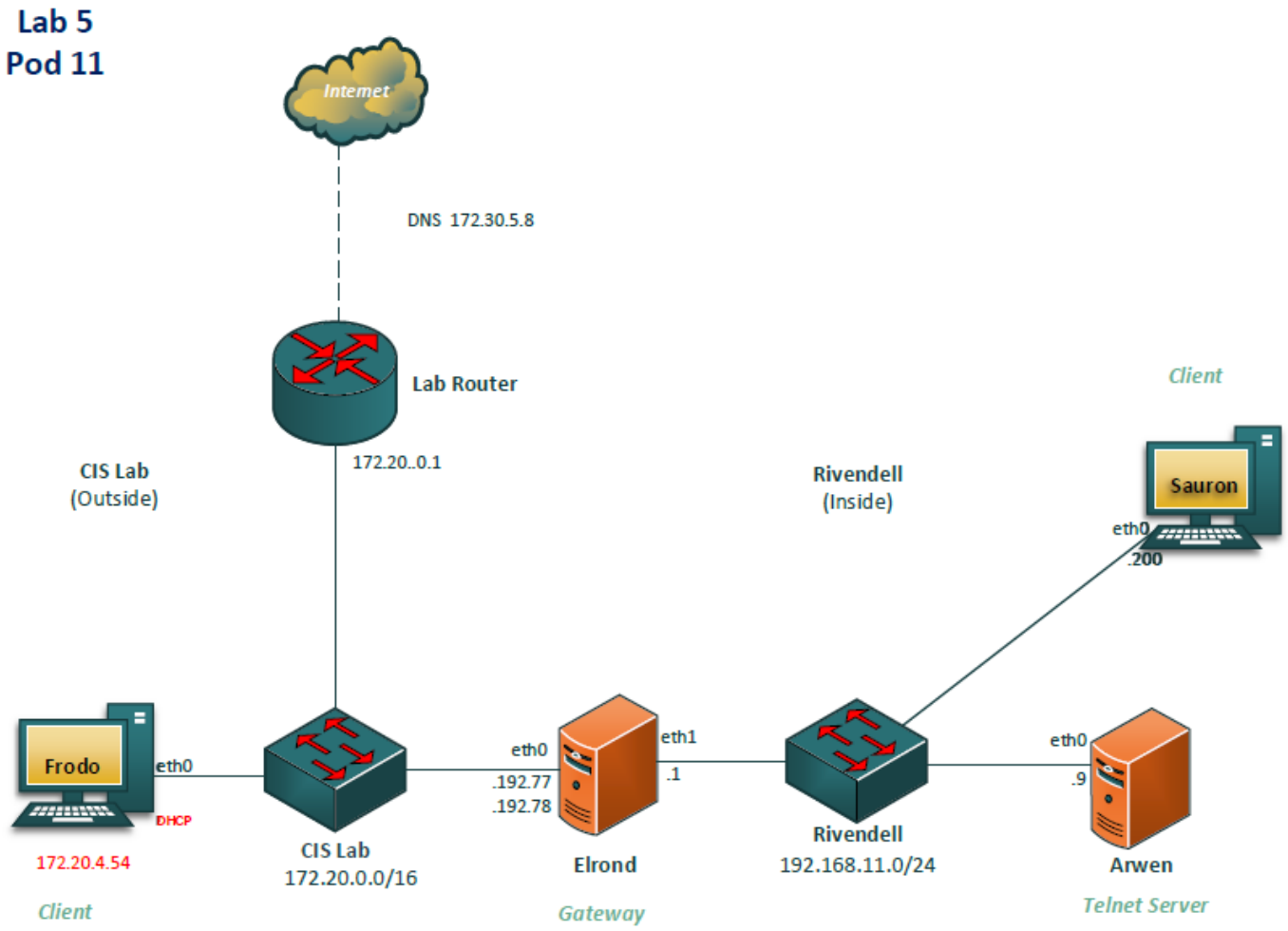
```
iptables  -P INPUT DROP
iptables  -P FORWARD DROP
iptables  -P OUTPUT DROP
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j
ACCEPT
iptables -A FORWARD  -s 192.168.19.0/24 -d 0/0 -m state --state
NEW -j ACCEPT
iptables -A FORWARD  -s 0/0 -d 192.168.19.9 -m state --state NEW
-p tcp --dport 23 -j ACCEPT
iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j
ACCEPT
iptables -A INPUT -i eth1 -s 192.168.19.0/24 -d 192.168.19.1 -m
state --state NEW -j ACCEPT
iptables -t nat -A PREROUTING -i eth0 -d 172.20.192.134 -j DNAT --
to-destination 192.168.19.9
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.19.9 -j SNAT --
to-source 172.20.192.134
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.19.0/24 -j
SNAT --to-source 172.20.192.134
iptables -A INPUT -j LOG --log-level info  --log-prefix "iptables
INPUT: "
iptables -A FORWARD -j LOG --log-level info  --log-prefix "iptables
FORWARD: "
```

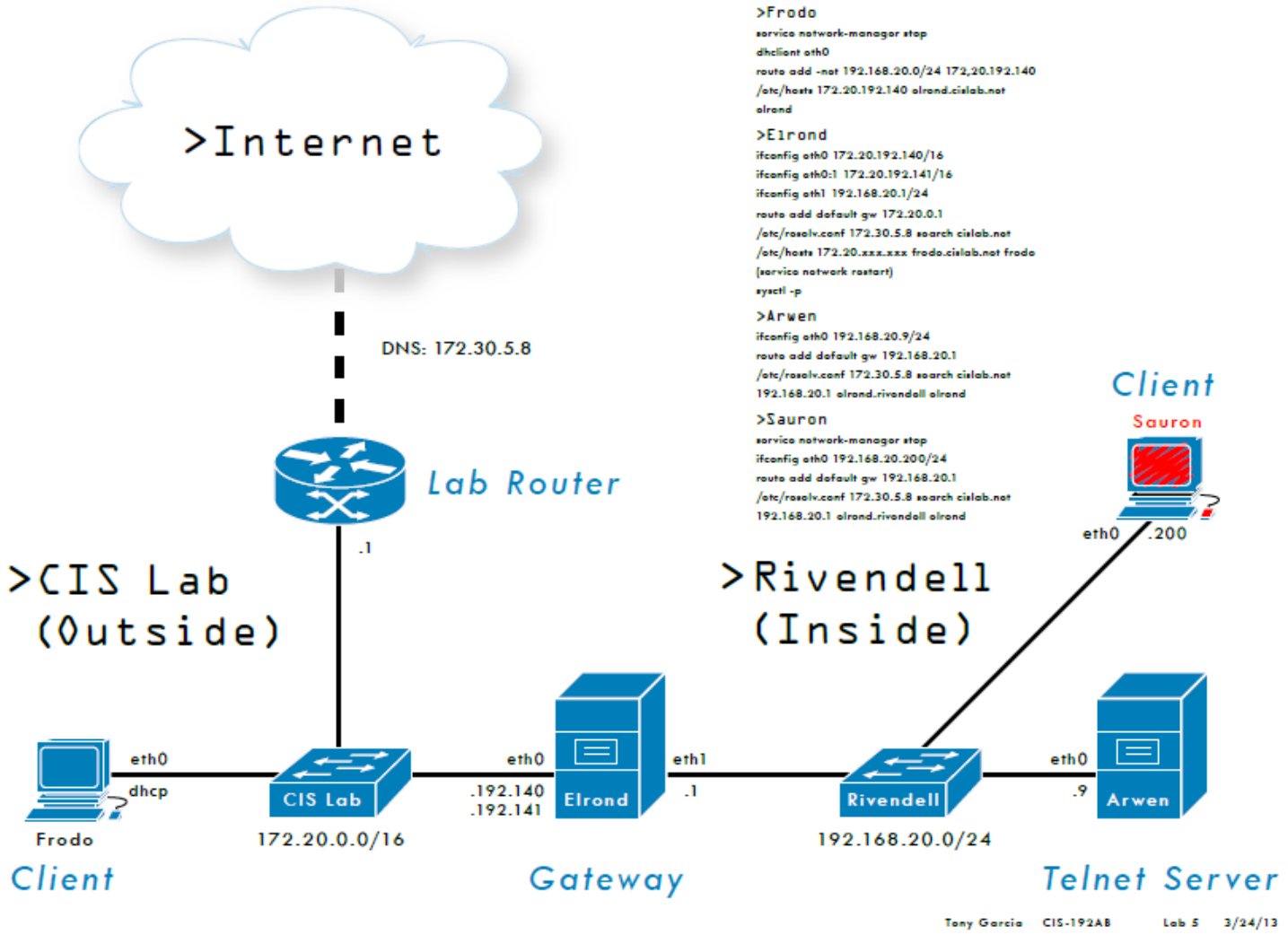
Arwen Crib Sheet

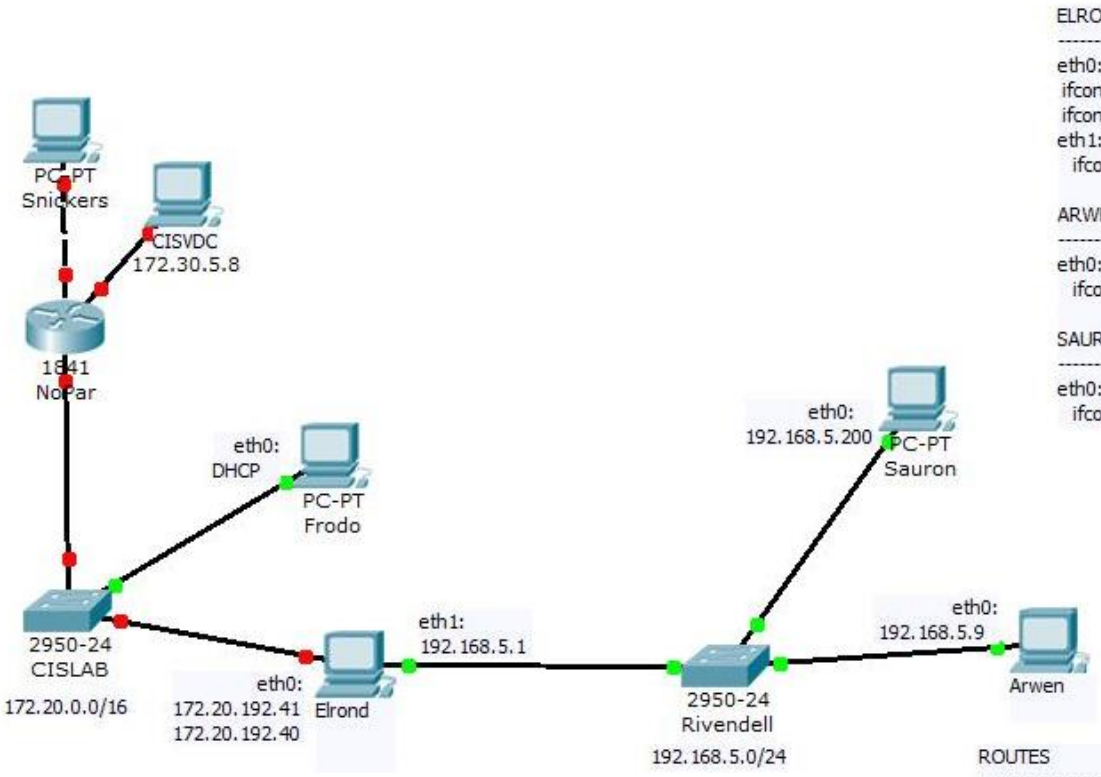
```
iptables -nL --line-numbers
iptables -I INPUT 7 -m state --state NEW -m tcp -p tcp --dport  23 -j
ACCEPT
Iptables -nL
Service iptables save
```




Lab 5
(pod 23)
Internet
DNS: 172.30.5.8
Lab Router
.1
CIS Lab
(Outside)
Rivendell
(Inside)
Client
Sauron
ubuntu
eth0
.200
ubuntu
eth0
.4.15
Frodo
Client
CIS Lab
172.20.0.0/16
eth0
.192.161
.192.162
CentOS
Elrond
Gateway
eth1
.1
Rivendell
192.168. 23 .0/24
eth0
.9
CentOS
Arwen
Telnet
Server


Lab 5
Pod 11
Internet
DNS 172.30.5.8
Lab Router
172.20..0.1
CIS Lab
(Outside)
Rivendell
(Inside)
Client
Sauron
eth0
.200
Frodo
eth0
DHCP
172.20.4.54
Client
CIS Lab
172.20.0.0/16
eth0
.192.77
.192.78
Elrond
Gateway
eth1
.1
Rivendell
192.168.11.0/24
eth0
.9
Arwen
Telnet Server


>Internet
DNS: 172.30.5.8
Lab Router
.1
>CIS Lab
(Outside)
>Rivendell
(Inside)
Client
Sauron
eth0
.200
>Frodo
service network-manager stop
dhclient eth0
route add -net 192.168.20.0/24 172.20.192.140
/etc/hosts 172.20.192.140 elrond.cislab.net
elrond
>Elrond
ifconfig eth0 172.20.192.140/16
ifconfig eth0:1 172.20.192.141/16
ifconfig eth1 192.168.20.1/24
route add default gw 172.20.0.1
/etc/resolv.conf 172.30.5.8 search cislab.net
/etc/hosts 172.20.xxx.xxx frodo.cislab.net frodo
(service network restart)
sysctl -p
>Arwen
ifconfig eth0 192.168.20.9/24
route add default gw 192.168.20.1
/etc/resolv.conf 172.30.5.8 search cislab.net
192.168.20.1 elrond.rivendell elrond
>Sauron
service network-manager stop
ifconfig eth0 192.168.20.200/24
route add default gw 192.168.20.1
/etc/resolv.conf 172.30.5.8 search cislab.net
192.168.20.1 elrond.rivendell elrond
eth0
dhcp
Frodo
Client
CIS Lab
172.20.0.0/16
eth0
.192.140
.192.141
Elrond
Gateway
eth1
.1
Rivendell
192.168.20.0/24
eth0
.9
Arwen
Telnet Server
Tony Garcia CIS-192AB Lab 5 3/24/13

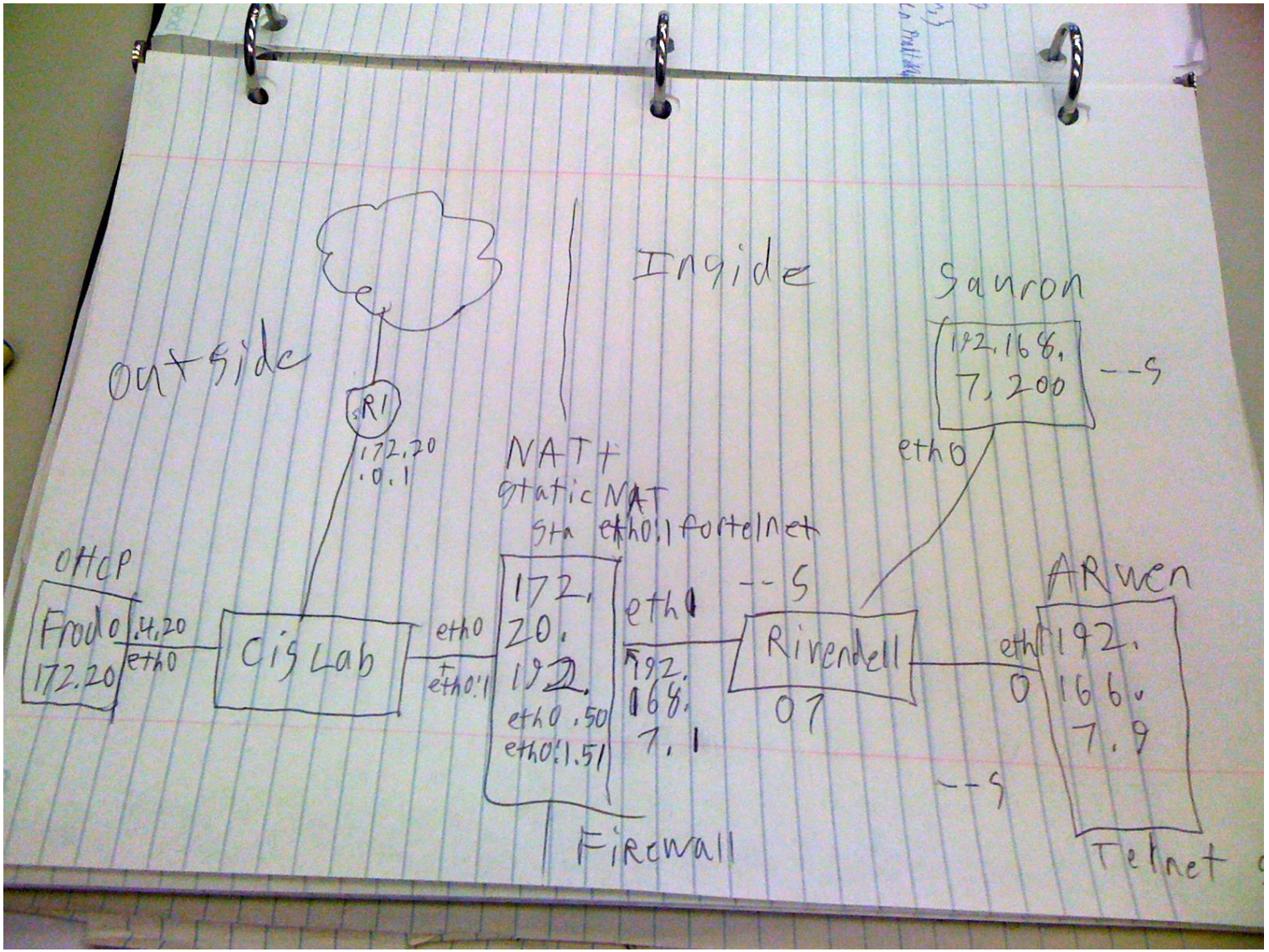


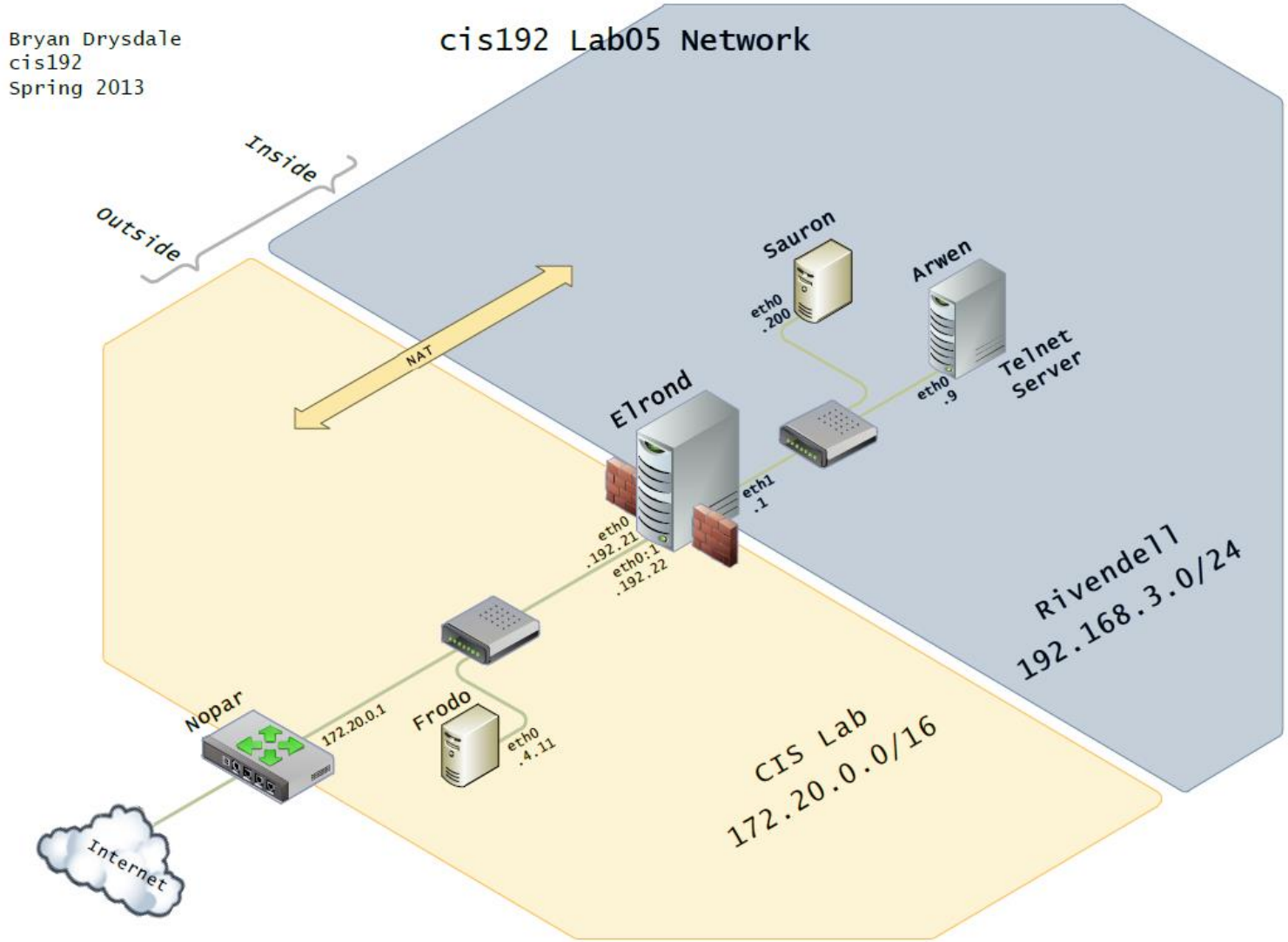

```
ELROND
------------------------
eth0:
 ifconfig eth0 172.20.192.40/16
 ifconfig eth0:1 172.20.192.41/16
eth1:
  ifconfig eth1 192.168.5.1/24

ARWEN:
------------------------
eth0:
  ifconfig eth0 192.168.5.9/24

SAURON
------------------------
eth0:
  ifconfig eth0 192.168.5.200/24
```

```
ROUTES
================
 ARWEN:
  route add default gw 192.168.5.1
-----------------
SAURON:
   route add default gw 192.168.5.1
-----------------
ELROND:
  route add default gw 172.20.0.1
-----------------
FRODO:
 route add -net 192.168.5.0/24 gw 172.20.192.40
```


Outside
Inside
R1
172.20
.0.1
NAT+
static NAT
Sta eth0:1 for telnet
DHCP
Frodo
172.20
.4.20
eth0
CisLab
eth0
eth0:1
172.
20.
192.
eth0 .50
eth0:1.51
Firewall
eth0
--s
192.
168.
7.1
Rivendell
01
Sauron
192.168.
7.200
--s
eth0
eth0
ARwen
192.
168.
7.9
--s
Telnet


Bryan Drysdale
cis192
Spring 2013
cis192 Lab05 Network
Inside
Outside
NAT
Sauron
eth0
.200
Arwen
eth0
.9
Telnet
Server
Elrond
eth1
.1
eth0
.192.21
eth0:1
.192.22
Rivendell
192.168.3.0/24
Nopar
172.20.0.1
Frodo
eth0
.4.11
CIS Lab
172.20.0.0/16
Internet

DHCP Module

DHCP Overview

DHCP

Dynamic Host Configuration Protocol

Defined by RFC 1541

- Extension of the bootstrap (bootp) protocol

Updated by RFC 2131

- adds DHCPINFORM and vendor specific options

Benefits:

- Solution for mobile computers
- Helps when too few IP addresses to go around
- Centralizes network configuration
- Minimizes network support and maintenance

DHCP

DHCP Architecture

DHCP Servers

- Scopes and exclusions
- Reservations
- Leases
- Options
  - IP Address and Netmask
  - Gateway
  - DNS Server
  - Domain name
  - others

DHCP Relay Agents

DHCP Clients

DHCP Servers *provide IP addresses and other network configuration information to clients wanting to join a network*

DHCP Relay Agents *lets one DHCP server service multiple non-connected subnets*

DHCP Clients *use the IP address and other network information obtained from the DHCP server to join a network automatically.*

DHCP

DHCP Architecture

DHCP Servers
- Scopes and exclusions
- Reservations
- Leases
- Options
  - IP Address and Netmask
  - Gateway
  - DNS Server
  - Domain name
  - others

DHCP Relay Agents

DHCP Clients

Scopes are used to define a pool of IP addresses for use by clients on a specific subnet.

For the DHCP Lab will we define 3 scopes for the three networks (Shire, Rivendell and Mordor)

DHCP

DHCP Architecture

DHCP Servers

- Scopes and exclusions
- Reservations
- Leases
- Options
  - IP Address and Netmask
  - Gateway
  - DNS Server
  - Domain name
  - others

DHCP Relay Agents

DHCP Clients

IP addresses can be reserved for specific interfaces using the MAC address to identify the interface.

DHCP

DHCP Architecture

DHCP Servers

- Scopes and exclusions
- Reservations
- Leases
- Options
  - IP Address and Netmask
  - Gateway
  - DNS Server
  - Domain name
  - others

DHCP Relay Agents

DHCP Clients

Clients no longer own their own IP address and instead lease one from a DHCP server.

The lease has a time limit but it can be renewed

DHCP

DHCP Architecture

DHCP Servers

- Scopes and exclusions
- Reservations
- Leases
- Options
  - IP Address and Netmask
  - Gateway
  - DNS Server
  - Domain name
  - others

DHCP Relay Agents

DHCP Clients

The DHCP server can provide not only an IP address but a lot of other network configuration information as well

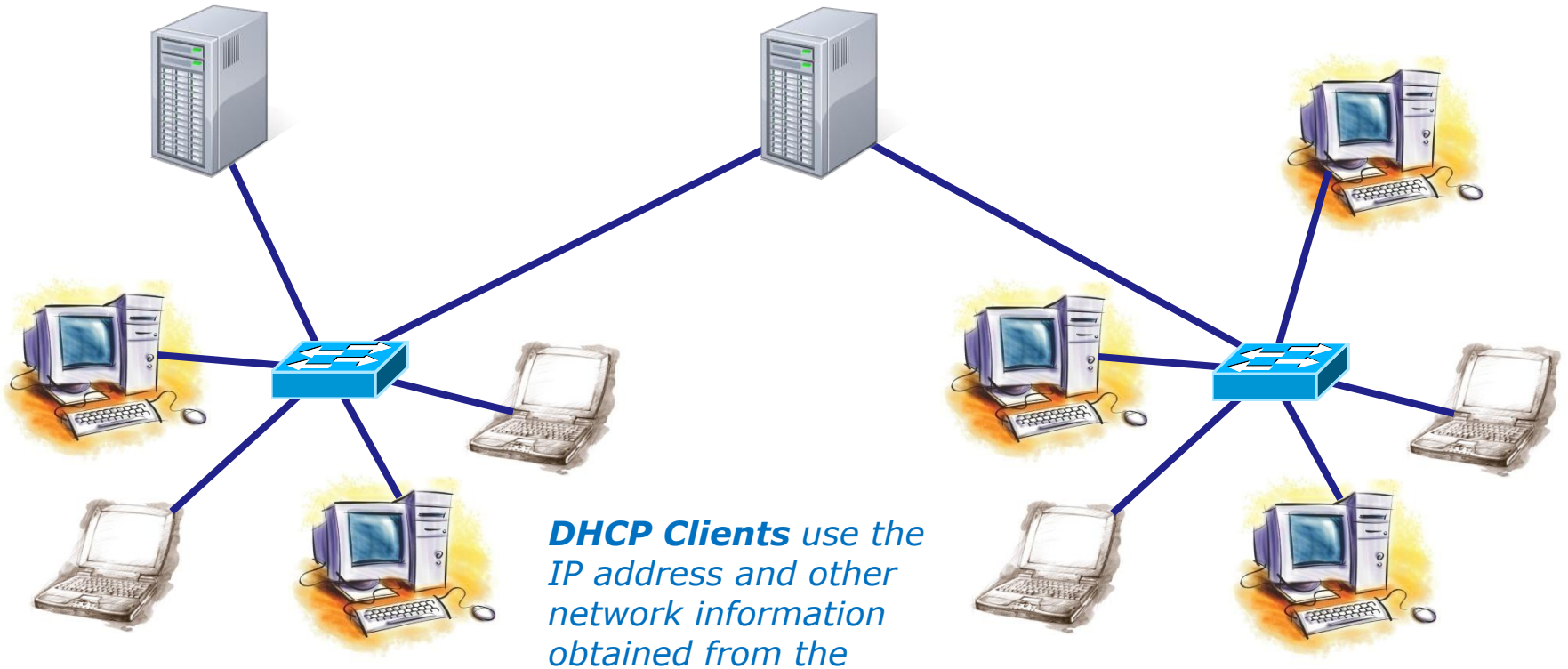
DHCP

DHCP Servers *provide network settings to clients*

DHCP Relays *allow the DHCP server to reach remote networks*

DHCP Server

DHCP Relay Agent (Linux Router)



DHCP Clients *use the IP address and other network information obtained from the DHCP server to join a network automatically.*

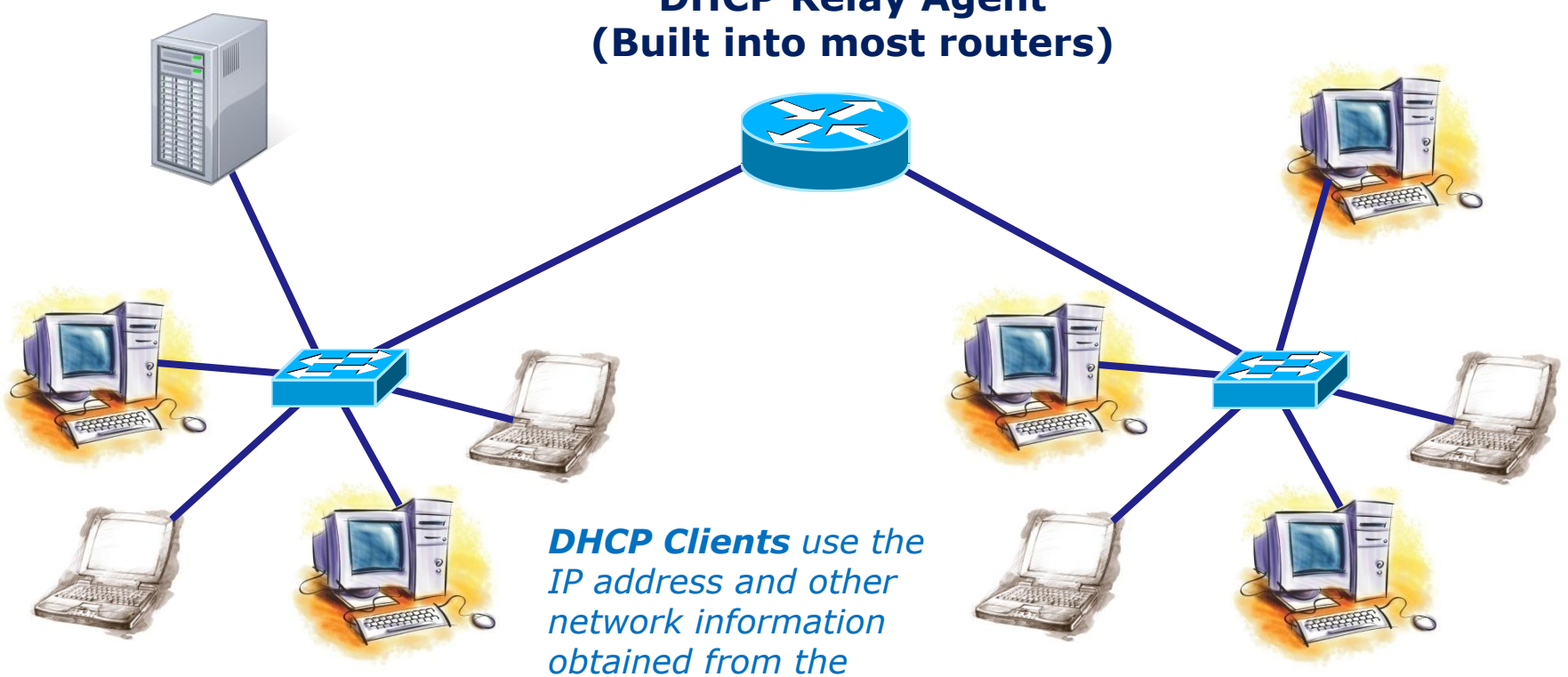
DHCP Clients

DHCP Clients

DHCP

DHCP Servers *provide network settings to clients*

DHCP Relays *allow the DHCP server to reach remote networks*



DHCP Clients *use the IP address and other network information obtained from the DHCP server to join a network automatically.*

DHCP

DHCP Protocol

DORA

- Discover
- Offer
- Request
- Acknowledge

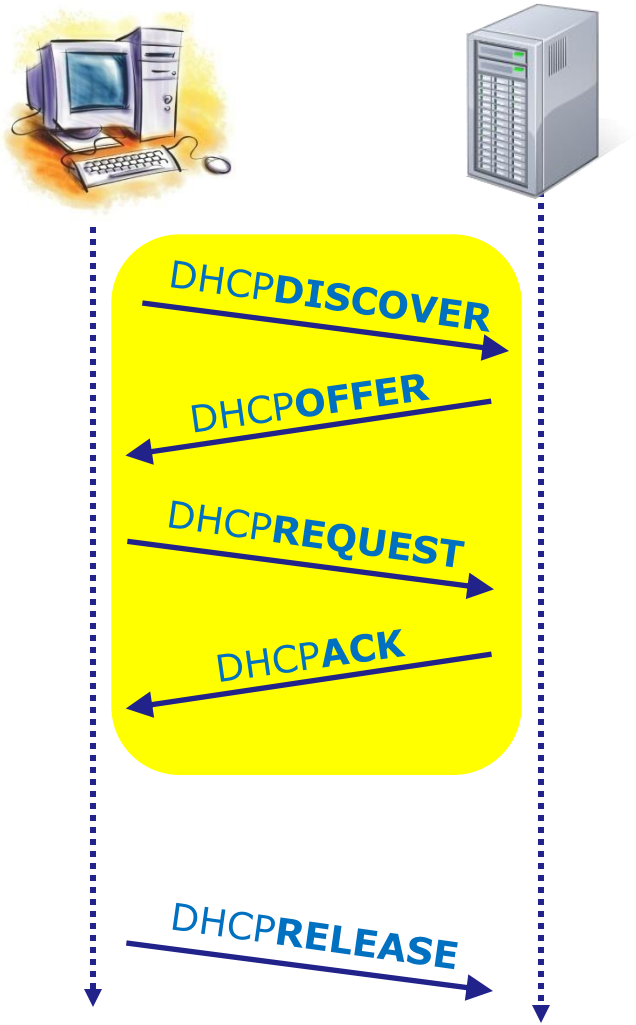
The DORA sequence is used by to join a new client to the network

And

- Release, Decline, NAK, Inform

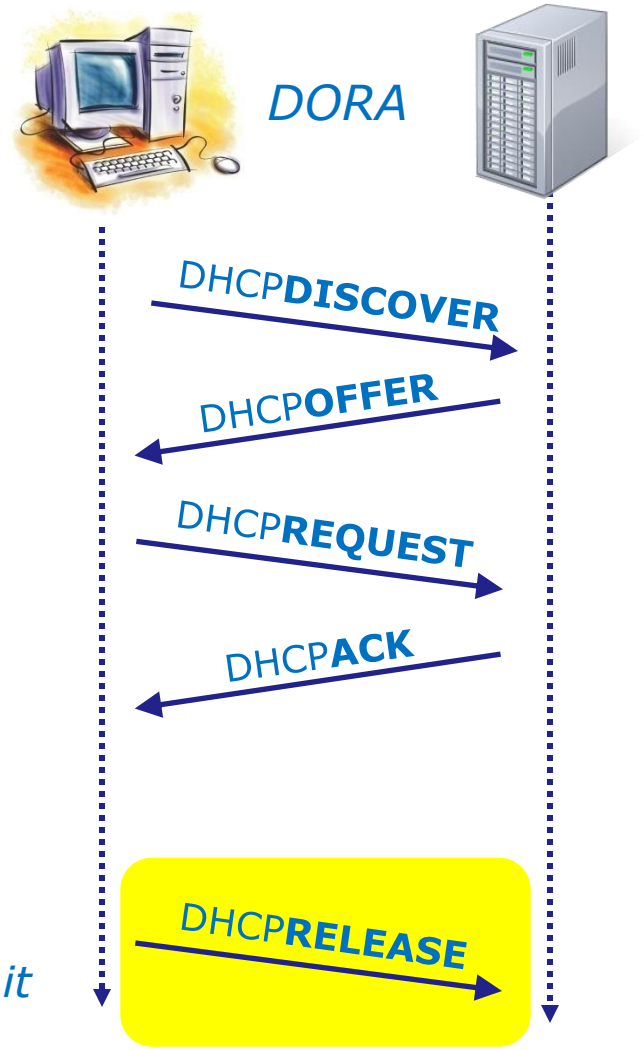
DHCP

Using the DORA steps, a client obtains an IP address and additional network configuration information to join the network



D *iscover*
O *ffer*
R *equest*
A *cknowledge*

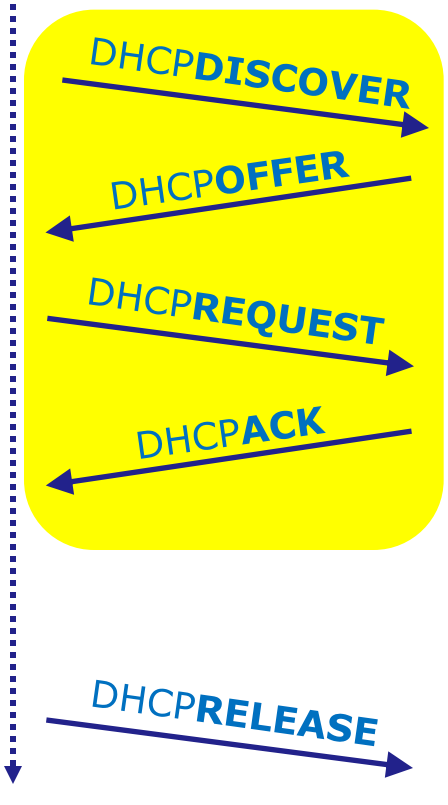
DHCP



When a client shuts down it will release the IP address assigned to it

DHCP

DORA

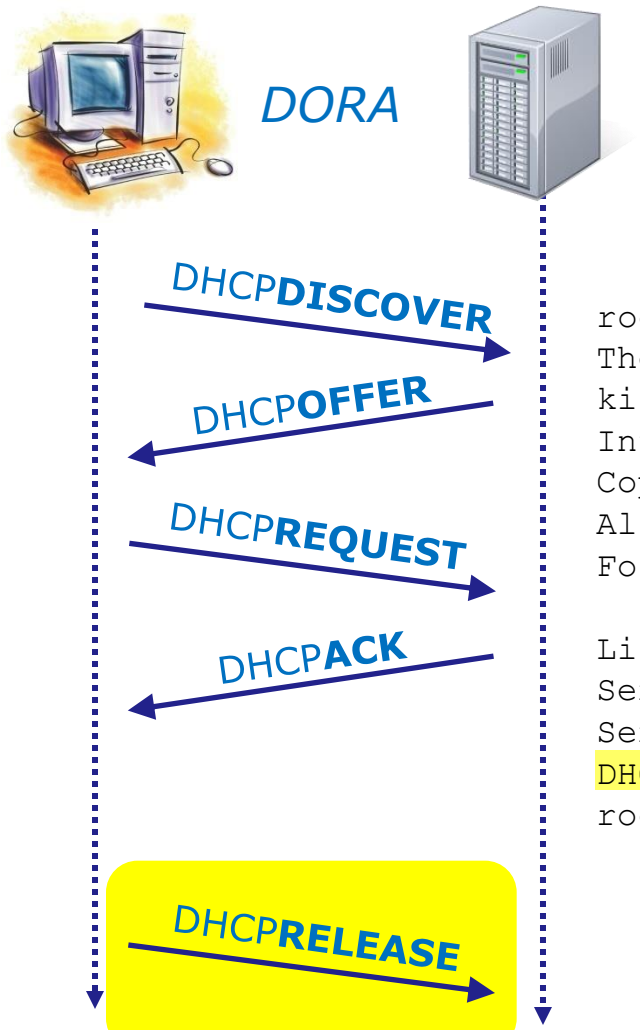


*The **dhclient** command illustrates the DORA steps*

```
root@frodo:~# dhclient -v eth0
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/00:0c:29:6f:53:d9
Sending on   LPF/eth0/00:0c:29:6f:53:d9
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
DHCPOFFER of 172.30.4.195 from 172.30.4.1
DHCPREQUEST of 172.30.4.195 on eth0 to 255.255.255.255 port 67
DHCPACK of 172.30.4.195 from 172.30.4.1
bound to 172.30.4.195 -- renewal in 9509 seconds.
root@frodo:~#
```

DHCP



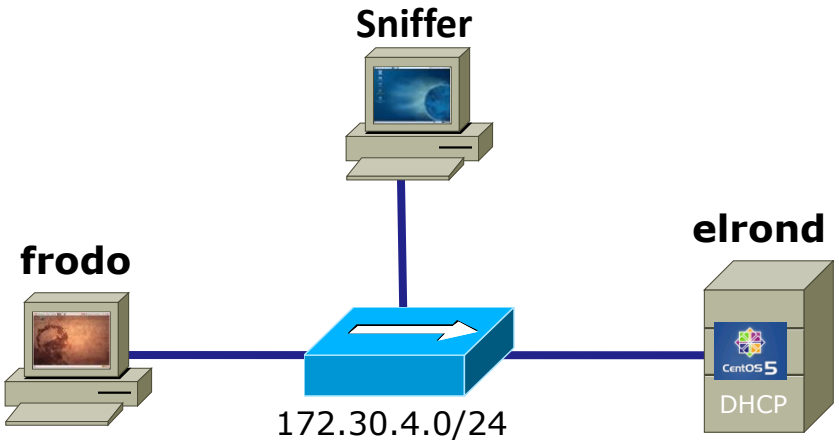
*The **dhclient –r** command does a DHCP release*

```
root@frodo:~# dhclient -v -r eth0
There is already a pid file /var/run/dhclient.pid with pid 9823
killed old client process, removed PID file
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/00:0c:29:6f:53:d9
Sending on   LPF/eth0/00:0c:29:6f:53:d9
Sending on   Socket/fallback
DHCPRELEASE on eth0 to 172.30.4.1 port 67
root@frodo:~#
```

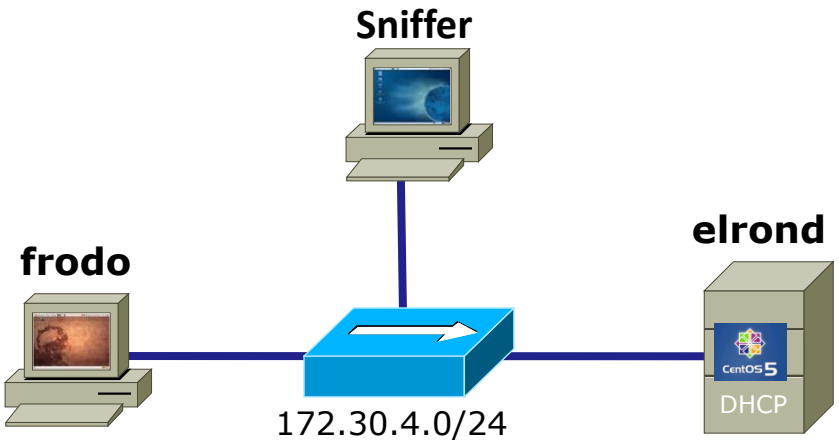
DHCP

Wireshark view of example DHCP operations



DHCP Client *DHCP Server*

Frodo starting up (needs IP address)



DHCP Client *DHCP Server*

frodo

*DHCP**DISCOVER***
(broadcast)

Hey, I need an IP address!

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

SIP	SP	DIP	DP	Protocol	Info
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Discover - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.1	67	172.30.4.195	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x222a860a

```
▷ Frame 4 (342 bytes on wire, 342 bytes captured)
▷ Ethernet II, Src: Vmware_6f:53:d9 (00:0c:29:6f:53:d9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
▷ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▽ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x222a860a
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
```

eth1: <live capture in progress> ... Packets: 135 Displayed: 5 Marked: 0 Profile: Default

UDP datagram is broadcast to port 67

Note the source IP = 0.0.0.0 because Frodo has no IP address!

frodo

*DHCP**DISCOVER***
(broadcast)

Hey, I need an IP address!

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

SIP	SP	DIP	DP	Protocol	Info
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Discover - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.1	67	172.30.4.195	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x222a860a

```
▷ Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 0.0.0.0 (0.0.0.0)
  Client MAC address: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
  Server host name not given
  Boot file name not given
  Magic cookie: (OK)
▷ Option: (t=53,l=1) DHCP Message Type = DHCP Discover
▷ Option: (t=12,l=5) Host Name = "frodo"
▷ Option: (t=55,l=11) Parameter Request List
  End Option
  Padding
```

Frodo sends its hostname

eth1: <live capture in progress> ... Packets: 135 Displayed: 5 Marked: 0 Profile: Default

frodo

*DHCP**DISCOVER** (broadcast)*

Hey, I need an IP address!

dhcp-frodo - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

SIP	SP	DIP	DP	Protocol	Info
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Discover - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.1	67	172.30.4.195	68	DHCP	DHCP Offer - Transaction ID 0x222a860a

```
Option: (t=55,l=11) Parameter Request List
    Option: (55) Parameter Request List
    Length: 11
    Value: 011C02030F06770C2C2F1A
    1 = Subnet Mask
    28 = Broadcast Address
    2 = Time Offset
    3 = Router
    15 = Domain Name
    6 = Domain Name Server
    119 = Domain Search
    12 = Host Name
    44 = NetBIOS over TCP/IP Name Server
    47 = NetBIOS over TCP/IP Scope
    26 = Interface MTU
```

Frame (frame), 342 bytes | Packets: 2400 Displayed: 35 Marked: 0 | Profile: Default

and a wish list of network configuration information it would like to get

elrond

*DHCP**OFFER***
(unicast)

Here is an IP address, want it?

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

SIP	SP	DIP	DP	Protocol	Info
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Discover - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.1	67	172.30.4.195	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x222a860a

```
▷ Frame 7 (342 bytes on wire, 342 bytes captured)
▷ Ethernet II, Src: Vmware_4e:21:9b (00:0c:29:4e:21:9b), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
▷ Internet Protocol, Src: 172.30.4.107 (172.30.4.107), Dst: 172.30.4.83 (172.30.4.83)
▷ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
▽ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x222a860a
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 172.30.4.83 (172.30.4.83)
```

eth1: <live capture in progress> ... Packets: 135 Displayed: 5 Marked: 0 Profile: Default

Offer of an IP address is sent to Frodo's MAC Address

elrond

*DHCP**OFFER***
(unicast)

Here is an IP address, want it?

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

SIP	SP	DIP	DP	Protocol	Info
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Discover - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.1	67	172.30.4.195	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x222a860a

```
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
  ▷ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
  ▷ Option: (t=54,l=4) Server Identifier = 172.30.4.107
  ▷ Option: (t=51,l=4) IP Address Lease Time = 6 hours
  ▷ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
  ▷ Option: (t=2,l=4) Time Offset = -7 hours
  ▷ Option: (t=3,l=4) Router = 192.168.2.107
  ▷ Option: (t=15,l=5) Domain Name = "shire"
  ▷ Option: (t=6,l=4) Domain Name Server = 207.62.187.54
```

eth1: <live capture in progress> ... Packets: 135 Displayed: 5 Marked: 0 Profile: Default

Additional network configuration is included in the offer

frodo

*DHCP**REQUEST***
(broadcast)

Yes, I want that one

eth1: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

SIP	SP	DIP	DP	Protocol	Info
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Discover - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.1	67	172.30.4.195	68	DHCP	DHCP Offer - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x222a860a

```
▷ Frame 8 (342 bytes on wire, 342 bytes captured)
▷ Ethernet II, Src: Vmware_6f:53:d9 (00:0c:29:6f:53:d9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▷ Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
▷ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▽ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x222a860a
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
```

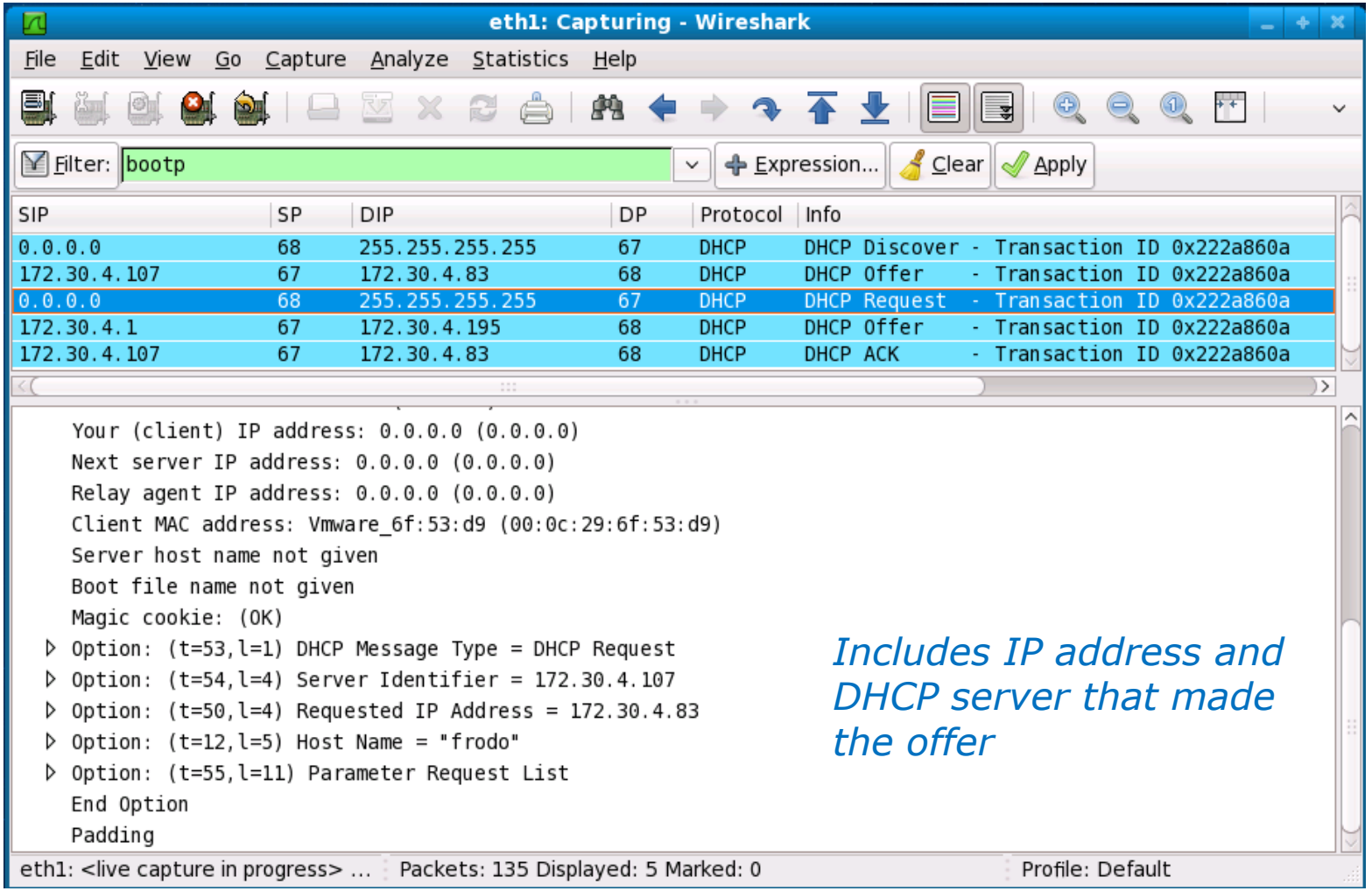
Request is broadcast back

eth1: <live capture in progress> ... Packets: 135 Displayed: 5 Marked: 0 Profile: Default

frodo

*DHCP**REQUEST** (broadcast)*

Yes, I want that one

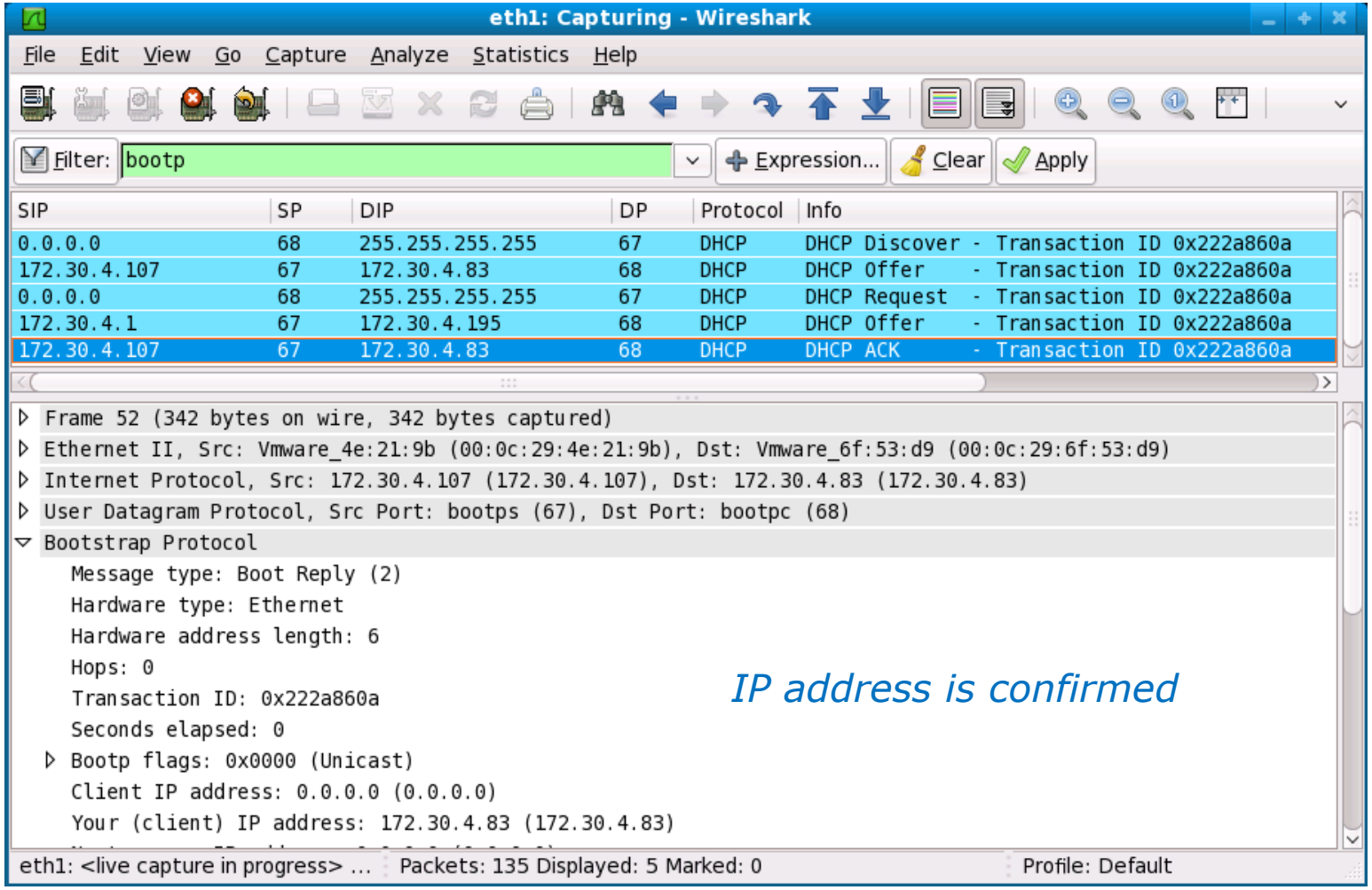


Includes IP address and DHCP server that made the offer

elrond

*DHCP**ACK***
(unicast)

You got it!

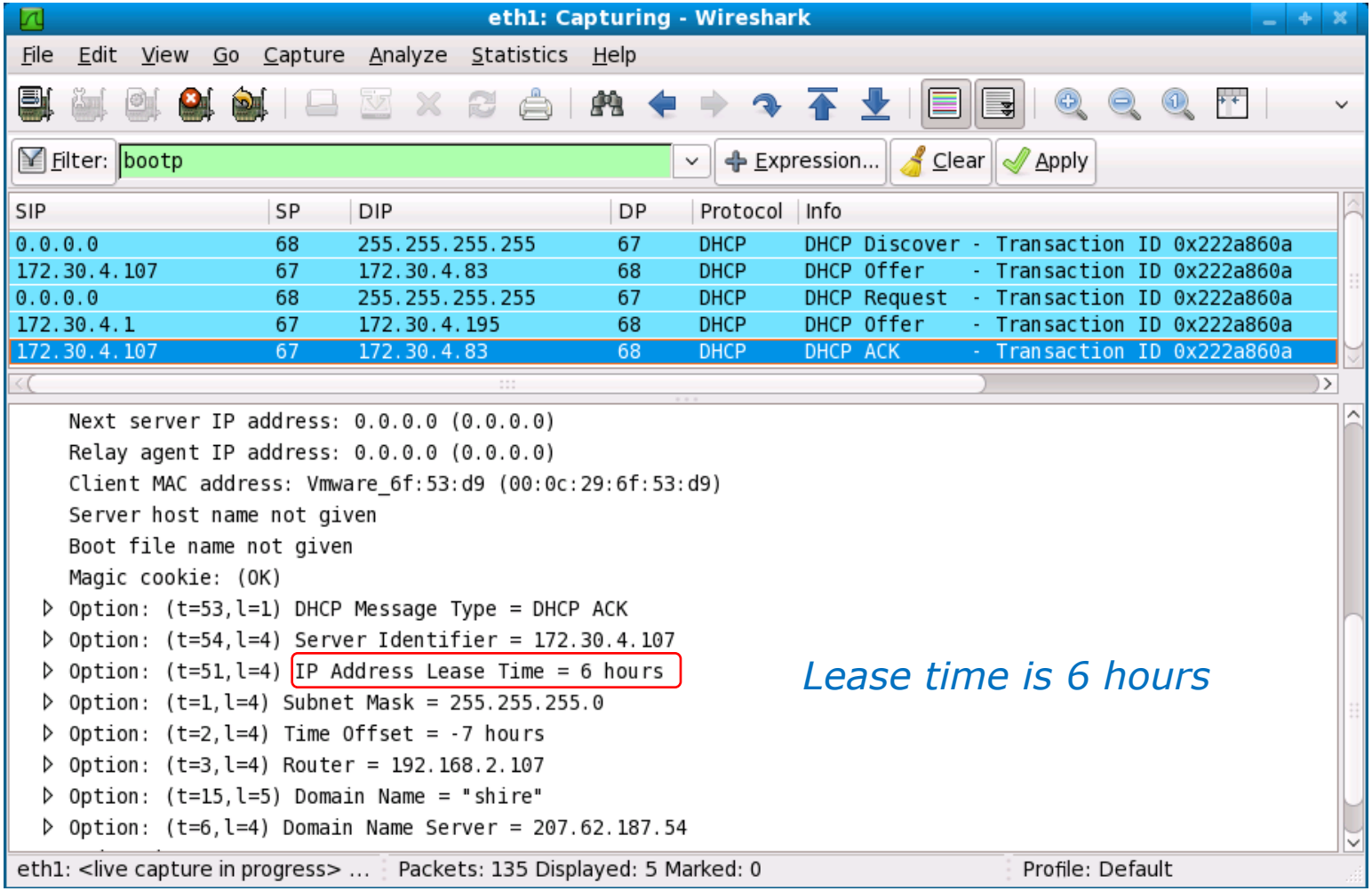


IP address is confirmed

elrond

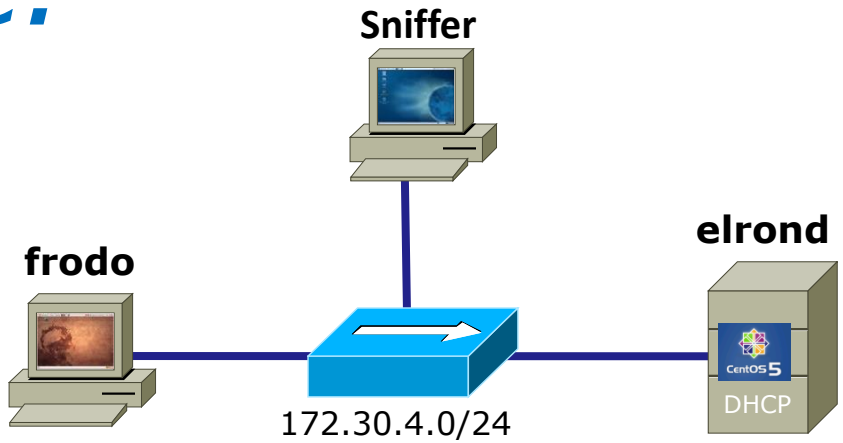
*DHCP**ACK***
(unicast)

You got it!



Lease time is 6 hours

Half of the lease time has expired. Frodo will attempt to renew the lease.



DHCP Client *DHCP Server*

frodo

*DHCP**REQUEST***
(unicast)

I want to renew the lease!

dhcp-frodo - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	68	172.30.4.107	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x222a860a
172.30.4.197	68	172.30.4.1	67	DHCP	DHCP Request - Transaction ID 0x2a2d5511
172.30.4.1	67	172.30.4.197	68	DHCP	DHCP ACK - Transaction ID 0x2a2d5511

```
▷ Frame 570 (342 bytes on wire, 342 bytes captured)
▷ Ethernet II, Src: Vmware_6f:53:d9 (00:0c:29:6f:53:d9), Dst: Vmware_4e:21:9b (00:0c:29:4e:21:9b)
▷ Internet Protocol, Src: 172.30.4.83 (172.30.4.83), Dst: 172.30.4.107 (172.30.4.107)
▷ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
▽ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x222a860a
    Seconds elapsed: 0
  ▷ Bootp flags: 0x0000 (Unicast)
    Client IP address: 172.30.4.83 (172.30.4.83)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
```

Request unicast to the DHCP server

IP address

File: "/dhcp-frodo" 379 KB 09:59:03 Packets: 2400 Displayed: 35 Marked: 0 Profile: Default

frodo

*DHCP**REQUEST***
(unicast)

I want to renew the lease!

dhcp-frodo - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	68	172.30.4.107	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x222a860a
172.30.4.197	68	172.30.4.1	67	DHCP	DHCP Request - Transaction ID 0x2a2d5511
172.30.4.1	67	172.30.4.197	68	DHCP	DHCP ACK - Transaction ID 0x2a2d5511

```
Option: (t=53,l=1) DHCP Message Type = DHCP Request
    Option: (53) DHCP Message Type
    Length: 1
    Value: 03
Option: (t=12,l=5) Host Name = "frodo"
    Option: (12) Host Name
    Length: 5
    Value: 66726F646F
Option: (t=55,l=11) Parameter Request List
    Option: (55) Parameter Request List
    Length: 11
    Value: 011C02030F06770C2C2F1A
    1 = Subnet Mask
    28 = Broadcast Address
    2 = Time Offset
```

File: "/dhcp-frodo" 379 KB 09:59:03 Packets: 2400 Displayed: 35 Marked: 0 Profile: Default

elrond

*DHCP**ACK***
(unicast)

You got it!

dhcp-frodo - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp | Expression... | Clear | Apply

SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	68	172.30.4.107	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x222a860a
172.30.4.197	68	172.30.4.1	67	DHCP	DHCP Request - Transaction ID 0x2a2d5511
172.30.4.1	67	172.30.4.197	68	DHCP	DHCP ACK - Transaction ID 0x2a2d5511

```
Frame 589 (342 bytes on wire, 342 bytes captured)
Ethernet II, Src: Vmware_4e:21:9b (00:0c:29:4e:21:9b), Dst: Vmware_6f:53:d9 (00:0c:29:6f:53:d9)
Internet Protocol, Src: 172.30.4.107 (172.30.4.107), Dst: 172.30.4.83 (172.30.4.83)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x222a860a
    Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
    Client IP address: 172.30.4.83 (172.30.4.83)
    Your (client) IP address: 172.30.4.83 (172.30.4.83)
    Next server IP address: 0.0.0.0 (0.0.0.0)
```

IP address is confirmed

File: "/dhcp-frodo" 379 KB 09:59:03 | Packets: 2400 Displayed: 35 Marked: 0 | Profile: Default

elrond

*DHCP**ACK***
(unicast)

You got it!

dhcp-frodo - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: bootp Expression... Clear Apply

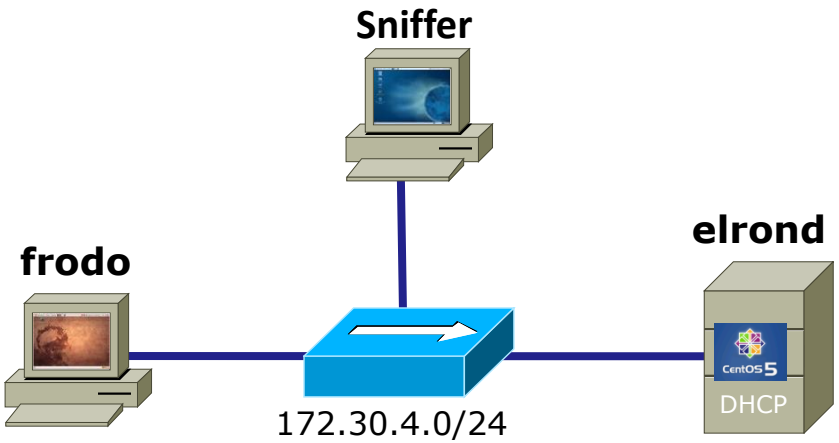
SIP	SP	DIP	DP	Protocol	Info
172.30.4.83	68	172.30.4.107	67	DHCP	DHCP Request - Transaction ID 0x222a860a
172.30.4.107	67	172.30.4.83	68	DHCP	DHCP ACK - Transaction ID 0x222a860a
172.30.4.197	68	172.30.4.1	67	DHCP	DHCP Request - Transaction ID 0x2a2d5511
172.30.4.1	67	172.30.4.197	68	DHCP	DHCP ACK - Transaction ID 0x2a2d5511

```
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
   Option: (53) DHCP Message Type
   Length: 1
   Value: 05
Option: (t=54,l=4) Server Identifier = 172.30.4.107
Option: (t=51,l=4) IP Address Lease Time = 6 hours
Option: (t=1,l=4) Subnet Mask = 255.255.255.0
Option: (t=2,l=4) Time Offset = -7 hours
Option: (t=3,l=4) Router = 192.168.2.107
Option: (t=15,l=5) Domain Name = "shire"
Option: (t=6,l=4) Domain Name Server = 207.62.187.54
End Option
Padding
```

Lease time is 6 hours

Frame (frame), 342 bytes | Packets: 2400 Displayed: 35 Marked: 0 | Profile: Default

Frodo is done and wants to end the lease

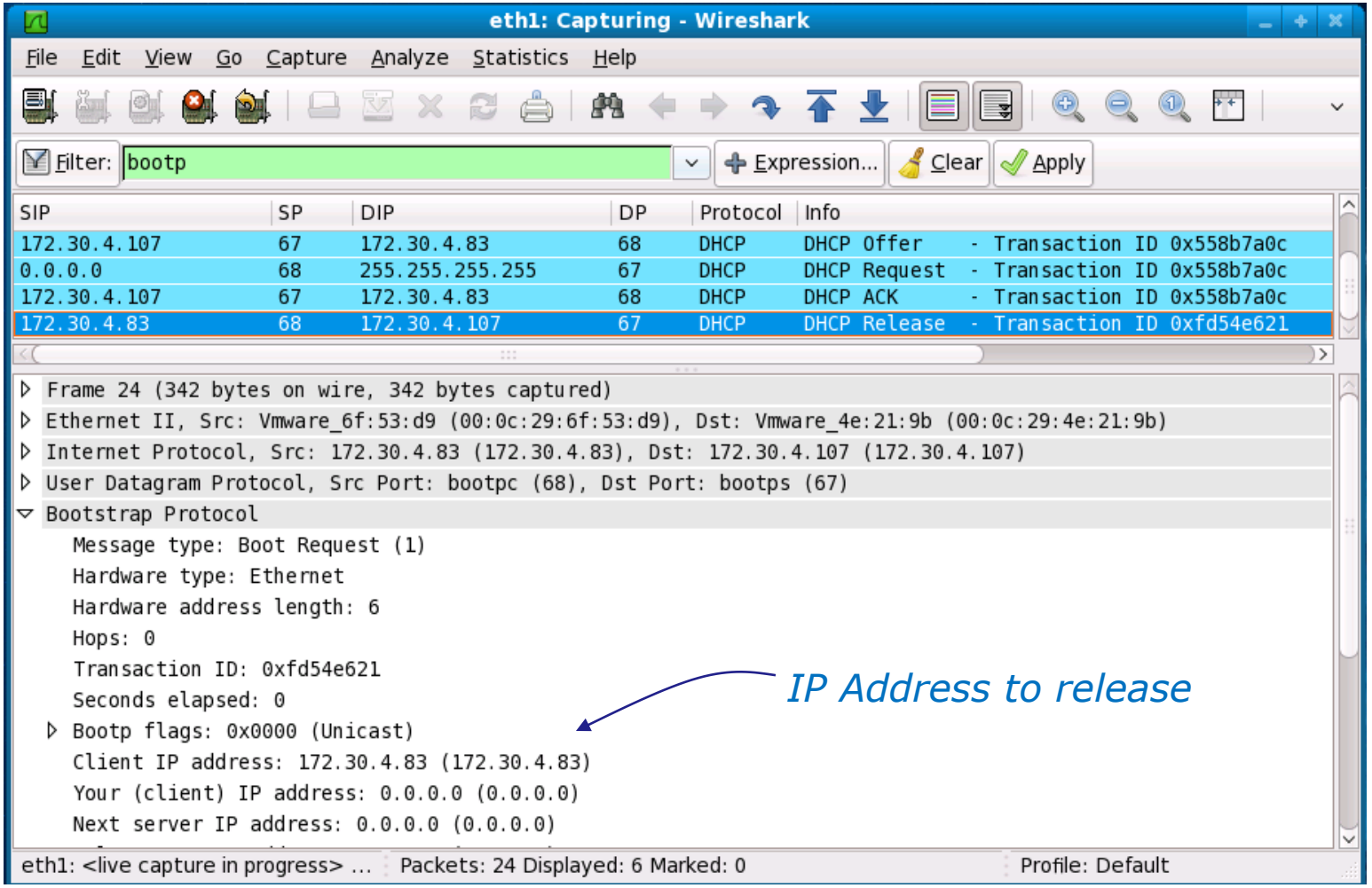


DHCP Client *DHCP Server*

frodo

*DHCP**RELEASE***
(unicast)

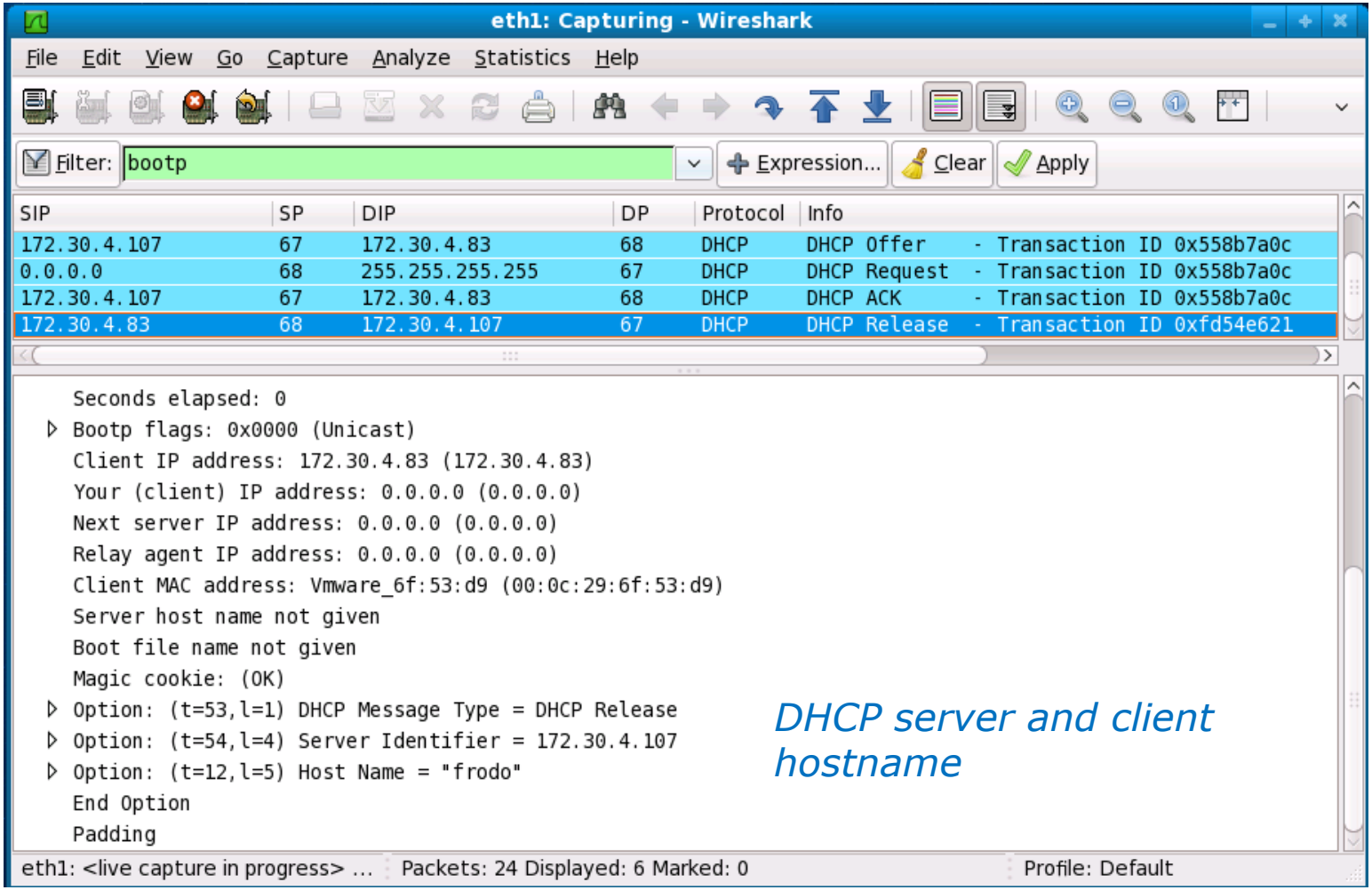
I want out!



frodo

*DHCP**RELEASE***
(unicast)

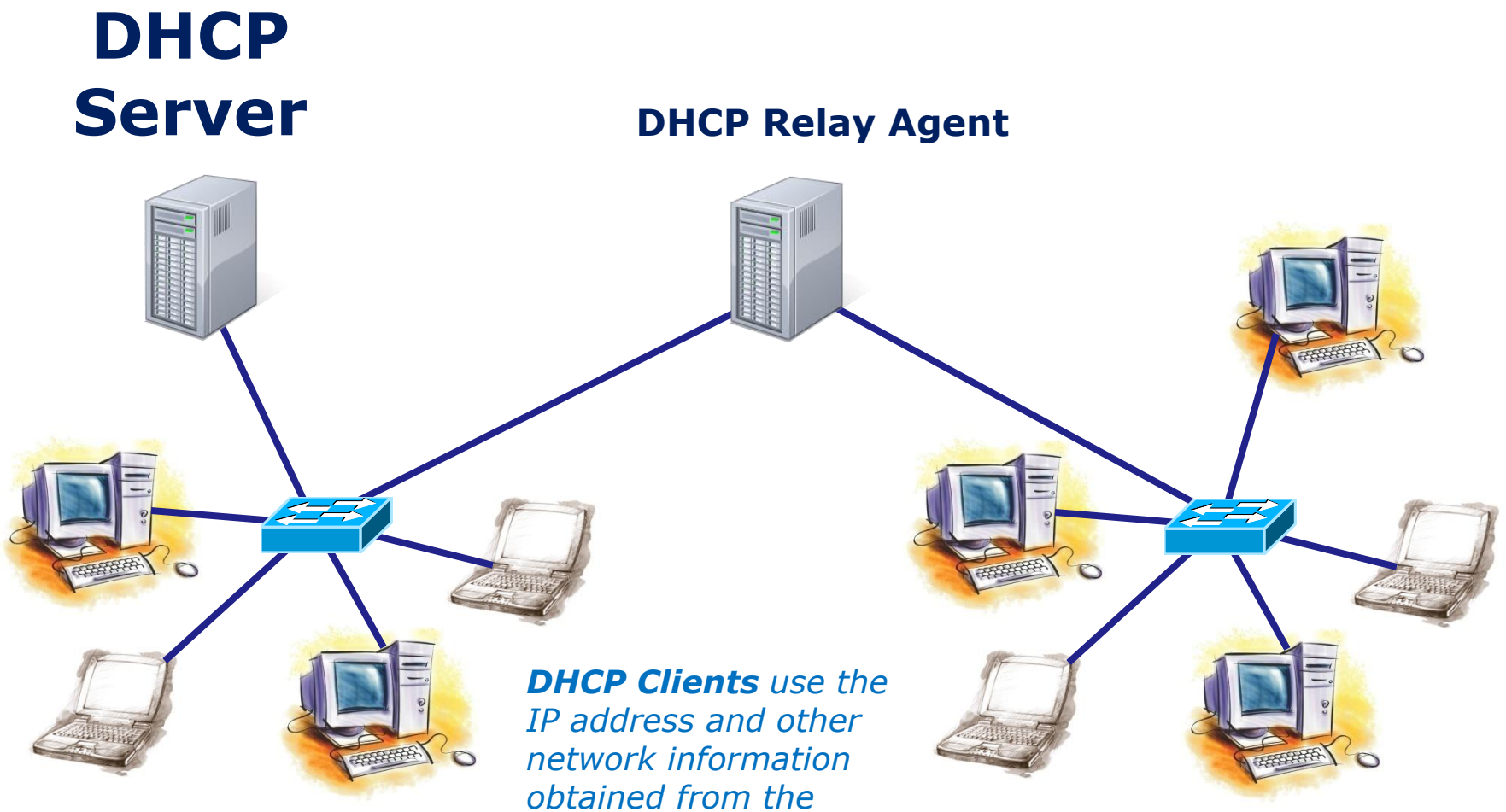
I want out!



DHCP server and client hostname

DHCP Client Configuration

DHCP



DHCP Clients *use the IP address and other network information obtained from the DHCP server to join a network automatically.*

DHCP

Temporary method to get DHCP IP and other configuration information

*Using **dhclient -v ethx** to get an IP address*

```
[root@legolas ~]# dhclient eth0
Internet Systems Consortium DHCP Client V3.0.5-RedHat
Copyright 2004-2006 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/00:0c:29:f9:1c:9c
Sending on   LPF/eth0/00:0c:29:f9:1c:9c
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 3
DHCPOFFER from 172.30.4.10
DHCPREQUEST on eth0 to 255.255.255.255 port 67
DHCPACK from 172.30.4.10
cp: cannot stat `/etc/resolv.conf': No such file or directory
bound to 172.30.4.155 -- renewal in 2804 seconds.
[root@legolas ~]# _
```

DHCP

Temporary method to get DHCP IP and other configuration information

*Using **dhclient -v -r ethx** to release an IP address*

```
[root@legolas ~]# dhclient -r
Internet Systems Consortium DHCP Client V3.0.5-RedHat
Copyright 2004-2006 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth1/00:0c:29:f9:1c:a6
Sending on   LPF/eth1/00:0c:29:f9:1c:a6
Listening on LPF/eth0/00:0c:29:f9:1c:9c
Sending on   LPF/eth0/00:0c:29:f9:1c:9c
Sending on   Socket/fallback
DHCPRELEASE on eth0 to 172.30.4.10 port 67
[root@legolas ~]# _
```

DHCP

Permanent method to configure DHCP on an interface

Ubuntu/Debian DHCP client example

```
root@frodo:~# cat /etc/network/interfaces
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

up route add -net 192.0.0.0/8 gw 172.30.4.107
root@frodo:~# /etc/init.d/networking restart
```

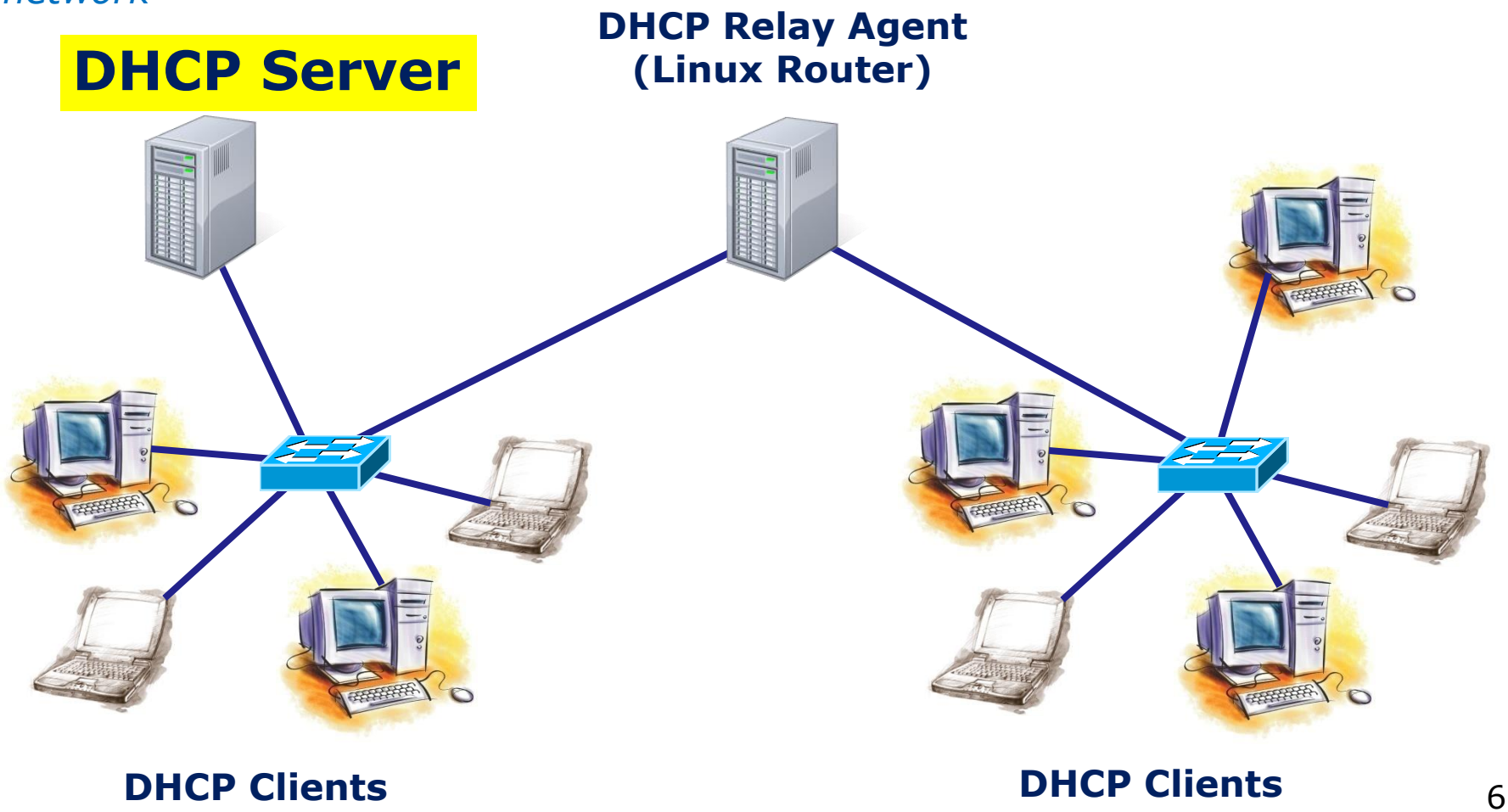
Red Hat Family DHCP client example

```
[root@legolas ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
# Advanced Micro Devices [AMD] 79c970 [PCnet32 LANCE]
DEVICE=eth0
HWADDR=00:0C:29:7C:18:F5
ONBOOT=yes
BOOTPROTO=dhcp
[root@legolas ~]# service network restart
```

DHCP Server Configuration

DHCP

DHCP Servers *provide IP addresses and other network configuration information to clients wanting to join a network*



Installing and Configuring DHCP server (ISC version on Red Hat Family)

DHCP

- Dynamic Host Configuration Protocol
- Client-server model
- Uses port 67 (for servers) and 68 (for clients)

DHCP uses bootp ports 67 and 68

```
[root@elrond ~]# cat /etc/services | grep bootp
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp          dhcpc           # BOOTP client
bootpc          68/udp          dhcpc
nuts_bootp      4133/tcp                        # NUTS Bootp Server
nuts_bootp      4133/udp                        # NUTS Bootp Server
[root@elrond ~]#
```

Application Layer

Steps to installing services

1. Install software package using **yum**, **rpm** or build from source code
2. Customize service's configuration file
3. Modify the firewall to allow access to the service
4. Customize SELinux context settings to allow use
5. Start the service
6. Configure service to automatically start when system boots
7. Monitor and verify service is running
8. Troubleshoot as necessary
9. Monitor log files as appropriate
10. Configure additional security

DHCP

DHCP installation and configuration

Step 1 • **yum install dhcp**

Step 2 • Edit /etc/dhcpd.conf
- see **man dhcpd.conf**
- See (CentOS) example in:
  /usr/share/doc/dhcp-*/dhcpd.conf.sample

Step 3 • Open port 67 to allow incoming DHCP requests

Step 4 • Leave SELinux as Enforcing

Step 5 • **service dhcpd start**

Step 6 • **chkconfig dhcpd on**

Step 7 • **service dhcpd status** and **netstat -uln**

Step 8 • Troubleshoot

Step 9 • Monitor log files:
  /var/lib/dhcpd/dhcpd.leases
  /var/log/messages | grep dhcp

DHCP

Is it already installed?

```
[root@p28-elrond ~]# rpm -qa | grep dhcp
dhcp-common-4.1.1-34.P1.el6.centos.x86_64   common files
dhcp-4.1.1-34.P1.el6.centos.x86_64   server
[root@p28-elrond ~]#
```

Is it already running?

```
[root@p28-elrond ~]# ps -ef | grep dhcpd
dhcpd     2127     1  0 10:38 ?        00:00:00 /usr/sbin/dhcpd -user dhcpd -group dhcpd
root      2194  1994  0 10:57 pts/0    00:00:00 grep dhcpd
```

```
[root@p28-elrond ~]# service dhcpd status
dhcpd (pid  2127) is running...
[root@p28-elrond ~]#
```

DHCP installation and configuration

Step 1 Install software package

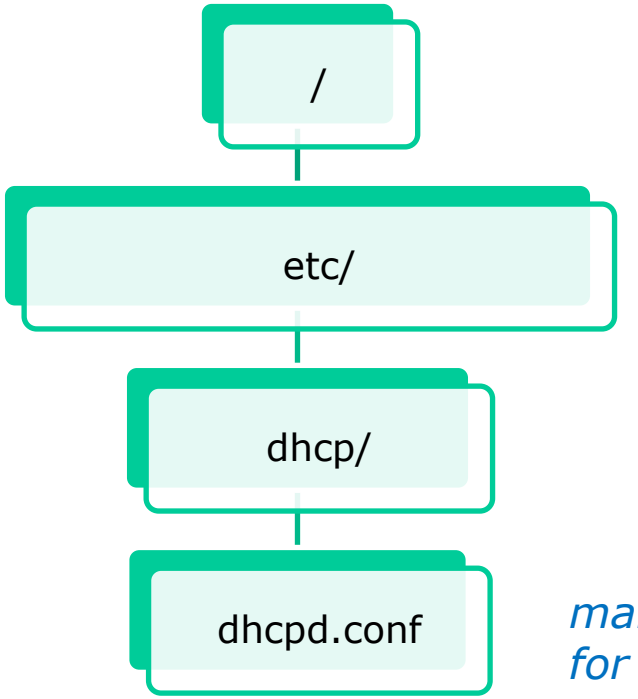
If connected to the Internet
yum install dhcp

If using CD with RPM files

```
[root@p28-legolas ~]# mount  /dev/cdrom /media
mount: block device /dev/sr0 is write-protected, mounting read-only
[root@p28-legolas ~]# cd /media/Packages/
[root@p28-legolas Packages]# rpm -hiv dhcp*
Preparing...                ########################################### [100%]
   1:dhcp-common            ########################################### [ 50%]
   2:dhcp                   ########################################### [100%]
[root@p28-legolas Packages]#
```

Configuring dhcpd

Step 2 *Customize the configuration file*



main configuration file for dhcpd

dhcpd.conf
sample walkthrough

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

Global settings

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

Subnet specific settings

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

DHCP options that can be assigned to clients

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

Which method to use to dynamically update the DNS (Ad-hoc or interim)

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

Either allow or ignore the clients intention to update its own DNS A record

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

Subnet specific settings.
Everything enclosed within the { } applies to just this specific subnet.

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

Default gateway to assign for this subnet

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

Default netmask to assign for this subnet

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

domain names to assign. NIS is a UNIX only domain used within an organization. DNS supports all OS's and spans the Internet

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

The DNS server to assign

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

Offset in seconds from GMT

-18000 = 5 hours (EST)
-25200 = 7 hours (PDT)
-28800 = 8 hours (PST)

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

Pool of IP addresses to assign

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

A client can request a length of time for the lease. If not specified this is how long the lease will be for.

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

The maximum amount of time that can be requested for a lease.

```
[root@elrond ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;

subnet 192.168.0.0 netmask 255.255.255.0 {

# --- default gateway
        option routers                  192.168.0.1;
        option subnet-mask              255.255.255.0;

        option nis-domain               "domain.org";
        option domain-name              "domain.org";
        option domain-name-servers      192.168.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
#       option netbios-node-type 2;

        range dynamic-bootp 192.168.0.128 192.168.0.254;
        default-lease-time 21600;
        max-lease-time 43200;

        # we want the nameserver to appear at a fixed address
        host ns {
                next-server marvin.redhat.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 207.175.42.254;
        }
}
[root@elrond ~]#
```

IP reservation based on MAC address

dhcpd.conf
for
the DHCP lab
(old)

elrond

DHCP

Global and specific settings for DHCP Lab Rivendell subnet

```
[root@elrond ~]# cat /etc/dhcpd.conf
ddns-update-style interim;
ignore client-updates;
option time-offset              -25200;  # Pacific Daylight Time (-7 HR)

#
#   R I V E N D E L L
#
subnet 192.168.2.0 netmask 255.255.255.0 {
        option routers                  192.168.2.1; # Default GW
        option subnet-mask              255.255.255.0;
        option domain-name              "rivendell";
        option domain-name-servers      207.62.187.53;

        range dynamic-bootp             192.168.2.50 192.168.2.99;
        default-lease-time              21600; # 6 hours
        max-lease-time                  43200; # 12 hours

        # reservations
        host legolas {
                hardware ethernet       00:0C:29:7C:18:F5;
                fixed-address           192.168.2.150;
        }
}
```

Will be the eth1 interface on your station's Elrond

DHCP

elrond

Settings for DHCP Lab Mordor subnet in /etc/dhcpd.conf

```
#
#   M O R D O R
#
subnet 192.168.3.0 netmask 255.255.255.0 {
        option routers                  192.168.3.150; # Default GW
        option subnet-mask              255.255.255.0;
        option domain-name              "mordor";
        option domain-name-servers      207.62.187.53;

        range dynamic-bootp             192.168.3.50 192.168.3.99;
        default-lease-time              21600; # 6 hours
        max-lease-time                  43200; # 12 hours
}
```

DHCP

elrond

Settings for DHCP Lab Shire subnet in /etc/dhcpd.conf

```
#
#   S H I R E
#
subnet 172.30.4.0 netmask 255.255.255.0 {
        option routers                  172.30.N.1;
        option subnet-mask              255.255.255.0;
        option domain-name              "shire";
        option domain-name-servers      207.62.187.53;

        range dynamic-bootp             172.30.N.80 172.30.N.84;
        default-lease-time              21600;
        max-lease-time                  43200;
}
[root@elrond ~]#
```

N=1 for the classroom and N=4 for the lab

Use the pool of addresses based on your station number to avoid conflicts!

dhcpd.conf
for
the DHCP lab
(newer)

elrond

DHCP

/etc/dhcp/dhcpd.conf for DHCP Lab

Global and specific settings for CIS Lab subnet

```
[root@elrond ~]# cat /etc/dhcp/dhcpd.conf
# Global declarations for Lab 06
option domain-name-servers 192.168.0.8, 10.240.1.2;
default-lease-time 3600;
max-lease-time 7200;
ddns-update-style none;

# Scope: CIS Lab network
subnet 172.30.4.0 netmask 255.255.255.0 {
  range 172.30.4.50 172.30.4.54;
  option domain-name "cisvlab.net";
  option routers 172.30.4.1;
}
```

Use the pool of addresses based on your station/pod number to avoid conflicts!

DHCP

/etc/dhcp/dhcpd.conf for DHCP Lab

elrond

Settings for Rivendell and Mordor subnets

```
# Scope: Rivendell network
subnet 192.168.2.0 netmask 255.255.255.0 {
  range 192.168.2.50 192.168.2.99;
  option domain-name "Rivendell";
  option routers 192.168.2.1;
  authoritative;

  host legolas {
    hardware ethernet 00:0c:29:1f:b1:48;
    fixed-address 192.168.2.150;
  }
}

# Scope: Mordor network
subnet 192.168.3.0 netmask 255.255.255.0 {
  range 192.168.3.50 192.168.3.99;
  option domain-name "Mordor";
  option routers 192.168.3.150;
  authoritative;
}
```

dhcpd.conf
for
the DHCP lab
(latest)

elrond

DHCP

/etc/dhcp/dhcpd.conf for DHCP Lab

Global and specific settings for CIS Lab subnet

```
[root@elrond ~]# cat /etc/dhcp/dhcpd.conf
# Global declarations for Lab 06
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;

# Scope: CIS Lab network
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 "cislab.net";

  range 172.20.192.198 172.20.192.202;
}
```

Use the pool of addresses based on your station/pod number to avoid conflicts!

DHCP

/etc/dhcp/dhcpd.conf for DHCP Lab

elrond

Settings for Rivendell subnet

```
# Scope: Rivendell network
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 "cislab.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;
  }
}
```

Note: pod number in red

DHCP

/etc/dhcp/dhcpd.conf for DHCP Lab

elrond

Settings for Mordor subnet

```
# Scope: Mordor network
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 "cislab.net";

  range 192.168.228.50 192.168.228.99;
}
```

Note: pod number in red

Installing and Configuring DHCP

Step 3 *Configure firewall*

Open UDP port 67 as a destination
iptables -I INPUT 4 -p udp -m udp --dport 67 -j ACCEPT

for default CentOS firewall

To make the firewall settings permanent
service iptables save

To backup current firewall settings to another file
iptables-save > /etc/sysconfig/iptables.lab06

Installing and Configuring DHCP

Step 3 *Configure firewall to open port 67*

```
[root@p28-elrond ~]# iptables -nL --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
4    ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:67
5    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
6    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
[root@p28-elrond ~]#
```

SELinux for DHCP (CentOS)

Step 4 *Configure SELinux*

```
[root@p28-elrond ~]# getenforce
Enforcing
```

No changes needed, leave as Enforcing

Installing and Configuring DHCP server (Red Hat Family)

Step 5 *Start or restart service*

```
[root@elrond ~]# service dhcpd start
Starting dhcpd:                                            [  OK  ]
```

Step 6 *Automatically start at system boot*

```
[root@elrond ~]# chkconfig dhcpd on

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

DHCP

Step 7 *Verify service is running*

```
[root@p28-elrond ~]# ps -ef | grep dhcpd
dhcpd     2127     1  0 10:38 ?        00:00:00 /usr/sbin/dhcpd -user dhcpd -group dhcpd
root      2222  1994  0 11:12 pts/0    00:00:00 grep dhcpd

[root@p28-elrond ~]# service dhcpd status
dhcpd (pid  2127) is running...

[root@p28-elrond ~]# netstat -uln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
udp        0      0 0.0.0.0:713                 0.0.0.0:*
udp        0      0 0.0.0.0:111                 0.0.0.0:*
udp        0      0 0.0.0.0:41209               0.0.0.0:*
udp        0      0 0.0.0.0:694                 0.0.0.0:*
udp        0      0 0.0.0.0:67                  0.0.0.0:*
udp        0      0 :::111                      :::*
udp        0      0 :::38015                    :::*
udp        0      0 :::694                      :::*
```

Installing and Configuring DHCP server

Step 8 Troubleshooting

Check layer 1 (cabling)
Check layer 2 (arp -n)
Check layer 3 (ifconfig and route –n)
Check that DHCP service is running
Check /etc/dhcpd.conf settings
Check firewall settings
Check client DHCP settings
Use Wireshark/tcpdump to observe DORA

```
[root@p28-elrond ~]# tcpdump -nv -i eth1 port 67
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 65535 bytes
11:25:42.579110 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 328)
    192.168.128.150.bootps > 192.168.128.1.bootps: BOOTP/DHCP, Request from 00:50:56:b7:ff:11, length 300, hops 1, x id 0x67886216, Flags [none]
          Gateway-IP 192.168.228.150
          Client-Ethernet-Address 00:50:56:b7:ff:11
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
            DHCP-Message Option 53, length 1: Discover
            Requested-IP Option 50, length 4: 192.168.228.50
            Hostname Option 12, length 10: "p28-sauron"
            Parameter-Request Option 55, length 13:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
              NTP
11:25:42.579337 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 328)
    192.168.128.1.bootps > 192.168.228.150.bootps: BOOTP/DHCP, Reply, length 300, hops 1, xid 0x67886216, Flags [non e]
          Your-IP 192.168.228.50
          Gateway-IP 192.168.228.150
          Client-Ethernet-Address 00:50:56:b7:ff:11
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
                    DHCP-Message Option 53, length 1: Offer
            Server-ID Option 54, length 4: 192.168.128.1
            Lease-Time Option 51, length 4: 3600
            Subnet-Mask Option 1, length 4: 255.255.255.0
            Default-Gateway Option 3, length 4: 192.168.228.150
            Domain-Name Option 15, length 6: "mordor"
            Domain-Name-Server Option 6, length 8: 172.30.5.8,10.240.1.2
            T119 Option 119, length 12: 107178355,1818321411,1852142592
11:25:42.581276 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 328)
    192.168.128.150.bootps > 192.168.128.1.bootps: BOOTP/DHCP, Request from 00:50:56:b7:ff:11, length 300, hops 1, x id 0x67886216, Flags [none]
          Gateway-IP 192.168.228.150
          Client-Ethernet-Address 00:50:56:b7:ff:11
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
                    DHCP-Message Option 53, length 1: Request
            Server-ID Option 54, length 4: 192.168.128.1
            Requested-IP Option 50, length 4: 192.168.228.50
            Hostname Option 12, length 10: "p28-sauron"
            Parameter-Request Option 55, length 13:
              Subnet-Mask, BR, Time-Zone, Default-Gateway
              Domain-Name, Domain-Name-Server, Option 119, Hostname
              Netbios-Name-Server, Netbios-Scope, MTU, Classless-Static-Route
              NTP
11:25:42.583523 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 328)
    192.168.128.1.bootps > 192.168.228.150.bootps: BOOTP/DHCP, Reply, length 300, hops 1, xid 0x67886216, Flags [non e]
          Your-IP 192.168.228.50
          Gateway-IP 192.168.228.150
          Client-Ethernet-Address 00:50:56:b7:ff:11
          Vendor-rfc1048 Extensions
            Magic Cookie 0x63825363
                    DHCP-Message Option 53, length 1: ACK
            Server-ID Option 54, length 4: 192.168.128.1
            Lease-Time Option 51, length 4: 3600
            Subnet-Mask Option 1, length 4: 255.255.255.0
            Default-Gateway Option 3, length 4: 192.168.228.150
            Domain-Name Option 15, length 6: "mordor"
            Domain-Name-Server Option 6, length 8: 172.30.5.8,10.240.1.2
            T119 Option 119, length 12: 107178355,1818321411,1852142592
```

Meet our new friend DORA using tcpdump

-n = no DNS lookups

-v = verbose

This is Sauron requesting an IP address

Installing and Configuring vsftpd

Step 9 Monitor log files

```
[root@arwen ~]# tail /var/log/messages | grep dhcp
Mar 26 11:33:21 p28-elrond dhcpd: Internet Systems Consortium DHCP Server 4.1.1-P1
Mar 26 11:33:21 p28-elrond dhcpd: Copyright 2004-2010 Internet Systems Consortium.
Mar 26 11:33:21 p28-elrond dhcpd: All rights reserved.
Mar 26 11:33:21 p28-elrond dhcpd: For info, please visit https://www.isc.org/software/dhcp/
Mar 26 11:33:21 p28-elrond dhcpd: WARNING: Host declarations are global.  They are not limited to the scope you
declared them in.
Mar 26 11:33:21 p28-elrond dhcpd: Not searching LDAP since ldap-server, ldap-port and ldap-base-dn were not
specified in the config file
Mar 26 11:33:21 p28-elrond dhcpd: Wrote 0 deleted host decls to leases file.
Mar 26 11:33:21 p28-elrond dhcpd: Wrote 0 new dynamic host decls to leases file.
Mar 26 11:33:21 p28-elrond dhcpd: Wrote 8 leases to leases file.
Mar 26 11:33:21 p28-elrond dhcpd: Listening on LPF/eth1/00:50:56:b7:80:a2/192.168.128.0/24
Mar 26 11:33:21 p28-elrond dhcpd: Sending on   LPF/eth1/00:50:56:b7:80:a2/192.168.128.0/24
Mar 26 11:33:21 p28-elrond dhcpd: Listening on LPF/eth0/00:50:56:b7:8e:8d/172.20.0.0/16
Mar 26 11:33:21 p28-elrond dhcpd: Sending on   LPF/eth0/00:50:56:b7:8e:8d/172.20.0.0/16
Mar 26 11:33:21 p28-elrond dhcpd: Sending on   Socket/fallback/fallback-net
```

The dhcpd service is restarted

Installing and Configuring vsftpd

Step 9 Monitor log files

```
[root@arwen ~]# tail /var/log/messages | grep dhcp
Mar 26 11:39:13 p28-elrond dhcpd: DHCPRELEASE of 192.168.228.50 from 00:50:56:b7:ff:11 (p28-sauron)
via eth1 (found)
Mar 26 11:39:13 p28-elrond dhcpd: DHCPRELEASE of 192.168.228.50 from 00:50:56:b7:ff:11 via
192.168.228.150 (found)
Mar 26 11:39:13 p28-elrond dhcpd: DHCPRELEASE of 192.168.228.50 from 00:50:56:b7:ff:11 via
192.168.128.150 (found)
Mar 26 11:39:16 p28-elrond dhcpd: DHCPDISCOVER from 00:50:56:b7:ff:11 via 192.168.228.150
Mar 26 11:39:17 p28-elrond dhcpd: DHCPOFFER on 192.168.228.50 to 00:50:56:b7:ff:11 (p28-sauron) via
192.168.228.150
Mar 26 11:39:17 p28-elrond dhcpd: DHCPREQUEST for 192.168.228.50 (192.168.128.1) from
00:50:56:b7:ff:11 (p28-sauron) via 192.168.228.150
Mar 26 11:39:17 p28-elrond dhcpd: DHCPACK on 192.168.228.50 to 00:50:56:b7:ff:11 (p28-sauron) via
192.168.228.150
```

*Sauron releases its IP address (**dhclient -v -r eth0**)*
*then requests an IP address (**dhclient -v eth0**)*

Installing and Configuring vsftpd

Step 9 Monitor log files

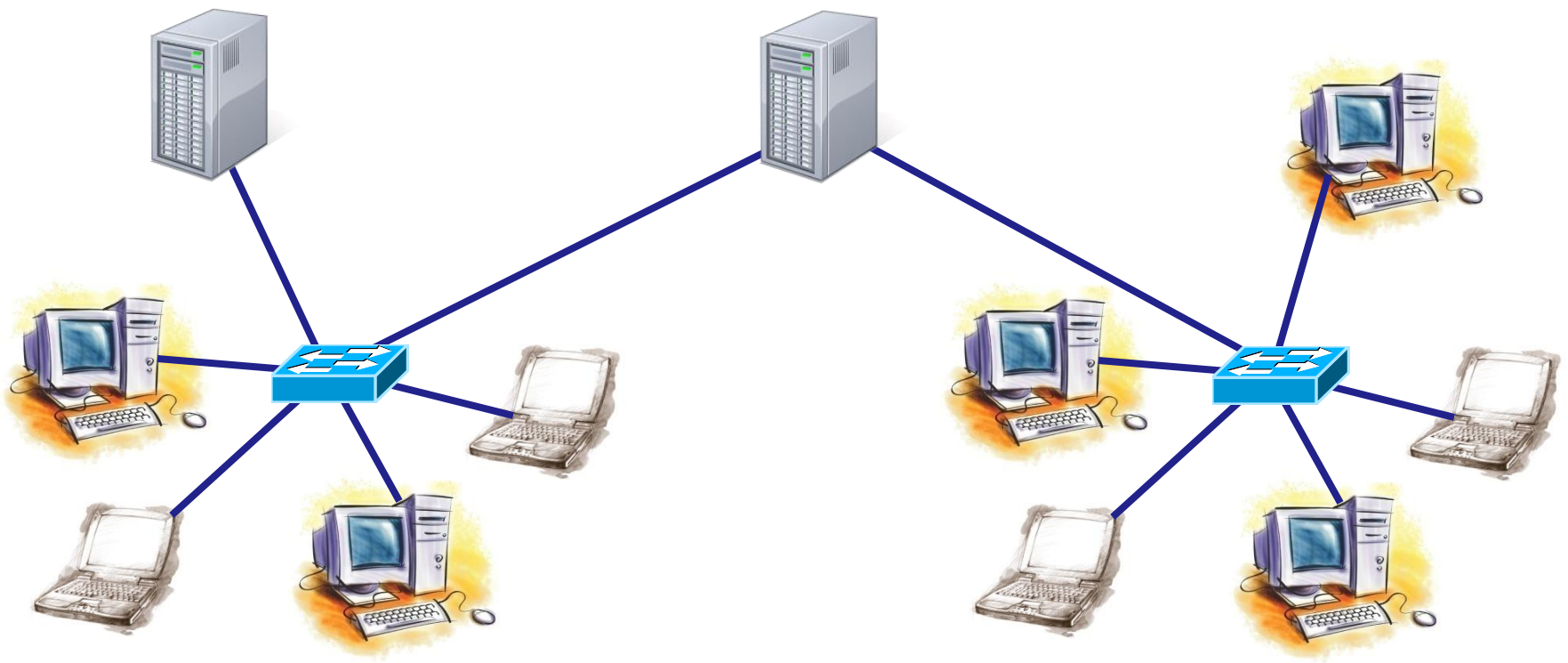
```
[root@arwen ~]# tail /var/log/messages | grep dhcp
Mar 26 11:35:19 p28-elrond dhcpd: DHCPRELEASE of 192.168.128.50 from 00:50:56:b7:e2:d6 (p28-william)
via eth1 (found)
Mar 26 11:35:26 p28-elrond dhcpd: DHCPDISCOVER from 00:50:56:b7:e2:d6 via eth1
Mar 26 11:35:27 p28-elrond dhcpd: DHCPOFFER on 192.168.128.50 to 00:50:56:b7:e2:d6 (p28-william) via
eth1
Mar 26 11:35:27 p28-elrond dhcpd: DHCPREQUEST for 192.168.128.50 (192.168.128.1) from
00:50:56:b7:e2:d6 (p28-william) via eth1
Mar 26 11:35:27 p28-elrond dhcpd: DHCPACK on 192.168.128.50 to 00:50:56:b7:e2:d6 (p28-william) via
eth1
Mar 26 11:35:27 p28-elrond dhcpd: DHCPREQUEST for 192.168.128.50 (192.168.128.1) from
00:50:56:b7:e2:d6 (p28-william) via 192.168.128.150
Mar 26 11:35:27 p28-elrond dhcpd: DHCPACK on 192.168.128.50 to 00:50:56:b7:e2:d6 (p28-william) via
192.168.128.150
```

*William releases (using **ipconfig /release**) then renews (with **ipconfig /renew**)*

dhcrelay

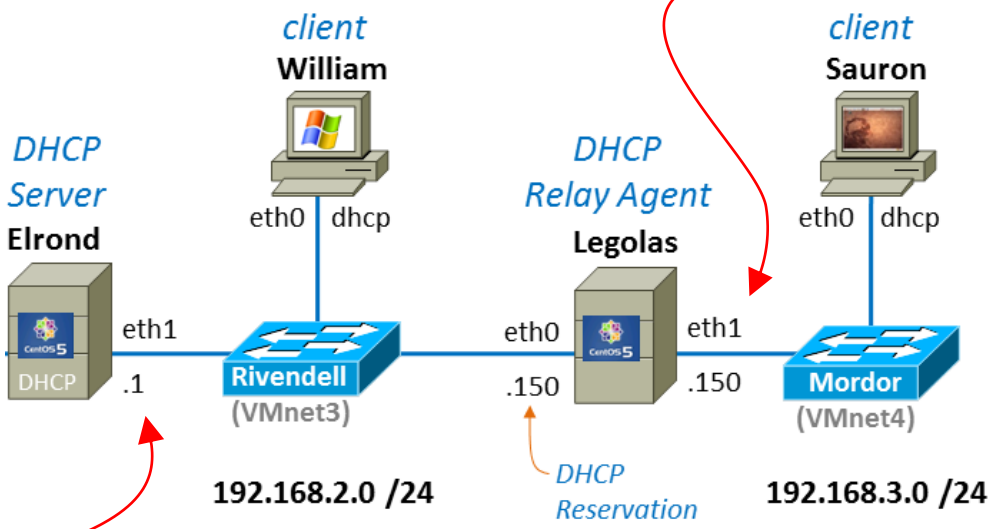
DHCP

The relay agent allows a DHCP server to service non-connected networks



DORA via DHCP Relay

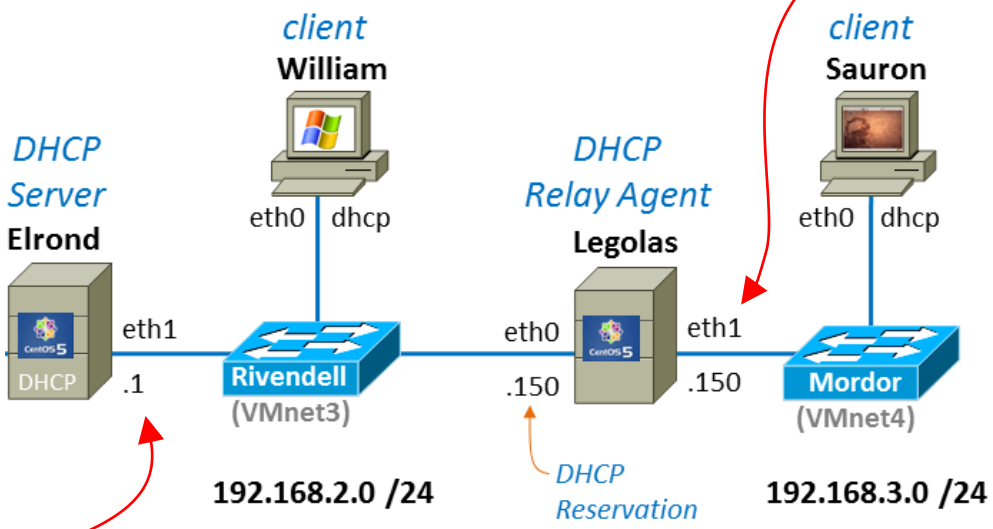
Source	SP	Destination	DP	Protocol	Info
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Discover - Transaction ID 0xad210e79
192.168.3.150	67	192.168.3.50	68	DHCP	DHCP Offer - Transaction ID 0xad210e79
0.0.0.0	68	255.255.255.255	67	DHCP	DHCP Request - Transaction ID 0xad210e79
192.168.3.150	67	192.168.3.50	68	DHCP	DHCP ACK - Transaction ID 0xad210e79



Source	SP	Destination	DP	Protocol	Info
192.168.2.150	67	192.168.2.1	67	DHCP	DHCP Discover - Transaction ID 0xad210e79
192.168.2.1	67	192.168.3.150	67	DHCP	DHCP Offer - Transaction ID 0xad210e79
192.168.2.150	67	192.168.2.1	67	DHCP	DHCP Request - Transaction ID 0xad210e79
192.168.2.1	67	192.168.3.150	67	DHCP	DHCP ACK - Transaction ID 0xad210e79

Release via DHCP Relay

Source	SP	Destination	DP	Protocol	Info
192.168.3.50	68	192.168.2.1	67	DHCP	DHCP Release - Transaction ID 0xbba8b329



Source	SP	Destination	DP	Protocol	Info
192.168.3.50	68	192.168.2.1	67	DHCP	DHCP Release - Transaction ID 0xbba8b329
192.168.2.150	67	192.168.2.1	67	DHCP	DHCP Release - Transaction ID 0xbba8b329
192.168.2.150	67	192.168.2.1	67	DHCP	DHCP Release - Transaction ID 0xbba8b329

DHCP

DHCP Architecture

DHCP Servers

- Scopes and exclusions
- Reservations
- Leases
- Options
  - IP Address and Netmask
  - Gateway
  - DNS Server
  - Domain name
  - others

DHCP Relay Agents

DHCP Clients

DHCP Relay Agents *lets one DHCP server service multiple non-connected subnets*

DHCP Relay Agent

DHCP Relay Agent installation and configuration

Step 1 • **yum install dhcp**

Step 2 • Edit /etc/sysconfig/dhcrelay
  • For details use **man dhcrelay**

Step 3 • Open port 67 to allow DHCP requests

Step 4 • Leave SELinux as Enforcing

Step 5 • **service dhcrelay start**

Step 6 • **chkconfig dhcrelay on**

Step 7 • **service dhcrelay status** and **netstat -uln**

Step 8 • Troubleshoot

Step 9 • Monitor log files:

DHCP Relay Agent

legolas

Is it installed?

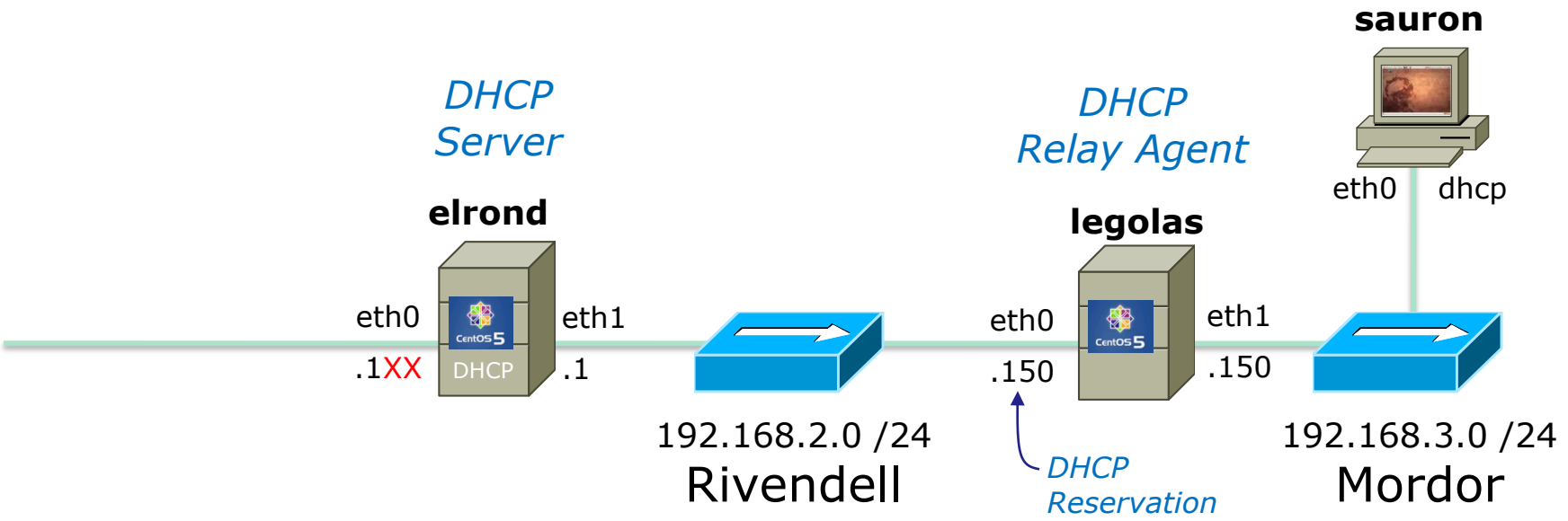
```
[root@legolas ~]# rpm -qa | grep dhcp
dhcp-3.0.5-13.el5
dhcpv6-client-1.0.10-4.el5_2.3
```

Is it running?

```
[root@legolas ~]# ps -ef | grep dhc
root      5250     1  0 16:57 ?     00:00:00 dhclient eth0
root      9614     1  0 19:13 ?     00:00:00 /usr/sbin/dhcrelay -i eth0 -i eth1 192.168.2.107
root     10015  9925  0 19:19 pts/0 00:00:00 grep dhc
[root@legolas ~]#

[root@legolas ~]# service dhcrelay status
dhcrelay (pid 9614) is running...
[root@legolas ~]#
```

DHCP Relay Agent



Step 2 *Edit configuration file*

```
[root@legolas ~]# cat /etc/sysconfig/dhcrelay
# Command line options here
INTERFACES="eth0 eth1"
DHCPSERVERS="192.168.2.1"
```

Must monitor interface that listens for new clients needing DHCP services as well as the interface that communicates to the DHCP server

Installing and Configuring DHCP relay agent

Step 3 *Configure firewall*

Open UDP port 67 as a destination
iptables -I INPUT 4 -p udp -m udp --dport 67 -j ACCEPT

To make the firewall settings permanent
service iptables save

To backup current firewall settings to another file
iptables-save > /etc/sysconfig/iptables.lab06

SELinux for DHCP relay agent (CentOS)

Step 4 *Configure SELinux*

```
[root@p28-elrond ~]# getenforce
Enforcing
```

No changes needed, leave as Enforcing

Installing and Configuring DHCP relay agent (Red Hat Family)

Step 5 *Start or restart service*

```
[root@elrond ~]# service dhcrelay start
Starting dhcrelay:                                         [  OK  ]
[root@elrond ~]#
```

Step 6 *Automatically start at system boot*

```
[root@elrond ~]# chkconfig dhcrelay on

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

DHCP relay agent

Step 7 *Verify service is running*

```
[root@elrond ~]# ps -ef | grep dhcrelay
root     11302     1  0 16:35 ?        00:00:00 /usr/sbin/dhcrelay -i eth0 -i eth1 192.168.2.1
root     11340 10938  0 16:44 pts/0    00:00:00 grep dhcrelay
[root@legolas ~]#

[root@legolas ~]# service dhcrelay status
dhcrelay (pid  11302) is running...

[root@legolas ~]# netstat -uln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address
State
udp        0      0 0.0.0.0:35091               0.0.0.0:*
udp        0      0 0.0.0.0:67                  0.0.0.0:*
udp        0      0 0.0.0.0:68                  0.0.0.0:*
udp        0      0 0.0.0.0:867                 0.0.0.0:*
udp        0      0 0.0.0.0:870                 0.0.0.0:*
udp        0      0 0.0.0.0:5353                0.0.0.0:*
udp        0      0 0.0.0.0:111                 0.0.0.0:*
udp        0      0 0.0.0.0:631                 0.0.0.0:*
udp        0      0 :::52227                    :::*
udp        0      0 :::5353                     :::*
```

Installing and Configuring DHCP server

Step 8 Troubleshooting

Check /var/log/messages and grep for dhcrelay
Check that dhcrelay service is running
Check /etc/sysconfig/dhcrelay settings
Check firewall settings
Use Wireshark to observe DORA

Installing and Configuring dhcrelay

Step 9 Monitor log files

```
[root@p28-legolas ~]# cat /var/log/messages | grep dhcrelay
Mar 24 09:50:43 p28-legolas dhcrelay: Internet Systems Consortium DHCP Relay
Agent 4.1.1-P1
Mar 24 09:50:43 p28-legolas dhcrelay: Copyright 2004-2010 Internet Systems
Consortium.
Mar 24 09:50:43 p28-legolas dhcrelay: All rights reserved.
Mar 24 09:50:43 p28-legolas dhcrelay: For info, please visit
https://www.isc.org/software/dhcp/
Mar 24 09:50:43 p28-legolas dhcrelay: Listening on
LPF/eth1/00:50:56:b7:7d:7e
Mar 24 09:50:43 p28-legolas dhcrelay: Sending on
LPF/eth1/00:50:56:b7:7d:7e
Mar 24 09:50:43 p28-legolas dhcrelay: Listening on
LPF/eth0/00:50:56:b7:cf:0b
Mar 24 09:50:43 p28-legolas dhcrelay: Sending on
LPF/eth0/00:50:56:b7:cf:0b
Mar 24 09:50:43 p28-legolas dhcrelay: Sending on   Socket/fallback
```

elrond

*Need to add settings for the DHCP Lab Mordor subnet in /etc/dhcpd.conf back on the **DHCP server***

```
#
#   M O R D O R
#
subnet 192.168.3.0 netmask 255.255.255.0 {
        option routers                  192.168.3.150; # Default GW
        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; # 6 hours
        max-lease-time                  43200; # 12 hours
}
```

lease files

DHCP

elrond

Lease tracking on the DHCP server

```
[cis192@p28-elrond ~]$ cat /var/lib/dhcpd/dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.1.1-P1

lease 172.20.192.199 {
  starts 2 2013/03/26 20:29:11;
  ends 2 2013/03/26 21:29:11;
  cltt 2 2013/03/26 20:29:11;
  binding state active;
  next binding state free;
  hardware ethernet 00:50:56:bd:c6:93;
  uid "\001\000PV\275\306\223";
  client-hostname "DJW-Server1";
}
lease 192.168.228.50 {
  starts 2 2013/03/26 20:34:12;
  ends 2 2013/03/26 21:34:12;
  cltt 2 2013/03/26 20:34:12;
  binding state active;
  next binding state free;
  hardware ethernet 00:50:56:b7:ff:11;
  client-hostname "p28-sauron";
}

< snipped >
```

DHCP

frodo

Lease tracking on Ubuntu client

```
root@p28-sauron:~# cat /var/lib/dhcp/dhclient.leases
lease {
  interface "eth0";
  fixed-address 192.168.228.50;
  option subnet-mask 255.255.255.0;
  option dhcp-lease-time 3600;
  option routers 192.168.228.150;
  option dhcp-message-type 5;
  option dhcp-server-identifier 192.168.128.1;
  option domain-name-servers 172.30.5.8,10.240.1.2;
  option domain-search "cislab.net.";
  option domain-name "mordor";
  renew 2 2013/03/26 20:34:39;
  rebind 2 2013/03/26 20:34:39;
  expire 2 2013/03/26 20:34:39;
}
```

< snipped >

DHCP

legolas

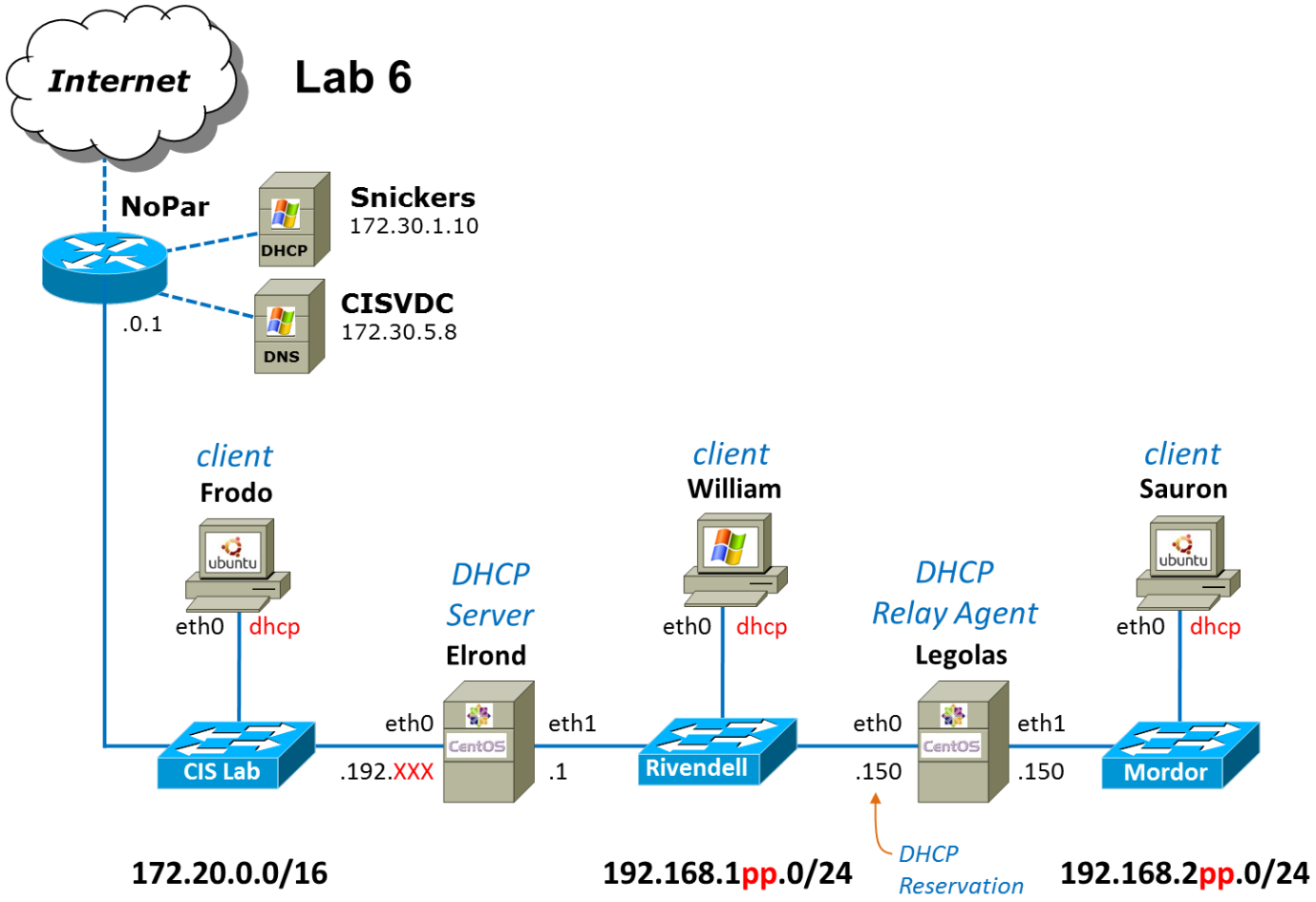
Lease tracking on Centos client

```
[cis192@p28-legolas ~]$ cat /var/lib/dhclient/dhclient.leases
lease {
  interface "eth0";
  fixed-address 192.168.128.150;
  option subnet-mask 255.255.255.0;
  option time-offset -25200;
  option routers 192.168.128.1;
  option dhcp-lease-time 21600;
  option dhcp-message-type 5;
  option domain-name-servers 172.30.5.8,10.240.1.2;
  option dhcp-server-identifier 192.168.128.1;
  option domain-search "rivendell.", "cislab.net.";
  option domain-name "rivendell";
  renew 0 2013/03/24 15:29:56;
  rebind 0 2013/03/24 15:29:56;
  expire 0 2013/03/24 15:29:56;
}
```

< snipped >

DHCP Lab

DHCP Lab


Internet
Lab 6
NoPar
.0.1
Snickers
172.30.1.10
DHCP
CISVDC
172.30.5.8
DNS
client
Frodo
ubuntu
eth0
dhcp
CIS Lab
DHCP
Server
Elrond
eth0
.192.XXX
CentOS
eth1
.1
client
William
eth0
dhcp
Rivendell
DHCP
Relay Agent
Legolas
eth0
.150
CentOS
eth1
.150
client
Sauron
ubuntu
eth0
dhcp
Mordor
DHCP
Reservation
172.20.0.0/16
192.168.1pp.0/24
192.168.2pp.0/24

Wrap

New commands, daemons:

service dhcpd restart

service dhcrelay restart

Daemons and related configuration files

/etc/dhcp/dhcpd.conf

/etc/sysconfig/dhcrelay

/var/lib/dhcpd/dhcpd.leases

/var/lib/dhclient/dhclient.leases (Red Hat)

/var/lib/dhcp/dhclient.leases (Ubuntu)

Next Class

Assignment: Check Calendar Page
http://simms-teach.com/cis192calendar.php

Lab 6
Five posts

Quiz questions for next class:

- What is the Wireshark filter string to view only DHCP transactions?
- What is the DHCP service configuration file on CentOS (Red Hat) family of servers?
- When a client wishes to renew a lease does it initially send the DHCPREQUEST as a broadcast or a unicast?

Lab 5 Workshop

Backup